Journal of Integer Sequences, Vol. 22 (2019),
Article 19.1.1

A Note on Polynomial Sequences Modulo Integers

Mohammad Javaheri
Department of Mathematics
School of Science
Siena College
Loudonville, NY 12211
USA
mjavaheri@siena.edu

Abstract

We study the uniform distribution of the polynomial sequence $\lambda(P) = (\lfloor P(k) \rfloor)_{k\geq 1}$ modulo 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 modulo every integer if and only if $P(x)$ has at least one irrational coefficient other than the constant term.

1 Introduction

A sequence $(r_k)_{k\geq 1}$ of real numbers is said to be *u.d. mod* 1 if for all $0 \leq a < b < 1$ we have

$$\lim_{N\to\infty} \frac{1}{N} \#\{k \in \{1, \ldots, N\} : a \leq \{r_k\} \leq b\} = b - a,$$

where $\{r_k\}$ denotes the fractional part of r_k. An integer sequence $(a_k)_{k\geq 1}$ is said to be *u.d. mod an integer* $m \geq 2$ if, for every integer i, one has

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

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 $(r_k)_{k\geq 1}$ of real numbers, if $(r_k/m)_{k\geq 1}$ is u.d. mod 1 for every $m \geq 2$, then $(\lfloor r_k \rfloor)_{k\geq 1}$ is u.d. in $\mathbb{Z}$ [5, Chap. 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 $(\lfloor P(k) \rfloor)_{k\geq 1}$ is u.d. in $\mathbb{Z}$; see [5, Chap. 5]. This result follows from the generalization of Weyl's distribution theorem which was proved by Weyl himself via his differencing method. Weyl's result was a generalization of Hardy and Littlewood's result on monomials [4]. We prove the converse of this statement for nonlinear polynomials in Theorems 10 and 11.

Example 2. If $f(x) = \beta x^\alpha$, where $\alpha \in (1,\infty)\backslash\mathbb{N}$ and $\beta \in (0,1]$, then $(\lfloor f(k) \rfloor)_{k\geq 1}$ is u.d. in $\mathbb{Z}$. This follows from Weyl's criterion together with van der Corput inequalities [5, Chap. 1].

Example 3. If $P(x) = \pm x + c$, $c \in \mathbb{R}$, then $(\lfloor P(k) \rfloor)_{k\geq 1}$ is clearly u.d. in $\mathbb{Z}$. Moreover, if $P(x) - P(0) \in \mathbb{Z}[x]$ and $(\lfloor P(k) \rfloor)_{k\geq 1}$ is u.d. in $\mathbb{Z}$, then $P(x) = \pm x + c$ for some $c \in \mathbb{R}$ [10].

Example 4. If $f(x) = \beta\alpha^x$ and $\beta > 0$, then the sequence $(\lfloor f(k) \rfloor)_{k\geq 1}$ is u.d. in $\mathbb{Z}$ for almost all $\alpha > 1$. This follows from Koksma's theorem [8].

Niven [10] showed that, given a nonlinear polynomial $P(x) \in \mathbb{Z}[x]$, there exist infinitely many integers m such that $(P(k))_{k\geq 1}$ is not u.d. mod m. 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. The sequence $(\lfloor P(k) \rfloor)_{k\geq 1}$ is u.d. in $\mathbb{Z}$ if and only if $P(x)$ has an irrational coefficient other than the constant term or $P(x) = x/l + P(0)$ for a nonzero integer l.*

In the linear case, Theorem 5 follows from Theorem 9, and in the nonlinear case, it follows from Theorem 10 or Theorem 11.

By adding the least integer operation to the arithmetic operations involved in defining polynomials, we obtain *generalized polynomials*. For example, $f(x) = \lfloor \lfloor a_1 x^2 + a_2 \rfloor x \rfloor + \lfloor a_3 x + a_4 \rfloor x^2$ is a generalized polynomial. Halånd [3] studied uniform distribution of generalized polynomials and showed that, under some conditions relating to the independence of coefficients of $f(x)$ over the rationals, the sequence $(f(k))_{k\geq 1}$ is u.d. mod 1. The second goal of this article is to study the range of the simplest generalized polynomials modulo integers, namely the range of $\lfloor P(x) \rfloor$ modulo 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 $\lfloor P(x) \rfloor \equiv n \pmod m$ 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 1 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 12). 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. Then the following statements are equivalent:*

