Journal of Number Theory 261 (2024) 220–240

Contents lists available at ScienceDirect

Journal of Number Theory

journal homepage: www.elsevier.com/locate/jnt

General Section

Square-free values of random polynomials

Tim D. Browning [a], Igor E. Shparlinski [b,*]

[a] *IST Austria, Am Campus 1, 3400 Klosterneuburg, Austria*
[b] *School of Mathematics and Statistics, University of New South Wales, Sydney, NSW 2052, Australia*

A R T I C L E   I N F O

Article history:
Received 19 July 2023
Received in revised form 22 February 2024
Accepted 29 February 2024
Available online 21 March 2024
Communicated by L. Smajlovic

MSC:
primary 11N32
secondary 11D79, 11K38, 11L15, 11P21

Keywords:
Polynomials
Square-free numbers

A B S T R A C T

The question of whether or not a given integral polynomial takes infinitely many square-free values has only been addressed unconditionally for polynomials of degree at most 3. We address this question, on average, for polynomials of arbitrary degree.

Contents

* Corresponding author.
E-mail addresses: tdb@ist.ac.at (T.D. Browning), igor.shparlinski@unsw.edu.au (I.E. Shparlinski).

https://doi.org/10.1016/j.jnt.2024.02.013

1. Introduction

Let $f \in \mathbb{Z}[X]$ be an irreducible polynomial of degree k, without a fixed square divisor. We denote by $S_f(N)$ the number of positive integers $n \leqslant N$ such that $f(n)$ is square-free. It is expected that

$$S_f(N) = c_f N + o(N), \tag{1.1}$$

as $N \to \infty$, where

$$c_f = \prod_{p \text{ prime}} \left(1 - \frac{\rho_f(p^2)}{p^2}\right)$$

and $\rho_f(m) = \#\{n \in \mathbb{Z}/m\mathbb{Z} : f(n) \equiv 0 \bmod m\}$, for any positive integer m. When $k \leqslant 3$ this expectation follows from pioneering work of Hooley [16]. (In fact, when $k = 3$, Reuss [23] has produced an asymptotic formula for $S_f(N)$ with a power saving error term.) However for polynomials of degree $k \geqslant 4$ we only have a conditional treatment under the *abc*-conjecture, thanks to work of Granville [14].

In this paper, for $k \geqslant 4$, we lend support to the expectation (1.1) by showing that it holds for almost all polynomials of degree k, when they are ordered by naive height. This sits in the framework of a great deal of recent work aimed at understanding the average size of various arithmetic functions over the values of random polynomials, with a focus on the von Mangoldt function Λ, the Liouville function λ and variants of the r-function [1,3,6,12,26]. Questions about square-free values of polynomials are easier than the corresponding primality questions. On the other hand, we establish results with substantially less averaging than what is used in the best known result [6] for prime polynomial values.

For positive integers H and $k \geqslant 2$, let

$$\mathcal{F}_k(H) = \{a_0 + \cdots + a_k X^k \in \mathbb{Z}[X] : \ (a_0, a_1, \ldots, a_k) \in \mathcal{B}_k(H)\},$$

where

$$\mathcal{B}_k(H) = \left\{ (a_0, \ldots, a_k) \in \mathbb{Z}^{k+1} : \begin{array}{c} \gcd(a_0, a_1, \ldots, a_k) = 1 \\ |a_0|, |a_1|, \ldots, |a_k| \leqslant H \end{array} \right\}.$$

For the problem of counting square-free values of polynomials, we are primarily interested in the largest allowable range of H, with respect to N, for which we can prove the existence of $\delta > 0$ such that

$$\frac{1}{\#\mathcal{F}_k(H)} \sum_{f \in \mathcal{F}_k(H)} |S_f(N) - c_f N| \ll N^{1-\delta}. \tag{1.2}$$

(See Section 2.1 for a precise definition of the symbol $\ll$.) A result of the form (1.2) would confirm that (1.1) holds unconditionally, on average over the polynomials of naive height at most H.

Obviously, we would like to be able to take H as small as possible, with respect to N, in assessing the validity of (1.2).

First we recall that Filaseta [11] has shown that almost all polynomials assume at least one square-free value (in fact the result of [11] is slightly more general). However, here we are interested in more precise counting results.

Let $A \geqslant 1$ and let $\varepsilon > 0$. The second author has shown in [25, Theorem 1.1] that there exists $\delta > 0$, depending only on ε such that (1.2) holds provided that

$$N^A \geqslant H \geqslant N^{k-1+\varepsilon},$$

and provided that we allow the implied constant to depend on A and ε. In this paper we revisit this argument using tools from the geometry of numbers and the determinant method, in order to increase the range of H, as follows.

Theorem 1.1. *Let $A \geqslant 1$ and $k \geqslant 4$ be fixed. Assume that*

$$N^A \geqslant H \geqslant N^{k-3+\varepsilon},$$

for $\varepsilon > 0$. Then there exists $\delta > 0$, depending only on ε, such that (1.2) holds, with the implied constant depending only on A, k and ε.

This is our main result. In fact, in Theorem 4.1 we also a more general upper bound for the left hand side of (1.2), from which Theorem 1.1 follows. An alternative approach to this problem is available through modifying the proof of [6, Theorem 2.2] to treat the function

$$F(n) = \mu^2(n) - \sum_{\substack{d^2 \mid n \\ d \leqslant D}} \mu(d),$$

for suitable $D \geqslant 1$. This has been carried out by Jelinek [18]. While this approach does not seem to offer an improvement over the range of H in Theorem 1.1, it does allow one to average over only two of the coefficients.

Inspired by recent work on Vinogradov's mean value theorem we can also treat a related problem in which we only vary one coefficient. Let

$$g(X) = b_1 X + \cdots + b_k X^k \in \mathbb{Z}[X]$$

be given and note that $g(0) = 0$. Then we may consider the set

$$\mathcal{G}_g(H) = \{a + g(X) \in \mathbb{Z}[X] : \ a \in \mathcal{I}_g(H)\},$$

where

$$\mathcal{I}_g(H) = \{a \in \mathbb{Z} : \ \gcd(a, b_1, \ldots, b_k) = 1, \ |a| \leqslant H\}.$$

While the approach of [25] also applies to polynomials from $\mathcal{G}_g(H)$, we supplement it with some new bounds for residues of polynomials falling in short intervals, which complement those of [2,8,9,13,19]. To formulate the result, we define

$$\eta(k) = \begin{cases} 2^{-k+1}, & \text{if } 2 \leqslant k \leqslant 5, \\ 1/(k(k-1)), & \text{if } k \geqslant 6, \end{cases} \tag{1.3}$$

with which notation we have following result.

