Earthline Journal of Mathematical Sciences
E-ISSN: 2581-8147
Volume 17, Number 1, February 2027, Pages 29-42
https://doi.org/10.34198/ejms.17127.02.0029

Prime Divisors of Polynomial Values Along Infinite Sequences

Mohammed Aassila

Académie de Strasbourg, F-67000 Strasbourg, France
e-mail: aassilam@gmail.com

Abstract

Let $P \in \mathbb{Z}[x]$ be nonzero and let $\mathcal{K} \subset \mathbb{Z}_{>0}$ be an infinite set of positive integers such that the nonzero values among $\{P(k) : k \in \mathcal{K}\}$ have prime divisors lying in a fixed finite set; no ordering or growth condition on $\mathcal{K}$ is assumed. We prove that P is either constant or a constant multiple of a power of a linear polynomial,

$$P(x) = c(ax+b)^n, \qquad \gcd(a,b) = 1,\ a > 0,$$

via a single mechanism: two distinct roots of P force an S-unit equation. The proof rests on the classical finiteness theorem for the two-variable S-unit equation over a number field (Siegel, Mahler, Parry, Lang). We then show that for structured sets $\mathcal{K}$ everything can be done by elementary means. First, an elementary density obstruction: if $\mathcal{K}$ grows at most polynomially, then no non-constant polynomial satisfies the hypothesis at all; this rests on the asymptotic $(\log X)^s/(s!\prod \log p_j)$ for the number of S-unit integers below X, and settles and strengthens a speculative remark in the author's original 2003 proposal of this problem. Second, for geometric progressions $k_i = A\alpha^i + B$, where non-constant solutions do exist, we prove by an elementary periodicity argument that the solutions are exactly the polynomials $c(x-B)^n$; the same argument gives a self-contained proof of Pólya's theorem on the prime divisors of $ab^n + c$. In our treatment the S-unit theorem is needed only for unstructured sets $\mathcal{K}$, for instance for infinite subsequences of a geometric progression.

1 Introduction

1.1 Statement of the main theorem

Theorem 1.1. *Let $P \in \mathbb{Z}[x]$ be a polynomial that is not identically zero, and let $\mathcal{K} \subset \mathbb{Z}_{>0}$ be an infinite set of positive integers such that the set of prime divisors of the nonzero integers among $\{P(k) : k \in \mathcal{K}\}$ is finite. Then either $\deg P = 0$, or*

$$P(x) = c(ax+b)^n$$

for some $c \in \mathbb{Z} \setminus \{0\}$, $n \geq 1$, and coprime integers $a, b \in \mathbb{Z}$ with $a > 0$. This representation is unique.

Only the *infinitude* of $\mathcal{K}$ is used in the proof; no ordering, density, or growth condition on $\mathcal{K}$ is needed for Theorem 1.1 itself (density and growth become relevant only once we ask, in Sections 4–5, which

Received: October 1, 2026; Received in revised form: November 18, 2026; Accepted: November 20, 2026;
Published online: November 23, 2026

2020 Mathematics Subject Classification: Primary 11D61; Secondary 11D45, 11A41, 11B37, 11C08.

Keywords and phrases: S-unit equations; prime divisors of polynomials; Schur's theorem; Pólya–Szegő theorem; Zsigmondy's theorem; primitive prime divisors; exponential Diophantine equations; Siegel's theorem.

Copyright 2027 the Author

polynomials P can actually *occur*). We state the hypothesis for a set rather than for a strictly increasing sequence $(k_i)_{i\geq 1}$ because any infinite subset of $\mathbb{Z}_{>0}$ has a canonical increasing enumeration, so nothing is gained by fixing one in advance, and the set formulation makes clear that the theorem is a statement about integer points, in the spirit of Remark 1.2 below.

Remark 1.1 (Informal summary)**.** *Theorem 1.1 says:* the only way a polynomial can take S-unit values at infinitely many integers is that, after an affine change of variable, it is a pure power. *Trivial examples are easy to produce: if $\mathcal{K}$ itself consists of S-unit integers (e.g. $\mathcal{K} = \{2^i 3^{2i} : i \geq 1\}$ for $S = \{2, 3\}$), then $P(x) = x^m$ satisfies the hypothesis for any $m \geq 1$, since $P(k) = k^m$ is again an S-unit for every $k \in \mathcal{K}$. Theorem 1.1 says that, up to the affine normalization, this is the* only *mechanism.*

Remark 1.2 (Geometric reformulation)**.** *Let $Z(P) \subset \overline{\mathbb{Q}}$ denote the (finite) set of roots of P, i.e. the support of the zero divisor of P on $\mathbb{A}^1$. The mechanism behind Theorem 1.1 (made precise in Proposition 3.1 below) is that if $Z(P)$ has two or more distinct points, then $\{k \in \mathbb{Z} : P(k)$ is an S-unit$\}$ is finite for every finite set S of primes: two roots already force an S-unit equation $u + v = 1$. So Theorem 1.1 is the statement that infinitely many S-integral points on the affine line $\mathbb{A}^1 \setminus Z(P)$ force $Z(P)$ to be a single point (with multiplicity); it is a one-dimensional instance of the general principle, familiar from the theory of integral points on curves, that a variety with enough points removed can carry only finitely many integral points.*

Remark 1.3 (Reformulation without reference to a sequence, and reduction to the linear case)**.** *For $P \in \mathbb{Z}[x] \setminus \{0\}$ and a finite set of primes S, write*

$$\mathcal{U}_S(P) = \{n \in \mathbb{Z}_{>0} : P(n) \neq 0 \text{ and } P(n) \text{ is an } S\text{-unit}\}.$$

