Journal of Combinatorics and Number Theory
Volume 12, Number 1, pp. 35–49

ISSN 1942-5600

DIVISIBILITY PROPERTIES OF SOME CURIOUSLY DEFINED SEQUENCES

Tamás Lengyel[*]
Mathematics Department, Occidental College,
Los Angeles, CA, US

Abstract

We generalize and solve a problem regarding the divisibility of a sequence defined as the lower integer part of powers of the largest root of a polynomial equation. Two solutions are presented using various root finding, root extraction as well as algebraic techniques. We rely on the periodic properties of linear recurrences and powers of integers modulo primes and apply methods for estimating power sums and for determining limit points of the fractional part of powers of the largest root. We also present examples and discuss numerical and computational concerns.

2020 Mathematics Subject Classification: Primary 11B37; Secondary 11B50, 11K16

1. INTRODUCTION

The motivation for this note comes from a recommended problem for the International Mathematical Olympiad (IMO) that was not used.

Problem. [DJMP, Problem 7, p. 226] (FRA 2) *Let r be the greatest positive root of the equation $x^3 - 3x^2 + 1 = 0$. Show that $\lfloor r^{1788} \rfloor$ and $\lfloor r^{1988} \rfloor$ are both divisible by 17, where $\lfloor x \rfloor$ denotes the integer part of a real number x.*

Two recommended solutions are presented in [DJMP, p. 504]. Our goal is to generalize this problem to other polynomials and divisors.

We use various techniques (e.g., Sturm theorem and Rouché's theorem) to locate the real and complex roots of polynomials of the form $f_d(x, a) = x^d - ax^{d-1} + 1$, $a, d \geq 3$ in $\mathbb{C}$ (cf. Theorems 3.2 and 3.3) and in $\mathbb{Z}/p\mathbb{Z}$ with given prime p (cf. Theorem 3.4). We discuss properties related to power sums and their estimations in Lemmas 3.6–3.9 and Theorem 3.1. As a general technique, we utilize the modular periodicity of linear recurrences of order d.

[*] E-mail address: lengyel@oxy.edu; Website: http://sites.oxy.edu/lengyel.

The main results are included in Theorems 3.1–3.4. In Section 2 we present the solutions to Problem 1 while Section 3 is devoted to the generalizations. As far as the root finding aspects are concerned, Sections 3.1–3.5 cover the analytic considerations while Section 3.6 deals with the algebraic approach. In Section 4 we illustrate the differences between the two approaches on some examples.

2. Methods

Two solutions are presented that use various root finding and root extraction methods and algebraic techniques. On one hand, we rely on the periodic properties of linear recurrences and powers of integers modulo primes, and on the other hand, we apply methods for estimating power sums and for determining limit points of the fractional part of powers of the largest root. First we describe the original solutions.

First take

Note that over the real numbers we have $x^3-3x^2+1=(x-r_1)(x-r_2)(x-r_3)$ with roots

$$r_1 \approx 2.87939 > r_2 \approx 0.652704 > r_3 \approx -0.532089; \tag{2.1}$$

and thus, clearly, $\lfloor r_1^n \rfloor = r_1^n + r_2^n + r_3^n - 1$ for $n \geq 1$ by the construction (2.2) and the explanation below. We want to find the exponents n for which $\lfloor r_1^n \rfloor \equiv 0 \pmod{17}$.

We define a sequence $\{T_n\}_{n\geq 0}$ of integers by the recurrence

$$T_n = 3T_{n-1} - T_{n-3} \tag{2.2}$$

for $n \geq 3$ and initial values $T_0 = 3, T_1 = 3$, and $T_2 = 9$. Latter one follows by the Newton-Girard formulas (cf. [S]) applied to the coefficients of x^3-3x^2+1:

$$(-1)^{k-1}kE_k = S_k - S_{k-1}E_1 + \cdots + (-1)^{k-1}S_1E_{k-1} \tag{2.3}$$

where

$$S_k = S_k(x_1, x_2, \ldots, x_d) = \sum_{i=1}^{d} x_i^k \tag{2.4}$$

is the kth power sum of the variables $x_1, x_2, \ldots, x_d$, and $E_k = \sum_{1\leq i_1<i_2<\cdots<i_k\leq d} x_{i_1}x_{i_2}\cdots x_{i_k}$ is the kth elementary symmetric polynomial of the same variables. Here $d=3$ and the x_is are the roots of the polynomial. Identity (2.3) leads to $S_2 = S_1^2 - 2E_2 = 3^2 = 9$. It is well known that $T_n = S_n(r_1, r_2, r_3) = r_1^n + r_2^n + r_3^n$ for all $n \geq 0$, after properly setting the initial values of T_n. In general, for a polynomial equation of degree d, we have $T_n = S_n(r_1, r_2, \ldots, r_d)$ with properly set initial values if the roots r_i are different. We have that $T_0 = S_0 = d$ by (2.4).

We look for 1 in the modulo 17 period of the sequence $\{T_n\}_{n\geq 0}$ and find that the length of the period is $\pi(17) = \pi(17; T_n) = 16$ and $n \equiv 4$ and $12 \pmod{16}$, i.e., $n \equiv 4 \pmod 8$ are the indices to give $T_n - 1 = \lfloor r_1^n \rfloor \equiv 0 \pmod{17}$. We find that 1788 and $1988 \equiv 4 \pmod 8$ and the divisibility by 17 follows. We conclude that both $\lfloor r_1^{1788} \rfloor$ and $\lfloor r_1^{1988} \rfloor$ are divisible by 17.

