Math. Res. Lett.
Volume 27, Number 1, 43–66, 2020

The smallest root of a polynomial congruence

Vlad Crişan and Paul Pollack

Fix $f(t) \in \mathbb{Z}[t]$ having degree at least 2 and no multiple roots. We prove that as k ranges over those integers for which the congruence $f(t) \equiv 0 \pmod{k}$ is solvable, the least nonnegative solution is almost always smaller than $k/(\log k)^{c_f}$. Here c_f is a positive constant depending on f. The proof uses a method of Hooley originally devised to show that the roots of f are equidistributed modulo k as k varies.

1. Introduction

Let $f(t)$ be a nonconstant polynomial with integer coefficients. For each pair of integers h, k with $k > 0$, put

$$S(h,k) = \sum_{\substack{\nu \bmod k \\ f(\nu)\equiv 0 \pmod{k}}} e(h\nu/k),$$

where as usual $e(x) = e^{2\pi i x}$. The exponential sums $S(h,k)$ were introduced by Hooley [11, 12] to study the distribution of roots of polynomial congruences.

For each k, let $\varrho(k)$ denote the number of roots of f modulo k, so that

$$|S(h,k)| \leq \varrho(k)$$

trivially. In [12], Hooley supposes f is irreducible (over $\mathbb{Q}$) of degree at least 2 and explains how to bound $\sum_{k\leq x} S(h,k)$ nontrivially, for each (fixed) h; "nontrivially" means that the upper bounds are of lower order than $\sum_{k\leq x} \varrho(k)$. Invoking Weyl's criterion, Hooley deduces that the roots of f modulo k are equidistributed, as k varies, in the following sense. For each positive integer k, let the roots of f modulo k belonging to the interval $[0,k)$ be $\nu_1, \nu_2, \ldots, \nu_{\varrho(k)}$.

(The ν_i may be taken in arbitrary order.) Then concatenating the lists

$$\frac{\nu_1}{k}, \frac{\nu_2}{k}, \ldots, \frac{\nu_{\varrho(k)}}{k}, \tag{1.1}$$

for $k = 1, 2, 3, \ldots$, yields a sequence that is uniformly distributed in $[0, 1)$. The assumption that $\deg f \geq 2$ is easily seen to be necessary; if $f(t) = at + b$ is linear, the corresponding sequence has all of its limit points rational numbers with denominator dividing $|a|$.

While Hooley assumes f is irreducible in [12], this is a technical convenience, and the method applies more generally to any f of degree at least 2 with distinct roots. We state this as our first theorem.

Theorem 1.1. *Suppose that $f(t) \in \mathbb{Z}[t]$ has degree at least 2 and no multiple roots. Then the roots of f modulo k are equidistributed, as k varies (in the above sense).*

We give the proof of Theorem 1.1 in §2. It should be noted that quadratic $f(t)$ with distinct rational roots were treated by Martin and Sitar already in [15].

While Theorem 1.1 seems useful to record, its proof does not involve any essential new ideas over and above [12]. The primary purpose of this article is to point out that the proof of Theorem 1.1 can be modified to give a seemingly new result concerning the smallest root of a polynomial congruence. Let $\mathscr{R}_f$ denote the set of positive integers k for which the congruence $f(t) \equiv 0 \pmod{k}$ is solvable.

Theorem 1.2. *Suppose that $f(t) \in \mathbb{Z}[t]$ has degree at least 2 and no multiple roots. There is a constant $c_f > 0$ such that, for almost all $k \in \mathscr{R}_f$, the least integer r with $f(r) \equiv 0 \pmod{k}$ satisfies $r < k/(\log k)^{c_f}$.*

In Theorem 1.2, "almost all" means that the complementary set has vanishing relative density; that is, the number of exceptional $k \leq x$ is $o(\#\mathscr{R}_f \cap [1, x])$, as $x \to \infty$. Theorem 1.2 is proved in §3.

While there is an obvious affinity between the assertion that the roots of f are equidistributed mod k, as k varies (Theorem 1.1), and the claim that when there is a root there is almost always a small root (Theorem 1.2), the latter statement does not follow from the former. Equidistribution has something to say about the number of small roots modulo k for $k \leq x$, relative to the size of the sum $\sum_{k \leq x} \varrho(k)$. However (as we will see later), that sum is dominated by atypical elements of $\mathscr{R}_f$, rendering it impossible to draw a conclusion about the roots of f modulo k for a typical $k \in \mathscr{R}_f$.

It is natural to wonder how sharp Theorem 1.2 is. If f has a nonnegative integer root, then its least such root is also the smallest root of f modulo k for all but finitely many k. Thus, the upper bound of Theorem 1.2 is rather poor here. In the remaining cases, Theorem 1.2 fares much better.

Proposition 1.3. *Suppose that $f(t)$ is a nonconstant polynomial in $\mathbb{Z}[t]$ with no nonnegative integer root. There is a constant $C_f > 0$ such that, for almost all $k \in \mathscr{R}_f$, the least integer r with $f(r) \equiv 0 \pmod{k}$ satisfies $r > k/(\log k)^{C_f}$.*

In particular, the bound of Theorem 1.2 is sharp up to the power of $\log k$ in the denominator. Proposition 1.3 is in fact a simple consequence of a theorem of van der Corput on the average order of $d(f(m))$ [22]; we explain this in §4.

In the fifth and final section of the paper, we provide a description of the set of quotients $|f(r_k)|/k$, where r_k denotes the least nonnegative root of f modulo k.

We will see below (Lemma 3.3) that for a typical $k \in \mathscr{R}_f \cap [1, x]$, we have $\varrho(k) \approx (\log x)^{\kappa}$ for a certain positive constant $\kappa = \kappa_f$. This suggests the conjecture that κ is the "correct" value of c_f in Theorem 1.2, in the sense that the smallest root of f modulo k is of size $k/(\log k)^{\kappa+o(1)}$ as $k \to \infty$ through a density 1 subset of $\mathscr{R}_f$.

The proof of Theorem 1.2 goes by applying the method of [12] to bound $\sum_k S(h,k)$ where, in contrast to [12], k runs (only) over a set of integers in $[1, x]$ on which $\varrho(k)$ exhibits its typical behavior. It is a testimony to the flexibility of Hooley's approach that this restriction on k does not lead to significant complications of the analysis. As further evidence for the reach of Hooley's method, we mention that this approach was recently used in [18] to show that the square roots of -1 mod k are equidistributed as k ranges over the shifted primes $p - 1$.

We would like to conclude this introduction by drawing attention to other work concerning small solutions of polynomial congruences. Here "small" is considerably smaller than in our results. In [17], Murty shows that if k is prime and $q \mid k-1$, and if $x^q \equiv a \pmod{k}$ is solvable, then there is a solution x_0 with $|x_0| \ll k^{3/2} q^{-1}$. In particular, if $q > k^{1/2+\epsilon}$, then we may take $|x_0| \ll k^{1-\epsilon}$. Various refinements are then discussed. For instance, using a character sum estimate of Bourgain–Glibichuk–Konyagin [3], Murty shows that if $q > k^{\delta}$, then one may take $|x_0| \ll k^{1-\epsilon}$ for some $\epsilon = \epsilon(\delta) > 0$. Gun obtains closely related results valid also for composite k in [9]. Konyagin and Steger consider the number of small solutions to polynomial congruences in [14]. In particular, they show that if $f(t) \in \mathbb{Z}[t]$ is monic of degree n, then there are only $O_{n,\epsilon}(1)$ roots of f modulo k belonging to the interval $[0, k^{1/n-\epsilon})$. Coppersmith has discussed extensively the computational problem of finding these very small roots of f [4–6].