The hypothesis of Theorem 1.1 holds for some infinite $\mathcal{K}$ if and only if $\mathcal{U}_S(P)$ is infinite for some finite S (take $\mathcal{K} = \mathcal{U}_S(P)$ for the "if" direction; for the "only if" direction let S be the finite set of primes dividing the nonzero values among $\{P(k) : k \in \mathcal{K}\}$, and note that $\mathcal{K}$ minus the finitely many zeros of P is then a subset of $\mathcal{U}_S(P)$). So Theorem 1.1 can equally be stated: if $\mathcal{U}_S(P)$ is infinite for some finite S, then P is constant or $P(x) = c(ax + b)^n$. *Moreover, for $P(x) = c(ax + b)^n$ with $n \geq 1$ one has*

$$\mathcal{U}_S(P) = \begin{cases} \{n \in \mathbb{Z}_{>0} : an + b \text{ is a nonzero } S\text{-unit}\} & \text{if } c \text{ is an } S\text{-unit}, \\ \emptyset & \text{otherwise.} \end{cases}$$

Thus the classification reduces the original, nonlinear-looking question about P to the same question about a single linear *polynomial $ax + b$. This reduction is used in the proof of Proposition 5.1.*

1.2 History and motivation

In 2003, the author proposed a version of this problem to the Canadian journal *Crux Mathematicorum* [1], as Problem 2838, for polynomials P with integer coefficients, asking to prove the stronger conclusion $P(x) = (ax + b)^n$ *without* a scalar factor c. No complete solution was received at the time. Revisiting the problem, we found (Remark 6.1 below) that this scalar-free conclusion is *false* once a, b are required to be

integers, and that our proof of the corrected statement requires machinery considerably heavier than the Olympiad-style phrasing suggests: namely the finiteness theorem for the two-variable S-unit equation [5], which is equivalent to the finiteness of S-integral points on $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ and closely related to Siegel's theorem on integral points on algebraic curves [16].

Beyond proving Theorem 1.1, the present note asks a second, complementary question:

> *For which choices of the set $\mathcal{K}$ can Theorem 1.1 be proved, or its hypothesis shown to be unsatisfiable, without invoking the finiteness theorem for S-unit equations?*

We obtain the following answers, in terms of the increasing enumeration $(k_i)_{i\geq 1}$ of $\mathcal{K}$.

- If $\mathcal{K}$ grows at most polynomially, $k_i = O(i^M)$, then, by a short and elementary counting argument (Theorem 4.1), *no non-constant P can satisfy the hypothesis at all.* This settles, and sharpens, a speculative remark from the 2003 proposal.
- If $\mathcal{K}$ is a geometric progression, $k_i = A\alpha^i + B$, then non-constant solutions do exist (e.g. $P(x) = x^n$, $k_i = \alpha^i$), and we determine them completely, again by a fully elementary argument (Lemma 5.2 and Theorem 5.2): they are exactly the polynomials $c(x - B)^n$.
- For an arbitrary infinite $\mathcal{K}$ – already for an infinite *subsequence* of a geometric progression (Proposition 5.1) – Theorem 1.1 is the answer, and we do not know how to avoid S-unit equations.

1.3 Organization

Section 2 fixes terminology and states the finiteness theorem for the two-variable S-unit equation, with its history. Section 3 proves Theorem 1.1, via a single proposition (Proposition 3.1). Section 4 proves the polynomial-growth obstruction. Section 5 treats polynomially parametrized sequences (via Schur's theorem), geometric progressions (with an elementary if-and-only-if classification), and subsequences of geometric progressions. Section 6 records three sharpness remarks for Theorem 1.1. Section 7 discusses further directions.

2 Preliminaries: S-unit equations

Throughout, $\mathcal{K}$ denotes an infinite set of positive integers, whereas number fields are denoted by F.

Definition 2.1. *Let F be a number field and let S_F be a finite set of places of F containing all archimedean places. The ring of S_F-*integers *is*

$$\mathcal{O}_{F,S_F} = \{x \in F : v(x) \geq 0 \text{ for every finite place } v \notin S_F\},$$

and its unit group, the group of S_F-units, *is*

$$\mathcal{O}_{F,S_F}^{\times} = \{x \in F^{\times} : v(x) = 0 \text{ for every finite place } v \notin S_F\}.$$

When $F = \mathbb{Q}$ *and* $S_F = S \cup \{\infty\}$ *for a finite set* $S = \{p_1, \dots, p_s\}$ *of rational primes,* $\mathcal{O}_{F,S_F}^{\times} = \{\pm p_1^{e_1} \cdots p_s^{e_s} : e_j \in \mathbb{Z}\}$ *is the group of rational* S-units, *and we simply write* S *in place of* S_F. *For a nonzero integer* n, *"*n *is an* S*-unit" thus means that every prime factor of* n *lies in* S. *In particular* ± 1 *are* S*-units for every* S, *including* $S = \emptyset$.

The key input for Theorem 1.1 is the finiteness theorem for the two-variable S-unit equation over a number field, which is equivalent to the finiteness of the set of S_F-integral points on $\mathbb{P}^1_F \setminus \{0, 1, \infty\}$.

Theorem 2.1 (Finiteness of the two-variable S-unit equation)**.** *Let* F *be a number field,* S_F *a finite set of places of* F *containing all archimedean places, and* $a, b \in F^{\times}$. *The equation*

$$a\,u + b\,v = 1, \qquad (u, v) \in \mathcal{O}_{F,S_F}^{\times} \times \mathcal{O}_{F,S_F}^{\times},$$

has only finitely many solutions (u, v).

For ordinary units (that is, when S_F consists of the archimedean places only) this finiteness statement is implicit in the work of Siegel [15] on the approximation of algebraic numbers. Mahler [8] proved it for S-units of $\mathbb{Q}$, and Parry [11] for S_F-units of an arbitrary number field F, which is the case stated in Theorem 2.1; Lang [7] extended it to arbitrary finitely generated multiplicative groups in fields of characteristic 0. All these proofs rest on Diophantine approximation of Thue–Siegel type and are ineffective: they give no bound for the size of the solutions. An effective proof, based on Baker's theory of linear forms in logarithms, was given by Győry [6], and Evertse [4] obtained an explicit upper bound for the *number* of solutions depending only on $[F : \mathbb{Q}]$ and the cardinality of S_F. Unit equations in more than two unknowns, which we do not need, lie deeper: their treatment requires the subspace theorem. We refer to the monograph of Evertse and Győry [5] for a comprehensive account, with precise references and quantitative versions, and to Bombieri and Gubler [3] for a textbook treatment via heights.