It is worth noting that this approach offers a somewhat unusual application of linear recurrences. Assume that the sequence $\{U_n\}_{n \geq 0}$ is defined by a linear recurrence of order d with constant coefficients and given initial values $U_n, n = 0, 1, \ldots, d-1$, and that all roots r_i of the characteristic equation are different. Typically, we rely on the usual ansatz with undetermined coefficients $a_i, 1 \leq i \leq d$, and featuring

$$U_n = \sum_{i=1}^{d} a_i r_i^n, n \geq 0. \tag{2.5}$$

We determine the a_is based on the first d initial values and calculate the sequence by (2.5) without applying the recurrence relation. Here, however, we use a kind of reverse engineering. In order to proceed according to (2.2), we determine the initial values of T_n after setting all a_is to 1 in (2.5).

Second take

The nice idea behind the other and more elegant recommended solution is that after factoring the polynomial $x^3 - 3x^2 + 1 \equiv (x-4)(x-5)(x-11) \pmod{17}$ in the field of modulo 17 integers $\mathbb{Z}/17\mathbb{Z}$, we can use Fermat's little theorem to see that the period of the sequence $\{4^n + 5^n + 11^n - 1 \pmod{17}\}_{n \geq 0}$ must be a divisor of 16 (in fact, $\pi(17) = 16$) and to obtain the congruence $\lfloor r_1^n \rfloor \equiv 4^n + 5^n + 11^n - 1 \pmod{17}$, which is true here for all $n \geq 1$. Now the relevant congruence $\lfloor r_1^n \rfloor \equiv 0 \pmod{17}$ is satisfied exactly if $n \equiv 4$ or $12 \pmod{16}$, and we conclude the same way as in the above solution. Note that this approach heavily depends on the fact that we can factor $x^3 - 3x^2 + 1$ modulo 17 into linear factors.

3. Results: The General Case with $d \geq 3$ and $a \geq 3$

We generalize the original cubic problem to the function $f_3(x, a) = x^3 - ax^2 + 1$ and then to $f_d(x, a) = x^d - ax^{d-1} + 1$, with $a, d \geq 3$ integers, and provide a way of solving it when the polynomial cannot be factored into linear factors over $\mathbb{Z}/p\mathbb{Z}$ for the given prime p.

3.1. The Generalized Cubic Example

In general, if $f_3(x, a) = x^3 - ax^2 + 1$ with $a \geq 2$, then for the roots we have that $-1 < r_3 < 0 < r_2 < 1 < r_1 < a$; indeed, it is easy to see that

$$a - \frac{1}{a^2} - \frac{2}{a^3} < r_1 < a \tag{3.1}$$

and thus,

$$r_2 + r_3 = a - r_1 > 0 \tag{3.2}$$

and, by the Sturm theorem [DF] about the number of real roots of a polynomial in a given interval, we get that $-1 < r_3 < 0 < r_2 < 1$ and $|r_3| < r_2$ by (3.2). For $d \geq 3$ we will use Rouché's theorem to locate all roots, not just the real ones, in Theorem 3.2 in Section 3.3.

3.2. The General Case

We note that for a prime power or composite modulus $\lfloor r_1^n \rfloor$ can be analyzed by the first method in Section 2 while the other method outlined in Section 2 based on the factorization of $f_d(x,a) = x^d - ax^{d-1} + 1$ might be prohibitive if we cannot find the factorization. In this section we generalize the first method while the second method is extended in Section 3.6. The locations and values of the real and complex roots of $f_d(x,a)$ are determined in Section 3.3. Properties of the auxiliary sequence $\{S_n^-\}_{n\geq 0}$ are discussed in Sections 3.4–3.5 and the proof of the main Theorem 3.1 is included in Section 3.4.

We set $f(x,a) = f_d(x,a) = x^d - ax^{d-1} + 1 = 0$ and its accompanying polynomial $g(x,a) = g_d(x,a) = x^d f(1/x) = x^d - ax + 1$. We use the notation $f(x,a)$ and $g(x,a)$ when there is no need to emphasize their degrees. We order the roots $r_i, i = 1, 2, \dots, d$, of $f_d(x,a)$: $|r_1| \geq |r_2| \cdots \geq |r_d|$.

We observe that all roots r_i of $f_d(x,a) = 0$ are different because the roots of $f'_d(x,a)$ are not roots of $f_d(x,a)$; cf. Theorem 3.2. We have the following standard identity for the generating function of the power sums.

Lemma 3.1. *We have*

$$\sum_{n=0}^{\infty} T_n x^n = \sum_{n=0}^{\infty} S_n(r_1, r_2, \dots, r_d) x^n = \frac{d-(d-1)ax}{g_d(x,a)}. \tag{3.3}$$

Proof of Lemma 3.1. We write $f_d(x,a) = x^d - ax^{d-1} + 1 = \prod_{i=1}^d (x - r_i)$ and $x^d f_d(1/x, a) = x^d - ax + 1 = g_d(x,a) = x^d \prod_{i=1}^d (1/x - r_i) = \prod_{i=1}^d (1 - r_i x)$. According to [B, (2.1)], we have

$$-x\frac{g'_d(x,a)}{g_d(x,a)} = \sum_{n=1}^{\infty} S_n(r_1, r_2, \dots, r_d) x^n.$$

It yields that

$$\sum_{n=0}^{\infty} S_n(r_1, r_2, \dots, r_d) x^n = d + \left(-x\frac{dx^{d-1} - a}{x^d - ax + 1}\right) = \frac{d-(d-1)ax}{x^d - ax + 1}.$$

Since the roots are different, we have that $T_n = S_n$. □

Identity (3.3) implies the recurrence relation

$$T_n = a\,T_{n-1} - T_{n-d} \tag{3.4}$$

with initial values $T_0 = d, T_k = a^k, 1 \leq k \leq d-1$ according to (2.3) and (2.4). With the above choice of initial values, $\{T_n\}_{n\geq 0}$ is a sequence of integers and

$T_n = \sum_{i=1}^{d} r_i^n = S_n(r_1, r_2, \dots, r_d)$ by (2.4). Note that from latter fact it is not obvious that the T_ns are integers. In order to investigate whether m divides T_n we consider the sequence $\{T_n \pmod{m}\}_{n \geq 0}$ defined by the congruential recurrence

$$T_n \equiv a\,T_{n-1} - T_{n-d} \pmod{m} \tag{3.5}$$

which is computationally more suitable than (3.4).