2. Equidistribution of roots of polynomial congruences: Proof of Theorem 1.1

Throughout this section, we assume that $f(t)$ is a fixed polynomial in $\mathbb{Z}[t]$ of degree $n \geq 2$ without multiple roots. Implied constants may always depend on f; further dependence will be noted explicitly.

2.1. Setup

We begin with four lemmas taken from [12]; the proofs given there carry over verbatim (irreducibility of f is never used).

Lemma 2.1. *For every integer h,*

$$\sum_{a \bmod k} |S(ah, k)|^2 = O(\varrho(k)k \cdot \gcd(h, k)).$$

Lemma 2.2. *If* $\gcd(k, k') = 1$*, then*

$$S(h, k)S(h', k') = S(hk' + h'k, kk').$$

Lemma 2.2 has the following immediate consequence.

Lemma 2.3. *If* $\gcd(k, k') = 1$*, then*

$$S(h, kk') = S(h\overline{k'}, k)S(h\overline{k}, k'),$$

where $\overline{k}$ is an inverse of k modulo k' and $\overline{k'}$ is an inverse of k' modulo k.

Write D for the discriminant of f. Note that $D \neq 0$, since the roots of f are assumed distinct.

Lemma 2.4. *We have*

(i) *$\varrho(k)$ is a multiplicative function of k;*

(ii) *if $p \nmid D$, then $\varrho(p) = \varrho(p^\alpha) \leq n$ for every positive integer α;*

(iii) *$\varrho(p^\alpha) = O(1)$;*

(iv) $\varrho(k) = O(n^{\omega(k)})$.

We will also use the following well-known upper bound for the mean values of nonnegative multiplicative functions. It is a simple consequence of Theorem 01 on p. 2 of [10].

Lemma 2.5. *Let F be a multiplicative function taking values in $\mathbb{R}_{\geq 0}$ whose values at prime powers are uniformly bounded. For all $x \geq 3$,*

$$\sum_{k \leq x} F(k) \ll \frac{x}{\log x} \prod_{p \leq x} \left(1 + \frac{F(p)}{p} + \frac{F(p^2)}{p^2} + \cdots\right).$$

The implied constant depends at most on the bound for the values of F at prime powers.

We are now ready to state what will be our workhorse estimate in the proofs of both Theorems 1.1 and 1.2. Recall that a number is said to be *z-smooth* if all of its prime factors are bounded by z and *z-rough* if all of its prime factors exceed z; the z-smooth, resp. z-rough, part of a number is its largest z-smooth, resp. z-rough, divisor.

Let $x \geq 10$, and let $\mathscr{K}$ be a subset of $[1, x]$. For h a nonzero integer, set

$$R(h, \mathscr{K}) = \sum_{k \in \mathscr{K}} |S(h, k)|.$$

Put

$$X = x^{1/\log\log x}.$$

Let

$$\mathscr{K}_{\text{smooth}} = \{k_1 : k_1 \text{ is the } X\text{-smooth part of some } k \in \mathscr{K}\}.$$

Proposition 2.6. *We have*

$$R(h, \mathscr{K}) \ll \frac{x}{\log x} (\log\log x)^{O(1)} \left(1 + \sum_{k_1 \in \mathscr{K}_{smooth}} \frac{\varrho(k_1)^{1/2} \gcd(h, k_1)^{1/2}}{k_1}\right).$$

Proof. For the start of this proof, we will use k_1 and k_2 to denote the X-smooth and X-rough parts of k, respectively. Then

$$R(h,\mathscr{K}) = \sum_{k\in\mathscr{K}} |S(h,k)| = \sum\nolimits_1 + \sum\nolimits_2,$$

where $\sum_1$ denotes the sum restricted to $k \in \mathscr{K}$ satisfying $k_1 \le x^{1/3}$ and $\sum_2$ denotes the sum over the remaining $k \in \mathscr{K}$. By Lemma 2.4 and Cauchy–Schwarz,

$$\begin{aligned}\sum\nolimits_2 \le \sum_{\substack{k\le x\\ k_1>x^{1/3}}} \varrho(k) &\ll \sum_{\substack{k\le x\\ k_1>x^{1/3}}} n^{\omega(k)}\\ &\le \Bigg(\sum_{\substack{k\le x\\ k_1>x^{1/3}}} 1\Bigg)^{1/2} \Bigg(\sum_{k\le x} n^{2\omega(k)}\Bigg)^{1/2}. \qquad (2.1)\end{aligned}$$

An application of Lemma 2.5 shows that the second sum on k in (2.1) is $\ll x(\log x)^{O(1)}$. On the other hand, a theorem of Tenenbaum concerning the count of numbers with large smooth components implies that the first sum on k is bounded, as $x \to \infty$, by

$$x\exp(-(1/3+o(1))\log\log x\cdot\log\log\log x),$$

which is $O(x/(\log x)^A)$ for any constant A. (See the estimate for $\Theta(x,y,z)$ at the bottom of p. 9 in [10].) It follows that

$$\sum\nolimits_2 = O(x/(\log x)^A) \qquad (2.2)$$

for every fixed A.

To deal with $\sum_1$, write $S(h,k) = S(h,k_1k_2) = S(h\overline{k_2},k_1)S(h\overline{k_1},k_2)$. Then

$$\begin{aligned}\sum\nolimits_1 = \sum_{k\in\mathscr{K}} |S(h\overline{k_2},k_1)S(h\overline{k_1},k_2)| &\le \sum_{\substack{k_1\le x^{1/3}\\ k_1\in\mathscr{K}_{\mathrm{smooth}}}} \sum_{\substack{k_2\le x/k_1\\ k_1k_2\in\mathscr{K}}} \varrho(k_2)|S(h\overline{k_2},k_1)|\\ &\le \sum_{\substack{k_1\le x^{1/3}\\ k_1\in\mathscr{K}_{\mathrm{smooth}}}} \Theta(x/k_1,k_1), \qquad (2.3)\end{aligned}$$

where for $y \in [x^{2/3}, x]$ and $k_1 \le x^{1/3}$ we set

$$\Theta(y, k_1) = \sum_{\substack{k_2 \le y \\ k_1 k_2 \in \mathscr{K}}} \varrho(k_2) |S(h\overline{k_2}, k_1)|.$$

(From here on in the argument, k_1 and k_2 denote generic X-smooth and X-rough numbers, respectively.) Discarding the condition that $k_1 k_2 \in \mathscr{K}$ and applying Cauchy–Schwarz, we see that

$$\Theta(y, k_1)^2 \le \left(\sum_{k_2 \le y} \varrho(k_2)^2 \right) \left(\sum_{k_2 \le y} |S(h\overline{k_2}, k_1)|^2 \right).$$