Lemma 2.1. *Let* F *be a number field, let* S_F *be a finite set of places of* F *containing all archimedean places, and let* $\gamma \neq \delta$ *be elements of* F. *Let* $S'_F \supseteq S_F$ *be the finite set of places obtained from* S_F *by adjoining all finite places* v *of* F *with* $v(\delta - \gamma) \neq 0$. *Then there are only finitely many* $x \in F$ *such that both* $x - \gamma$ *and* $x - \delta$ *are* S'_F*-units.*

Proof. Since $\delta - \gamma \neq 0$, there are only finitely many finite places v with $v(\delta - \gamma) \neq 0$, so S'_F is finite, and $\delta - \gamma$ is an S'_F-unit by construction. Set

$$u = \frac{x - \gamma}{\delta - \gamma}, \qquad v = \frac{\delta - x}{\delta - \gamma}.$$

Then $u + v = 1$, and $u, v \in \mathcal{O}_{F,S'_F}^{\times}$, because $x - \gamma$, $\delta - x = -(x - \delta)$ and $\delta - \gamma$ are S'_F-units. By Theorem 2.1 (with $a = b = 1$ and S'_F in place of S_F), the equation $u + v = 1$ has only finitely many solutions $(u, v) \in (\mathcal{O}_{F,S'_F}^{\times})^2$; since $x = \gamma + u(\delta - \gamma)$ is determined by u, there are only finitely many such x. □

3 Proof of the main theorem

3.1 The key mechanism: two distinct roots

The proof rests on a single proposition, which converts the arithmetic hypothesis (finitely many primes occur) into an algebraic one (the polynomial has only one root).

Proposition 3.1 (Key mechanism)**.** *Let $g \in \mathbb{Z}[x]$ be non-constant of degree n with leading coefficient a, and let $\gamma_1, \dots, \gamma_D \in \overline{\mathbb{Q}}$ be its* distinct *roots. Let $F = \mathbb{Q}(\gamma_1, \dots, \gamma_D)$ be the splitting field of g over $\mathbb{Q}$, let S be a finite set of rational primes containing all prime divisors of a, and let S_F be the set of places of F lying above $S \cup \{\infty\}$. If $k \in \mathbb{Z}$ is such that $g(k)$ is a nonzero S-unit, then $k - \gamma_l$ is an S_F-unit for every $l = 1, \dots, D$. Consequently, if $D \geq 2$, the set $\{k \in \mathbb{Z} : g(k)$ is a nonzero S-unit$\}$ is finite.*

Proof. Write $g(x) = a \prod_{l=1}^{D} (x - \gamma_l)^{m_l}$ with $m_l \geq 1$ the multiplicity of γ_l, so that $n = \sum_l m_l$. The polynomial $a^{n-1} g(y/a) \in \mathbb{Z}[y]$ is monic of degree n and has $a\gamma_l$ as a root, so each $a\gamma_l$ is an algebraic integer; hence $a(k - \gamma_l)$ is an algebraic integer for every l. We have

$$\prod_{l=1}^{D} \big(a(k - \gamma_l)\big)^{m_l} = a^n \prod_{l=1}^{D} (k - \gamma_l)^{m_l} = a^{n-1}\, g(k),$$

which is an S-unit, since the prime factors of a lie in S and $g(k)$ is an S-unit by hypothesis. In particular, for every finite place $v \notin S_F$,

$$\sum_{l=1}^{D} m_l\, v\big(a(k - \gamma_l)\big) = 0.$$

Each term $v(a(k - \gamma_l))$ is ≥ 0 because $a(k - \gamma_l)$ is an algebraic integer, and each $m_l \geq 1$; a sum of non-negative terms equal to 0 forces every term to vanish. Hence $a(k - \gamma_l)$ is an S_F-unit for every l, and since a is an S_F-unit, so is $k - \gamma_l = a(k - \gamma_l)/a$.

For the last statement, suppose $D \geq 2$ and apply Lemma 2.1 with $\gamma = \gamma_1$, $\delta = \gamma_2$: with $S'_F \supseteq S_F$ as in that lemma, there are only finitely many $x \in F$, hence only finitely many $k \in \mathbb{Z}$, such that $k - \gamma_1$ and $k - \gamma_2$ are S'_F-units. By the first part, every $k \in \mathbb{Z}$ for which $g(k)$ is a nonzero S-unit has this property. □

3.2 Proof of Theorem 1.1

Proof of Theorem 1.1. If $\deg P = 0$ there is nothing to prove, so assume $d := \deg P \geq 1$.

Let S be the finite set of prime divisors of all nonzero integers among $\{P(k) : k \in \mathcal{K}\}$. After discarding the at most d elements $k \in \mathcal{K}$ for which $P(k) = 0$, the value $P(k)$ is a nonzero S-unit for all remaining $k \in \mathcal{K}$, and the remaining set is still infinite. Write $P(x) = c_0\, Q(x)$ with $c_0 \in \mathbb{Z} \setminus \{0\}$ and $Q \in \mathbb{Z}[x]$ primitive, and enlarge S so that it contains the prime divisors of the leading coefficient of Q. Since $Q(k)$ divides $P(k)$, the integer $Q(k)$ is a nonzero S-unit for every remaining $k \in \mathcal{K}$.

Apply Proposition 3.1 to $g = Q$. If Q had two or more distinct roots, the set $\{k \in \mathbb{Z} : Q(k) \text{ is a nonzero } S\text{-unit}\}$ would be finite, contradicting the fact that it contains all but finitely many elements of the infinite set $\mathcal{K}$. Hence Q has exactly one root $\gamma \in \overline{\mathbb{Q}}$, of multiplicity $n := \deg Q = d \geq 1$: $Q(x) = a_0(x-\gamma)^n$, where a_0 is the leading coefficient of Q.