Remark 3.1. *We note that if $a = 2$ then $r_2 = 1$. For a partial analysis of the case with $a = 2$ see [W] and [FS, p. 309]. The ordinary generating function (OGF) of the number of compositions all of whose summands lie in $\{1, 2, \dots, d-1\}, d \geq 2$, is $(1-x)/g_d(x, 2)$; cf. [FS, p. 42] and also see [FS, p. 52] for a related OGF. For instance, it follows that if $d = 3$ then $x(1-x)/g_3(x, 2)$ is the OGF of the Fibonacci sequence.*

Historically, Newton and Bernoulli used the estimations $T_n \sim r_1^n$ and $T_n/T_{n-1} \approx r_1$, respectively. Their approach provided linear convergence to r_1, then Newton's (also known as the Newton–Raphson) method improved this to quadratic convergence; cf. Section 3.3. However, we need the exact value of T_n. We prove the following main theorem.

Theorem 3.1. *For any sufficiently large n we have that $T_n = \lfloor r_1^n \rfloor + 1$.*

In the proof we use the sum of powers $S_n^- = \sum_{k=2}^{d} r_k^n$ of the "small" roots in $R = \{r_2, r_3, \dots, r_{d-1}\}$. The largest root r_1 is real by Theorem 3.2; thus, for any complex root r_i its complex conjugate is also contained in R, which makes S_n^- real. We will prove that S_n^- is positive and bounded; cf. Lemmas 3.6 and 3.8.

Remark 3.2. *It appears that often there is a discrepancy between T_n and $\lfloor r_1^n \rfloor + 1$ if $a < d$ and $n = 0$ or $d - 1$ in which case $T_0 = d$ and $\lfloor r_1^0 \rfloor + 1 = 2$ and $T_{d-1} \geq \lfloor r_1^{d-1} \rfloor + 2$. For instance, if $a = 4$ and $d = 15$ then, in agreement with* (3.8)*, we have $S_{14}^- \approx (d-1)/a = 3.5$; and thus, $T_{14} = \lfloor r_1^{14} \rfloor + 4 = 268435456$.*

3.3. The Real and Complex Roots of $f_d(x, a)$

To see only that there are two or three real roots of the appropriate signs we note that $f_d(0, a) = 1$ and $f_d'(x, a) = x^{d-2}(dx - (d-1)a)$=0 has two roots and thus, $f_d(x, a)$ has two "turning points." We need a finer analysis and locate all d roots on the complex plane in the next theorem.

Theorem 3.2. *For $a \geq 3$, the largest root satisfies $a - 2/a^{d-1} < r_1 < a$. If $a, d \geq 3$ then all the other $d - 1$ roots $r = r_2, r_3, \dots, r_d$ with $|r_2| \geq |r_3| \geq \cdots \geq |r_d|$ are located in the unit disk so that $(a+1)^{-\frac{1}{d-1}} < |r| < (a-1)^{-\frac{1}{d-1}} < 1$ and $r_2 > 0$. The roots r_1 and r_2 are real numbers and all roots are different.*

Proof of Theorem 3.2. First we prove that all roots are different, then using continuity arguments we locate the largest root r_1 in the neighborhood of a and the second largest root r_2 in the interval $(0, 1)$. Finally, by Rouché's theorem we prove that all roots except r_1

are contained in an annulus centered at zero and enclosed in the unit disk.

All roots r_i are different because the roots of $f'_d(x,a)$ are not roots of $f_d(x,a)$ since $a(d-1)/d$ is rational while all roots are non-rational by Lemma 3.5.

Clearly, $f(a,a) = 1$ and $f(a - 2/a^{d-1}, a) = (-2)(1 - 2/a^d)^{d-1} + 1 < 0$ since $a, d \geq 3$. By the continuity of $f(x,a)$ it follows that there is a root in the range $(a - 2/a^{d-1}, a)$, and it turns out that this is the largest root, r_1.

By using an argument similar to that in [HW, p. 37], we can locate the other $d-1$ roots. There is a root of $f(x,a)$ in the interval $(0,1)$ since $f(0,a) = 1 > 0 > f(1,a) = 1 - a + 1$ with $a > 2$; it is the only real root in the interval $(0,1)$ since $f'(x,a) = x^{d-2}(dx - (d-1)a) < 0$ for $0 < x < 1 < \frac{a(d-1)}{d}$ if $d \geq 3$ and $a \geq 2$. Let r^* be the only real root in $(0,1)$ then for all roots r, except the largest one r_1, which is close to a, we have that $|r| < r^* + \epsilon < 1$ for some positive $\epsilon < 1 - r^*$ and $r^* - \delta < |r|$ for some positive $\delta < r^*$, by applying Rouché's theorem (cf. [FS] and [HW]) twice using the parameters ϵ and δ given by Lemmas 3.2 and 3.3. Indeed, $|x^d + 1| < |ax^{d-1}|$ on the circle $|x| = r^* + \epsilon$ yielding $d-1$ roots in the open disk $|x| < r^* + \epsilon$ and $1 > |ax^{d-1}|$ on the circle $|x| = r^* - \delta$ yielding no root in $|x| < r^* - \delta$.