Theorem 1.2. *Let $k \geqslant 2$ be fixed and assume that*

$$H \geqslant N^{(k-1)/2+\eta(k)+\varepsilon},$$

for $\varepsilon > 0$. Then, for a fixed polynomial $g \in \mathbb{Z}[X]$ of degree k, there exists $\delta > 0$ depending only on ε such that

$$\frac{1}{\#\mathcal{G}_g(H)} \sum_{f \in \mathcal{G}_g(H)} |S_f(N) - c_f N| \ll N^{1-\delta},$$

with the implied constant depending only on A, k and ε.

In Theorem 4.2 we prove a more general version of this result, without making any assumptions about the relative sizes of H and N. We note that the range for H in Theorem 1.2 is significantly broader than in Theorem 1.1, which seems counterintuitive, since we have less averaging in Theorem 1.2. However, the problem stems from the fact that the values of polynomials $f(n)$ with $f \in \mathcal{F}_k(H)$ and $1 \leqslant n \leqslant N$ could be of order HN^k, while for $f \in \mathcal{G}_g(H)$ they are of much smaller order $H + N^k$, which has a strong effect on the set of moduli for which we have to sieve.

Acknowledgements. The authors are very grateful to the referee for helpful comments. This work started during a very enjoyable visit by the second author to IST Austria whose hospitality and support are very much appreciated. The first author was supported by FWF grant P 36278 and the second author by ARC grant DP230100534.

2. Preliminaries

2.1. Notation and conventions

We adopt the Vinogradov notation $\ll$, that is,

$$C \ll D \iff C = O(D) \iff |C| \leqslant cD$$

for some constant $c > 0$ which is allowed to depend on the integer parameter $k \geqslant 1$ and the real parameters $A, \varepsilon > 0$. For a finite set $\mathcal{S}$ we use $\#\mathcal{S}$ to denote its cardinality. We also write $\mathbf{e}(z) = \exp(2\pi i z)$ and $\mathbf{e}_m(z) = \mathbf{e}(z/m)$. In what follows we make frequent use of the bound

$$\tau(r) \leqslant |r|^{o(1)}, \qquad \text{for } r \in \mathbb{Z},\ r \neq 0, \tag{2.1}$$

for the divisor function τ, and its cousins, as explained in [17, Equation (1.81)], for example. Finally, as usual, $\mu(r)$ denotes the Möbius function.

2.2. Lattice points in boxes

We use some tools from the geometry of numbers, as explained in Cassels [7]. Let

$$\Lambda = \{u_1\mathbf{b}_1 + \cdots + u_s\mathbf{b}_s : \ (u_1, \ldots, u_s) \in \mathbb{Z}^s\}$$

be an s-dimensional lattice defined by s linearly independent vectors $\mathbf{b}_1, \ldots, \mathbf{b}_s \in \mathbb{Z}^s$. We denote by $\lambda_1 \leqslant \ldots \leqslant \lambda_s$ the successive minima of Λ, which for $j = 1, \ldots, d$ is defined to be

$$\lambda_j = \inf\{\lambda > 0 : \ \lambda\mathfrak{B}_s \text{ contains } j \text{ linearly independent elements of } \Lambda\},$$

where $\lambda\mathfrak{B}_s$ is the homothetic image of $\mathfrak{B}_s$ of the unit ball $\mathfrak{B}_s \subseteq \mathbb{R}^s$ at the origin with the coefficient λ.

We also recall that the discriminant Δ of Λ is an invariant that is independent of the choice of basis for Λ. We have

$$\Delta \leqslant \lambda_1 \ldots \lambda_s \ll \Delta, \tag{2.2}$$

where the implied constant only depends on s.

Next, we need the following consequence of the classical result of Schmidt [24, Lemma 2] on counting lattice points in boxes.

Lemma 2.1. *Let λ_1 be the smallest successive minimum of a full rank lattice $\Lambda \subseteq \mathbb{Z}^s$ and let Δ be its discriminant. Then*

$$\#\left(\Lambda \cap [-H,H]^s\right) \ll \frac{H^s}{\Delta} + \left(\frac{H}{\lambda_1}\right)^{s-1} + 1,$$

where the implied constant depends only on s.

Proof. By [24, Lemma 2], we have the following asymptotic formula

$$\left|\#\left(\Lambda \cap [-H,H]^s\right) - \frac{(2H+1)^s}{\Delta}\right| \ll \sum_{j=0}^{s-1} \frac{H^j}{\lambda_1 \dots \lambda_j}.$$

It follows that

$$\#\left(\Lambda \cap [-H,H]^s\right) \ll \frac{H^s}{\Delta} + \sum_{j=0}^{s-1} \left(\frac{H}{\lambda_1}\right)^j,$$

which yields the result. □

2.3. Univariate polynomial congruences

For $f \in \mathbb{Z}[X]$, we define

$$\rho_f(m) = \#\{n \in \mathbb{Z}/m\mathbb{Z} : \ f(n) \equiv 0 \bmod m\}. \tag{2.3}$$

The associated discriminant $\Delta_f \in \mathbb{Z}$ is a form of degree $k(k-1)/2$ in the coefficients of f, if f has degree k.

To estimate $\rho_f(m)$ we may use the following result, in which the content of f is the greatest common divisor of the coefficients of f.

Lemma 2.2. *Let p be a prime and let $k \in \mathbb{N}$. Let $f \in \mathbb{Z}[X]$ be a polynomial of degree k. Assume that $\Delta_f \neq 0$ and f has content coprime to p. Then*

$$\rho_f(p^j) \leqslant k \min\left\{p^{j(1-\frac{1}{k})}, p^{j-1}\right\}.$$

Additionally, if $p \nmid \Delta_f$, then $\rho_f(p^k) \leqslant d$.

Proof. The final statement of the lemma is a straightforward consequence of Lagrange's theorem and Hensel's lemma. For the remaining bounds, the first bound follows from work of Stewart [27, Corollary 2 and Equation (44)] and the second bound is a consequence of Lagrange's theorem. □

The next bound is an easy consequence of Lemma 2.2 and the Chinese remainder theorem.

Corollary 2.3. *Let $f \in \mathbb{Z}[X]$ be a polynomial of degree k with content 1. For any square-free positive integer q we have*

$$\rho_f(q^2) \leqslant q^{o(1)} \gcd(\Delta_f, q).$$

Note that the bound of Lemma 2.3 also holds for $\Delta_f = 0$. We also need to look at averages of $\rho_f(m)$, for which we require the following useful result.