Rationality of γ. Since $Q \in \mathbb{Q}[x]$, every automorphism σ of $\overline{\mathbb{Q}}/\mathbb{Q}$ permutes the roots of Q; as γ is the only root, $\sigma(\gamma) = \gamma$ for every such σ. An element of $\overline{\mathbb{Q}}$ fixed by every automorphism of $\overline{\mathbb{Q}}/\mathbb{Q}$ lies in $\mathbb{Q}$. Hence $\gamma \in \mathbb{Q}$; write $\gamma = -b/a$ in lowest terms, with $a \geq 1$ and $\gcd(a,b) = 1$.

Normalization. We have $Q(x) = a_0(x + b/a)^n = (a_0/a^n)(ax+b)^n$. The polynomial $(ax+b)^n$ is primitive: for any prime p, the reduction of $ax+b$ modulo p is nonzero because $\gcd(a,b) = 1$, and $\mathbb{F}_p[x]$ is an integral domain, so the reduction of $(ax+b)^n$ modulo p is nonzero. Since Q is primitive as well, comparing contents (Gauss's lemma) gives $a_0/a^n = \pm 1$. Thus $Q(x) = \pm(ax+b)^n$, and absorbing the sign into the constant we obtain $P(x) = c(ax+b)^n$ with $c = \pm c_0 \neq 0$, $n \geq 1$, $a > 0$ and $\gcd(a,b) = 1$, as claimed.

Uniqueness. In any such representation, $n = \deg P$, the pair (a,b) with $a > 0$ and $\gcd(a,b) = 1$ is determined by the unique root $-b/a$ of P, and c is then determined by comparing leading coefficients. □

4 A polynomial-growth obstruction

We now prove that if $\mathcal{K}$ grows at most polynomially – meaning that its increasing enumeration $k_1 < k_2 < \cdots$ satisfies $k_i = O(i^M)$ for some fixed M – then the hypothesis of Theorem 1.1 forces P to be constant, with no need for S-unit equations. The point is an elementary counting fact: the S-unit integers up to X number only $O((\log X)^{|S|})$, so a polynomially bounded family of N distinct S-unit values cannot exist once N is large.

Lemma 4.1 (S-unit counting)**.** *Let $S = \{p_1, \ldots, p_s\}$ be a finite, nonempty set of primes, and let $N_S(X)$ denote the number of positive S-unit integers $\leq X$ (the integer 1 is an S-unit and is counted). Then*

$$N_S(X) \sim \frac{(\log X)^s}{s! \prod_{j=1}^{s} \log p_j} \qquad \text{as } X \to \infty.$$

In particular $N_S(X) = O((\log X)^s)$, the implied constant depending only on S, and the number of (positive or negative) S-unit integers of absolute value at most X is $2N_S(X)$.

Proof. A positive S-unit integer $\leq X$ is uniquely of the form $p_1^{e_1} \cdots p_s^{e_s}$ for an exponent vector $(e_1, \ldots, e_s) \in \mathbb{Z}_{\geq 0}^s$ with $\sum_j e_j \log p_j \leq \log X$. So $N_S(X)$ is exactly the number of lattice points of $\mathbb{Z}^s$ in the simplex

$$\Delta_X = \Big\{ y \in \mathbb{R}_{\geq 0}^s : \sum_{j=1}^{s} y_j \log p_j \leq \log X \Big\} = (\log X) \cdot \Delta,$$

where $\Delta := \{y \in \mathbb{R}_{\geq 0}^s : \sum_j y_j \log p_j \leq 1\}$. The number of lattice points in the dilate $T\Delta$ of a fixed compact convex set Δ with nonempty interior is asymptotic to $T^s \operatorname{vol}(\Delta)$ as $T \to \infty$, and $\operatorname{vol}(\Delta) = 1/(s! \prod_j \log p_j)$

(the volume of the simplex $\{y \geq 0 : \sum_j a_j y_j \leq 1\}$ being $1/(s! \prod_j a_j)$, by induction on s). This proves the asymptotic formula, and the remaining assertions are immediate. □

Theorem 4.1 (Polynomial-growth obstruction)**.** *Let $P \in \mathbb{Z}[x]$ be non-constant, and let $\mathcal{K} \subset \mathbb{Z}_{>0}$ be an infinite set whose increasing enumeration $k_1 < k_2 < \cdots$ satisfies $k_i = O(i^M)$ for some fixed $M > 0$. Then the set of prime divisors of the nonzero integers among $\{P(k) : k \in \mathcal{K}\}$ is infinite.*

Proof. Suppose, for contradiction, that all these prime divisors lie in a finite set $S = \{p_1, \ldots, p_s\}$ of primes. Enlarging S if necessary, we may assume $s \geq 1$. Then every nonzero value $P(k)$, $k \in \mathcal{K}$, is an S-unit (this includes the values ± 1).

Let $d = \deg P \geq 1$. Since P is non-constant, there is $x_0 \geq 1$ such that $|P|$ is strictly increasing and nowhere zero on $[x_0, \infty)$; fix i_0 with $k_{i_0} \geq x_0$. Then for every $N \geq i_0$ the integers $P(k_{i_0}), \ldots, P(k_N)$ are nonzero and have pairwise distinct absolute values, and each is an S-unit. Moreover, since $k_i = O(i^M)$ and $|P(x)| = O(x^d)$ for $x \geq 1$, there is a constant $C > 1$ with

$$|P(k_i)| \leq C\, i^{Md} \leq X_N := C\, N^{Md} \qquad \text{for all } 1 \leq i \leq N.$$

Thus $P(k_{i_0}), \ldots, P(k_N)$ are $N - i_0 + 1$ distinct S-unit integers of absolute value at most X_N, so by Lemma 4.1

$$N - i_0 + 1 \;\leq\; 2N_S(X_N) \;=\; O\big((\log X_N)^s\big) \;=\; O\big((\log N)^s\big).$$

Since $(\log N)^s / N \to 0$ as $N \to \infty$, this is impossible for N sufficiently large. □

Corollary 4.1. *If $\mathcal{K} \subset \mathbb{Z}_{>0}$ is infinite with increasing enumeration $k_i = O(i^M)$ for some fixed M, and $\mathcal{K}$ satisfies the hypothesis of Theorem 1.1 for a nonzero $P \in \mathbb{Z}[x]$, then P is constant. Equivalently: if P is non-constant and $\{P(k) : k \in \mathcal{K}\}$ has finitely many prime divisors for an infinite $\mathcal{K} \subset \mathbb{Z}_{>0}$, then $\mathcal{K}$ has* super-polynomial *growth, i.e. its increasing enumeration satisfies $k_i \neq O(i^M)$ for every fixed M.*