It follows that $r^* = r_2$. □

The next two lemmas suggest values for ϵ and δ to be used in the proof of Theorem 3.2.

Lemma 3.2. *Any $\epsilon > 0$ such that $(a-1)^{-\frac{1}{d-1}} - r^* < \epsilon < 1 - r^*$ guarantees that $|x^d + 1| < |ax^{d-1}|$ on the circle $|x| = r^* + \epsilon$.*

Proof. We need that $|x^d + 1| < |ax^{d-1}|$ on $|x| = r^* + \epsilon$, which can be achieved by solving $|x^d + 1| \leq |x|^d + 1 < a|x|^{d-1}$, i.e., $|x| + 1/|x|^{d-1} < 1 + 1/(r^* + \epsilon)^{d-1} < a$, which is satisfied if $(a-1)^{-\frac{1}{d-1}} - r^* < \epsilon$. □

Lemma 3.3. *Proper choices for $\delta > 0$ are given by $r^* - (a+1)^{-\frac{1}{d-1}} < \delta < r^*$.*

Proof. We need that $1 > |x^d - ax^{d-1}| = |x|^{d-1}|x - a|$ on $|x| = r^* - \delta$, which can be achieved by solving $1 > |r^* - \delta|^{d-1}|a + 1| > |r^* - \delta|^{d-1}|a + r^* - \delta| \geq |x^d - ax^{d-1}|$; and thus, if $(a+1)^{-\frac{1}{d-1}} > |r^* - \delta|$. □

Theorem 3.2 implies that we have either two positive or two positive and one negative real roots of $f_d(x,a)$, depending upon whether d is even or odd. The latter case can be proven similarly to the way we find r^* in the proof of Theorem 3.2 since if d is odd then $f_d(-1,a) = -1 - a + 1 = -a < 0 < 1 = f_d(0,a)$, and $f'(x,a) > 0$ for $x < 0$. Note that the real roots are irrational numbers; cf. Lemma 3.5.

We mention the following general lemma, which also gives some ideas about the signs of the roots. According to the lemma $f_d(x,a)$ has either two or no positive roots (indeed, there are two of them) and one or no negative roots if d is odd or even, respectively.

Lemma 3.4 (Descartes' rule of signs). *If $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ is a polynomial with real coefficients, then the number of positive roots of the polynomial equation $f(x) = 0$ is either equal to the number of times the coefficients in f change sign or less than that by an even number. The number of negative roots of f is obtained by applying the above rule to $f(-x)$ for the number of positive roots.*

Remark 3.3. *According to Theorem 3.2, we know that the $d-1$ small roots r are located in an annulus with radii $(a+1)^{-\frac{1}{d-1}}$ and $(a-1)^{-\frac{1}{d-1}}$ and centered at the origin on the complex plain. For example, if $a = d = 3$, then for the two small roots r_2 and r_3 of $f_3(x,3)$ we get that* $1/\sqrt{4} = 0.5 < |r_3| < |r_2| < 1/\sqrt{2} = 0.707$, *in agreement with* (2.1).

Note that if a or d is large then the width of the annulus becomes small and so does the difference $|r_2| - |r_d|$.

We can get better estimates for r_1. Newton's method suggests the approximation $a_1 = a - 1/a^{d-1}$ with initial value $a_0 = a$ for r_1. As we take more steps we observe that Newton's method provides fast convergence to r_1 although it overestimates r_1 as $f(a_n) > 0, f'(a_n) > 0$ with $n \geq 0$ and $f''(x) > 0$ in a neighborhood of $x = a$. Moreover, we can do much better according to Theorem 3.3 below since we can determine the exact value of r_1 in terms of a series.

The following lemma and theorem can be proven by modifying the argument in [W] that was used in the analysis of the equation $x^k - \sum_{i=0}^{k-1} x^i = 0$; which, by adding the extra root $x = 1$, is equivalent to $x^{k+1} - 2x^k + 1 = 0$, i.e., $f_{k+1}(x, 2)$.

Lemma 3.5. *The polynomial $f_d(x, a)$ is irreducible over the rationals if $a, d \geq 3$.*

Note that Lemma 3.5 also immediately follows by the rational root theorem which is a special case of Gauss's lemma; cf. [G, Problem 220].

Theorem 3.3. *Let $r_1 = a(1 - \varepsilon_d)$ be the positive real root about a of the characteristic equation $f_d(x, a) = 0$. Then*

$$\varepsilon_d = \sum_{i=0}^{\infty} \binom{di + d - 2}{i} \frac{1}{(i+1) a^{d(i+1)}}.$$

Note that above sum provides a series that converges quickly to r_1 if a and/or d is large, and $\varepsilon_d = 1/a^d + (2d-2)/(2a^{2d}) + \ldots$; thus,

$$r_1 = a(1 - \varepsilon_d) = a - 1/a^{d-1} - (d-1)/a^{2d-1} - \ldots.$$

For $d = 3$ we mentioned $r_1 > a - 1/a^2 - 2/a^3$ in (3.1), which is a better underestimate than the one suggested by Theorem 3.2, $r_1 > a - 2/a^2$. An even better overestimate follows by Theorem 3.3 for $d = 3$: $r_1 < a - 1/a^2 - 2/a^5$, while in general, we have $r_1 < a - 1/a^{d-1} - (d-1)/a^{2d-1}$.

3.4. Some Properties of the Power Sum S_n^-

To prove Theorem 3.1 we need some preparation provided by Lemmas 3.6 and 3.7 and finally by Lemma 3.8.

