Max-Planck-Institut für Mathematik
Bonn

A note on the squarefree density of polynomials

by

Robert C. Vaughan
Yuriy G. Zarhin

Max-Planck-Institut für Mathematik
Preprint Series 2023 (29)

Date of submission: December 10, 2023

A note on the squarefree density of polynomials

by

Robert C. Vaughan
Yuriy G. Zarhin

Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn
Germany

Department of Mathematics
Pennsylvania State University
University Park, PA 16802
USA

MPIM 23-29

A NOTE ON THE SQUAREFREE DENSITY OF POLYNOMIALS

R. C. VAUGHAN AND YU. G. ZARHIN

ABSTRACT. The conjectured squarefree density of an integral polynomial $\mathcal{P}$ in s variables is an Euler product $\mathfrak{S}_{\mathcal{P}}$ which can be considered as a product of local densities. We show that a necessary and sufficient condition for $\mathfrak{S}_{\mathcal{P}}$ to be 0 when $\mathcal{P} \in \mathbb{Z}(X_1, \ldots, X_s)$ is a polynomial in s variables over the integers, is that the polynomial is not squarefree as a polynomial. We also show that generally the upper squarefree density $\mathfrak{D}_{\mathcal{P}}$ satisfies $\mathfrak{D}_{\mathcal{P}} \le \mathfrak{S}_{\mathcal{P}}$.

1. INTRODUCTION

There is a long history of research into the squarefree density of polynomials in one, or more, variables. The progenitor of such conclusions is the famous estimate

$$\sum_{n \le X} \mu(n)^2 = \frac{6}{\pi^2} X + O\big(X^{1/2}\big)$$

of Gegenbauer [1885]. Let $\mathcal{P} \in \mathbb{Z}[X_1, \ldots, X_s]$ be a polynomial with integers coefficients and total degree

$$d = \deg(\mathcal{P}) \ge 2$$

and let for any integer $m > 1$

$$\rho_{\mathcal{P}}(m) = \mathrm{card}\{\mathbf{x} \in \mathbb{Z}^s/m\mathbb{Z}^s = (\mathbb{Z}/m\mathbb{Z})^s : \mathcal{P}(\mathbf{x}) \equiv 0 \pmod{m}\}. \tag{1.1}$$

Given $P_j \in \mathbb{R}$, $P_j \ge 1$ $(j = 1, \ldots s)$ and $h \in \mathbb{Z}$, we define

$$\mathbf{P} = \{\mathbf{x} = (x_1, \ldots, x_s) \mid x_j \in [-P_j, P_j] \cap \mathbb{Z}\}, \quad r_{\mathcal{P}}(h) = \mathrm{card}\{\mathbf{x} \in \mathbf{P} \mid \mathcal{P}(\mathbf{x}) = h\}. \tag{1.2}$$

Then we extend the definition of the Möbius function μ by taking $\mu(0) = 0$ and define

$$N_{\mathcal{P}}(\mathbf{P}) = \sum_{h \in \mathbb{Z}} \mu(|h|)^2 r_{\mathcal{P}}(h), \tag{1.3}$$

the number of squarefree values of $\mathcal{P}(\mathbf{x})$ with

$$\mathbf{x} \in \mathbf{P} = \mathbb{Z}^s \cap \prod_{j=1}^{s} [-P_j, P_j].$$

Research of RCV is partially supported by the Simons Foundation Collaboration Grant OSP1857531.

Research of YGZ is partially supported by the Simons Foundation Collaboration Grant # 585711. Part of this work was done during his stay at the Max-Planck Institut für Mathematik (Bonn, Germany), whose hospitality and support are gratefully acknowledged.

AMS Mathematics Subject Classification 2020: 11E76, 11N25, 11N32.

It is readily conjectured that

$$N_{\mathcal{P}}(\mathbf{P}) \sim 2^s P_1 \dots P_s \mathfrak{S}_{\mathcal{P}} \text{ as } \min_j P_j \to \infty \tag{1.4}$$

where

$$\mathfrak{S}_{\mathcal{P}} = \prod_p \left(1 - \frac{\rho_{\mathcal{P}}(p^2)}{p^{2s}}\right). \tag{1.5}$$

Here p runs through the set of all primes.

There is a considerable body of work on various special cases, some even quite general. See, for example, Bhargava [2014], Bhargava *et al* [2022], Filaseta [1994], Greaves [1992], Hooley [1967], [1977], [2009a],[2009b], Kowalski [2020], [2021], Kowalski and Vaughan [2023], Lapkova and Xiao [2021], Poonen [2003] Sanjaya and Wang [2023] and Uchiyama [1972]. In Kowalski and Vaughan [2023] it was noted that

$$\prod_{p\le n} \left(1 - \frac{\rho_{\mathcal{P}}(p^2)}{p^{2s}}\right)$$

is a non-negative decreasing sequence so it converges as $n \to \infty$ to a non-negative limit.

It seems that (1.4) should hold in all cases. Thus if $\mathcal{P}$ is such that it has a shortage of squarefree values, then we expect that

$$\mathfrak{S}_{\mathcal{P}} = 0. \tag{1.6}$$

Indeed the converse case (1.4) is easy to prove. See for instance Theorem 1.3 of Kowalski and Vaughan *ibidem*.

Let

$$\mathcal{P} \in \mathbb{Z}[X_1, \dots, X_s] \tag{1.7}$$

be a nonzero polynomial of degree d, which, except where otherwise stated explicitly, we will suppose satisfies $d \ge 2$.

Theorem 1.1. *For a polynomial $\mathcal{P}$ satisfying (1.7) and $s \ge 1$ we have*

$$\mathfrak{S}_{\mathcal{P}} = 0 \tag{1.8}$$

if and only if one of the following holds.

(a) There is a prime p such that $\mathcal{P}(a_1, \dots, a_s) \in p^2\mathbb{Z}$ for all $a_1, \dots, a_s \in \mathbb{Z}$.

(b) There are polynomials $\mathcal{L}_1, \mathcal{L}_2 \in \mathbb{Z}[x_1, \dots, x_s]$ such that $\deg(\mathcal{L}_2) \ge 1$ *and*

$$\mathcal{P}(\mathbf{x}) = \mathcal{L}_1(\mathbf{x})\mathcal{L}_2(\mathbf{x})^2. \tag{1.9}$$

In addition, if $d = \deg(\mathcal{P})$ is odd, then $\deg(\mathcal{L}_1) \ge 1$.

As an immediate corollary we have

Corollary 1.2. *If $\mathcal{P}$ satisfies (a), then*

$$N_{\mathcal{P}}(\mathbf{P}) = 0. \tag{1.10}$$

If it satisfies (b), then

$$N_{\mathcal{P}}(\mathbf{P}) \ll \frac{P_1 \dots P_s}{\min(P_1, \dots, P_s)}. \tag{1.11}$$

This improves upon Theorem 1.3 of Kowalski and Vaughan.