Lemma 2.4. *Let $f \in \mathbb{Z}[X]$ be a polynomial of degree k with $\Delta_f \neq 0$ and content 1. Then*

$$\sum_{m \leqslant M} \rho_f(m) \leqslant M^{1+o(1)},$$

uniformly over f.

Proof. Any $m \in \mathbb{N}$ admits a factorisation $m = e_1 e_2^2 \dots e_{k-1}^{k-1} h$ where

$$\mu^2(e_1 \dots e_{k-1}) = \gcd(e_1 \dots e_{k-1}, h) = 1$$

and h is k-full. Combining Lemma 2.2 with the Chinese remainder theorem, we deduce that

$$\rho_f(m) = \rho_f(e_1)\rho_f(e_2^2) \cdots \rho_f(e_{k-1}^{k-1})\rho_f(h) \leqslant m^{o(1)} \cdot e_2 e_3^2 \cdots e_{k-1}^{k-2} h^{1-1/k}.$$

Hence we deduce that

$$\begin{aligned}\sum_{m \leqslant M} \rho_f(m) &\leqslant M^{o(1)} \sum_{\substack{h \leqslant M \\ h\ k\text{-full}}} h^{1-1/k} \sum_{e_{k-1} \leqslant M} e_{k-1}^{k-2} \cdots \sum_{e_2 \leqslant M} e_2 \cdot \frac{M}{e_2^2 \cdots e_{k-1}^{k-1} h} \\ &\leqslant M^{1+o(1)} \sum_{\substack{h \leqslant M \\ h\ k\text{-full}}} \frac{1}{h^{1/k}} \sum_{e_{k-1} \leqslant M} \frac{1}{e_{k-1}} \cdots \sum_{e_2 \leqslant M} \frac{1}{e_2}.\end{aligned}$$

The sums over $e_2, \dots, e_{k-1}$ contribute $O((\log M)^{k-2})$. Moreover, the sum over h contributes $O(\log M)$, since there are $O(B^{1/k})$ k-full positive integers in the dyadic interval $(B/2, B]$, for any $B \geqslant 1$ and the result follows. □

2.4. Polynomial values with a large square divisor

For a given polynomial $f \in \mathbb{Z}[X]$, we are interested in the size of

$$Q_f(S, N) = \#\left\{(n, r, s) \in \mathbb{Z}^3 : 1 \leqslant n \leqslant N,\ 1 \leqslant s \leqslant S,\ f(n) = sr^2\right\},$$

for given $N, S \geqslant 1$. For a polynomial $f \in \mathcal{F}_k(H)$ with $\Delta_f \neq 0$, this quantity has been estimated in [22, Theorem 1.3], with the outcome that

$$Q_f(S,N) \leqslant N^{1/2}S^{3/4}(HN)^{o(1)}.$$

The following result improves on this via the determinant method.

Lemma 2.5. *Assume that $f \in \mathcal{F}_k(H)$ is not of the form $f(X) = g^2$ for some $g \in \mathbb{C}[X]$. Then*

$$Q_f(S,N) \leqslant \left(N^{1/2}S^{1/2} + S\right)(HN)^{o(1)}.$$

Proof. Note that the bound is trivial if $S > N$ and so we may proceed under the assumption that $S \leqslant N$. We fix a choice of s and begin by breaking into residue classes modulo s, giving

$$Q_f(S,N) \leqslant \sum_{0<s\leqslant S} \sum_{\substack{\nu=0 \\ f(\nu)\equiv 0 \bmod s}}^{s-1} N(s,\nu),$$

where

$$\begin{aligned} N(s,\nu) &= \#\left\{(n,r) \in \mathbb{Z}^2 :\ 1 \leqslant n \leqslant N,\ n \equiv \nu \bmod s,\ f(n) = sr^2\right\} \\ &\leqslant \#\left\{(u,r) \in \mathbb{Z}^2 :\ u \leqslant N/s + 1,\ f(\nu + su) = sr^2\right\}. \end{aligned}$$

At this point we call upon work of Heath-Brown [15, Theorem 15]. Given $\varepsilon > 0$ and an absolutely irreducible polynomial $F \in \mathbb{Z}[u,v]$ of degree D, this shows that there are at most

$$(UV)^{o(1)} \exp\left(\frac{\log U \log V}{\log T}\right) \tag{2.4}$$

choices of $(u,v) \in \mathbb{Z}^2$ such that $|u| \leqslant U$, $|v| \leqslant V$ and $F(u,v) = 0$. Here T is defined to be the maximum of $U^{e_1}V^{e_2}$, taken over all monomials $u^{e_1}v^{e_2}$ which appear in $F(u,v)$ with non-zero coefficient. Moreover, this is uniform over all absolutely irreducible polynomials F of a given degree D.

Next, we show that

$$F(u,v) = f(\nu + su) - sv^2 \tag{2.5}$$

is absolutely irreducible. Suppose for a contradiction that $F = F_1F_2$, for two polynomials $F_1, F_2 \in \mathbb{C}[u,v]$ of non-zero degree. Since v appears in $F(u,v)$ only with a scalar factor, both F_1 and F_2 must depend on v. Clearly they have to take the shape

$$F_i(u,v) = f_i(u) + s_i v, \qquad \text{for } i = 1,2.$$

Since $F(u,v)$ has no linear term in v we have $s_2 f_1(u) = -s_1 f_2(u)$, and hence the polynomial $f(\nu + su) = f_1(u)f_2(u)$ is proportional to a perfect square. This is impossible under our assumption on $f(u)$.

We now apply the bound (2.4) with $U = N/s+1$ and the polynomials F given by (2.5). In particular we may take $T \geqslant V^2$ and it follows that

$$Q_f(S,N) \leqslant (NH)^{o(1)} \sum_{0<s\leqslant S} \rho_f(s) \left(\frac{N}{s}+1\right)^{1/2},$$

where $\rho_f(s)$ is defined in (2.3). We now appeal to Lemma 2.4, which we combine with partial summation, to obtain the desired upper bound after recalling that $S \leqslant N$. □

2.5. Exponential sums and discrepancy

Given a sequence $\xi_n \in [0,1)$ for $n \in \mathbb{N}$, we denote by $\Delta(N)$ its *discrepancy*

$$\Delta(N) = \sup_{\alpha\in[0,1)} \left|\#\{n \leqslant N:\ \xi_n \leqslant \alpha\} - \alpha N\right|.$$

As explained in [21, Theorem 2.5], for example, the celebrated *Erdős-Turán inequality*, allows us to give an upper bound on the discrepancy $\Delta(N)$ in terms of exponential sums.