Applying Lemma 2.5 with $F(k) = \mathbb{1}_{\gcd(k, \prod_{p \le X} p) = 1} \cdot n^{2\omega(k)}$, we find that

$$\begin{aligned} \sum_{k_2 \le y} \varrho(k_2)^2 \ll \sum_{k_2 \le y} n^{2\omega(k_2)} &\ll \frac{y}{\log y} \prod_{X < p \le y} \left(1 + \frac{n^2}{p} + \frac{n^2}{p^2} + \cdots \right) \\ &\ll \frac{y}{\log x} (\log\log x)^{O(1)}. \end{aligned}$$

On the other hand,

$$\sum_{k_2 \le y} |S(h\overline{k_2}, k_1)|^2 = \sum_{\substack{0 \le a < k_1 \\ \gcd(a, k_1) = 1}} |S(ah, k_1)|^2 \sum_{\substack{k_2 \le y \\ k_2 \equiv \overline{a} \pmod{k_1}}} 1.$$

By Brun's sieve, the inner sum on k_2 is $O(\frac{y}{\varphi(k_1) \log X})$ (see Lemma 8 of [12]), so that

$$\begin{aligned} \sum_{k_2 \le y} |S(h\overline{k_2}, k_1)|^2 &\ll \frac{y}{\varphi(k_1) \log X} \sum_{a \bmod k_1} |S(ah, k_1)|^2 \\ &\ll \frac{y (\log\log x)^2}{k_1 \log x} \cdot \varrho(k_1) k_1 \cdot \gcd(h, k_1) \\ &= \frac{y (\log\log x)^2}{\log x} \varrho(k_1) \cdot \gcd(h, k_1). \end{aligned}$$

(To go from the first line to the second, we use the definition of X together with Lemma 2.1 and the bound $\varphi(k_1) \gg k_1 / \log\log(3k_1) \gg k_1 / \log\log x$.)

Combining the above estimates, we arrive at the upper bound

$$\Theta(y, k_1) \ll \frac{y}{\log x}(\log\log x)^{O(1)} \cdot \varrho(k_1)^{1/2}\gcd(h, k_1)^{1/2}.$$

Inserting this back into (2.3) shows that

$$\sum\nolimits_1 \ll \frac{x}{\log x}(\log\log x)^{O(1)} \sum_{\substack{k_1 \le x^{1/3} \\ k_1 \in \mathscr{K}_{\mathrm{smooth}}}} \frac{\varrho(k_1)^{1/2}\gcd(h, k_1)^{1/2}}{k_1}.$$

Putting this together with our earlier estimate (2.2) for $\sum_2$, with $A = 1$, completes the proof of the proposition. □

2.2. More on $\varrho(p)$

To proceed, we require somewhat precise information on the distribution of the values $\varrho(p)$, as p varies. Say that a set $\mathscr{P}$ of rational primes *has density* δ if for all $x \ge 3$,

$$\sum_{\substack{p \le x \\ p \in \mathscr{P}}} 1 = \delta\frac{x}{\log x} + O_{\mathscr{P}}\left(\frac{x}{(\log x)^2}\right).$$

Note that if $\mathscr{P}$ has density δ, one can deduce by partial summation that for all $x \ge 3$,

$$\sum_{\substack{p \le x \\ p \in \mathscr{P}}} \log p = \delta x + O_{\mathscr{P}}(x/\log x),$$

and that, for some constant $\kappa_{\mathscr{P}}$,

$$\sum_{\substack{p \le x \\ p \in \mathscr{P}}} \frac{1}{p} = \delta\log\log x + \kappa_{\mathscr{P}} + O_{\mathscr{P}}\left(\frac{1}{\log x}\right).$$

Write g for the number of monic irreducible factors of $f(t)$ in $\mathbb{Q}[t]$.

Lemma 2.7. *For each $j = 0, 1, 2, 3, \ldots$, the set of primes p with $\varrho(p) = j$ has a density. If we denote this density by δ_j, then*

(i) *$\delta_j = 0$ if $j > n$,*

(ii) *$\sum_{j \ge 0} \delta_j = 1$,*

(iii) *$\sum_{j \ge 0} j\delta_j = g$.*

Proof. We begin by recalling the notion of a Frobenian set of primes (in the terminology of Serre [20]). Let K be a number field with $K/\mathbb{Q}$ Galois, and let $\mathscr{C}$ be a subset of $\mathrm{Gal}(K/\mathbb{Q})$ stable under conjugation. We let $\mathscr{P}(K;\mathscr{C})$ denote the set of rational primes p unramified in K whose corresponding Frobenius conjugacy class Frob_p is a subset of $\mathscr{C}$. By a *Frobenian set of primes*, we mean any set of primes arising as $\mathscr{P}(K;\mathscr{C})$ for some K and $\mathscr{C}$, or a set of primes whose symmetric difference with some $\mathscr{P}(K;\mathscr{C})$ is finite. The Chebotarev density theorem with a reasonable error term (e.g., the form of the theorem appearing as [2, Satz 4]) implies that every Frobenian set has a density; more specifically, if $\mathscr{P} = \mathscr{P}(K;\mathscr{C})$ up to finitely many exceptions, then $\mathscr{P}$ has density $\#\mathscr{C}/[K:\mathbb{Q}]$.

Let p be a prime not dividing the leading coefficient of f. Then the mod p reduction of f has degree n, and the degrees of the irreducible factors of f mod p form a partition of n called the *factorization pattern of f modulo p*. A well-known consequence of the Chebotarev density theorem (see [21] or [19]) is that the set of primes p for which f has a given factorization pattern is a Frobenian set. More precisely, let K denote the splitting field of f over $\mathbb{Q}$, and view $\mathrm{Gal}(K/\mathbb{Q})$ as a subgroup of the symmetric group on the roots of f. Each $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ has a decomposition into disjoint cycles whose lengths describe a partition of n. Then — up to finitely many exceptions — the factorization pattern of f mod p coincides with the cycle type of Frob_p. (By the cycle type of a conjugacy class, we mean the common cycle type of any of its elements.)

As long as $p \nmid D$ — which occurs for all but finitely many p — the polynomial f factors into distinct irreducibles modulo p, so that $\varrho(p)$ is determined by the factorization pattern of f modulo p (being the number of linear factors). The existence of the densities δ_j follows immediately from the preceding discussion. Explicitly, δ_j is the proportion of $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ possessing precisely j fixed points when viewed as a permutation on the roots of f.