i. *$P(x)$ is complete modulo all primes large enough.*

ii. *$P(x)$ has an irrational coefficients other than the constant term.*

iii. *The sequence $(\lfloor P(k)\rfloor)_{k\geq 1}$ is u.d. in $\mathbb{Z}$.*

iv. *$P(x)$ is complete modulo all integers.*

We prove Theorem 7 in Section 3. Finally, in Section 4, we consider polynomials of the form $P(x) = ax^n + c$, where $n > 1$ and $a, c \in \mathbb{R}$. In Theorem 16, we show that $P(x)$ is complete modulo all primes large enough if and only if $a \notin \mathbb{Q}$.

2 u.d. polynomial sequences

In this section, we determine all polynomials $P(x) \in \mathbb{R}[x]$ for which the sequence $(\lfloor P(k)\rfloor)_{k\geq 1}$ is u.d. in $\mathbb{Z}$. Niven [10, Thm. 3.1] showed that the sequence $(\lfloor \alpha k\rfloor)_{k\geq 1}$ is u.d. in $\mathbb{Z}$ if and only if α is irrational or $\alpha = 1/l$ for some nonzero integer l. By Example 1, the sequence $(\lfloor \alpha k + \beta\rfloor)_{k\geq 1}$ is u.d. in $\mathbb{Z}$ for every irrational number α. We will prove in Theorem 9 that if the sequence $(\lfloor \alpha k + \beta\rfloor)_{k\geq 1}$ is u.d. in $\mathbb{Z}$, then either α is irrational or $\alpha = 1/l$ for some nonzero integer l. First, we need a lemma.

Lemma 8. *Let $a, b \in \mathbb{Z}$ such that $\gcd(a, b) = 1$ and $b > 0$. Let $\beta \in \mathbb{R}$. Then the sequence $(\lfloor ak/b + \beta\rfloor)_{k\geq 1}$ is u.d. mod m if and only if $\gcd(a, m) = 1$.*

Proof. First, suppose that the sequence $(\lfloor ak/b + \beta\rfloor)_{k\geq 1}$ is u.d. mod m. Suppose that $d = \gcd(a, m) > 1$, and we derive a contradiction. Since we have assumed that $(\lfloor ak/b + \beta\rfloor)_{k\geq 1}$ is u.d. mod m, it follows that the sequence $(\lfloor ak/b + \beta\rfloor)_{k\geq 1}$ is u.d. mod d [10, Thm. 5.1]. One notes that the sequence $(\lfloor ak/b + \beta\rfloor)_{k\geq 1}$ modulo d is periodic with period b. Therefore, if the number of solutions of $\lfloor ak/b + \beta\rfloor \equiv 0 \pmod{d}$ with $1 \leq k \leq b$ is given by t, then the number of solutions of $\lfloor ak/b + \beta\rfloor \equiv 0 \pmod{d}$ with $1 \leq k \leq sb$ is given by st, and so

$$\lim_{s\to\infty} \frac{1}{sb} \#\left\{k \in \{1, \ldots, sb\} : \lfloor ak/b + \beta\rfloor \equiv 0 \pmod{d}\right\} = \lim_{s\to\infty} \frac{st}{sb} = \frac{t}{b}.$$

On the other hand, this limit must equal $1/d$ by the definition of u.d. mod d (see equation (1)). 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 $(\lfloor ak/b+\beta\rfloor)_{k\geq 1}$ is periodic modulo 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 $\lfloor ak/b + \beta\rfloor \equiv i \pmod{m}$. 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

$$\lfloor a(t_j + b)/b + \beta\rfloor \equiv a + \lfloor at_j/b + \beta\rfloor \equiv a + i \pmod{m}.$$

In other words, the map $t_j \mapsto t_j + b$ is a one-to-one map from T_i to T_{a+i}, where $t_j + b$ is computed modulo bm and $a + i$ is computed modulo m. It follows that $|T_{a+i}| \geq |T_i|$, 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 $\lfloor ak/b + \beta \rfloor \equiv i \pmod{m}$ is between Qb and $(Q+1)b$, which is sufficient to verify the definition of u.d. mod m in (1). $\square$

