Invent. math. (2023) 231:673–739
https://doi.org/10.1007/s00222-022-01153-6

# Schinzel Hypothesis on average and rational points

**Alexei N. Skorobogatov**[1,2] · **Efthymios Sofos**[3]

Received: 7 November 2020 / Accepted: 18 August 2022 /
Published online: 28 September 2022


**Abstract** We resolve Schinzel's Hypothesis (H) for 100% of polynomials of arbitrary degrees. We deduce that a positive proportion of diagonal conic bundles over $\mathbb{Q}$ with any given number of degenerate fibres have a rational point, and obtain similar results for generalised Châtelet equations.

**Mathematics Subject Classification** 11N32 · 14G05

## Contents



✉ Alexei N. Skorobogatov
a.skorobogatov@imperial.ac.uk

Efthymios Sofos
efthymios.sofos@glasgow.ac.uk

[1] Department of Mathematics, South Kensington Campus, Imperial College London, London SW7 2AZ, UK

[2] Institute for the Information Transmission Problems, Russian Academy of Sciences, Moscow 127994, Russia

[3] Department of Mathematics, University of Glasgow, University Place, Glasgow G12 8QQ, UK

## 1 Introduction

Schinzel's Hypothesis (H) [53] has very strong implications for the local-to-global principles for rational points on conic bundles, as demonstrated by Colliot-Thélène and Sansuc in [17]. There have been many subsequent developments and applications to more general varieties by Serre, Colliot-Thélène, Swinnerton-Dyer and others. We call $P(t) \in \mathbb{Z}[t]$ a *Bouniakowsky polynomial* if the leading coefficient of $P(t)$ is positive and for every prime $\ell$ the reduction of $P(t)$ modulo $\ell$ is not a multiple of $t^\ell - t$. It is not hard to prove that an explicit positive proportion of polynomials of given degree are Bouniakowsky polynomials (Corollary 2.10 below). A conjecture stated by Bouniakowsky in 1854 [7, p. 328], now a particular case of Schinzel's Hypothesis (H), says that if $P(t)$ is an irreducible Bouniakowsky polynomial, then there are infinitely many natural numbers $n$ such that $P(n)$ is prime. Bouniakowsky added this remark: "*Il est à présumer que la démonstration rigoureuse du théorème énoncé sur les* progressions arithmétiques des ordres supérieurs *conduirait, dans l'état actuel de la théorie des nombres, à des difficultés insurmontables ; néanmoins, sa réalité ne peut pas être révoquée en doute*".

The inaccessibility of Schinzel's hypothesis and its quantitative version, the Bateman–Horn conjecture [6], in degrees greater than 1 or for more than one polynomial motivates a search for more accessible replacements. In the case of several multivariate polynomials of degree 1 such a replacement is provided by work of Green, Tao and Ziegler in additive combinatorics (see [32] and references there, and [11,33,34] for applications to rational points).

In this paper we study rational points on varieties in families, with the aim of proving that a positive proportion of varieties in a given family have rational points. To apply the method of Colliot-Thélène and Sansuc in this situation, one does not need the full strength of Bouniakowsky's conjecture, namely that *every* irreducible Bouniakowsky polynomial represents *infinitely many* primes: it is enough to know that *most* polynomials satisfying the obvious necessary condition represent *at least one* prime. We propose the following replacement for Bouniakowsky's conjecture. The *height* of a polynomial $P(t) \in \mathbb{Z}[t]$ is defined as the maximum of the absolute values of its coefficients.

**Theorem 1.1** *Let $d$ be a positive integer. When ordered by height, for* 100% *of Bouniakowsky polynomials $P(t)$ of degree $d$ there exists a natural number $m$ such that $P(m)$ is prime.*

This improves on previous work of Filaseta [26] who showed that a positive proportion of Bouniakowksy polynomials represent a prime. Note that stating Schinzel's Hypothesis for infinitely many primes is trivially equivalent to stating it for at least one prime [53, p. 188], but this is no longer so if we are only concerned with 100% of polynomials.