Let $\mathfrak{d}_{\mathcal{P}}$ and $\mathfrak{D}_{\mathcal{P}}$ denote the lower and upper densities

$$\mathfrak{d}_{\mathcal{P}} = \liminf_{\min\{P_1,\dots,P_s\}\to\infty} \frac{N_{\mathcal{P}}(\mathbf{P})}{2^s P_1 \dots P_s}$$

and

$$\mathfrak{D}_{\mathcal{P}} = \limsup_{\min\{P_1,\dots,P_s\}\to\infty} \frac{N_{\mathcal{P}}(\mathbf{P})}{2^s P_1 \dots P_s}$$

respectively. Then we have the following further consequence of Theorem 1.1 that will be proven in Section 4.

Corollary 1.3. *We have $\mathfrak{D}_{\mathcal{P}} \le \mathfrak{S}_{\mathcal{P}}$ and in particular if $\mathfrak{D}_{\mathcal{P}} > 0$, then $\mathfrak{S}_{\mathcal{P}} > 0$ and $\mathcal{P}$ is not of the kind described in (a) and (b) of Theorem 1.1.*

One can speculate as to whether it is possible to prove that $\mathfrak{d}_{\mathcal{P}} > 0$ without showing that $\mathfrak{d}_{\mathcal{P}} = \mathfrak{D}_{\mathcal{P}} = \mathfrak{S}_{\mathcal{P}} > 0$.

Remark 1.4. *In the course of the proof of Theorem 1.1, we will use induction on s. We may and will assume that all the variables appear in $\mathcal{P}$ explicitly, i.e., all the partial derivatives*

$$\mathcal{P}_j := \frac{\partial \mathcal{P}}{\partial x_j} \in \mathbb{Z}[x_1, \dots, x_s] \ (1 \le j \le s)$$

are **nonzero** *polynomials of degree $\le d-1$. Indeed, if not we can reduce to the case $s-1$ and use the induction assumption.*

With regard to notation we follow that enunciated by Schmidt [2004] in that quite often $x, y, z, \dots$ will be elements which lie in a ground field or are algebraic over a ground field, and $X, Y, Z, \dots$ will be algebraically independent over a ground field.

2. Proof of Theorem 1.1

In what follows we freely use standard classical results about convergence of infinite products, see G. M. Fikhtengol'ts [1965, Ch. 15, Sect. 5, Subsect. 250]. We will also need the following assertion that will be proven in Section 3

Lemma 2.1. *Let $s \ge 2$ and d be positive integers, and $f(X_1, \dots, X_s) \in \mathbb{Z}[X_1, \dots, X_s]$ be a nonzero polynomial of degree d. Then there are a set of primes $S = S(f)$ and positive real numbers $\delta = \delta(f)$ and $Q = Q(f)$ such that*

$$\rho_f(p) \ge \frac{1}{2} p^{s-1} \text{ for } p \in S(f) \tag{2.1}$$

and

$$\pi_S(R) = \mathrm{card}\{p \le R : p \in S\} \ge \frac{\delta R}{\log R} \text{ for } R \ge Q. \tag{2.2}$$

Now let us start the proof of Theorem 1.1. We first deal with the situation when (a) or (b) hold. If (a) holds, then at once $\rho_{\mathcal{P}}(p^2) = p^{2s}$ and so (1.8) holds trivially.

Let us assume that (a) does *not* hold but (b) holds. Then obviously

$$p^{2s} > \rho_{\mathcal{P}}(p^2) \geq \rho_{\mathcal{L}_2^2}(p^2) = \rho_{\mathcal{L}_2}(p) \cdot p^s. \tag{2.3}$$

Applying Lemma 2.1 with $f = \mathcal{L}_2$, we conclude that there is a set $S = S(\mathcal{L}_2)$ of primes p and positive real numbers δ and Q such that

$$\rho_{\mathcal{L}_2}(p) \geq \frac{1}{2}p^{s-1} \text{ for } p \in S \text{ and } \pi_S(R) > \frac{\delta R}{\log R} \text{ for } R \geq Q. \tag{2.4}$$

Combining the inequalities (2.3) and (2.4), when $p \in S$ we have

$$p^{2s} > \rho_{\mathcal{P}}(p^2) \geq \frac{1}{2}p^{2s-1}.$$

Thus

$$\begin{aligned}\prod_p \left(1 - \frac{\rho_{\mathcal{P}}(p^2)}{p^{2s}}\right) &\leq \prod_{p\in S(\mathcal{P})} \exp\left(\log\left(1 - \frac{\rho_{\mathcal{P}}(p^2)}{p^{2s}}\right)\right) \\ &\leq \exp\left(-\sum_{p\in S}\frac{1}{2p}\right)\end{aligned}$$

since $\log(1-z) \leq -z$ when $z < 1$. Now

$$\begin{aligned}\sum_{\substack{p\leq R\\ p\in S}} \frac{1}{2p} &= \sum_{\substack{p\leq R\\ p\in S}} \left(\frac{1}{2R} + \int_p^R \frac{dt}{2t^2}\right) \\ &= \frac{\pi_S(R)}{2R} + \int_1^R \frac{\pi_S(t)}{2t^2}dt \\ &\geq \int_Q^R \frac{\delta}{2t\log t}dt \\ &= \frac{\delta}{2}\log\frac{\log R}{\log Q} \\ &\to \infty \text{ as } R \to \infty.\end{aligned}$$

Thus

$$\prod_{p\in S}\left(1 - \frac{\rho_{\mathcal{P}}(p^2)}{p^{2s}}\right) = 0.$$

It follows readily that (1.8) holds.

Now suppose that (1.8) holds. One possibility is that there is a prime p such that

$$\rho_{\mathcal{P}}(p^2) = p^{2s}.$$

Thus

$$\mathcal{P}(a_1, \ldots, a_s) \equiv 0 \pmod{p^2}$$

for every $a_1, \dots, a_s \in \mathbb{Z}$, which means that (a) holds.

Thus we may henceforward suppose that (a) is false, (1.8) holds and that for all primes p we have

$$\rho_{\mathcal{P}}(p^2) < p^{2s}. \tag{2.5}$$

We need to prove that (b) holds.

At this stage it is useful to transform the polynomial so that at least one of the variables, for example X_1, has non-zero X_1^d term.

Lemma 2.2. *Given a nonzero form $\mathcal{P}_d$ (1.7) of degree $d \geq 1$, there is a unimodular transformation*

$$\mathcal{T} = \begin{pmatrix} 1 & t_2 & \cdots & t_s \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix},$$

$$\mathbf{X} = (X_1, \dots X_s) \mapsto \mathbf{X}\mathcal{T} = (X_1, t_2X_1 + X_2, \dots, t_sX_1 + X_s)$$

so that all $t_2, \dots, t_s$ are integers and

$$\mathcal{P}_d(\mathbf{X}\mathcal{T}) = \mathcal{P}^*(\mathbf{X})$$

where

$$\mathcal{P}_d^*(\mathbf{X}) = aX_1^d + \sum_{k=1}^{d} F_k X_1^{d-k}, \tag{2.6}$$

the integer

$$a = \mathcal{P}_d(1, t_2, \dots, t_s) \neq 0$$

and each $F_k \in \mathbb{Z}[X_2, \dots X_s]$ is a degree k form in $X_2, \dots, X_s$ with integer coefficients.