Assertions (i) and (ii) are now clear. To see (iii), notice that the sum $\sum_{j\geq 0} j\delta_j$ computes the expected number of fixed points of an element of $\mathrm{Gal}(K/\mathbb{Q})$ chosen uniformly at random. Factor $f = f_1 \cdots f_g$, where $f_1, \dots, f_g$ are irreducible over $\mathbb{Q}$ having degrees $n_1, \dots, n_g$ (so that $n_1 + \cdots + n_g = n$). List the roots of f_i as $\theta_{i,1}, \dots, \theta_{i,n_i}$. Then

$$\begin{aligned}\sum_{j\geq 0} j\delta_j &= \frac{1}{[K:\mathbb{Q}]} \sum_{\sigma\in\mathrm{Gal}(K/\mathbb{Q})} (\#\text{ of } \theta_{i,j} \text{ fixed by } \sigma)\\ &= \frac{1}{[K:\mathbb{Q}]} \sum_{i=1}^{g}\sum_{j=1}^{n_i} \sum_{\substack{\sigma\in\mathrm{Gal}(K/\mathbb{Q})\\ \sigma(\theta_{i,j})=\theta_{i,j}}} 1.\end{aligned}$$

The innermost right-hand sum evaluates to $\#\mathrm{Gal}(K/\mathbb{Q}(\theta_{i,j})) = [K : \mathbb{Q}(\theta_{i,j})]$. Since

$$\frac{[K : \mathbb{Q}(\theta_{i,j})]}{[K : \mathbb{Q}]} = \frac{1}{[\mathbb{Q}(\theta_{i,j}) : \mathbb{Q}]} = \frac{1}{n_i},$$

we conclude that

$$\sum_{j\geq 0} j\delta_j = \sum_{i=1}^{g}\sum_{j=1}^{n_i}\frac{1}{n_i} = \sum_{i=1}^{g} 1 = g,$$

as desired. □

2.3. Completion of the proof of Theorem 1.1

Let $s_1, s_2, s_3, \ldots$ be the sequence obtained by concatenating the lists (1.1), for $k = 1, 2, 3, \ldots$. By Weyl's criterion, establishing that $\{s_m\}$ is uniformly distributed in $[0, 1)$ comes down to checking that for each (fixed) nonzero integer h, we have

$$\sum_{m\leq M} e(hs_m) = o(M), \qquad \text{as } M \to \infty.$$

It will be enough (for reasons explained at the end of this section) to check this for M of the form $\varrho(1) + \varrho(2) + \cdots + \varrho(m)$, i.e., to show that for each nonzero h,

$$\sum_{k\leq x} S(h, k) = o\left(\sum_{k\leq x}\varrho(k)\right), \qquad \text{as } x \to \infty.$$

We now take up the task of estimating $\sum_{k\leq x}\varrho(k)$ and $\sum_{k\leq x} S(h, k)$.

Lemma 2.8. *For some positive constant C depending on f, we have*

$$\sum_{k\leq x}\varrho(k) \sim Cx(\log x)^{g-1}, \qquad \textit{as } x \to \infty.$$

The following is a weakened form of a celebrated theorem of Wirsing [23, Satz 1]. It asserts that if the values of F at the primes have a well-defined positive average, then the upper bound of Lemma 2.5 can be sharpened to an asymptotic formula.

Proposition 2.9. *Let F be a multiplicative function taking values in $\mathbb{R}_{\geq 0}$ and whose values at prime powers are bounded. Suppose that for some $\tau > 0$, we have*

$$\sum_{p\leq x} F(p)\log p = (\tau + o(1))x, \qquad \text{as } x \to \infty. \tag{2.4}$$

Then, as $x \to \infty$,

$$\sum_{k\leq x} F(k) = \frac{x}{\log x}\frac{e^{-\gamma\tau}}{\Gamma(\tau)}\prod_{p\leq x}\left(1 + \frac{F(p)}{p} + \frac{F(p^2)}{p^2} + \cdots\right). \tag{2.5}$$

Here γ is the Euler–Mascheroni constant and $\Gamma(\cdot)$ is the usual Gamma-function.

Proof of Lemma 2.8. We apply Proposition 2.9 with $F = \varrho$. That ϱ is bounded on prime powers is Lemma 2.4(iii). We proceed to verify the hypothesis (2.4). Since $\varrho(p) \leq n$ for all but finitely many p (in fact, for all p not dividing the content of f),

$$\begin{aligned}\sum_{p\leq x}\varrho(p)\log p &= O(1) + \sum_{0\leq j\leq n} j \sum_{\substack{p\leq x\\ \varrho(p)=j}} \log p\\ &= O(1) + \sum_{0\leq j\leq n} j\left(\delta_j x + O(x/\log x)\right)\\ &= \left(\sum_{j\geq 0} j\delta_j + o(1)\right)x = (g + o(1))x.\end{aligned}$$

Thus, (2.4) holds with $\tau = g$. Examining the right-hand side of (2.5), we see that Lemma 2.8 will follow if it is shown that the product on p in (2.5) is asymptotic to a constant multiple of $(\log x)^g$. Since

$$\log\left(1 + \frac{\varrho(p)}{p} + \frac{\varrho(p^2)}{p^2} + \cdots\right) = \frac{\varrho(p)}{p} + O\left(\frac{1}{p^2}\right),$$

it suffices to show that

$$\sum_{p\leq x}\frac{\varrho(p)}{p} - g\log\log x \tag{2.6}$$

tends to a limit as $x \to \infty$. There are constants $\kappa_0, \dots, \kappa_n$ such that

$$\sum_{p \le x} \frac{\varrho(p)}{p} - \sum_{\substack{p \le x \\ \varrho(p) > n}} \frac{\varrho(p)}{p} = \sum_{0 \le j \le n} j \sum_{\substack{p \le x \\ \varrho(p) = j}} \frac{1}{p}$$
$$= \sum_{0 \le j \le n} j(\delta_j \log\log x + \kappa_j + O(1/\log x)).$$

It follows that (2.6) tends to $\sum_{0 \le j \le n} j\kappa_j + \sum_{p:\ \varrho(p) > n} \frac{\varrho(p)}{p}$, as $x \to \infty$. $\square$

Lemma 2.10. *For each fixed nonzero value of h,*

$$\sum_{k \le x} S(h,k) \ll x(\log x)^{g-1-(n-n^{1/2})/n!}(\log\log x)^{O(1)}.$$

Here the constant implied by "$\ll$" may depend both on f (as usual) and on h.

Remark. The term $n!$ appearing in the exponent of $\log x$ can sometimes be substantially reduced. For instance, if f is a normal polynomial (meaning that f is irreducible over $\mathbb{Q}$ and that f splits upon adjoining any one of its roots to $\mathbb{Q}$), then $n!$ can be replaced with n. This will be clear from our proof.