Theorem 1.1 is a particular case of a more general result for $n$ polynomials, where certain congruence conditions are allowed. We denote the height of $P(t) \in \mathbb{Z}[t]$ by $|P|$. The height of an $n$-tuple of polynomials $\mathbf{P} = (P_1(t), \dots, P_n(t)) \in (\mathbb{Z}[t])^n$ is defined as $|\mathbf{P}| = \max_{i=1,\dots,n}(|P_i|)$. We call $\mathbf{P}$ a *Schinzel $n$-tuple* if for every prime $\ell$ the reduction modulo $\ell$ of the product $P_1(t)\dots P_n(t)$ is not divisible by $t^\ell - t$, and the leading coefficient of each $P_i(t)$ is positive.

**Theorem 1.2** *Let $d_1, \dots, d_n$ be positive integers. Fix integers $n_0$ and $M$. Assume we are given $Q_1(t), \dots, Q_n(t)$ in $\mathbb{Z}[t]$ such that $\prod_{i=1}^n Q_i(n_0)$ and $M$ are coprime, and $\deg(Q_i(t)) \leqslant d_i$ for $i = 1, \dots, n$. When ordered by height, for 100% of Schinzel $n$-tuples $(P_1(t), \dots, P_n(t))$ such that $\deg(P_i(t)) = d_i$ and $P_i(t) - Q_i(t) \in M\mathbb{Z}[t]$ for each $i = 1, \dots, n$, there exists a natural number $m \equiv n_0 \pmod M$ such that $P_1(m), \dots, P_n(m)$ are pairwise different primes.*

The special case $M = 1$ shows that, with probability 100%, an $n$-tuple of integer polynomials satisfying the necessary local conditions simultaneously represent primes. Theorem 1.1 is the special case for $n = 1$. The proof of Theorem 1.2 occupies most of the paper; we give more details about the strategy of proof later in this introduction.

In this paper we apply our analytic results to rational points on varieties in families, where the parameter space is the space of coefficients of generic polynomials of fixed degrees. Among many potential applications we choose to consider generalised Châtelet varieties (1.1) and diagonal conic bundles (1.2). Using Theorem 1.2 we obtain a weaker version of the Hasse principle for equations

$$\mathrm{N}_{K/\mathbb{Q}}(\mathbf{z}) = P(t) \neq 0, \tag{1.1}$$

where $K$ is a fixed cyclic extension of $\mathbb{Q}$ and $\mathrm{N}_{K/\mathbb{Q}}(\mathbf{z})$ is the associated norm form, for 100% of Bouniakowsky polynomials $P(t)$ of given degree, see Theorem 5.3. (See also Theorem 5.8 for the case when $P(t)$ is a product of generic Bouniakowsky polynomials.) It implies

**Theorem 1.3** *Let $d$ be a positive integer. For a positive proportion of polynomials $P(t) \in \mathbb{Z}[t]$ of degree $d$ ordered by height, the affine variety given by (1.1) has a $\mathbb{Q}$-point.*

Explicit estimates in the case $K = \mathbb{Q}(\sqrt{-1})$ are given in Sect. 7. If $K$ is a totally imaginary abelian extension of $\mathbb{Q}$ of class number 1, then the same statement holds, with the following easy proof. By the Kronecker–Weber theorem we have $K \subset \mathbb{Q}(\zeta_M)$ for some $M \geqslant 1$. Hence all primes in the arithmetic progression $1 \pmod M$ split in $K$. Theorem 1.2 implies that a random Bouniakowsky polynomial of degree $d$ congruent to the constant polynomial 1 modulo $M$ represents a prime. This prime $p$ is the norm of a principal integral ideal $(x) \subset K$. Since $K$ is totally imaginary, we have $p = \mathrm{N}_{K/\mathbb{Q}}(x)$. (See Theorem 5.7 for a more general statement.) Here, at the expense of the condition on the class number of $K$, we do not require $K$ to be cyclic over $\mathbb{Q}$ and we find an integral (and not just rational) solution of (1.1).

A stronger version of Theorem 1.2, where we require primes represented by polynomials to satisfy additional conditions in terms of quadratic residues, is obtained by incorporating into our technique an estimate for certain character sums due to Heath-Brown [35, Cor. 4]. This leads to the following result, proved in Sect. 6.4 as a consequence of Theorem 6.1.