Lemma 3.6. *Let* $S_n^- = \sum_{k=2}^d r_k^n$ *and* $0 < \varepsilon < 1$. *We have*

$$|S_n^-| \le R_n^- = \sum_{k=2}^d |r_k|^n < (d-1)(a-1)^{-\frac{n}{d-1}} < \varepsilon$$

if $(d-1)\ln((d-1)/\varepsilon)/\ln(a-1) < n$ *and* $a > 2$.

Remark 3.4. *We can also derive the above inequality for* $|S_n^-|$ *in a slightly improved form by the general power sum inequality for complex numbers given in [B], which claims that*

$$|S_n^-| \le (d-1)\left(\max_{2\le k\le d} |r_k|\right)^n = (d-1)r_2^n$$

for all $n = 1, 2, \ldots$. *According to our estimate on* r_2 *we can conclude that*

$$|S_n^-| < (d-1)(a-1)^{-\frac{n}{d-1}} \quad \textit{for } n = 2, 3, \ldots$$

as in Lemma 3.6.

Proof of Lemma 3.6. The proof follows by Theorem 3.2. As $|r_k|^n < (a-1)^{-\frac{n}{d-1}}$ for all $k \ge 2$, we have

$$\sum_{k=2}^d |r_k|^n < (d-1)(a-1)^{-\frac{n}{d-1}} < \varepsilon$$

in the given range for n. □

In this case, we get that $T_n = \lfloor r^n \rfloor + 1$ by Lemma 3.7 and the fact that $T_n = S_n = r_1^n + S_n^-$ is an integer. Our goal is to evaluate S_n^- in order to compute S_n by the recurrence relation for T_n.

The next lemma follows by results regarding the fractional parts of powers of Pisot numbers.

Lemma 3.7. $S_n^- = \sum_{k=2}^d r_k^n > 0$ *for all sufficiently large* n.

Proof of Lemma 3.7. We know that the sequence of fractional parts $\{r^n\}$ $(n = 0, 1, \ldots)$ cannot have 0 as the unique limit point if $r > 1$ is an algebraic number other than an integer, which result is due to Luca [L] and Dubickas [D1]. By Lemma 3.6 it follows that the fractional parts $\{r_1^n\}$ must be close to 0 or 1 if n is large since $T_n = r_1^n + S_n^-$ is an integer. Therefore, we need that 1 is the unique limit point. In fact, 1 is the unique limit point of the sequence of the fractional parts $\{r_1^n\}$ by [D2, Theorem 2(iii)] since r_1 is a strong Pisot number; cf. [D2]. □

Apparently, we can strengthen Lemma 3.7 and prove that $S_n^- > 0$ for all $n \geq 0$ as it is stated in Lemma 3.8. On the other hand, it is possible that $S_n^- > 1$, e.g., $a = 4$, $d = 15$, and $n = 14$, in which case $S_n^- = T_n - r_1^n > 3$; cf. Remark 3.2.

Lemma 3.8. $S_n^- = \sum_{k=2}^d r_k^n > 0$ *for all* $n \geq 0$.

Proof of Lemma 3.8. Clearly, $S_0^- = d-1$ and $S_n^- = S_n - r_1^n > 0$ for $n = 1, 2, \ldots, d-1$, by Theorem 3.2. We prove that $S_n^- > 0$ for all $n \geq 0$ by induction. Assume that $S_{n-1}^- > 0$, with $1 \leq n \leq n'$. We apply the Newton-Girard formulas for the sums of powers of the $d-1$ roots of

$$\frac{f_d(x,a)}{x - r_1} = x^{d-1} - b_1 x^{d-2} - b_2 x^{d-3} - \cdots - b_{d-2} x - b_{d-1}.$$

Note that $b_{d-1} = 1/r_1 > 0$ and the identity

$$f_d(x,a) = x^d - ax^{d-1} + 1 = (x - r_1)(x^{d-1} - b_1 x^{d-2} - \cdots - b_{d-2} x - b_{d-1})$$

also implies that $-b_1 - r_1 = -a$, i.e., $b_1 = a - r_1 > 0$, $-b_2 + r_1 b_1 = 0$, i.e., $b_2 = r_1 b_1 > 0$, $-b_3 + r_1 b_2 = 0$, i.e., $b_3 = r_1 b_2 > 0$, etc., $-b_{d-2} + r_1 b_{d-3} = 0$, i.e., $b_{d-2} = r_1 b_{d-3} > 0$. By the Newton-Girard formulas we have

$$S_n^- - b_1 S_{n-1}^- - b_2 S_{n-2}^- - \cdots - b_{d-1} S_{n-d+1}^- = 0$$

for $n \geq d$. It implies that $S_n^- > 0$ for $n = n'$ since $b_i > 0$, $i = 1, 2, \ldots, d-1$ and by the induction hypothesis $S_n^- > 0$, $n = 1, 2, \ldots, n' - 1$. □

Now we are ready to complete the proof of Theorem 3.1.

Proof of Theorem 3.1. By Lemmas 3.6 and 3.8 we have that $0 < S_n^- < 1$ if n is sufficiently large, which implies that $T_n = S_n = r_1^n + S_n^- = \lfloor r_1^n \rfloor + 1$ for any sufficiently large n. □

3.5. Properties of S_n^- for Small Values of n

After some numerical experimentation, we approximate S_n^- for a certain set of n values. Although the approximation provides only supplementary information on S_n^- we included it for illustrative purposes. Indeed, we observe that $S_{d-1}^- \approx 1$ with $a = d-1$ and $S_{d-2}^- \approx 1/(d-2)$ with $a = d-2$.