Proof. The proof is essentially inductive on d. The case $d = 1$ is easy. Suppose $d \geq 2$ and the lemma is established with d replaced by $d - 1$. When $\mathcal{P}_d$ is divisible by X_1 in $\mathbb{Z}[X_1, \dots X_s]$ the inductive hypothesis at once gives the desired conclusion. Thus we may assume that $\mathcal{P}_d$ is not divisible by X_1 in $\mathbb{Z}[X_1, \dots X_s]$, i.e.,

$$\mathcal{P}_d(0, X_2, \dots, X_s) \not\equiv 0.$$

We now argue by contradiction. Suppose on the contrary that $\mathcal{P}_d(1, t_2, \dots, t_s) = 0$ for all integers $t_2, \dots, t_s$. Since $\mathcal{P}_d$ is a form, it follows that

$$\mathcal{P}_d\left(\frac{1}{N}, \frac{t_2}{N}, \dots, \frac{t_s}{N}\right) = \frac{1}{N^d}\mathcal{P}_d(1, t_2, \dots, t_s) = 0$$

for any positive integer N. Let $r_2, \dots r_s \in \mathbb{R}$ be any $(s-1)$-tuple of real numbers. There exist integers $t_{2,N}, \dots, t_{s,N}$ such that

$$\left| r_j - \frac{t_{j,N}}{N} \right| \leq \frac{1}{N} \; \forall j = 2, \dots s.$$

Since $\mathcal{P}_d$ is a continuous function on $\mathbb{R}^s$,

$$\mathcal{P}_d(0, r_2, \dots, r_s) = \lim_{N\to\infty} \mathcal{P}_d\left(\frac{1}{N}, \frac{t_{2,N}}{N}, \dots, \frac{t_{s,N}}{N}\right) = 0,$$

which implies that the form $\mathcal{P}_d(0, X_2, \dots, X_s) \equiv 0$. This gives us a contradiction that proves the desired result. $\square$

Let us return to the case of an arbitrary nonzero polynomial $\mathcal{P} \in \mathbb{Z}[X_1, \dots X_s]$ of degree d and present $\mathcal{P}$ as a sum

$$\mathcal{P} = \sum_{i=0}^{d} \mathcal{P}_i$$

of degree i forms $\mathcal{P}_i \in \mathbb{Z}[X_1, \dots X_s]$. Notice that $\mathcal{P}_d \neq 0$. Applying to $\mathcal{P}_d$ Lemma 2.2, we conclude that there is a unimodular transformation

$$\mathbf{X} = (X_1, \dots X_s) \mapsto \mathbf{X}\mathcal{T} = (X_1, t_2X_1 + X_2, \dots, t_sX_1 + X_s)$$

so that all $t_2, \dots, t_s$ are integers and

$$\mathcal{P}(\mathbf{X}\mathcal{T}) = \mathcal{P}^*(\mathbf{X})$$

where

$$\mathcal{P}^*(\mathbf{X}) = aX_1^d + \sum_{k=1}^{d} F_k X_1^{d-k}, \tag{2.7}$$

the integer

$$a = \mathcal{P}_d(1, t_2, \dots, t_s) \neq 0$$

and each $F_k \in \mathbb{Z}[X_2, \dots X_s]$ is a polynomial of degree $\leq k$ in $X_2, \dots, X_s$ with integer coefficients.

Clearly, $\rho_{\mathcal{P}}(p^2) = \rho_{\mathcal{P}^*}(p^2)$ for all primes p, which implies (in light of (2.5)) that

$$\rho_{\mathcal{P}^*}(p^2) = \rho_{\mathcal{P}}(p^2) < p^{2s}, \ \mathfrak{S}_{\mathcal{P}^*} = \mathfrak{S}_{\mathcal{P}}. \tag{2.8}$$

So the assertion of Theorem 1.1 holds for the polynomial $\mathcal{P}$ if and only if it holds for the polynomial $\mathcal{P}^*$. If one of partial derivatives $\frac{\partial \mathcal{P}^*}{\partial X_j}$ of $\mathcal{P}^*$ is identically 0, then $\mathcal{P}^*$ may be viewed as a degree d polynomial in the remaining $(s-1)$ variables and the assertion of Theorem 1.1 holds for $\mathcal{P}^*$ by the induction assumption and therefore holds for $\mathcal{P}$ as well. Thus we may assume that all the partial derivatives $\frac{\partial \mathcal{P}^*}{\partial X_j}$ are not identically 0 and so are nonzero polynomials of degree $\leq (d-1)$ in $X_1, \dots, X_s$ with integer coefficients. Hence, where necessary replacing $\mathcal{P}$ by $\mathcal{P}^*$, we may and will assume that

$$\mathcal{P}(\mathbf{X}) = aX_1^d + \sum_{k=1}^{d} F_k X_1^{d-k}, \tag{2.9}$$

where a is a *nonzero* integer and each polynomial $F_k \in \mathbb{Z}[X_2, \dots X_s]$ is a polynomial in $X_2, \dots, X_s$ of degree $\leq k$ with integer coefficients. In addition, all the partial derivatives $\frac{\partial \mathcal{P}}{\partial X_j}$ of $\mathcal{P}$ are *nonzero* polynomials of degree $\le (d-1)$ in $X_1, \ldots, X_s$ with integer coefficients.

By (2.5) and Lemma 3.1 of Chapter 4 of Schmidt [2004], for every prime p not dividing a we have

$$\rho_{\mathcal{P}}(p) \le dp^{s-1}.$$

Moreover each non-singular solution $(b_1, \ldots, b_s) \in (\mathbb{Z}/p\mathbb{Z})^s$ of the congruence

$$\mathcal{P}(X_1, \ldots, X_s) \equiv 0 \pmod{p}$$

modulo p lifts to precisely p^{s-1} solutions modulo p^2. Strangely we can find no reference for this in the published literature, but see Theorem 2.1 of Conrad [unpub.]. Of course it is readily seen by expanding each monomial $(X_j + pY_j)^k$ by the binomial theorem and collecting terms together that

$$\mathcal{P}(X_1 + pY_1, \ldots, X_s + pY_s) \equiv \mathcal{P}(X_1, \ldots, X_s) + p\mathbf{y} \cdot \nabla \mathcal{P}(X_1, \ldots, X_s) \pmod{p^2}$$

and that if $\partial \mathcal{P}(X_1, \ldots, X_s)/\partial X_j \not\equiv 0 \pmod{p}$ for some j then there are exactly p^{s-1} choices for $\mathbf{Y}$ which ensure that $\mathcal{P}(X_1 + pY_1, \ldots, X_s + pY_s) \equiv 0 \pmod{p^2}$. Thus if there are no singular solutions modulo p, i.e., $\mathcal{P}$ is "non-singular" modulo p, then

$$\rho_{\mathcal{P}}(p^2) \le dp^{2s-2}.$$

Let $H(\mathcal{P})$ denote the height of $\mathcal{P}$, i.e., $H(\mathcal{P})$ is the maximum of the absolute values of the coefficients of the polynomial $\mathcal{P}$, and let $\mathfrak{R}$ denote the set of primes p such that

(i) $p \le \max\{d, H(\mathcal{P})\}$, or

(ii) $\rho_{\mathcal{P}}(p^2) \le (d^3 + d)\, p^{2s-2}$.