Proof. Applying Proposition 2.6 with $\mathscr{K}$ the full set of integers in $[1,x]$, and bounding $\gcd(h,k_1)$ trivially by h, we find that

$$\sum_{k \le x} S(h,k) \ll \sum_{k \le x} |S(h,k)| \ll \frac{x}{\log x}(\log\log x)^{O(1)} \sum_{\substack{k_1 \le x^{1/3} \\ k_1\ X\text{-smooth}}} \frac{\varrho(k_1)^{1/2}}{k_1}. \tag{2.7}$$

Now

$$\sum_{\substack{k_1 \le x^{1/3} \\ k_1\ X\text{-smooth}}} \frac{\varrho(k_1)^{1/2}}{k_1} \le \prod_{p \le X}\left(1 + \frac{\varrho(p)^{1/2}}{p} + \frac{\varrho(p^2)^{1/2}}{p^2} + \cdots\right)$$
$$\le \exp\left(\sum_{p \le X}\left(\frac{\varrho(p)^{1/2}}{p} + \frac{\varrho(p^2)^{1/2}}{p^2} + \cdots\right)\right)$$
$$\ll \exp\left(\sum_{p \le X} \frac{\varrho(p)^{1/2}}{p}\right).$$

The remaining sum on p satisfies

$$\begin{aligned}\sum_{p\le X}\frac{\varrho(p)^{1/2}}{p} &\le \sum_{0\le j\le n} j^{1/2}\sum_{\substack{p\le x\\ \varrho(p)=j}}\frac{1}{p}+O(1)\\ &\le \sum_{j=0}^{n} j^{1/2}(\delta_j\log\log x+O(1))+O(1)\\ &\le \left(\sum_{j\ge 0} j^{1/2}\delta_j\right)\log\log x+O(1).\end{aligned}$$

Hence, the sum on the right-hand side of (2.7) is $O\left((\log x)^{\sum_{j\ge 0} j^{1/2}\delta_j}\right)$. To conclude, it suffices to observe that

$$g-\sum_{j\ge 0} j^{1/2}\delta_j=\sum_{j\ge 0}(j-j^{1/2})\,\delta_j\ge (n-n^{1/2})\,\delta_n,$$

and that (from our description of the δ_j in the proof of Lemma 2.7, and with K denoting the splitting field of f over $\mathbb{Q}$) $\delta_n=\frac{1}{[K:\mathbb{Q}]}\ge\frac{1}{n!}$. □

Proof of Theorem 1.1. Fix $h\ne 0$. Comparing the estimates of Lemmas 2.8 and 2.10, keeping in mind that $n\ge 2$, we find that

$$\sum_{k\le x} S(h,k)=o\left(\sum_{k\le x}\varrho(k)\right),\qquad \text{as } x\to\infty.$$

In other words, $\sum_{m\le M} e(hs_m)=o(M)$, as $M\to\infty$ through values of the form $M=\varrho(1)+\varrho(2)+\cdots+\varrho(m)$. To complete the proof, it suffices to remove the restriction on the form of M. To this end, for each M define $m=m_M$ as the largest positive integer m with $\sum_{k\le m}\varrho(k)\le M$. Then

$$\frac{1}{M}\left|\sum_{m\le M} e(hs_m)\right|\le\frac{1}{\sum_{k\le m}\varrho(k)}\left|\sum_{k\le m} S(h,k)\right|+\frac{1}{\sum_{k\le m}\varrho(k)}\varrho(m+1).$$

We have seen already that the first term on the right goes to 0, as M (or equivalently, m) tends to infinity. The second term also tends to 0, since the denominator has size $\asymp m(\log m)^{g-1}$ while the numerator is $\ll n^{\omega(m+1)}\ll_\epsilon m^\epsilon$ for any $\epsilon>0$. □

3. Polynomial congruences usually have small roots: Proof of Theorem 1.2

3.1. $\mathscr{R}_f$ and its typical elements

The following asymptotic formula for the counting function of $\mathscr{R}_f$ can be proved analogously to Lemma 2.8, by applying Wirsing's mean value theorem (Proposition 2.9) with $F = \mathbb{1}_{\mathscr{R}_f}$. Note that $\mathbb{1}_{\mathscr{R}_f}$ is indeed a multiplicative function and that the the hypothesis (2.4) is satisfied with $\tau = 1 - \delta_0$, which is positive since $1 - \delta_0 = \sum_{j \geq 1} \delta_j \geq \delta_n \geq \frac{1}{n!}$.

Lemma 3.1. *For a certain positive constant C depending on f (not necessarily the same C as in Lemma 2.8),*

$$\sum_{\substack{k \in \mathscr{R}_f \\ k \leq x}} 1 \sim Cx/(\log x)^{\delta_0}, \qquad \text{as } x \to \infty.$$

Next, we consider the behavior of $\varrho(k)$ for a typical $k \in \mathscr{R}_f$. For each j, let $\omega_j(k)$ denote the number of (distinct) primes p dividing k with $\varrho(p) = j$.

Lemma 3.2. *Let $\epsilon > 0$. As $x \to \infty$, all but $o(\#\mathscr{R}_f \cap [1, x])$ elements $k \in \mathscr{R}_f \cap [1, x]$ satisfy*

$$|\omega_j(k) - \delta_j \log\log x| < \epsilon \log\log x \tag{3.1}$$

for all $j = 1, 2, 3, \ldots, n$.

Proof. We fix $j \in \{1, 2, \ldots, n\}$ and show that only $o(\#\mathscr{R}_f \cap [1, x])$ elements $k \in \mathscr{R}_f \cap [1, x]$ violate (3.1). Let $z \in [1/2, 3/2]$. Applying Lemma 2.5 with $F(k) = z^{\omega_j(k)} \cdot \mathbb{1}_{\mathscr{R}_f}(k)$, we find that

$$\begin{aligned}
\sum_{\substack{k \leq x \\ k \in \mathscr{R}_f}} z^{\omega_j(k)} &\ll \frac{x}{\log x} \left(\prod_{\substack{1 \leq j' \leq n \\ j' \neq j}} \prod_{\substack{p \leq x \\ \varrho(p) = j'}} \left(1 + \frac{1}{p} + \cdots\right) \right) \prod_{\substack{p \leq x \\ \varrho(p) = j}} \left(1 + \frac{z}{p} + \cdots\right) \\
&\ll \frac{x}{\log x} \exp\left((z-1) \sum_{\substack{p \leq x \\ \varrho(p) = j}} \frac{1}{p} + \sum_{1 \leq j' \leq n} \sum_{\substack{p \leq x \\ \varrho(p) = j'}} \frac{1}{p} \right) \\
&\ll \frac{x}{\log x} (\log x)^{(z-1)\delta_j + \delta_1 + \cdots + \delta_n} = \frac{x}{(\log x)^{\delta_0}} (\log x)^{(z-1)\delta_j}. \qquad (3.2)
\end{aligned}$$

If we choose $z \geq 1$, then any k with $\omega_j(k) \geq (\delta_j + \epsilon) \log\log x$ makes a contribution to the left-hand side of (3.2) of size at least $(\log x)^{(\delta_j+\epsilon)\log z}$. Hence, the number of these k is

$$\ll \frac{x}{(\log x)^{\delta_0}} (\log x)^{\delta_j(z-1-\log z)-\epsilon\log z}.$$

The final exponent of $\log x$, viewed as a function of z, vanishes when $z = 1$ and is decreasing at $z = 1$ (with derivative $-\epsilon$ at $z = 1$). Now fixing $z \in [1, 3/2]$ slightly larger than 1, we deduce that the number of $k \in \mathscr{R}_f \cap [1, x]$ with $\omega_j(k) \geq (\delta_j + \epsilon) \log\log x$ is $o(x/(\log x)^{\delta_0})$, and (by Lemma 3.1) is therefore $o(\#\mathscr{R}_f \cap [1, x])$, as $x \to \infty$.