Theorem 9. *Let $\alpha, \beta \in \mathbb{R}$. Then the sequence $(\lfloor \alpha k + \beta \rfloor)_{k \geq 1}$ is u.d. in $\mathbb{Z}$ if and only if α is irrational or $\alpha = 1/l$ for some nonzero integer l.*

Proof. If α is irrational, then the claim follows from Example 1 [10, Thm. 3.2]. If $\alpha = 1/l$ for some nonzero integer l, then the sequence $(\lfloor k/l + \beta \rfloor)_{k \geq 1}$ is u.d. mod m for every m by Lemma 8. Thus, suppose that $\alpha = a/b$ for integers a, b with $\gcd(a, b) = 1$, $|a| > 1$, and $b > 0$. It follows from Lemma 8 that the sequence $(\lfloor ak/b + \beta \rfloor)_{k \geq 1}$ is not u.d. mod $|a|$, hence it is not u.d. in $\mathbb{Z}$. $\square$

Next, we discuss nonlinear polynomials. Niven [10, Thm. 4.1] proved that if $P(x)$ is a nonlinear polynomial with integer coefficients, then there exist infinitely many integers m such that $(P(k))_{k \geq 1}$ is not u.d. mod m. We prove generalizations of this statement in the next two theorems.

Theorem 10. *Let $P(x)$ be a nonlinear polynomial with real coefficients. If $P(x)$ has no irrational coefficients other than the constant term, then there exists infinitely many mutually coprime integers m such that $(\lfloor P(k) \rfloor)_{k \geq 1}$ is not u.d. mod m.*

Proof. Let $P(x) = \sum_{i=0}^{n} a_i x^i$ 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, $1 \leq i \leq n$, and let $Q(x) = N(P(x) - P(0)) \in \mathbb{Z}[x]$. 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 nonconstant polynomial). We define $f(x) = Q(x) - Q(a)$. Then $f(a) \equiv 0 \pmod{p^2}$ and $f'(a) \equiv 0 \pmod{p}$. It follows from Hensel's Lemma [2, Thm. 3.4.1] that $f(a + kp) \equiv f(a) \equiv 0 \pmod{p^2}$ for all integer values of k. In particular, the equation $Q(x) \equiv Q(a) \pmod{p^2}$ has at least p solutions for $x \in \{1, \ldots, p^2\}$. It follows that, given an integer $s \geq 1$, we have $|T| \geq sp$, where T denotes the set of solutions $x \in \{1, \ldots, sp^2\}$ of $Q(x) \equiv Q(a) \pmod{p^2}$.

We show that the sequence $(\lfloor P(k) \rfloor)_{k \geq 1}$ is not u.d. mod $m = p^2$. On the contrary, suppose that $(\lfloor P(k) \rfloor)_{k \geq 1}$ is u.d. mod p^2. It follows from the definition that for each $0 \leq t < p^2$,

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

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

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

for all $0 \le t < p^2$. 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 $\lfloor (Q(a) + (\beta + N)p^2)/N \rfloor \equiv \lfloor (Q(a) + \beta p^2)/N \rfloor \pmod{p^2}$ for every $\beta \in \mathbb{Z}$, hence there are at most N congruence classes modulo p^2 among the values $\lfloor P(x) - P(0) \rfloor$. Since $|T| \ge sp > 6sN$, it follows that there exists an integer r such that the equation $\lfloor P(x) - P(0) \rfloor \equiv r \pmod{p^2}$ has more than $6s$ solutions in the set $\{1, \ldots, sp^2\}$. Let S be the set of $x \in T$ such that $\lfloor P(x) - P(0) \rfloor \equiv r \pmod{p^2}$. In particular $|S| > 6s$.

For every $x \in \mathbb{Z}$, we have $\lfloor P(x) \rfloor = \lfloor P(x) - P(0) \rfloor + \lfloor P(0) \rfloor + u$ for some $u \in \{-1, 0, 1\}$, and so $S \subseteq S_{t_{-1}} \cup S_{t_0} \cup S_{t_1}$, where $t_u = r + \lfloor P(0) \rfloor + u$ (computed modulo p^2). Therefore,

$$\frac{1}{sp^2}|S_{t_{-1}}| + \frac{1}{sp^2}|S_{t_0}| + \frac{1}{sp^2}|S_{t_1}| \ge \frac{1}{sp^2}\left|S_{t_{-1}} \cup S_{t_0} \cup S_{t_1}\right| \ge \frac{1}{sp^2}\,|S| > \frac{6}{p^2},$$

which contradicts the inequality (2) as $s \to \infty$. □

We now prove a statement that is stronger than the statement of Theorem 10.