Lemma 2.6. *Let ξ_n, $n \in \mathbb{N}$, be a sequence in $[0,1)$. Then for any integer $L \geqslant 1$, its discrepancy $\Delta(N)$ satisfies*

$$\Delta(N) \ll \frac{N}{L} + \sum_{h=1}^{L} \frac{1}{h} \left|\sum_{n=1}^{N} \mathbf{e}(h\xi_n)\right|.$$

We proceed by recalling some bounds of exponential sums with polynomial arguments. We make use of a bound which follows from the recent spectacular results of Bourgain, Demeter and Guth [5] (for $k \geqslant 4$) and Wooley [28,29] (for $k = 3$), towards the optimal form of the *Vinogradov mean value theorem*.

The current state-of-the-art bounds for *Weyl sums* has been conveniently summarised by Bourgain [4]. We need the following special case covered by [4, Theorems 4 and 5], for which we do not assume anything about the arithmetic structure of the modulus.

Lemma 2.7. *For any fixed polynomial $g \in \mathbb{Z}[X]$ of degree $k \geqslant 2$ and any integers $m, N \geqslant 1$ we have*

$$\left|\sum_{n=1}^{N} \mathbf{e}_m\left(hg(n)\right)\right| \leqslant N^{1+o(1)} \left(\frac{\gcd(h,m)}{m} + \frac{1}{N} + \frac{m}{\gcd(h,m)N^k}\right)^{\eta(k)},$$

where $\eta(k)$ is given by (1.3).

3. Solutions to families of polynomial congruences

3.1. Preliminaries

Let $U_k(m, H, N)$ be the number of solution to the congruence

$$a_0 + a_1 n + \cdots + a_k n^k \equiv 0 \pmod{m},$$

in the variables

$$(a_0, \ldots, a_k) \in \mathcal{B}_k(H) \qquad \text{and} \qquad 1 \leqslant n \leqslant N.$$

Similarly, for given $g \in \mathbb{Z}[X]$, let $W_g(m, H, N)$ be the number of solution to the congruence

$$a + g(n) \equiv 0 \pmod{m},$$

in the variables

$$a \in \mathcal{I}_g(H) \qquad \text{and} \qquad 1 \leqslant n \leqslant N.$$

It is observed in [25, Equation (3.2)] that we have the trivial upper bounds

$$U_k(m, H, N) \ll H^k (H/m + 1)N$$

and

$$W_g(m, H, N) \ll (H/m + 1)N. \tag{3.1}$$

Our aim is to improve on these bounds in appropriate ranges of H and N.

3.2. Using exponential sum bounds and discrepancy

Our next result is based on treating the question of estimating $W_g(m, H, N)$ as a question of unifomity of distribution and hence we use the tools from Section 2.5.

Lemma 3.1. *Let $g \in \mathbb{Z}[T]$ be of degree $k \geqslant 2$. For any positive integers $H \leqslant m$ and N, we have*

$$W_g(m, H, N) = \frac{HN}{m} + O\left(N\left(\frac{1}{m} + \frac{1}{N} + \frac{m}{N^k}\right)^{\eta(k)} (mN)^{o(1)}\right)$$

where $\eta(k)$ is given by (1.3).

Proof. We observe that $W_g(m, H, N)$ is the number of fractional parts $\{g(n)/m\}$ which fall in the interval $[1 - H/m, 1]$. Hence, on taking $L = N$ in Lemma 2.6, we obtain

$$W_g(m, H, N) = \frac{HN}{m} + O(\Delta), \tag{3.2}$$

where

$$\Delta \ll 1 + \sum_{h=1}^{N} \frac{1}{h} \left| \sum_{n=1}^{N} \mathbf{e}_m\left(\frac{hg(n)}{m}\right) \right|. \tag{3.3}$$

Lemma 2.7 yields

$$\begin{aligned}
&\sum_{h=1}^{N} \frac{1}{h} \left| \sum_{n=1}^{N} \mathbf{e}_m\left(\frac{hg(n)}{m}\right) \right| \\
&\qquad \leqslant N^{1+o(1)} \sum_{h=1}^{N} \frac{1}{h} \left(\frac{\gcd(h,m)}{m} + \frac{1}{N} + \frac{m}{\gcd(h,m)N^k}\right)^{\eta(k)} \\
&\qquad \leqslant N^{1+o(1)} \sum_{h=1}^{N} \frac{1}{h} \left(\frac{\gcd(h,m)}{m} + \frac{1}{N} + \frac{m}{N^k}\right)^{\eta(k)} \\
&\qquad \leqslant N^{1+o(1)} \sum_{h=1}^{N} \frac{\gcd(h,m)^{\eta(k)}}{hm^{\eta(k)}} + N^{1+o(1)} \left(\frac{1}{N} + \frac{m}{N^k}\right)^{\eta(k)} \sum_{h=1}^{N} \frac{1}{h} \\
&\qquad = \frac{N^{1+o(1)}}{m^{\eta(k)}} \sum_{h=1}^{N} \frac{\gcd(h,m)^{\eta(k)}}{h} + N^{1+o(1)} \left(\frac{1}{N} + \frac{m}{N^k}\right)^{\eta(k)}.
\end{aligned}$$

Furthermore,

$$\begin{aligned}
\sum_{h=1}^{N} \frac{\gcd(h,m)^{\eta(k)}}{h} \leqslant \sum_{r \mid m} r^{\eta(k)} \sum_{\substack{h=1 \\ \gcd(h,m)=r}}^{N} \frac{1}{h} \leqslant \sum_{r \mid m} r^{\eta(k)} \sum_{1 \leqslant h \leqslant N/r} \frac{1}{hr} \\
\ll \tau(m) \log N.
\end{aligned}$$

Recalling (2.1), the lemma follows from (3.2) and (3.3). $\square$

3.3. Using the geometry of numbers

We now use Lemma 2.1 to estimate $U_k(q^2, H, N)$ on average over square-free integers q in a dyadic interval.