**Theorem 1.4** *Let $n_1, n_2, n_3$ be integers such that $n_1 > 0$, $n_2 > 0$, and $n_3 \geqslant 0$, and let $n = n_1 + n_2 + n_3$. Let $a_1, a_2, a_3$ be non-zero integers, and let $d_{ij}$ be natural numbers for $i = 1, 2, 3$ and $j = 1, \ldots, n_i$. Then for a positive proportion of $n$-tuples $(P_{ij}) \in \mathbb{Z}[t]^n$ with $\deg(P_{ij}(t)) = d_{ij}$, ordered by height, the following conic bundle surface has a $\mathbb{Q}$-point contained in a smooth fibre:*

$$a_1 \prod_{j=1}^{n_1} P_{1,j}(t)\, x^2 + a_2 \prod_{k=1}^{n_2} P_{2,k}(t)\, y^2 + a_3 \prod_{l=1}^{n_3} P_{3,l}(t)\, z^2 = 0. \qquad (1.2)$$

By [8, Thm. 1.4] (see also [46, Thm. 1.3]) in a dominant, everywhere locally solvable family of quasi-projective varieties over an affine space such that the fibres at the points of codimension 1 are split and enough real fibres have real points, a positive proportion of rational fibres are everywhere locally solvable. Thus, the results of Theorems 1.3 and 1.4 are expected consequences of a conjecture of Colliot-Thélène which predicts that the Hasse principle for rational points on smooth, projective, geometrically rational varieties is controlled by the Brauer–Manin obstruction, and generic triviality of the Brauer group in our families. (Note that in these cases Colliot-Thélène's conjecture follows from Schinzel's Hypothesis (H), see [20, Thm. 14.2.4].) A known non-trivial case of this conjecture for conic bundles (1.2) is when the total degrees of coefficients are (2, 2, 0); natural smooth projective models of such surfaces are del Pezzo surfaces of degree 4 for which the result is due to Colliot-Thélène [15]. The question is open already in the case of total degrees (2, 2, 2), which corresponds to a particular kind of del Pezzo surfaces of degree 2 (cf. [11, Prop. 5.2]). The conjecture for smooth projective varieties birationally equivalent to (1.1) is known when $\deg(P(t)) \leqslant 4$ (and in some cases when $\deg(P(t)) = 6$) and $[K : \mathbb{Q}] = 2$ (Colliot-Thélène, Sansuc and Swinnerton-Dyer [18], [56], see [55, §7.2, §7.4]), $\deg(P(t)) \leqslant 3$ and $[K : \mathbb{Q}] = 3$ (Colliot-Thélène and Salberger [16]), $\deg(P(t)) \leqslant 2$ and $[K : \mathbb{Q}]$ arbitrary [10,19,25,36]. There seem to be no known unconditional results about the Hasse principle when the number of degenerate fibres is greater than 6. In contrast, for our statistical approach to the existence of rational points the number of degenerate fibres is immaterial.

In the rest of the introduction we give more details about our main analytic results; for this we need to introduce some more notation. We write $P > 0$ to denote that the leading coefficient of $P(t)$ is positive. For a prime $\ell$ and a polynomial $P(t) \in \mathbb{F}_\ell[t]$ we define

$$Z_P(\ell) := \sharp\{s \in \mathbb{F}_\ell : P(s) = 0\}.$$

In particular, $\mathbf{P}$ is a Schinzel $n$-tuple if and only if $Z_{P_1 \dots P_n}(\ell) \neq \ell$ for all primes $\ell$ and $P_i > 0$ for each $i = 1, \dots, n$. Fix integers $n_0$ and $M$, and polynomials $Q_i(t) \in \mathbb{Z}[t]$ of degree at most $d_i$ for $i = 1, \dots, n$ such that $\prod_{i=1}^n Q_i(n_0)$ and $M$ are coprime. For $H \geqslant 1$ define

$$\texttt{Poly}(H) := \big\{\mathbf{P} \in (\mathbb{Z}[t])^n : |\mathbf{P}| \leqslant H, \deg(P_i) = d_i, P_i > 0, \\ P_i \equiv Q_i \ (\mathrm{mod}\ M) \ \text{ for } i = 1, \dots, n\big\}.$$

**The least prime represented by a polynomial**

For $C > 0$ define

$$S_C(\mathbf{P}) := \{m \in \mathbb{N} : m \leqslant (\log |\mathbf{P}|)^C, m \equiv n_0 \ (\mathrm{mod}\ M), P_i(m) \text{ is prime for } i = 1, \dots, n\}.$$

Theorem 1.2 is an immediate consequence of the following more precise quantitative result.