Theorem 11. *Let $P(x)$ be a nonlinear polynomial with real coefficients. If the sequence $(\lfloor P(k) \rfloor)_{k \ge 1}$ 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 $1 \le i \le n$. Let N be the least common multiple of s_i, $1 \le i \le n$. Since the sequence $(\lfloor P(k) \rfloor)_{k \ge 1}$ is assumed to be u.d. mod all primes large enough, the sequence $(N\lfloor P(k) \rfloor)_{k \ge 1}$ is u.d. mod all primes p large enough. The value $N\lfloor P(k) \rfloor$ is periodic modulo p with period Np. Therefore, it follows from the uniform distribution of $(N\lfloor P(k) \rfloor)_{k \ge 1}$ modulo p that, with $\mathcal{U} = \{0, \ldots, p-1\} \times \{0, \ldots, N-1\}$, we have

$$\#\{(t, j) \in \mathcal{U} : N\lfloor P(Nt + j) \rfloor \equiv i \pmod{p}\} = N, \tag{3}$$

for every integer i. Let $P_j(x) = N\lfloor P(Nx + j) \rfloor \in \mathbb{Z}[x]$ for $0 \le j < N$. Choose M large enough so that the polynomials $f_j(x) = P_j(x) + M$, $0 \le j < N$, are all irreducible over $\mathbb{Q}[x]$ (the existence of M follows from Hilbert's irreducibility theorem [6, Chap. 9]). Let $f(x) = f_0(x) \cdots f_{N-1}(x)$ and

$$R = \prod_{0 \le i < j < N} \mathrm{Res}(f_i, f_j) \in \mathbb{Z},$$

where $\mathrm{Res}(f_i, f_j)$ 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 zeros for all $0 \le i < j < N$, we must have $\mathrm{Res}(f_i, f_j) \ne 0$, and so $R \ne 0$. Therefore, for any prime $p > p_0$, $\mathrm{Res}(f_i, f_j) \not\equiv 0 \pmod{p}$, where p_0 is the greatest prime factor of R. In other words, for any prime $p > p_0$, the polynomials f_j,

$0 \le j < N$, have no common zeros modulo p. By the Chebotarev density theorem [1, 7], 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 zeros modulo p. Therefore, the number of solutions of $N\lfloor P(Nt+j)\rfloor \equiv -M \pmod{p}$ is at least $nN > N$. This is in contradiction with equation (3), and the claim follows. □

3 Complete even-degree polynomials

Let $P(x)$ be a polynomial such that $P(x) - P(0) \in \mathbb{Q}[x]$. Since the sequence $(\lfloor P(k)\rfloor)_{k\ge 1}$ modulo any integer m is periodic, it follows from Definition 6 that the polynomial $P(x)$ is complete modulo m if and only if

$$\lim_{N\to\infty} \frac{1}{N} \# \{k \in \{1,\dots,N\} : \lfloor P(k)\rfloor \equiv i \pmod{m}\} > 0, \tag{4}$$

for every integer i. Condition (4) is weaker than condition (1). Therefore, if $(\lfloor P(k)\rfloor)_{k\ge 1}$ is u.d. mod 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 12. *The linear polynomial $P(x) = \alpha x + \beta$ is complete in $\mathbb{Z}$ if and only if either $|\alpha| \in (0, 1]$ or α is irrational.*

Proof. If α is irrational, then the claim follows from Theorem 9. Thus, suppose $\alpha = a/b$ where a, b are coprime integers, $a \ne 0$, and $b > 0$. Suppose that $P(x)$ is complete in $\mathbb{Z}$, and so the set $\{\lfloor \alpha k + \beta\rfloor : k \ge 1\}$ contains the numbers $0, \dots, |a| - 1$ modulo $|a|$. Let $k = bq + l$ where $0 \le l < b$. Then

$$\left\lfloor \frac{a}{b}(bq+l) + \beta \right\rfloor = aq + \left\lfloor \frac{al}{b} + \beta \right\rfloor .$$

Therefore, the b numbers $\lfloor al/b + \beta\rfloor$, $0 \le l < b$, must contain the numbers $0, \dots, |a| - 1$ modulo $|a|$. In particular $b \ge |a|$ and so $\alpha \in [-1, 0) \cup (0, 1]$.