In this section we discuss the behavior of S_n^- for small values of n. We use the idea of bootstrapping since $ar_k^{d-1} = r_k^d + 1$; therefore, we can write for the $d-1$ "small" roots of $x^d - ax^{d-1} + 1 = 0$ that

$$r_k = \left(\frac{1 + r_k^d}{a}\right)^{\frac{1}{d-1}} e^{\frac{2\pi i}{d-1}(k-2)}, \; 2 \leq k \leq d, \tag{3.6}$$

which results in

$$\begin{aligned} r_k^n &= a^{-\frac{n}{d-1}}\left(1+\frac{n}{d-1}r_k^d+O\left(\left|\frac{n^2}{(d-1)^2}r_k^{2d}\right|\right)\right)e^{\frac{2\pi i(k-2)n}{d-1}} \\ &= a^{-\frac{n}{d-1}}\left(1+\frac{n}{d-1}r_k^d(1+o(1))\right)e^{\frac{2\pi i}{d-1}(k-2)n}, \end{aligned}$$

if n is sufficiently small to make $n/(d-1)|r_k|^d \leq n/(d-1)(a-1)^{-d/(d-1)}$ small, by Theorem 3.2. We want to make sure that n is relatively small with respect to $(d-1)a^{d/(d-1)}$ (cf. Lemma 3.9), although it does not necessarily imply that a must be large; cf. Remark 3.2. Note that here, in a rather unusual fashion, $o(1)$ means a quantity which is small when n is sufficiently small as noted above, and in general, $o(A)$ means a quantity such that $|o(A)|/|A|$ is small when n is sufficiently small. $O(A)$ is defined in a similar fashion: it means that $|O(A)|/|A|$ is bounded from above by a finite constant if n is small.

We add these terms with $k = 2, 3, \ldots, d$, and approximate $\sum_{k=2}^{d} r_k^n$ by (3.6) in

$$\sum_{k=0}^{d-2} r_k^n = \sum_{k=0}^{d-2} a^{-\frac{n}{d-1}}e^{\frac{2\pi i}{d-1}nk} + \frac{n}{d-1}a^{-\frac{n+d}{d-1}}\sum_{k=0}^{d-2} e^{\frac{2\pi i}{d-1}(d+n)k}(1+o(1)) \tag{3.7}$$

if $|r_k^d| < (a-1)^{-d/(d-1)}$ is sufficiently small. If $d-1 \mid n$ then the first sum in (3.7) contributes $(d-1)a^{-n/(d-1)}$ to $\sum_{k=0}^{d-2} r_k^n$ while the second sum contributes $o(na^{-(n+d)/(d-1)})$. On the other hand, if $d-1 \mid n+d$, i.e., $d-1 \mid n+1$ then the second sum contributes $na^{-(n+d)/(d-1)}$ and the error term combined with the first sum amounts to $o(na^{-(n+d)/(d-1)})$.

In summary, we get

Lemma 3.9. *If $n \ll (d-1)(a-1)^{d/(d-1)}$, then*

$$S_n^- \approx \begin{cases} a^{-\frac{n}{d-1}}(d-1) & \textit{if } d-1 \mid n, \\ na^{-\frac{n+d}{d-1}} & \textit{if } d-1 \mid n+1. \end{cases} \tag{3.8}$$

Remark 3.5. *By Lemma 3.9 it follows that $S_{d-1}^- \approx 1$ if $a = d-1$, and $S_{d-2}^- \approx \frac{1}{d-2}$ if $a = d-2$.*

Remark 3.6. *By* (3.8), *if $m \in \{0, 1\}$ and $m \equiv -n \pmod{d-1}$ then*

$$S_n^- \approx \binom{n}{m}a^{-\frac{n+md}{d-1}}(d-1)^{-m+1}. \tag{3.9}$$

Therefore, in the special case $d = 3$, as $2 \mid n$ or $2 \mid n+1$, the approximation (3.9) *provides a fairly good estimate of S_n^- for relatively small values of n by Lemma 3.9.*

3.6. The Roots of $f_d(x,a)$ in $\mathbb{Z}/p\mathbb{Z}$

Our method based on the recurrence (3.5) works for any composite modulus m, however, it requires the analysis of the members of its modulo m period and that n is sufficiently large in order to have $T_n - 1 \equiv \lfloor r_1^n \rfloor \pmod{m}$. As before, p denotes a prime. The elegant alternative approach outlined in Section 2 and generalized in the current section, assumes that $f_d(x,a)$ can be factored into linear factors in the polynomial ring $(\mathbb{Z}/p\mathbb{Z})[x]$ for all prime divisors p of m and then it works for all sufficiently large n. (Both methods work for all $n \geq 1$ if $d = 3$ by Theorem 3.2.) This method captures and utilizes the information coded in the polynomial $f_d(x,a)$ in terms of its roots in $\mathbb{Z}/p\mathbb{Z}$. The good news is that Lemma 3.5 about its factorization over the rationals has no bearing on whether $f_d(x,a)$ can be factored into linear factors in $(\mathbb{Z}/p\mathbb{Z})[x]$. Note that, e.g., x^2+1 cannot be factored over $\mathbb{Z}$ but $x^2+1 = (x-2)(x-3)$ in $(\mathbb{Z}/5\mathbb{Z})[x]$, which then leads to the roots $...431212_5$ and $...013233_5$ in the ring of 5-adic integers $\mathbb{Z}_5$ by Hensel's lemma (cf. [G]). This approach offers a direct method to evaluate $\lfloor r_1^n \rfloor$ modulo primes and prime powers; cf. Example 4.2 for $f_3(x,3)$ and $p = 17$.