**Theorem 1.5** *Fix $A > 0$. In the assumptions of Theorem 1.2 for all $H \geqslant 3$ we have*

$$\frac{\sharp\{\mathbf{P} \in \texttt{Poly}(H) : \mathbf{P} \text{ is Schinzel}, \ \sharp S_{n+A}(\mathbf{P}) \geqslant (\log |\mathbf{P}|)^{A/3}\}}{\sharp\{\mathbf{P} \in \texttt{Poly}(H) : \mathbf{P} \text{ is Schinzel}\}} \\ = 1 + O\left(\frac{(\log\log\log H)^{d-n}}{\sqrt{\log\log H}}\right), \tag{1.3}$$

*where $d = d_1 + \ldots + d_n$. The implied constant depends on $d$, $A$ and $M$, but not on $H$.*

Recall that Linnik's constant is the smallest $L > 0$ such that every primitive degree 1 polynomial $P(x) = qx + a$ with $0 < a < q$ represents a prime of size $\ll q^L = |P|^L$. This subject has rich history, see [39, §18], for example. GRH implies that $L \leqslant 2 + \varepsilon$ for every $\varepsilon > 0$ and it is known that $L \leqslant 5$, see [60]. Furthermore, one cannot have $L < 1$, see [44] for accurate lower bounds.

Theorem 1.5 shows that the analogue of the Linnik constant for polynomials of given degree is at most $1+\varepsilon$ for every $\varepsilon > 0$.

**Corollary 1.6** *Let $\varepsilon > 0$ and fix $d, n_0, M \in \mathbb{N}$. For 100% of Bouniakowsky polynomials $P$ of degree $d$ with $\gcd(P(n_0), M) = 1$, there exists a natural number $m \leqslant (\log|P|)^{1+\varepsilon}$ such that $m \equiv n_0 \pmod M$ and $P(m)$ is a prime bounded by $|P|(\log|P|)^{d+\varepsilon}$.*

Indeed, Theorem 1.5 with $n = 1$ and $A = \varepsilon/(2d)$ shows the existence of a natural number $m \leqslant (\log|P|)^{1+\varepsilon/(2d)}$ such that $P(m)$ is prime; furthermore, we have

$$P(m) \leqslant (d+1)|P|m^d \leqslant (d+1)|P|(\log|P|)^{(1+\varepsilon/(2d))d} \\ \ll |P|(\log|P|)^{d+\varepsilon/2} \leqslant |P|(\log|P|)^{d+\varepsilon}.$$

These bounds are intimately related to the efficacy of algorithms for factorisation of polynomials, see the work of Adleman and Odlyzko [1], and for finding efficient cryptographic parameters as in the work of Freeman, Scott and Teske [28, § 2.1]. McCurley [47] has shown that for certain polynomials the least representable prime has to be rather large. The case $d = 2$ of Corollary 1.6 is closely related to hard questions on the size of class numbers that go all the way back to Euler; see the survey of Mollin [49].

#### Smallest height of a rational point

Bounding the least height of a $\mathbb{Q}$-point on a variety $V$ over $\mathbb{Q}$ is a hard problem whose solution implies Hilbert's 10th Problem for $\mathbb{Q}$. Amongst the Fano varieties it is only for quadrics that the known bound is essentially best possible, which is due to Cassels [12]. Tschinkel gave a conjecture for the size of the smallest $\mathbb{Q}$-point [57, Section 4.16]. In this direction we have the following result.

**Corollary 1.7** *Let $\varepsilon > 0$, $a \in \mathbb{Z}$, $a \neq 0$, and $d \in \mathbb{N}$. For a positive proportion of polynomials $P(t) \in \mathbb{Z}[t]$ of degree $d$, the equation $x^2 - ay^2 = P(t)z^2$ has a solution $(x, y, z, t) \in \mathbb{N}^4$ with*