For the converse, suppose $b \ge |a|$. Then the numbers $al/b + \beta$, $0 \le l \le b$ are apart by $|a/b| \le 1$, and they stretch from β to $a + \beta$. Therefore, the numbers $\lfloor al/b + \beta\rfloor$, $0 \le l < b$, include $|a|$ consecutive integers, say $s, \dots, s + |a| - 1$. Given any $i, j \in \mathbb{Z}$, we show that there exists an integer x such that $\lfloor ax/b + \beta\rfloor \equiv i \pmod{j}$. 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 $q \ge 1$ and $u \in \{0, \dots, |a| - 1\}$. Since there exists an integer $0 \le l < b$ such that $\lfloor al/b + \beta\rfloor = s + u$, with $x = bq + l$, we have $\lfloor ax/b + \beta\rfloor = aq + \lfloor al/b + \beta\rfloor \equiv aq + s + u \equiv i$ $\pmod{j}$. 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 13. *Let $R(x)$ be a polynomial with integer coefficients and no real zeros. Then there exist infinitely many primes p such that $R(x)$ has no zeros modulo p.*

Proof. Suppose on the contrary that $R(x)$ has a zero modulo all primes large enough. It follows from the Chebotarev density theorem [1, 7] that every element of the Galois group of the splitting field of $R(x)$ has a fixed point in the action on the zeros. In particular, complex conjugation must have a fixed point on the set of the zeros of $R(x)$, which contradicts our assumption that $R(x)$ has no real zeros. □

Lemma 14. *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 $Q(x) + A_i \not\equiv m \pmod{p}$ 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 zeros for all $0 \le i < N$. We let

$$R(x) = (Q(x) + M + A_0) \cdots (Q(x) + M + A_{N-1}).$$

Then $R(x)$ has no real zeros. By Lemma 13, 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 $i \in \{0, \ldots, N-1\}$. □

We are now ready to prove Theorem 7.

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

$$\lfloor P(Nk + j) \rfloor = \lfloor P(j) \rfloor + \sum_{i=1}^{n} \frac{r_i}{s_i}((Nk + j)^i - j^i).$$

And so

$$\begin{aligned} N\lfloor P(Nk + j) \rfloor &= N\lfloor P(j) \rfloor + N\sum_{i=1}^{n} \frac{r_i}{s_i}((Nk + j)^i - j^i). \\ &= N\lfloor P(j) \rfloor - \sum_{i=1}^{n} r_i \frac{N}{s_i} j^i + Q(Nk + j) \\ &= A_j + Q(Nk + j), \end{aligned} \tag{5}$$

where $Q(x) = N(P(x) - P(0)) \in \mathbb{Z}[x]$ and $A_j \in \mathbb{Z}$ depending on j and $P(x)$, $0 \le j < N$. By Lemma 14, there exist an arbitrarily large prime $p > N$ and an integer m such that $Q(x) + A_j \not\equiv m \pmod{p}$ for all $x \in \mathbb{Z}$ and $j \in \{0, \ldots, N-1\}$. We claim that $P(x)$ is not complete modulo p. On the contrary, suppose there exists an integer x such that $\lfloor P(x) \rfloor \equiv K \pmod{p}$, where K is such that $NK \equiv m \pmod{p}$. But then, writing $x = Nk + j$ with $0 \le j < N$, we have $Q(Nk + j) + A_j \equiv N\lfloor P(Nk + j) \rfloor \equiv NK \equiv m \pmod{p}$. This is a contradiction, and so (i) implies (ii). The implication (ii) ⇒ (iii) was discussed in Example 1. The implications (iii) ⇒ (iv) and (iv) ⇒ (i) are straightforward, and the proof of Theorem 7 is completed. □

4 Complete monomials

Let p be a prime and n be a positive integer that divides $p-1$. An nth power *character* modulo p is any homomorphism $\chi : \mathbb{Z}_p^* \to \mathbb{C}$ that is onto the group of nth roots of unity. By a theorem of A. Brauer [11], given $n, l \geq 1$, there exists a constant $z(n,l)$ such that for every prime $p > z(n,l)$ and any nth power character χ modulo p, there exists an integer t such that

$$\chi(t) = \chi(t+1) = \cdots = \chi(t+l-1). \tag{6}$$

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

Lemma 15. *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 nth power non-residues modulo p for some positive integer t.*