Remark 3.7. *In $(\mathbb{Z}/p\mathbb{Z})[x]$ only a fraction $\binom{p}{d}/p^d$ of general monic polynomials of degree d have d different linear factors.*

Theorem 3.4. *If $f_d(x,a)$ can be factored in $(\mathbb{Z}/p\mathbb{Z})[x]$ into the product of linear factors with or without multiple factors then, with its roots R_k, $k = 1,2,\ldots,d$, we have*

$$f_d(x,a) \equiv \prod_{k=1}^{d} (x - R_k) \pmod{p} \tag{3.10}$$

and

$$\sum_{n=0}^{\infty} T_n x^n = \frac{d-(d-1)ax}{g_d(x,a)} \equiv \sum_{k=1}^{d} \frac{1}{1-R_k x} \pmod{p}, \tag{3.11}$$

which for all $n \geq 0$ leads to the congruence

$$T_n \equiv \sum_{k=1}^{d} R_k^n \pmod{p}. \tag{3.12}$$

Proof of Theorem 3.4. The proof follows by adapting that of Lemma 3.1 to modulo p, e.g., we have that $g_d(x,a) \equiv \prod_{k=1}^{d}(1 - R_k x) \pmod{p}$. □

For example, if $g_2(x,a) = (1-mx)^2 = 1 - 2mx + m^2x$ with $a = 2m$ and $m^2 \equiv 1 \pmod{p}$, i.e., corresponding to $g_2(x,a) \equiv 1 - ax + x^2 \pmod{p}$, then we get that $T_n \equiv 2m^n \pmod{p}$. Note that here m is a multiple root.

If we do not have multiple factors in (3.10) then the congruence (3.11) can be lifted to prime powers p^k with any $k \geq 1$ in order to determine $T_n \pmod{p^k}$; cf. Example 4.2. If we have multiple factors then we cannot lift. For example, if we set $p = 3$ in the original example then $f_3(x,3) \equiv (x+1)^3 \pmod 3$; and thus, $\lfloor r_1^n \rfloor \equiv 3(-1)^n - 1 \equiv 2 \pmod 3$. The above method does not help us to find the proper congruence, similar to (3.11), when the modulus is 3^k, $k \geq 2$, since -1 is a multiple root. Note, however, that for all $n \geq 1$ one can easily find that $\lfloor r_1^n \rfloor \equiv 7 + 8 \times 2^n + 8 \times 4^n + 3 \times 5^n + 2 \times 7^n + 1 \times 8^n \equiv 3 \times 2^{5n} + 2^{4n+1} - 2^{2n} - 2^n + (-1)^n - 2 \pmod 9$ by standard algebraic approach and these representations are not unique.

Remark 3.8. *Assume that m has the prime number factorization $m = \prod_{i=1}^s p_i^{e_i}$. If the above factorization method works modulo m with different linear factors then in the properly updated congruence* (3.12) *we have $d \times s$ terms to find out whether and when $\lfloor r_1^n \rfloor$ is divisible by m. The final step is to look into the modulo m period whose length is*

$$\operatorname{lcm}\{\pi(p_i^{e_i}; T_n), i = 1, 2, \ldots, s\} \tag{3.13}$$

and the sequence $\{T_n\}_{n\geq 0}$ corresponds to the characteristic polynomial $f_d(x,a)$. Note that $\pi(p_i^{e_i}) \mid p_i \pi(p_i^{e_i-1})$ with $e_i \geq 2$. No need to use the recurrence (3.4) *since the updated congruence* (3.12) *suffices in order to obtain $T_n \pmod m$ and $\pi(m) \mid \phi(m)$ by Fermat's little theorem as we have already observed in Section 2.*

4. Examples and Computational Concerns

In this section we list three examples to illustrate the two basic techniques with their benefits and limitations.

Note that for a composite modulus m the second method requires that we factorize $f_d(x,a)$ with respect to all prime divisors of m and if we succeed with the factorization into linear factors, then we can proceed by the lifting (cf. Example 4.2) if necessary, and then use the Chinese remainder theorem twice: to find the right congruence modulo m and the right indices to guarantee divisibility; cf. Example 4.3. Other computational concerns are addressed in Remark 3.8.

On the other hand, the first method allows us to work out the solutions in a single step, using the recurrence relation (3.4) modulo m and then exploring the period (cf. (3.5) and (3.13)), without the factorization requirement or regard to the composite nature of the modulus; cf. Example 4.1. Note that determining $\lfloor r_1^n \rfloor$ for large n would require high precision calculations; and thus, the use of (3.5) is advisable.

Example 4.1. *We look into the modulo 5 and modulo 25 periods of $\lfloor r_1^n \rfloor$ with $(a,d) = (4,5)$ via the recurrence* (3.5). *We find that $\pi(5) = 24$ and $5 \mid \lfloor r_1^n \rfloor$ exactly if $n \equiv 2, 4, 10, 12, 20 \pmod{24}$ while $\pi(25) = 120$ and $25 \mid \lfloor r_1^n \rfloor$ exactly if $n \equiv 20, 34, 60, 100 \pmod{120}$. The last index with $T_n \neq \lfloor r_1^n \rfloor + 1$ is $n = d - 1 = 4$ and $T_4 = \lfloor r_1^4 \rfloor + 2$ in agreement with Lemma 3.9. For a similar reason $T_n - \lfloor r_1^n \rfloor$ is "relatively large," in the sense that it exceeds 0.11, when $n = 3, 4, 7$ and 8. Note that*

$$f_5(x,4) = x^5 - 4x^4 + 1 \equiv (x+2)(x^2+x+1)(x^2+3x+3) \pmod 5$$

cannot be factored into linear factors in $(\mathbb{Z}/5\mathbb{Z})[x]$.