Corollary 4.1 settles, and strengthens, the speculation in the 2003 proposal that "algebraic number theory or primitive-prime-divisor methods (Zsigmondy-type results) seem to suffice" for $k_i = O(i^M)$: no such refined tools are needed, and moreover the true state of affairs is not merely that Theorem 1.1 admits an elementary proof in this regime, but that its hypothesis is *never* satisfied by a non-constant P. Non-constant examples only appear once $\mathcal{K}$ grows faster than every fixed power of i, for instance exponentially (Section 5.2); see, however, Section 7.2 for intermediate growth rates.

5 Structured sequences

In this section we treat two families of structured sequences by congruence arguments. For polynomially parametrized sequences (Section 5.1) the conclusion is a special case of Corollary 4.1; we include the short alternative proof, which goes back to Schur, because the same idea – produce infinitely many indices

at which the values are congruent to a fixed nonzero integer modulo high powers of the hypothetical finitely many primes – is what settles the case of geometric progressions (Section 5.2), where non-constant solutions exist and Theorem 4.1 does not apply.

5.1 Polynomially parametrized sequences: Schur's theorem

The following theorem is due to Schur [14]; see also [13, Part VIII, Problem 108] and the expository treatments of Murty and Thain [10] and Pollack [12]. We give the short proof to keep the note self-contained.

Lemma 5.1 (Schur)**.** *Let $f \in \mathbb{Z}[x]$ be non-constant. Then the set of primes dividing some nonzero value $f(n)$, $n \geq 1$, is infinite.*

Proof. If $f(0) = 0$, then $p \mid f(p)$ for every prime p, and $f(p) \neq 0$ for all but finitely many p; so every sufficiently large prime occurs.

Assume now $c := f(0) \neq 0$, and write $f(x) = c + x\,h(x)$ with $h \in \mathbb{Z}[x]$, $h \neq 0$. Suppose, for contradiction, that $p_1, \dots, p_r$ ($r \geq 0$) are *all* the primes dividing nonzero values $f(n)$, $n \geq 1$, and let $m = p_1 \cdots p_r$ (so $m = 1$ if $r = 0$). For a positive integer t put $n_t := |c|\, m\, t \geq 1$. Then

$$f(n_t) = c + n_t\, h(n_t) = c\big(1 + w(t)\big), \qquad w(t) := \operatorname{sgn}(c)\, m\, t\, h(n_t) \in \mathbb{Z}.$$

Since h has only finitely many roots, $h(n_t) \neq 0$ and hence $|w(t)| \geq t$ for all large t; fix t with $|w(t)| \geq 3$. Then $|1 + w(t)| \geq 2$, so $f(n_t) \neq 0$ and $1 + w(t)$ has a prime factor q. Since $m \mid w(t)$, we have $1 + w(t) \equiv 1 \pmod{p_j}$ for every j, so $q \neq p_j$ for every j. But q divides the nonzero value $f(n_t)$ with $n_t \geq 1$, contradicting the choice of $p_1, \dots, p_r$. □

Theorem 5.1 (Polynomially parametrized sequences)**.** *Let $\pi \in \mathbb{Z}[x]$ be non-constant, let $i_0 \geq 1$ be such that $\pi(i) > 0$ for all $i \geq i_0$, and let $\mathcal{K} = \{\pi(i) : i \geq i_0\}$. If a nonzero polynomial $P \in \mathbb{Z}[x]$ satisfies the hypothesis of Theorem 1.1 for this $\mathcal{K}$, then P is constant.*

Proof. Suppose $\deg P \geq 1$. Then $f(x) := P(\pi(x + i_0 - 1)) \in \mathbb{Z}[x]$ has degree $\deg P \cdot \deg \pi \geq 1$. By Lemma 5.1, infinitely many primes divide nonzero values $f(n) = P(\pi(n + i_0 - 1))$, $n \geq 1$, and these are values of P on $\mathcal{K}$: a contradiction. □

In particular, the hypothesis of Theorem 1.1 is never satisfied by a non-constant P when $\mathcal{K}$ is the set of all positive integers ($\pi(x) = x$) or an arithmetic progression ($\pi(x) = \alpha x + \beta$ with $\alpha \geq 1$). For instance, for $\mathcal{K} = \mathbb{Z}_{>0}$ and $P(x) = cx^n$ with $n \geq 1$, every prime p divides $P(p)$. As already said, Theorem 5.1 also follows from Corollary 4.1, because π is eventually strictly increasing and hence the increasing enumeration of $\mathcal{K}$ is $O(i^{\deg \pi})$.

5.2 Geometric progressions

We now turn to $k_i = A\alpha^i + B$ with $\alpha \geq 2$. Such a sequence grows exponentially, so it escapes Theorem 4.1, and non-constant solutions do exist. The following lemma is the exponential counterpart of Lemma 5.1; it uses only Euler's theorem.

Lemma 5.2 (Periodicity lemma)**.** *Let $A \in \mathbb{Z} \setminus \{0\}$, $B \in \mathbb{Z}$, and let $\alpha \geq 2$ be an integer; put $k_i = A\alpha^i + B$ for $i \geq 1$. Let $g \in \mathbb{Z}[x]$ be non-constant with $g(B) \neq 0$. Then the set of primes dividing some nonzero term of the sequence $\big(g(k_i)\big)_{i\geq 1}$ is infinite.*

Proof. The integers k_i are pairwise distinct and $|k_i| \to \infty$; hence $g(k_i) \neq 0$ for all sufficiently large i, and $|g(k_i)| \to \infty$ as $i \to \infty$. Fix an index $r \geq 1$ with $g(k_r) \neq 0$.