Since

$$\sum_{p \in \mathfrak{R}} \frac{\rho_{\mathcal{P}}(p^2)}{p^{2s}}$$

converges and (2.5) holds for every p, so that every factor in the product below is positive, it follows that

$$\lambda = \prod_{p \in \mathfrak{R}} \left(1 - \frac{\rho_{\mathcal{P}}(p^2)}{p^{2s}}\right) > 0.$$

Let

$$\mathfrak{R}' := \{p \mid p \notin \mathfrak{R}\}.$$

The condition (i) implies no prime $p \in \mathfrak{R}'$ divides a and $p > d$. In addition, the reduction modulo p of each of the partial derivatives $\mathcal{P}_j$ is a nonzero polynomial of degree $\le (d-1)$ with coefficients in $\mathbb{F}_p$.

By (1.8),

$$\prod_{p \in \mathfrak{R}'} \left(1 - \frac{\rho_{\mathcal{P}}(p^2)}{p^{2s}}\right) = 0.$$

For this to occur, by (2.5), $\mathfrak{R}'$ will have to be infinite. Moreover, for each prime $p \in \mathfrak{R}'$, we have (in light of condition (ii))

$$\rho_{\mathcal{P}}(p^2) > \left(d^3 + d\right) p^{2s-2}.$$

Recall that all the partial derivatives $\mathcal{P}_j$ modulo p are *nonzero* polynomials of degree $\leq d - 1$. Since $\rho_{\mathcal{P}}(p) \leq dp^{s-1}$ and each non-singular solution of the congruence

$$\mathcal{P}(x_1, \ldots, x_s) \equiv 0 \pmod{p}$$

modulo p can lift to precisely p^{s-1} solutions of $\mathcal{P} \equiv 0$ modulo p^2, there are more that d^3p^{s-2} solutions which lift from singular solutions modulo p. But each singular solution to

$$\mathcal{P}(x_1, \ldots, x_s) \equiv 0 \pmod{p},$$

can lift to at most p^s solutions modulo p^2 so there will be more than d^3p^{s-2} *singular points* $\mathbf{x} = (x_1, \ldots, x_s) \in \mathbb{F}_p^s$, i.e., points such that $\mathcal{P}(x_1, \ldots, x_s) = 0$ and for every j

$$\mathcal{P}_j(x_1, \ldots, x_s) = \frac{\partial \mathcal{P}}{\partial x_j}(x_1, \ldots, x_j) = 0.$$

On the other hand Lemma 3.4 of Chapter 4 of Schmidt [2004] states (in particular) the following.

Lemma 2.3. *Suppose that $s \geq 2$ and $t \geq 2$. Let $u_1(X_1, \ldots, X_s), \ldots, u_t(X_1, \ldots, X_s)$ be nonzero polynomials without common non-constant factor over the field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ of respective total degrees at most e. Then the number of their common zeros in $\mathbb{F}_p^s$ is at most*

$$p^{s-2}e^3.$$

Remark 2.4. *Notice that Lemma 2.3 automatically holds when $s = 1$, because in this case the number of common zeros is just 0.*

Let us continue our proof. Using Lemma 2.3 and Remark 2.4, and taking into account that all $(s + 1)$ polynomials

$$\mathcal{P} \bmod p;\ \mathcal{P}_1 \bmod p, \ldots, \mathcal{P}_s \bmod p \in \mathbb{F}_p[X_1, \ldots, X_s],$$

have degrees $\leq d$ and $t := s + 1 \geq 2$, we conclude that all these polynomials have a common factor of *positive degree* in the polynomial ring $\mathbb{F}_p[X_1, \ldots, X_s]$, say,

$$w(X_1, \ldots, X_n) \in \mathbb{F}_p[X_1, \ldots, X_s].$$

Our conditions on p imply that the coefficient at X_1^d of the degree d polynomial

$$\mathcal{P}(X_1, \ldots, X_s) \bmod p \in \mathbb{F}_p[X_1, \ldots, X_s]$$

is a nonzero element of $\mathbb{F}_p$ while the coefficient at X_1^{d-1} of the degree $(d-1)$ polynomial $\mathcal{P}_1(X_1, \ldots, X_s) \bmod p$ is also a nonzero element of $\mathbb{F}_p$.

Lemma 2.5. *Let $r = \deg(w) \geq 1$ be the total degree of w. Then the coefficient of w at X_1^r is nonzero, i.e., the X_1-degree $\deg_{X_1}(w)$ of w is also r.*

Proof of Lemma 2.5. There exists a nonzero polynomial $v \in \mathbb{F}_p[X_1, \dots, X_s]$ such that $\mathcal{P} \bmod p = wv$. Taking into account that the total degree, deg, of any polynomial is greater or equal than its X_1-degree $\deg_{X_1}$, so that

$$\deg(w) \geq \deg_{X_1}(w), \quad \deg(v) \geq \deg_{X_1}(v)$$

we get

$$\begin{aligned} d = \deg(\mathcal{P} \bmod p) &= \deg(w) + \deg(v) \\ &\geq \deg_{X_1}(w) + \deg_{X_1}(v) \\ &= \deg_{X_1}(wv) \\ &= \deg_{X_1}(\mathcal{P} \bmod p) = d. \end{aligned}$$

Therefore we have equality throughout and so we conclude that $\deg(w) = \deg_{X_1}(w)$ which ends the proof. □