Proof. We can assume, without loss of generality, that n is prime and $l \geq 4$. By a result of Mills [9, Thm. 3], for every $m \geq 1$, there exist infinitely many primes p with an nth power character χ modulo p such that

$$\chi(2) \neq 1,\ \forall 2 \leq i \leq m:\ \chi(p_i) = 1,$$

where p_i is the ith prime. Let t be defined by (6). We can choose $t > 1$ by adding multiples of p if necessary. Choose an integer m 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 equation (6) that $\chi(t) = \chi(t+1) = \cdots = \chi(t+l-1) \neq 1$ i.e., none of the values $t, t+1, \ldots, t+l-1$, are nth power residues modulo p. $\square$

Theorem 16. *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 modulo all primes large enough, hence $(\lfloor P(k) \rfloor)_{k \geq 1}$ is not u.d. in $\mathbb{Z}$.*

Proof. Let $a = M/N$, where M and N are integers and $M > 0$. Let $Q(x) = Mx^n$ and $A_0, \ldots, A_{N-1}$ be given by equation (5). On the contrary, suppose $P(x)$ is complete modulo all primes p large enough. By Lemma 15, 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 nth 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 $M^{n-1}L \equiv K \pmod p$. Since $P(x)$ is complete modulo p, there exists an integer x such that $N\lfloor P(x) \rfloor \equiv L \pmod p$. Writing $x = Nk + j$ with $0 \leq j < N$, we have

$$M^{n-1}(Q(x) + A_j) \equiv M^{n-1}N\lfloor P(x) \rfloor \equiv M^{n-1}L \equiv K \pmod p.$$

Since $t \le K - M^{n-1}A_j < t + l$ and $K - M^{n-1}A_j \equiv M^{n-1}Q(x) \equiv (Mx)^n \pmod{p}$ is an nth power residue modulo p, we have a contradiction, and the claim follows. □

Remark 17. In light of the proofs of Theorems 7 and 16, one can generalize Theorem 7 to all nonlinear polynomials if the following statement is true: Given a nonlinear 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 $P(x) \not\equiv k + i \pmod{p}$ for all $i = 0, \ldots, l-1$.

5 Acknowledgment

I would like to thank Siena College for providing a sabbatical leave during which this work was completed. I would also like to thank the referee for many useful comments and suggestions.

References

[1] M. D. Fried and M. Jarden, *Field Arithmetic*, Third Edition, Springer-Verlag, 2008.

[2] F. Q. Gouvêa, *p-adic Numbers: an Introduction*, Second Edition, Springer-Verlag, 1997.

[3] I. J. Halånd, Uniform distribution of generalized polynomials, *J. Number Theory* **45** (1993), 327–366.

[4] G. H. Hardy and J. E. Littlewood, Some problems of Diophantine approximation: part I. The fractional part of $n^k\theta$, *Acta Math.* **37** (1914), 155–191.

[5] L. Kuipers and H. Niederreiter, *Uniform Distribution of Sequences*, Wiley, 1974.

[6] S. Lang, *Fundamentals of Diophantine Geometry*, Springer, 1983.

[7] H. W. Lenstra, Jr. and P. Stevenhagen, Chebotarev and his density theorem, *Math. Intelligencer* **18** (1996), 26–37.

[8] W. J. LeVeque, Note on a theorem of Koksma, *Porc. Amer. Math. Soc.* **1** (1950), 380–383.

[9] W. H. Mills, Characters with preassigned values, *Canad. J. Math.* **15** (1963), 169–171.

[10] I. Niven, Uniform distribution of sequences of integers, *Trans. Amer. Math. Soc.* **98** (1961), 52–61.

[11] J. R. Rabung and J. H. Jordan, Consecutive power residues or nonresidues, *Math. Comp.* **24** (1970), 737–740.

2010 *Mathematics Subject Classification*: Primary 11K36.
Keywords: uniform distribution, polynomial sequence.

Received September 11 2018; revised version received December 16 2018. Published in *Journal of Integer Sequences*, December 17 2018.

Return to Journal of Integer Sequences home page.