Suppose, for contradiction, that all primes dividing nonzero terms $g(k_i)$ lie in a finite set S. For a prime p and a nonzero integer z, let $v_p(z)$ denote the exponent of p in z. Choose an integer $E \geq 1$ such that

$$E > v_p\big(g(k_r)\big) \qquad \text{for every } p \in S \text{ with } p \nmid \alpha,$$
$$E > v_p\big(g(B)\big) \qquad \text{for every } p \in S \text{ with } p \mid \alpha,$$

let L be the least common multiple of the integers $\varphi(p^E)$, $p \in S$, $p \nmid \alpha$ (with $L = 1$ if there is no such prime), where φ is Euler's function, and consider the infinite set of indices

$$I = \{i \geq \max(E, r) : \ i \equiv r \pmod{L}\}.$$

Let $i \in I$ and $p \in S$.

If $p \nmid \alpha$, then $\alpha^L \equiv 1 \pmod{p^E}$ by Euler's theorem, so $\alpha^i \equiv \alpha^r$, $k_i \equiv k_r$ and $g(k_i) \equiv g(k_r) \pmod{p^E}$. Since $v_p(g(k_r)) < E$, this gives $g(k_i) \neq 0$ and $v_p(g(k_i)) = v_p(g(k_r))$.

If $p \mid \alpha$, then $p^E \mid \alpha^i$ because $i \geq E$, so $k_i \equiv B$ and $g(k_i) \equiv g(B) \pmod{p^E}$. Since $v_p(g(B)) < E$, this gives $g(k_i) \neq 0$ and $v_p(g(k_i)) = v_p(g(B))$.

Consequently, for every $i \in I$ with $g(k_i) \neq 0$ (that is, for all but finitely many $i \in I$), all prime divisors of $g(k_i)$ lie in S and

$$|g(k_i)| = \prod_{p\in S} p^{v_p(g(k_i))} = \prod_{p\in S,\ p\nmid\alpha} p^{v_p(g(k_r))} \prod_{p\in S,\ p\mid\alpha} p^{v_p(g(B))}$$

is a number independent of i. This contradicts $|g(k_i)| \to \infty$. □

The hypothesis $g(B) \neq 0$ cannot be omitted, since $g(x) = x - B$ gives $g(k_i) = A\alpha^i$. Taking $B = 0$ and $g(x) = x + c$ in Lemma 5.2 we recover a classical theorem of Pólya [13, Part VIII, Problem 107]; see also the survey of Meštrović [9].

Corollary 5.1 (Pólya)**.** *Let $a, c \in \mathbb{Z} \setminus \{0\}$ and let $b \geq 2$ be an integer. Then the set of primes dividing some nonzero term of the sequence $\big(ab^n + c\big)_{n\geq 1}$ is infinite.*

Note that the freedom in the choice of the index r in the proof of Lemma 5.2 takes care of the case $a + c = 0$, i.e. of the sequence $a(b^n - 1)$: one may take $r = 1$, since $a(b - 1) \neq 0$.

Theorem 5.2 (Geometric progressions)**.** *Let $A \geq 1$, $\alpha \geq 2$ and B be integers such that $k_i = A\alpha^i + B$ is positive for every $i \geq 1$, and let $\mathcal{K} = \{k_i : i \geq 1\}$. For a nonzero polynomial $P \in \mathbb{Z}[x]$, the following are equivalent:*

(i) *the set of prime divisors of the nonzero integers among $\{P(k) : k \in \mathcal{K}\}$ is finite;*

(ii) *$P(x) = c\,(x - B)^n$ for some $c \in \mathbb{Z} \setminus \{0\}$ and some integer $n \geq 0$.*

In particular, in the conclusion of Theorem 1.1 one has $a = 1$ and $b = -B$ for every non-constant solution.

Proof. (ii)⇒(i): $P(k_i) = c\,(A\alpha^i)^n = cA^n\alpha^{ni}$, whose prime divisors are among those of $cA\alpha$.

(i)⇒(ii): Let $n \geq 0$ be the multiplicity of B as a root of P, so that $P(x) = (x-B)^n R(x)$ with $R \in \mathbb{Z}[x]$ and $R(B) \neq 0$. Since $k_i - B = A\alpha^i \neq 0$, we have $P(k_i) \neq 0$ if and only if $R(k_i) \neq 0$, and $R(k_i)$ divides $P(k_i)$. If R were non-constant, Lemma 5.2 (applied to $g = R$) would give infinitely many primes dividing nonzero terms $R(k_i)$, hence dividing nonzero values $P(k_i)$, contradicting (i). Therefore R is a nonzero constant c, and $P(x) = c(x - B)^n$. □

The proof of Theorem 5.2 is entirely elementary: it uses neither Theorem 1.1 nor the S-unit theorem (Theorem 2.1). As for the comparison with Theorem 1.1: the conclusion for geometric progressions is sharper, because the linear factor is pinned to the exact shift $x - B$ compensating the additive constant B in k_i.

Example 5.1. *Take $A = 1$, $\alpha = 2$, $B = 0$, so $k_i = 2^i$. For $P(x) = x$, the values $P(k_i) = 2^i$ have the single prime divisor 2, in accordance with Theorem 5.2. By contrast, $P(x) = x - 1$ gives the Mersenne numbers $P(k_i) = 2^i - 1$, whose set of prime divisors is infinite by Corollary 5.1. (The theorem of Zsigmondy [17] gives the sharper statement that $2^i - 1$ has a* primitive *prime divisor for every $i > 1$ other than $i = 6$.)*

5.3 Subsequences of geometric progressions

The classification of Theorem 5.2 persists if only infinitely many terms of the geometric progression are retained. Here, however, our proof uses Theorem 1.1 and Theorem 2.1.