We can bound the number of $k \leq x$ in $\mathscr{R}_f$ with $\omega_j(k) \leq (\delta_j - \epsilon) \log\log x$ similarly. If $z \leq 1$, each such k contributes at least $(\log x)^{(\delta_j-\epsilon)\log z}$ to the left-hand side of (3.2). Arguing as above, if we now take $z \in [1/2, 1]$ to be slightly smaller than 1, then we obtain a bound on the number of these k is that is $o(x/(\log x)^{\delta_0})$. □

Put

$$\kappa = \sum_{j\geq 1} \delta_j \log j.$$

Lemma 3.3. *For each $\epsilon > 0$, all but $o(\#\mathscr{R}_f \cap [1, x])$ elements $k \in \mathscr{R}_f \cap [1, x]$ satisfy*

$$(\log x)^{\kappa-\epsilon} < \varrho(k) < (\log x)^{\kappa+\epsilon}.$$

Proof. For $k \in \mathscr{R}_f$, write $k = k'k''$, where every prime dividing k' divides D, and k'' is coprime to D. Since $\varrho(\cdot)$ is bounded on prime powers and only finitely many primes divide D,

$$\varrho(k'') \leq \varrho(k')\varrho(k'') = \varrho(k) \ll \varrho(k'').$$

Moreover, if $p^\alpha \parallel k''$, then $1 \leq \varrho(p) = \varrho(p^\alpha) \leq n$. Thus,

$$\varrho(k'') = \prod_{1\leq j\leq n} j^{\omega_j(k'')}.$$

Since $\omega_j(k'') = \omega_j(k) + O(1)$, we conclude that

$$\varrho(k) \asymp \prod_{j=1}^{n} j^{\omega_j(k)}$$

for all $k \in \mathscr{R}_f$. Now apply Lemma 3.2. □

3.2. Detecting k for which f admits no small roots

We let ϵ, c denote positive constants whose values will be fixed later.

Let $\mathscr{E}$ denote the set of $k \in \mathscr{R}_f \cap [1, x]$ for which the least root of f modulo k exceeds $k/(\log k)^c$. We let $\mathscr{E}'$ be the subset of $\mathscr{E}$ consisting of those k satisfying

$$(\log x)^{\kappa-\epsilon} < \varrho(k) < (\log x)^{\kappa+\epsilon}.$$

By Lemma 3.3, passing from $\mathscr{E}$ to $\mathscr{E}'$ requires discarding only $o(\#\mathscr{R}_f \cap [1, x])$ elements, as $x \to \infty$. Thus, to prove Theorem 1.2, with $c_f = c$, it will be enough to show that $\#\mathscr{E}' = o(\#\mathscr{R}_f \cap [1, x])$, as $x \to \infty$.

To detect elements of $\mathscr{E}'$, we use a result of Montgomery [16, Corollary 1.2].

Proposition 3.4. *Let $s_1, s_2, s_3, \ldots, s_M$ be real numbers. Suppose that H is a positive integer for which*

$$\sum_{h \le H} \left| \sum_{m \le M} e(h s_m) \right| < \frac{1}{10} M.$$

Then for every pair α, β satisfying $\alpha \le \beta \le \alpha + 1$ and

$$\beta - \alpha \ge \frac{4}{H+1}, \tag{3.3}$$

we have that

$$\#\{m \le M : s_m \in [\alpha, \beta] \bmod 1\} \ge \frac{1}{2}(\beta - \alpha) M. \tag{3.4}$$

Let $\{s_m\}$ be the sequence obtained by concatenating the lists (1.1) for $k \in \mathscr{E}'$. Thus,

$$M = \sum_{k \in \mathscr{E}'} \varrho(k).$$

Put $\alpha = 0$, $\beta = 1/(\log x)^c$; then (3.3) holds if we take $H = \lfloor 4(\log x)^c \rfloor$. By the choice of $\mathscr{E}$, each $s_m \in (1/(\log x)^c, 1)$, so that the left-hand side of (3.4) vanishes. So either (3.4) fails or $M=0$; in either case, we deduce that

$$M \le 10 \sum_{h\le H} \left| \sum_{m\le M} e(hs_m) \right|.$$

Thus,

$$(\log x)^{\kappa-\epsilon}\cdot \#\mathscr{E}' \le \sum_{k\in\mathscr{E}'} \varrho(k) = M \le 10 \sum_{h\le H} \left| \sum_{k\in\mathscr{E}'} S(h,k) \right|,$$

so that

$$\#\mathscr{E}' \ll (\log x)^{-\kappa+\epsilon} \sum_{h\le H} \left| \sum_{k\in\mathscr{E}'} S(h,k) \right|. \tag{3.5}$$

By Proposition 2.6 (with $\mathscr{K}=\mathscr{E}'$),
(3.6)

$$\sum_{k\in\mathscr{E}'} S(h,k) \ll \frac{x}{\log x}(\log\log x)^{O(1)} \left(1+\sum_{k_1\in\mathscr{E}'_{\mathrm{smooth}}} \frac{\varrho(k_1)^{1/2}\gcd(h,k_1)^{1/2}}{k_1}\right).$$

If $k_1\in\mathscr{E}'_{\mathrm{smooth}}$ is the X-smooth part of the integer $k\in\mathscr{E}'$, then k,k_1 both belong to $\mathscr{R}_f$. By the proof of Lemma 3.3,

$$\varrho(k) \asymp \prod_{j=1}^{n} j^{\omega_j(k)}, \quad \varrho(k_1) \asymp \prod_{j=1}^{n} j^{\omega_j(k_1)};$$

as $\omega_j(k_1)\le\omega_j(k)$ for each j, we have that

$$\varrho(k_1) \ll \varrho(k) < (\log x)^{\kappa+\epsilon}.$$

Using these observations in (3.6), we find that
(3.7)

$$\sum_{k\in\mathscr{E}'} S(h,k) \ll x(\log x)^{\kappa/2+\epsilon/2-1}(\log\log x)^{O(1)} \left(\sum_{k\in\mathscr{R}_f\cap[1,x]} \frac{\gcd(h,k)^{1/2}}{k}\right).$$

If h is a positive integer not exceeding H, $k \in \mathscr{R}_f \cap [1,x]$, and $\gcd(h,k) = d$, then $d \le H$, and $k' := k/d$ is itself an element of $\mathscr{R}_f \cap [1,x]$. Thus,

$$\begin{aligned}\sum_{h \le H} \sum_{k \in \mathscr{R}_f \cap [1,x]} \frac{\gcd(h,k)^{1/2}}{k} &\le \sum_{d \le H} d^{1/2} \Bigg(\sum_{\substack{h \le H \\ d \mid h}} 1 \Bigg) \sum_{k' \in \mathscr{R}_f \cap [1,x]} \frac{1}{dk'} \\ &\ll H \sum_{d \le H} d^{-3/2} \sum_{k' \in \mathscr{R}_f \cap [1,x]} \frac{1}{k'} \\ &\ll H (\log x)^{1-\delta_0} \ll (\log x)^{1+c-\delta_0}.\end{aligned}$$

(We used the bound $\sum_{k \in \mathscr{R}_f \cap [1,x]} k^{-1} \ll (\log x)^{1-\delta_0}$, which follows from Lemma 3.1 by partial summation.) Using this in (3.5) and (3.7), we conclude that

$$\#\mathscr{E}' \ll \frac{x}{(\log x)^{\delta_0}} (\log\log x)^{O(1)} (\log x)^{3\epsilon/2 + c - \kappa/2}.$$

Fixing $c < \kappa/2$, we then choose $\epsilon > 0$ so that the final exponent of $\log x$ on the right-hand side is negative. Then

$$\#\mathscr{E}' = o(x/(\log x)^{\delta_0}) = o(\#\mathscr{R}_f \cap [1,x]).$$

This shows that Theorem 1.2 holds with any value of $c_f < \kappa/2$. (This result should be measured against the conjecture from the introduction that any $c_f < \kappa$ is admissible.)