Example 4.2. *We take $f_3(x,3) = x^3 - 3x^2 + 1$ and consider $\lfloor r_1^n \rfloor \pmod{17^2}$. Recall that the modulo 17 roots (in base 17) are b (corresponding to $(11)_{17}$), 5, and 4. Now the modulo 17^2 roots are $215 = cb_{17}$, $158 = 95_{17}$, and $208 = c4_{17}$. In fact, we can find the 17-adic roots by the Sage package (based on Hensel's lemma) and obtain $\ldots d85cb_{17}$, $\ldots fad95_{17}$, and $\ldots 4eec4_{17}$. We get that*

$$T_n - 1 = \lfloor r_1^n \rfloor \equiv 215^n + 158^n + 208^n - 1 \pmod{17^2},$$

and $\lfloor r_1^n \rfloor$ is divisible by 17^2 exactly if $n \equiv 68$ or $204 \pmod{272}$, i.e., $n \equiv 68 \pmod{136}$ since $\pi(17^2) = 16 \times 17 = 272$.

Note that there are 680 monic polynomials of degree three (out of $17^3 = 4913$) in $(\mathbb{Z}/17\mathbb{Z})[x]$ that can be factored into three different linear factors while 289 of them have multiple (linear) factors and 2312 of them have only one linear factor. The remaining 1632 polynomials are irreducible in $\mathbb{Z}/17\mathbb{Z}$.

Theorem 4.1 states that in general, among all monic polynomials of degree 3 there is an interesting relation among the numbers of different possibilities regarding their factorization properties. We set $I_n = I_n(p) = \frac{1}{n}\sum_{k|n} \mu(k)p^{n/k}$ for the number of monic irreducible polynomials of degree n over $\mathbb{Z}/p\mathbb{Z}$ where μ is the Möbius function; cf. [FS, p. 91]. More related results can be found in [FS, pp. 449 and 672].

Theorem 4.1. *Consider all general monic polynomials of degree 3 in $(\mathbb{Z}/p\mathbb{Z})[x]$. For their factorization property over $\mathbb{Z}/p\mathbb{Z}$, we set*

- *$A_1 = \binom{p}{3}$, the number of polynomials that can be factored into three different (linear) factors;*
- *$A_2 = I_3$, the number of polynomials that are irreducible;*
- *$A_3 = pI_2$, the number of polynomials that have one linear factor and an irreducible quadratic factor;*
- *$A_4 = p$, the number of polynomials that have a multiple linear factor of multiplicity 3;*
- *$A_5 = 2\binom{p}{2} + p$, the number of polynomials that have multiple (linear) factors (of multiplicity 2 or 3).*

Then $A_1 + A_2 + A_3 + A_5 = p^3$ and $A_1 + A_2 = A_3$.

Proof of Theorem 4.1. The given A_i values and the first summation identity are self-explanatory. We have $I_2 = (p^2 - p)/2$ and $I_3 = (p^3 - p)/3$, which imply $A_1 + A_2 = \binom{p}{3} + (p^3 - p)/3 = (p^3 - p^2)/2 = pI_2 = A_3$. □

Example 4.3 (Example 4.2 continued)**.** *If we switch to the composite modulus* $17^2 \times 37 = 10693$ *in Example 4.2 then we get*

$$\begin{aligned} T_n - 1 =& \lfloor r_1^n \rfloor \\ \equiv& (158^n + 208^n + 215^n) \times 4625 \\ &+ (15^n + 29^n + 33^n) \times 6069 - 1 \pmod{10693}, \end{aligned}$$

by the Chinese Remainder Theorem. Then $\lfloor r_1^n \rfloor$ *is divisible by* $17^2 \times 37$ *exactly if* $n \equiv 748 \pmod{1224}$ *by using the extended Chinese Remainder Theorem since* $\gcd(\pi(17^2), \pi(37)) = \gcd(16 \times 17, 36) = 4.$ *Note that* $\pi(17^2 \times 37) = 2448$ *divides* $\phi(17^2 \times 37) = 9792.$

Acknowledgments

We thank Georges Győry for bringing the original problem to our attention and for some discussions. We also thank the referee for the careful reading of the manuscript, some corrections, and helpful suggestions.

References

[B] Buckholtz J. D., *Sums of powers of complex numbers*, J. Math. Anal. Appl. **17** (1967), 269–279.

[DJMP] Djukić D., Janković V., Matić I., and Petrović N., *The IMO Compendium, A Collection of Problems Suggested for the International Mathematical Olympiads: 1959-2004*, Springer, New York, 2006.

[D1] Dubickas A., *A note on powers of Pisot numbers*, Publ. Math. Debrecen **56** (2000), 141–144.

[D2] Dubickas A., *On the limit points of the fractional parts of powers of Pisot numbers*, Arch. Math. (Brno) **42** (2006), 151–158.

[DF] Dummit D. and Foote R., *Abstract Algebra*, 3rd Edition, Wiley, New York, 2003.

[FS] Flajolet P. and Sedgewick R., *Analytic Combinatorics*, Cambridge University Press, Cambridge, 2009.

[G] Gouvêa F. Q., *p-adic Numbers. An introduction*, Universitext. Springer-Verlag, Berlin, 1993.

[HW] Hua L. K. and Wang Y., *Application of Number Theory in Numerical Analysis*, Springer, Berlin/Heidelberg/New York; Science Press, Beijing, 1981.

[L] Luca F., *On a question of G. Kuba*, Arch. Math. (Basel) **74** (2000), 269–275.

[S] Stanley R., *Enumerative Combinatorics, Vol. 2.*, Cambridge University Press, Cambridge, 1999.

[W] Wolfram D. A., *Solving generalized Fibonacci recurrences*, Fibonacci Quart. **36** (1998), 129–145.

MA