Lemma 3.2. *For $Q \geqslant 1$, we have*

$$\sum_{q \sim Q} \mu^2(q) U_k(q^2, H, N) \ll Z(NQ)^{o(1)},$$

where

$$Z = \frac{H^{k+1}N}{Q} + NQ + H^k Q + H^k N Q^{2/(k+1)}.$$

Proof. For $m, n \in \mathbb{N}$ we define the lattice

$$\Lambda_{m,n} = \left\{ \mathbf{a} \in \mathbb{Z}^{k+1} : \ \mathbf{a} \cdot \mathbf{n} \equiv 0 \pmod{m} \right\},$$

where $\mathbf{n} = \left(1, n, \ldots, n^k\right) \in \mathbb{N}^{k+1}$ and $\mathbf{a} \cdot \mathbf{n}$ is the scalar product. Note that $\Lambda_{m,n}$ has full rank and let $\Delta_{m,n}$ be the discriminant. We claim that

$$\Delta_{m,n} = m. \tag{3.4}$$

To see this we note that $m\mathbb{Z}^{k+1} \subseteq \Lambda_{m,n} \subseteq \mathbb{Z}^{k+1}$. Hence, since the discriminant of $\Lambda_{m,n}$ is the index of $\Lambda_{m,n}$ in $\mathbb{Z}^{k+1}$, we obtain

$$\Delta_{m,n} = [\mathbb{Z}^{k+1}, \Lambda_{m,n}] = \frac{[\mathbb{Z}^{k+1} : m\mathbb{Z}^{k+1}]}{[\Lambda_{m,n} : m\mathbb{Z}^{k+1}]}.$$

The numerator is m^{k+1} and denominator is the number of cosets of $\Lambda_{m,n}$ modulo m. Since $\gcd(\mathbf{n}, m) = \gcd(1, n, \ldots, n^k, m) = 1$, it follows that there are m^k values of $\mathbf{a}$ modulo m such that $\mathbf{a} \cdot \mathbf{n} \equiv 0 \pmod{m}$. The claim (3.4) is now clear.

By Lemma 2.1, we have

$$U_k(q^2, H, N) \ll \sum_{1 \leqslant n \leqslant N} \left(\frac{H^{k+1}}{q^2} + \frac{H^k}{s(q^2, n)^k} + 1 \right)$$

where $s(q^2, n)$ is the smallest successive minima of $\Lambda_{q^2,n}$. Therefore,

$$U_k(q^2, H, N) \ll \frac{H^{k+1}N}{q^2} + N + H^k S_k(q, N), \tag{3.5}$$

where

$$S_k(q, N) = \sum_{1 \leqslant n \leqslant N} \frac{1}{s(q^2, n)^k}.$$

Since $s(q^2, n)$ is the smallest successive minimum of $\Lambda_{q^2,n}$, it follows from (2.2) and (3.4) that $s(q^2, n)^{k+1} \ll \Delta_{q^2,n} = q^2$, whence

$$s(q^2, n) \leqslant q^{2/(k+1)}.$$

We now define an integer $I \ll \log Q$ by the inequalities

$$2^{I-1} < Q^{2/(k+1)} \leqslant 2^I$$

and write

$$S_k(q, N) \leqslant \sum_{i=0}^{I} \sum_{\substack{1 \leqslant n \leqslant N \\ s(q^2,n) \sim 2^i}} \frac{1}{s(q^2, n)^k} \ll \sum_{i=0}^{I} 2^{-ik} \sum_{\substack{1 \leqslant n \leqslant N \\ s(q^2,n) \sim 2^i}} 1. \tag{3.6}$$

Note that if $s(q^2, n) \leqslant t$ then there is a non-zero vector $\mathbf{c} \in \Lambda_{q^2,n}$ such that $\|\mathbf{c}\|_2 \leqslant t$. Therefore

$$\sum_{\substack{1 \leqslant n \leqslant N \\ s(q^2,n) \sim 2^i}} 1 \leqslant \sum_{\substack{\mathbf{c}=(c_0,\dots,c_k) \in \mathbb{Z}^{k+1} \\ 0 < \|\mathbf{c}\|_2 \leqslant 2^i}} \rho_{f_{\mathbf{c}}}(q^2, N), \tag{3.7}$$

where

$$f_{\mathbf{c}}(X) = c_0 + c_1 X + \cdots + c_k X^k$$

and

$$\rho_f(m, N) = \#\{n \in [1, N] : \ f(n) \equiv 0 \bmod m\}. \tag{3.8}$$

Using (3.6) and then changing the order of summation in (3.7), we obtain

$$\sum_{q \sim Q} \mu^2(q) S_k(q, N) \ll \sum_{i=0}^{I} 2^{-ik} R\left(Q, N, 2^i\right), \tag{3.9}$$

where

$$R(Q, N, t) = \sum_{\substack{\mathbf{c} \in \mathbb{Z}^{k+1} \\ 0 < \|\mathbf{c}\|_2 \leqslant t}} \sum_{q \sim Q} \mu^2(q) \rho_{f_{\mathbf{c}}}(q^2, N).$$

But clearly

$$\begin{aligned} R(Q, N, t) &\leqslant \sum_{\substack{\mathbf{c} \in \mathbb{Z}^{k+1} \\ 0 < \|\mathbf{c}\|_2 \leqslant t}} \sum_{q \leqslant Q} \sum_{\substack{n \leqslant N \\ q^2 \mid f_{\mathbf{c}}(n)}} 1 \\ &\leqslant \sum_{n \leqslant N} \sum_{\substack{\mathbf{c} \in \mathbb{Z}^{k+1} \\ \|\mathbf{c}\|_2 \leqslant t}} \#\left\{q \leqslant Q : \ q^2 \mid f_{\mathbf{c}}(n)\right\}. \end{aligned}$$

If $f_{\mathbf{c}}(n) = 0$ then there are Q choices for q. Let $\mathbf{c}$ be a non-zero vector such that $f_{\mathbf{c}}$ has a root over $\mathbb{Z}$. Then $f_{\mathbf{c}}$ must be reducible over $\mathbb{Z}$. There are at most $t^{k+o(1)}$ choices of non-zero vectors $\mathbf{c}$ for which $f_{\mathbf{c}}$ is reducible over $\mathbb{Z}$, on appealing to work of Kuba [20]. (See also [10] and the references therein.) Moreover, each such vector $\mathbf{c}$ yields at most k choices for n. If $f_{\mathbf{c}}(n) \neq 0$, on the other hand, then we have at most $(tN)^{o(1)}$ choices for q by the divisor bound (2.1). Hence we arrive at the bound

$$R(Q, N, t) \leqslant \left(Qt^k + Nt^{k+1}\right)(Nt)^{o(1)}.$$

On returning to (3.9), we therefore obtain

$$\sum_{q \sim Q} \mu^2(q) S_k(q, N) \leqslant \sum_{i=0}^{I} \left(Q + N2^i\right)(2^i Q)^{o(1)}$$
$$\leqslant \left(Q + NQ^{2/(k+1)}\right) Q^{o(1)}.$$

We substitute this into (3.5) and sum over q. This yields

$$\sum_{q \sim Q} \mu^2(q) U_k(q^2, H, N) \leqslant \frac{H^{k+1}N}{Q} + NQ + \left(Q + NQ^{2/(k+1)}\right) H^k (NQ)^{o(1)},$$

and the result now follows. □

4. Proofs of main results

4.1. Proof of Theorem 1.1

Fix a choice of $A \geqslant 1$. We proceed under the assumption that $N^{1/k} \leqslant H \leqslant N^A$, and allow all of our implied constants to depend on A. There are $O(H^{k+o(1)})$ choices of polynomials $f \in \mathcal{F}_k(H)$ for which f fails to be irreducible, the latter bound following from work of Kuba [20], as in the proof of Lemma 3.2. The overall contribution from such f is therefore $O(H^{k+o(1)}N)$. We may henceforth restrict to the set $\mathcal{F}_k^*(H)$ of irreducible polynomials $f \in \mathcal{F}_k(H)$.