Proposition 5.1 (Subsequences)**.** *Let $A \geq 1$, $\alpha \geq 2$, B and $k_i = A\alpha^i + B > 0$ be as in Theorem 5.2, let $I \subset \mathbb{Z}_{>0}$ be an infinite set of indices, and let $P \in \mathbb{Z}[x]$ be nonzero. If the set of prime divisors of the nonzero integers among $\{P(k_i) : i \in I\}$ is finite, then $P(x) = c\,(x - B)^n$ for some $c \in \mathbb{Z} \setminus \{0\}$ and $n \geq 0$.*

Proof. If P is constant there is nothing to prove. Otherwise, Theorem 1.1 applied to the infinite set $\{k_i : i \in I\}$ gives $P(x) = c(ax + b)^n$ with $c \neq 0$, $n \geq 1$, $a > 0$ and $\gcd(a, b) = 1$. Let S be a finite set of

primes containing the prime divisors of α and of all nonzero values $P(k_i)$, $i \in I$, and put $C := aB + b$. For $i \in I$, the integer

$$u_i := ak_i + b = aA\alpha^i + C$$

vanishes for at most one i; for all other $i \in I$ it is a nonzero divisor of $P(k_i)$ and hence an S-unit, as is α^i. Suppose $C \neq 0$. Then

$$\frac{1}{C}\, u_i - \frac{aA}{C}\, \alpha^i = 1,$$

so the equation $a'u + b'v = 1$ with $a' = 1/C$, $b' = -aA/C \in \mathbb{Q}^\times$ has the infinitely many pairwise distinct solutions $(u, v) = (u_i, \alpha^i)$ in S-units, contradicting Theorem 2.1 (with $F = \mathbb{Q}$). Hence $C = 0$, i.e. $b = -aB$. Then $a \mid b$, and $\gcd(a, b) = 1$ with $a > 0$ forces $a = 1$ and $b = -B$. □

Remark 5.1. *The argument of Lemma 5.2 does not apply directly to subsequences. Given S and E, an infinite set I of indices does meet some residue class r modulo L infinitely often; but L depends on E, so r can only be chosen after E, and nothing guarantees that $v_p(g(k_r)) < E$ for the primes $p \in S$ not dividing α. We do not know whether Proposition 5.1 can be proved without Theorem 2.1.*

6 Sharpness: three necessary hypotheses

Remark 6.1 (The scalar factor c is necessary)**.** *If a, b are required to be* integers*, the theorem is false without the scalar factor c: one cannot in general write $P(x) = (ax + b)^n$ with $a, b \in \mathbb{Z}$. For example, $P(x) = 2x^2$ satisfies the hypothesis of Theorem 1.1 with $\mathcal{K} = \{2^m : m \geq 1\}$, since $P(2^m) = 2^{2m+1}$ has only the prime divisor 2, but $2x^2$ is not a power of a linear polynomial with integer coefficients. (Over $\mathbb{R}$, of course, $2x^2 = (\sqrt{2}\, x)^2$; the scalar is forced because the coefficient domain is $\mathbb{Z}$, as it is throughout this note and as it was in the original 2003 problem.)*

Remark 6.2 (The hypothesis $P \not\equiv 0$ is necessary)**.** *If $P \equiv 0$, there are no nonzero integers among the values $P(k)$, $k \in \mathcal{K}$, so the hypothesis of Theorem 1.1 holds vacuously; yet the zero polynomial is neither of degree 0 nor of the form $c(ax + b)^n$ with $c \neq 0$.*

Remark 6.3 (Infinitude of $\mathcal{K}$ is necessary)**.** *For any* finite *set of positive integers $\mathcal{K}$ and any nonzero polynomial P, the values $P(k)$, $k \in \mathcal{K}$, trivially have only finitely many prime divisors, with no constraint on the shape of P. Infinitude of $\mathcal{K}$ is thus essential; and, as noted in the paragraph following Theorem 1.1, it is all that is used: no growth or density condition on $\mathcal{K}$ enters the proof of Theorem 1.1.*

7 Concluding remarks

7.1 Where elementary methods stand

The results above can be summarized as follows; the list describes which *proof technique* applies in each regime.

- **Polynomial growth.** By Theorem 4.1, no non-constant P can satisfy the hypothesis; an elementary counting argument settles this regime completely. (When $\mathcal{K} = \{\pi(i) : i \geq i_0\}$ for a fixed polynomial π, Theorem 5.1 gives a second, congruence-theoretic proof via Schur's theorem.)
- **Geometric progressions, $k_i = A\alpha^i + B$.** Non-constant solutions exist, and Theorem 5.2 determines them completely, as an if-and-only-if, by an elementary periodicity argument (Lemma 5.2).
- **Arbitrary infinite sets.** Here Theorem 1.1 is the answer, and its proof uses the S-unit theorem. This is already the case for infinite subsequences of a geometric progression (Proposition 5.1, Remark 5.1).

7.2 Growth rate is not the right invariant

Combining Theorem 4.1 with the example $k_i = \alpha^i$, $P(x) = x$, one might guess that there is a growth-rate threshold, somewhere between polynomial and exponential, separating "only constants work" from "non-constant examples exist". This guess is wrong.

Example 7.1 (Growth rate alone does not determine the phenomenon)**.** *Fix a finite set of primes S with $|S| = s \geq 2$, e.g. $S = \{2, 3\}$, and let $\mathcal{K} = \mathcal{U}_S(x)$ (Remark 1.3) be the set of all positive S-unit integers, i.e. $\mathcal{K} = \{2^e 3^f : e, f \geq 0\}$ for $S = \{2, 3\}$. Trivially, $P(x) = x$ satisfies the hypothesis of Theorem 1.1 along $\mathcal{K}$. Yet the increasing enumeration (k_j) of $\mathcal{K}$ is very far from exponential: by Lemma 4.1, $j = N_S(k_j) \sim (\log k_j)^s/(s! \prod_{p\in S} \log p)$, so*

$$\log k_j \;\sim\; \Big(s!\, j \prod_{p\in S} \log p\Big)^{1/s},$$

e.g. $\log k_j \sim \sqrt{2j \log 2 \log 3}$ for $S = \{2, 3\}$. This is strictly between polynomial growth of k_j (excluded by Theorem 4.1) and the growth $\log k_j \asymp j$ of a geometric progression, and $\log k_j$ grows like $j^{1/s}$ with s as large as one likes if S is enlarged.