Lemma 2.5 implies that the common factor $w(X_1, \dots, X_n)$ does depend on X_1, i.e., does *not* lie in $\mathbb{F}_p[X_2, \dots, X_s]$. In light of Cox, Little & O'Shea [1998, Ch. 3, Sect. 5, Prop. 8], it follows that if we consider $\mathcal{P} \bmod p$ as the degree d polynomial in X_1 with the coefficients in $\mathbb{F}_p[X_2, \dots, X_s]$ then its discriminant (i.e., the resultant of $\mathcal{P}$ and $\mathcal{P}_1$)

$$\Delta_p \in \mathbb{F}_p[X_2, \dots, X_s]$$

is actually 0. Since this holds for all primes p from the infinite set $\mathfrak{R}'$, the similar assertion holds for $\mathcal{P}$. Namely, let us consider $\mathcal{P}$ as the degree d polynomial

$$\mathcal{P} = f(X_1) = aX_1^d + \sum_{k=1}^{d} F_k X_1^{d-k}, \; F_k \in \mathbb{Z}[X_2, \dots, X_s] \tag{2.10}$$

in X_1 and let $\Delta \in \mathbb{Z}[X_2, \dots, X_s]$ be its discriminant. Since $\Delta \bmod p \in \mathbb{F}_p[X_2, \dots, X_s]$ coincides with $\Delta_p = 0$ for infinitely many primes p, we conclude that

$$\Delta \equiv 0 \in \mathbb{Z}[X_2, \dots, X_s].$$

We will need the following elementary assertion Cox, Little & O'Shea [1998, Ch. 3, Sect. 5, Ex. 8] that will be proven later.

Lemma 2.6. *Let $d \geq 2$ be in integer and K be a field of characteristic 0. Further, let $h(x) \in K[x]$ be a degree d polynomial in the independent variable x with leading coefficient a and discriminant 0. Then there are monic polynomials $u(x), v(x) \in K[x]$ such that $\deg(u) \geq 1$ and*

$$h(x) = a \cdot u(x)v(x)^2.$$

Moreover, if d is odd, then $\deg(u) \geq 1$.

We apply Lemma 2.6 to the field $K = \mathbb{Q}(X_2, \dots X_s)$ of rational functions in $X_2, \dots, X_s$ with coefficients in the field $\mathbb{Q}$ of rational numbers and the degree d polynomial $f(X_1)$ defined in (2.10). Recall that the leading coefficient a is a nonzero integer. By Lemma 2.6, there are monic polynomials $u(x), v(x) \in K[x]$ such that $\deg(v) \geq 1$ and

$$f(X_1) = au(X_1)v(X_1)^2.$$

Multiplying by a^{d-1}, we get

$$(aX_1)^d + \sum_{k=1}^{d} a^k F_k (aX_1)^{d-k} = a^{d-1} f(X_1)$$
$$= a^d u(X_1)v(X_1)^2 = \left(a^{\deg u} u(X_1)\right)\left(a^{\deg(v)} v(X_1)\right)^2. \quad (2.11)$$

Clearly there are monic polynomials $\tilde{u}(x) \in K[x]$ and $\tilde{v}(x) \in K[x]$ (of degree $\deg(v) \geq 1$) such that

$$\tilde{u}(ax) = a^{\deg(u)} u(x),\ \tilde{v}(ax) = a^{\deg(v)} u(x). \quad (2.12)$$

It follows that if we consider the degree d monic polynomial

$$\tilde{f}(x) := x^d + \sum_{k=0}^{d-1} a^k F_k x^{d-k}$$

in x with coefficients in the ring $\mathbb{Z}[X_2, \ldots, X_s]$ then

$$\tilde{f}(x) = \tilde{u}(x)\tilde{v}(x)^2.$$

Since $\mathbb{Z}[X_2, \ldots, X_n]$ is integrally closed with field of fractions K, and $\tilde{f}(x)$ is monic, it follows from a variant of Gauss' Lemma, see Dummit & Foot [2004, Sect. 9.3, Cor. 6 on p. 304], that both monic polynomials $\tilde{u}(x)$ and $\tilde{v}(x)$ also have coefficients in $\mathbb{Z}[X_2, \ldots, X_s]$. Combining this with (2.12), we conclude that the polynomials $u(x)$ and $v(x)$ have coefficients in $\frac{1}{a^{\deg(u)}}\mathbb{Z}[X_2, \ldots, X_s]$ and $\frac{1}{a^{\deg(v)}}\mathbb{Z}[X_2, \ldots, X_s]$ respectively. It follows that

$$\tilde{L}_1 := a^{\deg(u)} u(X_1) \in \mathbb{Z}[X_1, X_2, \ldots, X_s],\ \tilde{L}_2 := a^{\deg(v)} v(X_1) \in \mathbb{Z}[X_1, X_2, \ldots, X_s].$$

Hence, by (2.11), in $\mathbb{Z}[X_1, X_2, \ldots, X_s]$ we have the equality

$$a^{d-1}\mathcal{P} = \tilde{L}_1 \tilde{L}_2^2.$$

Since $\mathcal{P}$ is a nonzero polynomial and $a \neq 0$, the product $a^{d-1}\mathcal{P}$ is also a nonzero polynomial in $X_1, \ldots, X_s$. Now the desired result follows readily from the following assertion.

Lemma 2.7. *Let $\mathcal{F} \in \mathbb{Z}[X_1, \ldots, X_s]$ be a nonzero polynomial of degree $d \geq 2$. Suppose that there are a nonzero integer b and polynomials $\mathcal{N}_1, \mathcal{N}_2 \in \mathbb{Z}[X_1, \ldots, X_s]$ such that* $\deg(\mathcal{N}_1) \geq 1$ *and*

$$b\mathcal{F} = \mathcal{N}_1 \mathcal{N}_2^2.$$

Then there are exist polynomials $\tilde{\mathcal{N}}_1, \tilde{\mathcal{N}}_2 \in \mathbb{Z}[X_1, \ldots, X_s]$ such that $\tilde{\mathcal{N}}_2$ is an irreducible polynomial over $\mathbb{Q}$ (in particular, $\deg(\tilde{\mathcal{N}}_2) \geq 1$*) and*

$$\mathcal{F} = \tilde{\mathcal{N}}_1 \tilde{\mathcal{N}}_2^2.$$

Proof of Lemma 2.7. Replacing if necessary $\mathcal{N}_1$ by $-\mathcal{N}_1$ and b by $-b$, we may and will assume that b is a *positive* integer. Let $\mathcal{H}_2 \in \mathbb{Q}[X_1, \ldots, X_s]$ be an *irreducible* polynomial that divides $\mathcal{N}_2$ in $\mathbb{Q}[X_1, \ldots, X_s]$. Without loss of generality, we may and will assume that

$$\mathcal{H}_2 \in \mathbb{Z}[X_1, \ldots, X_s].$$

It follows that both $\mathcal{H}_2$ and $\mathcal{H}_2^2$ divide the polynomial $b\mathcal{F}$ in $\mathbb{Q}[X_1, \ldots, X_s]$. The latter means that there is a polynomial $\mathcal{E} \in \mathbb{Q}[X_1, \ldots, X_s]$ such that

$$b\mathcal{F} = \mathcal{H}_2^2\mathcal{E}.$$

Notice that there is a positive integer b_0 such that $\mathcal{E}' = b_0\mathcal{E} \in \mathbb{Z}[X_1, \ldots, X_s]$ and therefore $b_0 \cdot b$ is a positive integer such that

$$(b_0 b)\mathcal{F} = \mathcal{H}_2^2(b_0\mathcal{E}) = \mathcal{H}_2^2 \cdot \mathcal{E}'.$$

Consider the set Z of positive integers c such that there exist polynomials $\mathcal{D}_1, \mathcal{D}_2 \in \mathbb{Z}[X_1, \ldots, X_s]$ for which $\mathcal{D}_2$ is irreducible over $\mathbb{Q}$ and

$$c\mathcal{F} = \mathcal{D}_1\mathcal{D}_2^2.$$

The set Z is non-empty, because it contains $b_0 b$. Let c be the smallest element of Z and $\mathcal{D}_1, \mathcal{D}_2$ be the corresponding polynomials in $X_1, \ldots, X_s$ with integer coefficients. If $c = 1$ then we are done.