Our argument proceeds along standard lines, beginning with an application of Möbius inversion to interpret

$$\mu^2(n) = \sum_{d^2 \mid n} \mu(d)$$

as a sum over divisors. This leads to the expression

$$S_f(H) = \sum_{d \ll \sqrt{HN^k}} \mu(d) \rho_f(d^2, N),$$

where $\rho_f(m,N)$ is given by (3.8). Hence, for arbitrary $E \geqslant D \geqslant 1$, we have

$$S_f(N) = M_f(N) + O(R_f^{(1)}(N)) + O(R_f^{(2)}(N)),$$

where

$$M_f(N) = \sum_{d \leqslant D} \mu(d)\rho_f(d^2, N)$$

and

$$R_f^{(1)}(N) = \sum_{D<d\leqslant E} \mu^2(d)\rho_f(d^2,N), \quad R_f^{(2)}(N) = \sum_{E<d\ll\sqrt{HN^k}} \mu^2(d)\rho_f(d^2,N).$$

To begin with, it is shown in [25, Equation (4.8)] that

$$M_f(N) = c_f N + O\left(DH^{o(1)} + ND^{-1}H^{o(1)}\right), \tag{4.1}$$

where the implied constant in this estimate depends only on k.

Next, on recalling the notation $Q_f(S,N)$ that has been defined in Section 2.4, we may write

$$R_f^{(2)}(N) \leqslant Q_f(S,N) + Q_{-f}(S,N),$$

for some $S \ll HN^k/E^2$. Thus, Lemma 2.5 implies that

$$R_f^{(2)}(N) \leqslant \left(N^{1/2}\left(\frac{HN^k}{E^2}\right)^{1/2} + \frac{HN^k}{E^2}\right)(HN)^{o(1)}. \tag{4.2}$$

Turning to the remaining error term $R_f^{(1)}(N)$, we are only able to estimate it well on average over $f \in \mathcal{F}_k^*(H)$. Recall the definition of $U_k(d^2,H,N)$ from Section 3.1. On changing the order of summation, we obtain

$$\sum_{f\in\mathcal{F}_k^*(H)} R_f^{(1)}(N) \leqslant \sum_{D<d\leqslant E} \mu^2(d)U_k(d^2,H,N).$$

To estimate the right hand side, we use Lemma 3.2. After splitting the summation range in dyadic intervals, we derive

$$\sum_{f\in\mathcal{F}_k^*(H)} R_f^{(1)}(N) \leqslant \left(\frac{H^{k+1}N}{D} + NE + H^kE + H^kNE^{2/(k+1)}\right)H^{o(1)}.$$

Since we are assuming $N \leqslant H^k$, we may drop the second term in this estimate. Hence

$$\sum_{f\in\mathcal{F}_k^*(H)} R_f^{(1)}(N) \leqslant \left(\frac{H^{k+1}N}{D} + H^kE + H^kNE^{2/(k+1)}\right)H^{o(1)}. \tag{4.3}$$

On accounting for the $O(H^{k+o(1)})$ choices of $f \in \mathcal{F}_k(H) \setminus \mathcal{F}_k^*(H)$, it therefore follows from (4.1)–(4.3) that

$$\begin{aligned}\sum_{f\in\mathcal{F}_k(H)} |S_f(N) - c_fN| \leqslant\ & H^{k+o(1)}N + \left(D + ND^{-1}\right)H^{k+1+o(1)} \\ & + \left(N^{1/2}\left(\frac{HN^k}{E^2}\right)^{1/2} + \frac{HN^k}{E^2}\right)H^{k+1+o(1)} \\ & + \left(\frac{H^{k+1}N}{D} + H^kE + H^kNE^{2/(k+1)}\right)H^{o(1)}.\end{aligned}$$

Hence, on noting that $\#\mathcal{F}_k(H) \gg H^{k+1}$, it follows that

$$\frac{1}{\#\mathcal{F}_k(H)}\sum_{f\in\mathcal{F}_k(H)} |S_f(N) - c_fN| \leqslant \Delta H^{o(1)},$$

where

$$\Delta = D + \frac{N}{D} + \frac{E}{H} + \frac{NE^{2/(k+1)}}{H} + \frac{H^{1/2}N^{(k+1)/2}}{E} + \frac{HN^k}{E^2}.$$

We take $D = N^{1/2}$, leading to

$$\frac{1}{\#\mathcal{F}_k(H)}\sum_{f\in\mathcal{F}_k(H)} |S_f(N) - c_fN| \leqslant \Delta_0H^{o(1)},$$

where

$$\Delta_0 = \inf_{\sqrt{N}\leqslant E\ll\sqrt{HN^k}} \Delta_0(E)$$

and

$$\Delta_0(E) = N^{1/2} + \frac{E}{H} + \frac{NE^{2/(k+1)}}{H} + \frac{H^{1/2}N^{(k+1)/2}}{E} + \frac{HN^k}{E^2}.$$

We expect the dominant contribution to come from the second and fourth terms and so we choose

$$E = \min\left\{H^{3/4}N^{(k+1)/4}, \sqrt{HN^k}\right\},$$

in order to minimise their contribution. Note that $E \geqslant \sqrt{N}$ with this choice. This therefore leads to the bound

$$\Delta_0 \ll N^{1/2} + \frac{N^{(k+1)/4}}{H^{1/4}} + \frac{N^{3/2}}{H^{1-3/(2k+2)}} + \frac{N^{(k-1)/2}}{H^{1/2}},$$

which thereby concludes the proof of the following result.