Remark. Fix $c < \kappa/2$. The following result in Diophantine approximation can be shown by an argument analogous to the above. For every $\alpha \in \mathbb{R}$, almost all $k \in \mathscr{R}_f$ are such that there is an integer ν satisfying both

$$f(\nu) \equiv 0 \pmod{k} \qquad \text{and} \qquad \left\| \frac{\nu}{k} - \alpha \right\| \le \frac{1}{(\log k)^c}. \tag{3.8}$$

(As is customary, $\|\cdot\|$ denotes distance to the nearest integer.) In this connection, we note that Hooley [13] has proved the existence of an infinite sequence of $k \in \mathscr{R}_f$ for which (3.8) is solvable with $(\log k)^c$ replaced by a certain positive power of k.

4. Small but not too small: Proof of Proposition 1.3

The following estimate is due to van der Corput [22].

Proposition 4.1. *Let $f(t)$ be a nonconstant polynomial in $\mathbb{Z}[t]$. For all $x \geq 3$,*

$$\sum_{\substack{r \leq x \\ f(r) \neq 0}} d(f(r)) \ll x(\log x)^{O(1)}, \tag{4.1}$$

where the implied constants may depend on f.

Subsequent ideas of Erdős can be used to prove Proposition 4.1 with $x(\log x)^g$ on the right-hand side of (4.1). (As usual, g denotes the number of monic irreducible factors of f over $\mathbb{Q}$.) See [8]. There Erdős assumes f is irreducible, but that assumption can be dispensed with, as detailed in [7, Theorem 7.1].

Proof of Proposition 1.3. Assume that $f(t) \in \mathbb{Z}[t]$ is nonconstant with no nonnegative integer roots. Fix a constant C_f having the property that, as $x \to \infty$,

$$\sum_{0 \leq r \leq x/(\log x)^{C_f}} d(f(r)) = o(x/(\log x)^{\delta_0});$$

such a choice of C_f is possible by Proposition 4.1. In fact, by the remarks above, we can take any value of $C_f > g + \delta_0$.

Let x be a large real number. If $k \in [x/2, x]$ and f has a root r modulo k, where $0 \leq r \leq k/(\log k)^{C_f}$, then

$$k \mid f(r), \quad \text{and} \quad r \leq x/(\log x)^{C_f}.$$

Thus, k is counted by the sum $\sum_{0 \leq r \leq x/(\log x)^{C_f}} d(f(r))$, and so there are $o(x/(\log x)^{\delta_0})$ possibilities for k. Summing dyadically, we deduce that there are only $o(x/(\log x)^{\delta_0})$ values of $k \in [1, x]$ for which f has a root modulo k not exceeding $k/(\log k)^{C_f}$. Since $\#\mathscr{R}_f \cap [1, x] \asymp x/(\log x)^{\delta_0}$, Proposition 1.3 follows. □

5. A parting shot: Root quotient sets

We define the *root quotient set* $\mathscr{Q}_f$ corresponding to a given $f(t) \in \mathbb{Z}[t]$ as follows. For each $k \in \mathscr{R}_f$, we let r_k denote the smallest nonnegative integer r with $f(r) \equiv 0 \pmod{k}$. Then

$$\mathscr{Q}_f := \{|f(r_k)|/k : k = 1, 2, 3, \ldots\}.$$

In the case when f has no nonnegative integer roots, it is easy to see that $\mathscr{Q}_f \subset \mathscr{R}_f$. We conclude the paper by proving the following.

Theorem 5.1. *Suppose that $f(t) \in \mathbb{Z}[t]$ has at least two distinct roots and no nonnegative integer root. Then*

$$\mathscr{Q}_f = \mathscr{R}_f.$$

For the polynomials $f(t) = (t+2)^n - 1$ (with $n \geq 2$), Theorem 5.1 was proved by Andrica and Crişan in [1]. It is easy to see that neither assumption on f in the statement of Theorem 5.1 can be removed.

Proof. We may assume that the leading coefficient of f is positive. We have already remarked that $\mathscr{Q}_f \subset \mathscr{R}_f$, so we focus on proving that $\mathscr{R}_f \subset \mathscr{Q}_f$.

Fix $R \in \mathscr{R}_f$. A moment's thought shows that $R \in \mathscr{Q}_f$ if there are infinitely many positive integers k with

$$Rk \in f(\mathbb{Z}_{\geq 0}), \quad \text{but} \quad k, 2k, 3k, \dots, (R-1)k \notin f(\mathbb{Z}_{\geq 0}). \tag{5.1}$$

Indeed, our assumption that f has no nonnegative integer roots implies that $r_k \to \infty$ with k. Since f is eventually positive and increasing, and tends to infinity, all but finitely many of the k satisfying (5.1) will satisfy $|f(r_k)|/k = Rk/k = R$.

Since $R \in \mathscr{R}_f$, for large K there are $\gg K^{1/n}$ positive integers $k \leq K$ with $Rk \in f(\mathbb{Z}_{\geq 0})$. It is therefore enough to show that for each fixed $R' \in \{1, 2, 3, \dots, R-1\}$, only $o(K^{1/n})$ integers $k \leq K$ have both Rk and $R'k$ lying in $f(\mathbb{Z}_{\geq 0})$, as $K \to \infty$. (Here, as usual, n denotes the degree of f.) To this end, suppose that

$$f(u) = Rk, \quad f(u') = R'k, \qquad \text{where } u, u' \in \mathbb{Z}_{\geq 0}. \tag{5.2}$$

Note that the point (u, u') lies on the curve $f(x) = \frac{R}{R'} f(y)$. There is by now a well-developed theory of integral points on curves of the form $f(x) = g(y)$, but for our purposes it is simpler to argue as follows.