Suppose that $c > 1$. Then there is a prime p dividing c. This means that there is a positive integer c_1 such that $c = pc_1$ and

$$pc_1\mathcal{F} = \mathcal{D}_1\mathcal{D}_2^2.$$

Hence,

$$(\mathcal{D}_1 \bmod p)\,(\mathcal{D}_2 \bmod p)^2 \equiv 0$$

in the polynomial ring $\mathbb{F}_p[x_1, \ldots, x_s]$. Since this ring is a domain, either $\mathcal{D}_1 \bmod p \equiv 0$ or $\mathcal{D}_2 \bmod p \equiv 0$. Thus either $\mathcal{D}_1 \in p \cdot \mathbb{Z}[X_1, \ldots, X_s]$ or $\mathcal{D}_2 \in p \cdot \mathbb{Z}[X_1, \ldots, X_s]$.

In the former case, there is a polynomial $\tilde{\mathcal{D}}_1 \in \mathbb{Z}[X_1, \ldots, X_s]$ such that $\mathcal{D}_1 = p\tilde{\mathcal{D}}_1$ and therefore

$$pc_1\mathcal{F} = p\tilde{\mathcal{D}}_1\mathcal{D}_2^2,$$

which implies that

$$c_1\mathcal{F} = \tilde{\mathcal{D}}_1\mathcal{D}_2^2$$

and therefore $c_1 \in Z$. Since, $c_1 < c$, it contradicts the minimality of $c \in Z$.

It follows that $\mathcal{D}_2 \in p \cdot \mathbb{Z}[X_1, \ldots, X_s]$, i.e., there is a form $\tilde{\mathcal{D}}_2 \in \mathbb{Z}[X_1, \ldots, X_s]$ such that $\mathcal{D}_2 = p\tilde{\mathcal{D}}_2$ and therefore $\tilde{\mathcal{D}}_2$ is also irreducible over $\mathbb{Q}$ and

$$pc_1\mathcal{F} = p^2\mathcal{D}_1\tilde{\mathcal{D}}_2^2,$$

which implies that

$$c_1\mathcal{F} = (p\mathcal{D}_1)\,\tilde{\mathcal{D}}_2^2$$

and therefore $c_1 \in Z$, which again contradicts the minimality of $c \in Z$.

Hence $c = 1$ and we are done. □

Proof of Lemma 2.6. Without loss of generality we may assume that $h(x)$ is monic. Let L be the splitting field of $h(x)$, which is a finite Galois extension of K with (finite) Galois group G.

The vanishing of the discriminant of $h(x)$ means that the (finite) set $\Sigma \subset L$ of repeated roots α of $h(x)$ is nonempty. Since all the coefficients of $h(x)$ lie in K, the set Σ is G-invariant and therefore the monic polynomial

$$v(x) = \prod_{\alpha\in\Sigma}(x-\alpha) \in L[x]$$

actually lies in $K[x]$. As Σ is nonempty, $\deg(v) \geq 1$. Moreover, since each $\alpha \in \Sigma$ is a repeated root of $h(x)$, the product

$$\prod_{\alpha\in\Sigma}(x-\alpha)^2 = v(x)^2$$

divides $h(x)$ in $L[x]$. Since both $h(x)$ and $v(x)^2$ lie in $K[x]$, the ratio $h(x)/v(x)^2$ actually lies in $K[x]$, i.e., there is $u(x) \in K[x]$ such that

$$h(x) = u(x)v(x)^2.$$

If $d = \deg(h)$ is odd, $\deg(u) = d - 2\deg(v)$ is also odd and therefore ≥ 1.

□

Remark 2.8. *Lemma 2.6 remains true without restrictions on the characteristic of K, see Cox, Little & O'Shea* [1998, Ch. 3, Sect. 5, Ex. 8] *where the proof is sketched.*

3. Proof of Lemma 2.1

Step 1. First, let us assume that our polynomial f is *absolutely irreducible*, i.e., is irreducible over an algebraic closure $\bar{\mathbb{Q}}$ of the field $\mathbb{Q}$ of rational numbers. Then our assertion is contained in Schmidt [2004, Ch. 5, Cor. 5.1 on p. 164–165] where one may take as $S(f)$ the set of all primes $p > p_0(f)$ for a suitable $p_0(f)$

Step 2. Each non-constant polynomial $f \in \mathbb{Z}[X_1, \dots X_s]$ splits in $\mathbb{Q}[X_1, \dots X_s]$ into a product

$$f = \prod_{i=1}^{r} f_i$$

of irreducible polynomials $f_i \in \mathbb{Q}[X_1, \dots X_s]$. For each i there is a positive integer b_i such that the polynomial $b_i f_i$ has integer coefficients; in addition, $b_i f_i$ remains irreducible in $\mathbb{Q}[X_1, \dots X_s]$. If we put $b = \prod_{i=1}^{r} b_i$ then

$$bf = \prod_{i=1}^{r}(b_i f_i)$$

splits in $\mathbb{Z}[X_1, \dots X_s]$ into a product of polynomials $b_i f_i$ irreducible over $\mathbb{Q}$. This implies that for all primes p not dividing b

$$\rho_f(p) = \rho_{bf}(p) \geq \rho_{b_i f_i}(p) \quad \forall i.$$

If some f_i is *absolutely irreducible*, then $b_i f_i$ is also absolutely irreducible. In light of Step 1 (applied to $b_i f_i$) our assertion would hold for $S(bf)$, and thus for $S(f)$ taken to be $S(bf) \setminus \{p : p|b\}$.