Theorem 4.1. *Let $A \geqslant 1$ and $k \geqslant 2$ be fixed and assume that $H, N \to \infty$ in such a way that $N^{1/k} \leqslant H \leqslant N^A$. Then we have*

$$\frac{1}{\#\mathcal{F}_k(H)} \sum_{f \in \mathcal{F}_k(H)} |S_f(N) - c_f N| \leqslant \left(N^{1/2} + \frac{N^{(k+1)/4}}{H^{1/4}} + \frac{N^{3/2}}{H^{1-3/(2k+2)}} + \frac{N^{(k-1)/2}}{H^{1/2}}\right) H^{o(1)}.$$

To deduce Theorem 1.1 we assume that $k \geqslant 4$ and proceed to assess when each of the terms is $O(N^{1-\delta})$ for some $\delta > 0$. The first term is obviously satisfactory. One sees that the second term and fourth terms are satisfactory if $H \geqslant N^{k-3+\varepsilon}$ for some $\varepsilon > 0$. Finally, the third term is only satisfactory if $H \geqslant N^{1/2+3/(4k-2)+\varepsilon}$, but this is implied by the latter condition. This completes the proof of Theorem 1.1.

4.2. Proof of Theorem 1.2

The aim of this section is to estimate the quantity

$$\Sigma = \sum_{f \in \mathcal{G}_g(H)} |S_f(N) - c_f N| .$$

It is convenient to define

$$M = \max\{H, N^k\},$$

so that $f(n) = a + g(n) = O(M)$ if $f \in \mathcal{G}_g(H)$ and $1 \leqslant n \leqslant N$. Mimicking the previous argument and using (4.1), we obtain

$$\Sigma \leqslant DH^{1+o(1)} + \frac{NH^{1+o(1)}}{D} + \sum_{D<d\leqslant c\sqrt{M}} W_g(d^2, H, N), \tag{4.4}$$

where $c > 0$ is a constant depending only on the polynomial g and $W_g(d^2, H, N)$ is defined in Section 3.1.

Suppose first that $H \geqslant N^k$. Then we simply apply (3.1) and get

$$\begin{aligned}\Sigma &\ll DH^{1+o(1)} + \frac{NH^{1+o(1)}}{D} + \sum_{D<d\leqslant c\sqrt{H}} (H/d^2 + 1)N \\ &\leqslant \left(DH + \frac{HN}{D} + H^{1/2}N\right) H^{o(1)}.\end{aligned}$$

Taking $D = N^{1/2}$, we derive

$$\Sigma \leqslant \left(HN^{1/2} + H^{1/2}N\right) H^{o(1)} \leqslant H^{1+o(1)}N^{1/2}, \tag{4.5}$$

if $H \geqslant N^k$.

We may henceforth assume that $H \leqslant N^k$ and thus $M = N^k$. We now choose $D = N^{1/2}$ and two more parameters F and E with $F \geqslant E \geqslant N^{1/2}$. Then we may write

$$\sum_{N^{1/2} < d \leqslant c\sqrt{M}} W_g(d^2, H, N) = \mathfrak{W}_1 + \mathfrak{W}_2 + \mathfrak{W}_3 \tag{4.6}$$

where

$$\mathfrak{W}_1 = \sum_{N^{1/2} < d \leqslant E} W_k(d^2, H, N),$$
$$\mathfrak{W}_2 = \sum_{E < d \leqslant F} W_k(d^2, H, N),$$
$$\mathfrak{W}_3 = \sum_{F < d \leqslant cN^{k/2}} W_k(d^2, H, N).$$

To begin with, we appeal to (3.1) to estimate

$$\mathfrak{W}_1 \ll \sum_{N^{1/2} < d \leqslant E} (H/d^2 + 1)N \ll HN^{1/2} + EN. \tag{4.7}$$

It is convenient to choose $E = \max\{H^{1/2}, N^{1/2}\}$, so that

$$\mathfrak{W}_1 \ll HN^{1/2} + H^{1/2}N. \tag{4.8}$$

Indeed, for $H \leqslant N$ we have $E = N^{1/2}$ and thus $\mathfrak{W}_1 = 0$, while for $H > N$ we have $E = H^{1/2}$ and (4.8) follows from (4.7).

Therefore, combining (4.4), (4.6) and (4.8), we obtain

$$\Sigma \ll H^{1+o(1)}N^{1/2} + H^{1/2}N + \mathfrak{W}_2 + \mathfrak{W}_3. \tag{4.9}$$

It remains to estimate $\mathfrak{W}_2$ and $\mathfrak{W}_3$.

To estimate $\mathfrak{W}_2$ we appeal to Lemma 3.1 to derive

$$\mathfrak{W}_2 \ll \sum_{E < d \leqslant F} \left(\frac{HN}{d^2} + N^{1+o(1)} \left(\frac{1}{d^2} + \frac{1}{N} + \frac{d^2}{N^k} \right)^{\eta(k)} \right),$$

where $\eta(k)$ is given by (1.3). Therefore, noticing that we have

$$\frac{1}{d^2} < \frac{1}{N}$$

for $d > E \geqslant N^{1/2}$, we obtain

$$\begin{aligned}\mathfrak{W}_2 &\ll HN/E + FN^{1-\eta(k)+o(1)} + F^{1+2\eta(k)}N^{1-k\eta(k)+o(1)} \\ &\leqslant HN^{1/2} + FN^{1-\eta(k)+o(1)} + F^{1+2\eta(k)}N^{1-k\eta(k)+o(1)}.\end{aligned} \tag{4.10}$$

Finally, as in the proof of Theorem 4.1, we treat $\mathfrak{W}_3$ via Lemma 2.5. Recalling our assumption $H \leqslant N^k$ and observing that there are $O(1)$ choices of $f \in \mathcal{G}_g(H)$ that fail to be irreducible, we derive

$$\begin{aligned}\mathfrak{W}_3 &\leqslant \left(N + HN^{1/2}\left(N^k/F^2\right)^{1/2} + HN^k/F^2\right)N^{o(1)} \\ &\leqslant \left(N + HN^{(k+1)/2}/F + HN^k/F^2\right)N^{o(1)}.\end{aligned} \tag{4.11}$$

We now observe that if $N^{(k+1)/2}/F \geqslant N$, which is equivalent to $F \leqslant N^{(k-1)/2}$, then the bound becomes trivial. Thus we always assume that

$$F \geqslant N^{(k-1)/2},$$

in which case we see that the third term in (4.11) is dominated by the second term.