We can write $f(x) = \alpha(x+\beta)^n + O(x^{n-2})$ (for large x), where α, β are rational numbers depending only on f. Assuming k is sufficiently large (which implies that u and u' are also large, and that $u \asymp u'$), we deduce from (5.2) that

$$\left(\left(\frac{R}{R'}\right)^{1/n} \cdot \frac{u'+\beta}{u+\beta}\right)^n = 1 + O\left(\frac{1}{u^2}\right).$$

Taking nth roots and rearranging,

$$\frac{u'+\beta}{u+\beta} = \left(\frac{R'}{R}\right)^{1/n} + O\left(\frac{1}{u^2}\right),$$

and hence

$$u' + \beta - (u+\beta)\left(\frac{R'}{R}\right)^{1/n} = O\left(\frac{1}{u}\right). \tag{5.3}$$

Writing $\beta = A/B$ in lowest terms, and then multiplying the last display through by B, we find that

$$\|(Bu + A)\cdot (R'/R)^{1/n}\| \ll u^{-1}. \tag{5.4}$$

If $(R'/R)^{1/n}$ is irrational, we continue as follows. By a famous theorem of Bohl–Sierpiński–Weyl, the positive integer multiples of $(R'/R)^{1/n}$ are equidistributed mod 1. This implies that (5.4) is satisfied for only $o(U)$ integers $u \le U$, as $U \to \infty$. Since $f(u) = Rk$ and $k \le K$, we have $u \ll K^{1/n}$. Hence, the number of values of u that arise is $o(K^{1/n})$, as $K \to \infty$. Noting that u determines k gives the desired upper bound in this case.

To conclude the proof, we assume that $(R'/R)^{1/n}$ is rational and deduce a contradiction to our hypothesis that f has at least two distinct roots. In this case, the left-hand side of (5.3) has bounded denominator; so (5.3) implies that the left-hand side vanishes if k is sufficiently large. Thus,

$$u' = \delta u + \gamma, \qquad \text{where } \ \delta = (R'/R)^{1/n},\ \gamma = \beta((R'/R)^{1/n} - 1).$$

Moreover,

$$f(u) = \frac{R}{R'} f(u') = \frac{R}{R'} f(\delta u + \gamma).$$

For this situation to arise for infinitely many different values of k, we need $f(t) = \frac{R}{R'} f(\delta t + \gamma)$ identically. In that case, the map $\theta \mapsto \delta\theta + \gamma$ induces a permutation on the roots of f. If the permutation has order j (say), then every root of f is fixed by the map

$$\theta \mapsto \delta^j \theta + \gamma \frac{\delta^j - 1}{\delta - 1}.$$

But $\delta^j \ne 1$, and so this map has a unique fixed point. Hence, f has a unique root. $\square$

Acknowledgements

The second author (P. P.) is supported by NSF award DMS-1402268. We thank the referee for comments that led to improvements in the exposition.

References

[1] D. Andrica and V. Crişan, *The smallest nontrivial solution to $x^k \equiv 1 \pmod{n}$ and related sequences*, Amer. Math. Monthly **126** (2019), 173–178.

[2] E. Artin, *Über eine neue Art von L-Reihen*, Abh. Math. Sem. Univ. Hamburg **3** (1924), 89–108.

[3] J. Bourgain, A. A. Glibichuk, and S. Konyagin, *Estimates for the number of sums and products and for exponential sums in fields of prime order*, J. London Math. Soc. **73** (2006), 380–398.

[4] D. Coppersmith, *Finding a small root of a univariate modular equation*, Advances in cryptology—EUROCRYPT '96 (Saragossa, 1996), Lecture Notes in Comput. Sci., Vol. 1070, Springer, Berlin, (1996), pp. 155–165.

[5] D. Coppersmith, *Small solutions to polynomial equations, and low exponent RSA vulnerabilities*, J. Cryptology **10** (1997), no. 4, 233–260.

[6] D. Coppersmith, *Finding small solutions to small degree polynomials*, Cryptography and lattices (Providence, RI, 2001), Lecture Notes in Comput. Sci., Vol. 2146, Springer, Berlin, (2001), pp. 20–31.

[7] C. Elsholtz and T. Tao, *Counting the number of solutions to the Erdős-Straus equation on unit fractions*, J. Aust. Math. Soc. **94** (2013), 50–105.

[8] P. Erdős, *On the sum* $\sum_{k=1}^{x} d(f(k))$, J. London Math. Soc. **27** (1952), 7–15.

[9] S. Gun, *On solutions of polynomial congruences*, Acta Arith. **144** (2010), 151–158.

[10] R. R. Hall and G. Tenenbaum, Divisors, Cambridge Tracts in Mathematics, Vol. 90, Cambridge University Press, Cambridge, (1988).

[11] C. Hooley, *On the number of divisors of a quadratic polynomial*, Acta Math. **110** (1963), 97–114.

[12] C. Hooley, *On the distribution of the roots of polynomial congruences*, Mathematika **11** (1964), 39–49.

[13] C. Hooley, *On the location of the roots of polynomial congruences*, Glasgow Math. J. **32** (1990), 309–316.

[14] S. V. Konyagin and T. Steger, *Polynomial congruences*, Mat. Zametki **55** (1994), no. 6, 73–79, 158; translation in Math. Notes **55** (1994), no. 5–6, 596–600.

[15] G. Martin and S. Sitar, *Erdős-Turán with a moving target, equidistribution of roots of reducible quadratics, and Diophantine quadruples*, Mathematika **57** (2011), 1–29.

[16] H. L. Montgomery, *Ten lectures on the interface between analytic number theory and harmonic analysis*, CBMS Regional Conference Series in Mathematics, vol. 84, published for the Conference Board of the Mathematical Sciences, Washington, DC by the American Mathematical Society, Providence, RI, (1994).

[17] M. R. Murty, *Small solutions of polynomial congruences*, Indian J. Pure Appl. Math. **41** (2010), 15–23.

[18] P. Pollack, *Nonnegative multiplicative functions on sifted sets, and the square roots of* -1 *modulo shifted primes*, Glasg. Math. J. **62** (2020), 187–199.

[19] M. Rosen, *Polynomials modulo p and the theory of Galois sets*, Theory and Applications of Finite Fields, Contemp. Math., Vol. 579, Amer. Math. Soc., Providence, RI, (2012), pp. 163–178.

[20] J.-P. Serre, *Divisibilité de certaines fonctions arithmétiques*, Séminaire Delange-Pisot-Poitou, 16e année (1974/75), Théorie des nombres, Fasc. 1, Exp. No. 20, Secrétariat Mathématique, Paris, (1975), 28 pages.

[21] P. Stevenhagen and H. W. Lenstra, Jr., *Chebotarëv and his density theorem*, Math. Intelligencer **18** (1996), no. 2, 26–37.

[22] J. G. van der Corput, *Une inégalité relative au nombre des diviseurs*, Nederl. Akad. Wetensch., Proc. **42** (1939), 547–553.

[23] E. Wirsing, *Das asymptotische Verhalten von Summen über multiplikative Funktionen*, Math. Ann. **143** (1961), 75–102.

Mathematisches Institut der Universität Göttingen
37073 Göttingen, Germany
E-mail address: vlad.crisan@mathematik.uni-goettingen.de

Department of Mathematics, University of Georgia
Athens, GA 30602, USA
E-mail address: pollack@uga.edu

Received February 18, 2018
Accepted February 13, 2019