Step 3. In general, our non-constant f splits in $\bar{\mathbb{Q}}$ into a product

$$f = \prod_{j=1}^{m} h_j \tag{3.1}$$

of irreducible polynomials $h_j \in \bar{\mathbb{Q}}[X_1, \ldots, X_s]$. In particular

$$\deg(h_j) \leq d.$$

There is a finite Galois field extension $K/\mathbb{Q}$ such that all

$$h_j \in K[X_1, \ldots, X_s] \subset \bar{\mathbb{Q}}[X_1, \ldots, X_s].$$

Notice that one may view K as a subfield of $\bar{\mathbb{Q}}$ and the latter is an algebraic closure of K. Let O_K be the ring of integers in K. Similarly to the previous case, for each j there is a positive integer c_j such that the polynomial $c_j h_j$ has coefficients in O_K and remains irreducible in $\bar{\mathbb{Q}}[X_1, \ldots X_s]$. In addition, if we put $c = \prod_{j=1}^{m} c_j$, then the polynomial cf splits in $O_K[X_1, \ldots X_s]$ into a product of polynomials $c_j h_j$ which are irreducible over $\bar{\mathbb{Q}}$,

$$cf = \prod_{j=1}^{m} (c_j h_j)$$

Clearly, for all primes p not dividing c

$$\rho_f(p) = \rho_{cf}(p).$$

Since the set of prime divisors of c is finite, we may assume (replacing f by cf and every h_j by $c_j h_j$) without loss of generality that all h_j have coefficients in O_K and the equality (3.1) holds in $O_K[X_1, \ldots X_s]$.

Step 4. We keep the notation and assumption of Step 3. Let $\mathfrak{P}$ be a maximal ideal in O_K. Then one may assign to $\mathfrak{P}$ its *residual characteristic* p that is a prime that is uniquely determined by the following equivalent properties.

The residue field $k(\mathfrak{P}) := O_K/\mathfrak{P}$ *is a (finite) field of characteristic* p;

$$\textit{the intersection } \mathfrak{P} \cap \mathbb{Z} = p \cdot \mathbb{Z}. \tag{3.2}$$

We have in the polynomial ring

$$k(\mathfrak{P})[X_1, \ldots X_s] = O_K[X_1, \ldots X_s]/\mathfrak{P} O_K[X_1, \ldots X_s]$$

the equality

$$f \bmod \mathfrak{P} = \prod_{j=1}^{m} (h_j \bmod \mathfrak{P}).$$

We claim that if $k(\mathfrak{P})$ is the *prime* finite field $\mathbb{F}_p$, then $\rho_f(p)$ is greater or equal than the number $N_{j,\mathfrak{P}}$ of zeros of h_j mod $\mathfrak{P}$ in $k(\mathfrak{P})^s = \mathbb{F}_p^s$ for any j. (More precisely, each zero of h_j mod $\mathfrak{P}$ is a zero of f in $\mathbb{F}_p^s$.) Indeed, let

$$\alpha = (\alpha_1, \dots, \alpha_s) \in k(\mathfrak{P})^s = \mathbb{F}_p^s = \mathbb{Z}^s/p\mathbb{Z}^s$$

be a zero of h_j mod $\mathfrak{P}$. This means that if

$$(\alpha_1, \dots, \alpha_s) = (a_1, \dots, a_s) + p\mathbb{Z}^s \quad \text{for some } (a_1, \dots, a_s) \in \mathbb{Z}^s \subset O_K^s$$

then $h_j(a_1, \dots, a_s) \in \mathfrak{P}$. On the other hand, since each h_l is a polynomial with coefficients in O_K, its value $h_l(a_1, \dots, a_s)$ lies in O_K for all $l = 1, \dots, m$. It follows that

$$f(a_1, \dots, a_s) = \prod_{l=1}^{m} h_l(a_1, \dots a_r) = h_j(a_1, \dots, a_s) \cdot \prod_{l \neq j} h_l(a_1, \dots, a_s) \in \mathfrak{P} \cdot O_K = \mathfrak{P}.$$

Since $f(a_1, \dots, a_s) \in \mathbb{Z}$, it follows from (3.2) that $f(a_1, \dots, a_s) \in p\mathbb{Z}$, i.e.,

$$(\alpha_1, \dots, \alpha_s) = (a_1 \bmod p, \dots, a_s \bmod p)$$

is a zero of f in $\mathbb{F}_p^s$. This implies that

$$\rho_f(p) \geq N_{j,\mathfrak{P}} \quad \text{if } k(\mathfrak{P}) = \mathbb{F}_p. \tag{3.3}$$

By the Chebotarev density theorem ([1989, Ch. I, Sect. 2.2], [1996]), there is a set S_K of primes p, of positive density in the primes, so that each prime p *splits completely* in K. In particular, for each $p \in S_K$ there is a maximal ideal $\mathfrak{P}$ of O_K with residual characteristic p such that $k(\mathfrak{P}) = \mathbb{F}_p$.

By a theorem of Ostrowski-Noether [2000, Sect. 3.1, Cor. 4 on p. 203], for all but finitely many maximal ideals $\mathfrak{P}$ of O_K the reduction modulo $\mathfrak{P}$ of the polynomial h_1,

$$\tilde{h}_1 = h_1 \bmod \mathfrak{P} \in (O_K/\mathfrak{P})[X_1, \dots X_s]$$

is *absolutely irreducible*, i.e., irreducible over an algebraic closure of $k(\mathfrak{P})$; in addition, the degrees of h_1 and $\tilde{h}_1$ coincide and do not exceed d. By removing from S_K a finite set of primes, we get a set S of primes having positive density in the primes and which enjoys the following properties.

If $p \in S$ then there is a maximal ideal $\mathfrak{P}$ of O_K such that:

(a) $k(\mathfrak{P}) = \mathbb{F}_p, \quad \mathfrak{P} \cap \mathbb{Z} = p \cdot \mathbb{Z}$;

(b) the polynomial

$$\tilde{h}_1 := h_1 \bmod \mathfrak{P} \in k(\mathfrak{P})[X_1, \dots X_s] = \mathbb{F}_p[X_1, \dots, X_s]$$

is *absolutely irreducible*.

By Schmidt [1974, p. 448], the absolute irreducibility of $h_1 \bmod \mathfrak{P}$ implies the existence of a positive real number C such that C depends only on s and d (but does not depend on a choice of p and $\mathfrak{P}$) such that

$$N_{1,\mathfrak{P}} \geq p^{d-1} - Cp^{d-(3/2)}.$$

It remains to observe that $\rho_f(p) \geq N_{1,\mathfrak{P}}$, and then Lemma 2.1 follows on taking Q sufficiently large.