Substituting the bounds (4.10) and (4.11) in (4.9), we are led to the upper bound

$$\Sigma \leqslant \left(HN^{1/2} + H^{1/2}N + FN^{1-\eta(k)} + F^{1+2\eta(k)}N^{1-k\eta(k)} + HN^{(k+1)/2}/F\right)H^{o(1)}.$$

Since $F \geqslant N^{(k-1)/2}$, we see that $FN^{1-\eta(k)} \leqslant F^{1+2\eta(k)}N^{1-k\eta(k)}$ and so

$$\Sigma \leqslant \left(HN^{1/2} + H^{1/2}N + F^{1+2\eta(k)}N^{1-k\eta(k)} + HN^{(k+1)/2}/F\right)H^{o(1)}. \tag{4.12}$$

To optimise (4.12), we choose

$$F = \max\left\{\left(HN^{(k-1)/2+k\eta(k)}\right)^{1/(2+2\eta(k))}, N^{(k-1)/2}\right\}$$

for which

$$\begin{aligned}F^{1+2\eta(k)}N^{1-k\eta(k)} &= HN^{(k+1)/2}/F \\ &= H^{1-\frac{1}{2+2\eta(k)}}N^{(k+3)/4-\frac{(k+1)\eta(k)}{4+4\eta(k)}}.\end{aligned}$$

After substitution in (4.12), this completes our treatment of the case $H \leqslant N^k$. Taken together with (4.5), and observing that $\#\mathcal{G}_g(H) \gg H$, this therefore concludes the proof of the following theorem.

Theorem 4.2. *For a fixed polynomial $g \in \mathbb{Z}[X]$ of degree $k \geqslant 2$, we have*

$$\frac{1}{\#\mathcal{G}_g(H)} \sum_{f \in \mathcal{G}_g(H)} |S_f(N) - c_f N| \leqslant \left(N^{1/2} + \frac{N}{H^{1/2}} + \frac{N^{(k+1)/2-\eta(k)}}{H} + \frac{N^{(k+3)/4-\frac{(k+1)\eta(k)}{4+4\eta(k)}}}{H^{\frac{1}{2+2\eta(k)}}} \right) H^{o(1)},$$

where $\eta(k)$ is given by (1.3).

Finally, to deduce Theorem 1.2 we need to discover when each of the terms is $O(N^{1-\delta})$ for some $\delta > 0$. The first term is obviously satisfactory. One sees that the second term is satisfactory if $H \geqslant N^{\varepsilon}$ for any $\varepsilon > 0$. Finally, the fourth term is only satisfactory if $H \geqslant N^{(k-1)/2+\eta(k)+\varepsilon}$, under which assumption the third term is also satisfactory. This therefore completes the proof of Theorem 1.2.

Data availability

No data was used for the research described in the article.

References

[1] S. Baier, L. Zhao, Primes in quadratic progressions on average, Math. Ann. 338 (2007) 963–982.
[2] R.C. Baker, M. Munsch, I.E. Shparlinski, Additive energy and a large sieve inequality for sparse sequences, Mathematika 68 (2022) 362–399.
[3] F. Balestrieri, N. Rome, Average Bateman–Horn for Kummer polynomials, Acta Arith. 207 (2023) 315–350.
[4] J. Bourgain, On the Vinogradov mean value, Proc. Steklov Math. Inst. 296 (2017) 30–40.
[5] J. Bourgain, C. Demeter, L. Guth, Proof of the main conjecture in Vinogradov's mean value theorem for degrees higher than three, Ann. Math. 184 (2016) 633–682.
[6] T. Browning, E. Sofos, J. Teräväinen, Bateman-Horn, polynomial Chowla and the Hasse principle with probability 1, Preprint, arXiv:2212.10373 [arxiv.org/abs/2212.10373], 2022.
[7] J.W.S. Cassels, An Introduction to the Geometry of Numbers, Springer, Berlin, 1971.
[8] M.–C. Chang, J. Cilleruelo, M.Z. Garaev, J. Hernández, I.E. Shparlinski, A. Zumalacárregui, Points on curves in small boxes and applications, Mich. Math. J. 63 (2014) 503–534.
[9] J. Cilleruelo, M.Z. Garaev, A. Ostafe, I.E. Shparlinski, On the concentration of points of polynomial maps and applications, Math. Z. 272 (2012) 825–837.
[10] A. Dubickas, Bounding univariate and multivariate reducible polynomials with restricted height, Period. Math. Hung. 78 (2019) 98–109.
[11] M. Filaseta, Squarefree values of polynomials, Acta Arith. 60 (1992) 213–231.
[12] T. Foo, L. Zhao, On primes represented by cubic polynomials, Math. Z. 274 (2013) 323–340.
[13] O. Garcia-Morchon, R. Rietman, I.E. Shparlinski, L. Tolhuizen, Interpolation and approximation of polynomials in finite fields over a short interval from noisy values, Exp. Math. 23 (2014) 241–260.
[14] A. Granville, ABC allows us to count squarefrees, Int. Math. Res. Not. 19 (1998) 991–1009.
[15] D.R. Heath-Brown, Counting rational points on algebraic varieties, in: Analytic Number Theory, in: Lecture Notes in Math., vol. 1891, Springer, Berlin, 2006, pp. 51–95.
[16] C. Hooley, On the power-free values of polynomials, Mathematika 14 (1967) 21–26.
[17] H. Iwaniec, E. Kowalski, Analytic Number Theory, Amer. Math. Soc., Providence, RI, 2004.
[18] P. Jelinek, Square-free values of polynomials on average, Preprint, arXiv:2308.15146 [https://arxiv.org/abs/2308.15146], 2023.

[19] B. Kerr, A. Mohammadi, Points on polynomial curves in small boxes modulo an integer, J. Number Theory 223 (2021) 64–78.
[20] G. Kuba, On the distribution of reducible polynomials, Math. Slovaca 59 (2009) 349–356.
[21] L. Kuipers, H. Niederreiter, Uniform Distribution of Sequences, Wiley-Intersci, New York-London-Sydney, 1974.
[22] F. Luca, I.E. Shparlinski, Quadratic fields generated by polynomials, Arch. Math. 91 (2008) 399–408.
[23] T. Reuss, Power-free values of polynomials, Bull. Lond. Math. Soc. 47 (2015) 270–284.
[24] W. Schmidt, Asymptotic formulae for point lattices of bounded determinant and subspaces of bounded height, Duke Math. J. 35 (1968) 327–339.
[25] I.E. Shparlinski, On the average number of square-free values of polynomials, Can. Math. Bull. 56 (2013) 844–849.
[26] A.N. Skorobogatov, E. Sofos, Schinzel hypothesis on average and rational points, Invent. Math. 231 (2023) 673–739.
[27] C.L. Stewart, On the number of solutions of polynomial congruences and Thue equations, J. Am. Math. Soc. 4 (1991) 793–835.
[28] T.D. Wooley, The cubic case of the main conjecture in Vinogradov's mean value theorem, Adv. Math. 294 (2016) 532–561.
[29] T.D. Wooley, Nested efficient congruencing and relatives of Vinogradov's mean value theorem, Proc. Lond. Math. Soc. 118 (2019) 942–1016.