So growth alone is only a *sufficient* obstruction (Theorem 4.1: polynomial growth always fails), never a classification: for every $\varepsilon > 0$ there is an infinite $\mathcal{K}$ with $\log k_j = O(j^\varepsilon)$ along which a non-constant P works. What makes Example 7.1 succeed is not its growth rate but its *arithmetic structure*: $\mathcal{K}$ was built entirely out of S-units.

> *Problem. Beyond cardinality and growth rate, what structural conditions on an infinite set $\mathcal{K} \subset \mathbb{Z}_{>0}$ permit a non-constant $P \in \mathbb{Z}[x]$ with $\{P(k) : k \in \mathcal{K}\}$ of finite prime support?*

By Theorem 1.1 and Remark 1.3, this is the question of describing the infinite subsets of the sets $\{n \in \mathbb{Z}_{>0} : an + b \text{ is an } S\text{-unit}\}$. We record it only as a natural direction for further work.

7.3 Further directions

A number-field version. The ingredients of Section 3 – Theorem 2.1, Lemma 2.1, and Proposition 3.1 – are valuation-theoretic and are stated over a general number field. This suggests a natural extension: for a number field F, a finite set of places S_F containing the archimedean ones, and $P \in F[x]$, one can ask what P can look like if $P(x)$ is an S_F-unit for infinitely many $x \in \mathcal{O}_{F,S_F}$. The mechanism of Proposition 3.1 suggests the analogous conclusion $P(x) = c(x-\gamma)^n$ for a single $\gamma \in F$. We have not written this out, because some points that are automatic over $\mathbb{Q}$ – notably the notion of a primitive polynomial, which requires care with the class group of F – would need to be handled properly.

Linear recurrence sequences. For $g \in \mathbb{Z}[x]$ of degree δ, the sequence $g(A\alpha^i + B) = \sum_{j=0}^{\delta} c_j \alpha^{ji}$, with constants $c_j \in \mathbb{Z}$ independent of i, is a linear recurrence sequence with characteristic roots among $1, \alpha, \ldots, \alpha^{\delta}$, and Lemma 5.2 is a statement about its prime divisors. One may ask more generally: for a linear recurrence sequence (k_i), say $k_{i+2} = uk_{i+1} + vk_i$, for which (u, v) and which initial conditions can a non-constant P have $\{P(k_i)\}$ of finite prime support? The proof of Lemma 5.2 used that $A\alpha^i + B$ is, along suitable arithmetic progressions of indices, constant modulo arbitrarily high prime powers; this is special to geometric progressions. For general recurrences the question connects with the literature on S-unit equations, recurrence sequences and primitive divisors [2], and we do not pursue it here.

Acknowledgment

The author is grateful to the anonymous referee for a very careful reading of the manuscript. In particular, the periodicity argument behind Lemma 5.2 is due to the referee; it removes the dependence of Theorem 5.2 on S-unit equations that was asserted in an earlier version of this note. The referee also corrected the historical account in Section 2.

References

[1] Aassila, M. (2003). Problem 2838. *Crux Mathematicorum*, *29*, 238; solution/comment in *30* (2004), 192.

[2] Bilu, Y., Hanrot, G., & Voutier, P. M. (2001). Existence of primitive divisors of Lucas and Lehmer numbers (with an appendix by M. Mignotte). *Journal für die reine und angewandte Mathematik*, *539*, 75–122. https://doi.org/10.1515/crll.2001.080

[3] Bombieri, E., & Gubler, W. (2006). *Heights in Diophantine geometry* (New Mathematical Monographs, Vol. 4). Cambridge University Press. https://doi.org/10.1017/CBO9780511542879

[4] Evertse, J.-H. (1984). On equations in S-units and the Thue–Mahler equation. *Inventiones Mathematicae*, *75*, 561–584. https://doi.org/10.1007/BF01388644

[5] Evertse, J.-H., & Győry, K. (2015). *Unit equations in Diophantine number theory* (Cambridge Studies in Advanced Mathematics, Vol. 146). Cambridge University Press.

[6] Győry, K. (1979). On the number of solutions of linear equations in units of an algebraic number field. *Commentarii Mathematici Helvetici*, *54*, 583–600.

[7] Lang, S. (1960). Integral points on curves. *Publications Mathématiques de l'IHÉS*, *6*, 27–43.

[8] Mahler, K. (1933). Zur Approximation algebraischer Zahlen. I. (Über den größten Primteiler binärer Formen). *Mathematische Annalen*, *107*, 691–730.

[9] Meštrović, R. (2023). *Euclid's theorem on the infinitude of primes: a historical survey of its proofs (300 B.C.–2022) and another new proof.* arXiv preprint. https://arxiv.org/abs/1202.3670

[10] Murty, M. R., & Thain, N. (2006). Prime numbers in certain arithmetic progressions. *Functiones et Approximatio Commentarii Mathematici*, *35*, 249–259. https://doi.org/10.7169/facm/1229442627

[11] Parry, C. J. (1950). The $\mathfrak{p}$-adic generalisation of the Thue–Siegel theorem. *Acta Mathematica*, *83*, 1–100.

[12] Pollack, P. (2009). *Not always buried deep: A second course in elementary number theory.* American Mathematical Society.

[13] Pólya, G., & Szegő, G. (1925). *Aufgaben und Lehrsätze aus der Analysis* (Vol. II). Springer.

[14] Schur, I. (1912). Über die Existenz unendlich vieler Primzahlen in einigen speziellen arithmetischen Progressionen. *Sitzungsberichte der Berliner Mathematischen Gesellschaft*, *11*, 40–50.

[15] Siegel, C. L. (1921). Approximation algebraischer Zahlen. *Mathematische Zeitschrift*, *10*, 173–213.

[16] Siegel, C. L. (1929). Über einige Anwendungen diophantischer Approximationen. *Abhandlungen der Preussischen Akademie der Wissenschaften, Physikalisch-Mathematische Klasse*, Nr. 1.

[17] Zsigmondy, K. (1892). Zur Theorie der Potenzreste. *Monatshefte für Mathematik und Physik*, *3*, 265–284. https://doi.org/10.1007/BF01692444

This is an open access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted, use, distribution and reproduction in any medium, or format for any purpose, even commercially provided the work is properly cited.