4. Proof of Corollary 1.2

The first part of Corollary 1.2 is clear. Thus we may suppose that (b) of Theorem 1.1 holds. if necessary by relabeling we can suppose that $P_1 = \min_j P_j$. Then, by Lemma 2.2 there are s integers $t_1, \ldots, t_s$ such that (in the notation of Lemma 2.2)

$$\mathcal{L}_2(\mathbf{Y}\mathcal{T}) = \mathcal{L}^*(\mathbf{Y})$$

where

$$\mathcal{L}^* = aY_1^d + \sum_{k=1}^{d} F_k Y_1^{d-k}$$

and F_k is a polynomial in $Y_2, \ldots, Y_s$ of degree $\leq k$ with integer coefficients and a is a *nonzero* integer. Hence the number of solutions $\mathbf{y} = (y_1, \ldots, y_s)$ of

$$\mathcal{L}_2(\mathbf{y}\mathcal{T}) = \pm 1$$

in integers $y_1, \ldots, y_s$ with $|y_1| \leq P_1$ and $|y_j| \leq P_j + |t_j|P_1$ $(2 \leq j \leq s)$ is at most

$$2d \prod_{j=2}^{s} (2P_j + 2|t_j|P_1 + 1) \ll P_2 \ldots P_s.$$

Moreover for any $\mathbf{x} = (x_1, \ldots, x_s)$ with integers x_j such that $|x_j| \leq P_j$ there is a unique $\mathbf{y} = (y_1, \ldots y_s)$ with integers y_j such that $\mathbf{y}\mathcal{T} = \mathbf{x}$ given by $\mathbf{y} = \mathbf{x}\mathcal{T}^{-1}$. Thus $|y_1| = |x_1| \leq P_1$ and $|y_j| = |x_j - t_j x_1| \leq P_j + |t_j|P_1$ $(2 \leq j \leq s)$. Hence the number of possible $\mathbf{x}$ with $|x_j| \leq P_j$ and

$$\mathcal{L}_2(\mathbf{x}) = \pm 1$$

is

$$\ll P_2 \ldots P_s,$$

as required.

5. Proof of Corollary 1.3

Let M be a positive number at our disposal and define

$$r = \prod_{p \leq M} p.$$

Then

$$N_{\mathcal{P}}(\mathbf{P}) \leq \sum_{\mathbf{x} \in \mathbf{P}} \sum_{\substack{m|r \\ m^2|\mathcal{P}(\mathbf{x})}} \mu(m) = \sum_{m|r} \mu(m) \sum_{\substack{\mathbf{y} \pmod{m^2} \\ m^2|\mathcal{P}(\mathbf{y})}} \sum_{\substack{\mathbf{x} \in \mathbf{P} \\ x_j \equiv y_j \pmod{m^2}}} 1$$

$$= \sum_{m|r} \mu(m)\rho(m^2) \left(\frac{P_1}{m^2} + O(1) \right) \ldots \left(\frac{P_s}{m^2} + O(1) \right).$$

Hence

$$\mathfrak{D}_{\mathcal{P}} \le \sum_{m|r} \mu(m)\frac{\rho(m^2)}{m^{2s}} = \prod_{p\le M}\left(1-\frac{\rho(p^2)}{p^{2s}}\right)$$

and so letting $M\to\infty$

$$\mathfrak{D}_{\mathcal{P}} \le \mathfrak{S}_{\mathcal{P}}.$$

References

[2014] Manjul Bhargava, The geometric sieve and the density of squarefree values of invariant polynomials, arXiv:1402.0031 [math.NT]. https://doi.org/10.48550/arXiv.1402.0031

[2022] Manjul Bhargava, Arul Shankar, and Xiaoheng Wang, Squarefree values of polynomial discriminants I, Invent. Math. **228** (2022), no. 3, 1037–1073.

[unpub.] K. Conrad, A multivariable Hensel's lemma, unpublished. https://kconrad.math.uconn.edu/blurbs/gradnumthy/multivarhensel.pdf

[1998] D. Cox, J. Little, D. O'Shea, Ideals, Varieties and Algorithms, Corrected second printing. Springer-Verlag New York Inc., 1998.

[2004] D.S. Dummit & R.M. Foot, Abstract Algebra, 3rd edition. John Wiley & Sons, Inc., 2004.

[1965] G. M. Fikhtengol'ts, The Fundamentals of Mathematical Analysis, volume 2. Pergamon Press, 1965.

[1994] M. Filaseta, Powerfree values of binary forms. J. Number Theory **49** (1994), 250–268.

[1885] L. Gegenbauer, Asymptotische Gesetze der Zahlentheorie, Denkschriften Österreich. Akad. Wiss. Math.-Natur. Cl. **49** (1885), 37–80.

[1992] G. Greaves, Power-free values of binary forms, Quarterly J. Math, **43** (1992), 45–65.

[1967] C. Hooley, On the power-free values of polynomials, Mathematika, **14** (1967), 21–26.

[1977] C. Hooley, On the power-free numbers and polynomials II, J. Reine Angew. Math., **295** (1977), 1–21.

[2009a] C. Hooley, On the power-free values of polynomials in two variables, Analytic number theory, 235–266.

[2009b] C. Hooley, On the power-free values of polynomials in two variables: II, Journal of Number Theory, **129** (2009), 1443–1455.

[2020] J. M. Kowalski, On the squarefree values of polynomials, Ph.D. Thesis, Penn State University, 2020. https://etda.libraries.psu.edu/catalog/17522jmk672

[2021] J. M. Kowalski, On the proportion of squarefree numbers among sums of cubic polynomials, Ramanujan J., **54** (2021), 343–354.

[2023] J. M. Kowalski & R. C. Vaughan, Squarefree density of cubic forms, to appear in Acta Arithmetica.

[2021] K. Lapkova & S. Y. Xiao, Density Of Power-Free Values Of Polynomials II. arXiv:2005.14655 [math.NT] https://doi.org/10.48550/arXiv.2005.14655

[2006] H. L. Montgomery & R. C. Vaughan, Multiplicative Number Theory I. Classical Theory, Cambridge University Press, xii + 516pp, 2006.

[2003] B. Poonen, Squarefree values of multivariable polynomials, Duke Math. J., **118** (2003), 353–373.

[2023] G. C. Sanjaya & X. Wang, On the squarefree values of a^4+b^3, Math. Annalen, **386** (2023), 1237–1265.

[2000] A. Schinzel, Polynomials with special regard to reducibility. With an appendix by Umberto Zannier. Encyclopedia Math. Appl., **77** Cambridge University Press, Cambridge, 2000. x+558 pp.

[1974] W. M. Schmidt, A lower bound for the number of solutions of equations over finite fields. J. Number Theory **6** (1974), 448-480.

[2004] W. M. Schmidt, Equations over Finite Fields, An Elementary Approach, Second Edition, Kendrick Press, 2004.

[1989] J.-P. Serre, Abelian ℓ-adic representations and elliptic curves, Second Edition. Addison Wesley Publishing Company, Inc., 1989.

[1996] P. Stevenhagen and H.W. Lenstra, Jr, Chebotarëv and his Density Theorem. Math. Intelligencer **18:2** (1996), 26–37.

[1972] S. Uchiyama, On the power-free values of a polynomial. Tensor (N.S.), **24** (1972), 43–48.

RCV: Dept. of Mathematics, Pennsylvania State University, University Park, PA 16802, USA.

Email address: rcv4@psu.edu

YGZ: Dept. of Mathematics, Pennsylvania State University, University Park, PA 16802, USA.

Email address: zarhin@math.psu.edu