$$\max\{x, y, z, t\} \leqslant |a|^{1/2}|P|^{1/2}(\log|P|)^{d/2+\varepsilon}.$$

To prove this we first note that the density of Bouniakowsky polynomials $P(t)$ of degree $d$ with $P(t) \equiv 1 \pmod{8a}$ exists and is positive; this is a special case of Corollary 2.9. Since these $P(t)$ satisfy $\gcd(P(0), 8a) = 1$, we use Corollary 1.6 with $n_0 = 0$ and $M = 8a$ to see that for 100% of Bouniakowsky polynomials $P(t)$ of degree $d$ with $P(t) \equiv 1 \pmod{8a}$ there exists a natural number $m \leqslant (\log|P|)^{1+\varepsilon}$ such that $P(m)$ is a prime $p$ satisfying $p \leqslant |P|(\log|P|)^{d+\varepsilon}$ and $p \equiv P(0) \equiv 1 \pmod{8a}$. Holzer's theorem [37] states that if $f_1, f_2, f_3$ are square-free pairwise coprime integers, not all of the same sign and such that $-f_i f_j$ is a quadratic residue modulo $f_k$ for all permutations $\{i, j, k\} = \{1, 2, 3\}$, then there exists $(x_1, x_2, x_3) \in \mathbb{Z}^3 \setminus \{(0, 0, 0)\}$ such that $\sum_{i=1}^3 f_i x_i^2 = 0$ and $|x_i| \leqslant \sqrt{|f_j f_k|}$. Writing $a = a_0 b^2$, where $a_0$ is square-free, we can apply Holzer's theorem for $f_1 = -1$, $f_2 = a_0$, $f_3 = p$. Indeed, if $a_0 = s 2^\pi w$, where $s \in \{\pm 1\}$, $\pi \in \{0, 1\}$, and $w$ is a positive odd integer, then the quadratic Jacobi symbols satisfy

$$\left(\frac{a_0}{p}\right) = \left(\frac{w}{p}\right) = \left(\frac{p}{w}\right) = 1,$$

due to $p \equiv 1 \pmod 8$ and $p \equiv 1 \pmod w$. Thus $a_0$ is a square modulo $p$. Clearly, $p$ is a square modulo $a_0$. By Holzer's theorem the equation given by $x^2 - a_0 y^2 = pz^2$ has a non-zero integer solution $(x_0, y_0, z_0)$ with $\max\{|x_0|, |y_0|, |z_0|\} \leqslant (|a_0|p)^{1/2}$. Then $(x_1, y_1, z_1) = (bx_0, y_0, bz_0)$ is a non-zero solution of $x^2 - ay^2 = pz^2$ that satisfies

$$\max\{|x_1|, |y_1|, |z_1|\} \leqslant b(|a_0|p)^{1/2} = (|a|p)^{1/2} \leqslant |a|^{1/2}|P|^{1/2}(\log|P|)^{d/2+\varepsilon}.$$

**The Bateman–Horn conjecture**

Theorem 1.5 is a corollary of Theorem 1.9 below. To state it we introduce a prime counting function and a truncated singular series.

**Definition 1.8** Let $\mathbf{P} \in (\mathbb{Z}[t])^n$, $P_i > 0$, let $n_0 \in \mathbb{Z}$, and let $M \in \mathbb{N}$. For $x \geqslant 1$ define the functions

$$\theta_{\mathbf{P}}(x) = \sum_{\substack{m \in \mathbb{N} \cap [1, x] \\ m \equiv n_0 \pmod M \\ P_i(m) \text{ prime for } i=1,\ldots,n}} \prod_{i=1}^n \log P_i(m), \tag{1.4}$$

$$\mathfrak{S}_{\mathbf{P}}(x) = \frac{\mathbb{1}(\gcd(M, \prod_{i=1}^n P_i(n_0)) = 1)}{\varphi(M)^n M^{1-n}} \prod_{\substack{\ell \text{ prime},\ \ell \nmid M \\ \ell \leqslant \log x}} \frac{1 - \ell^{-1} Z_{P_1 \ldots P_n}(\ell)}{\left(1 - \ell^{-1}\right)^n}. \tag{1.5}$$

The function $\mathfrak{S}_{\mathbf{P}}(x)$ is a truncated version of the Hardy–Littlewood singular series associated to Schinzel's Hypothesis for the polynomials $P_1(n_0 + Mt), \ldots, P_n(n_0 + Mt)$, see [6]. The reason for considering $P_i(n_0 + Mt)$ instead of $P_i(t)$ is because $\theta_{\mathbf{P}}(x)$ involves the condition $m \equiv n_0 \pmod M$.

A standard argument based on the prime number theorem for number fields shows that for a fixed $\mathbf{P}$ the product $\mathfrak{S}_{\mathbf{P}}(x)$ converges as $x \to \infty$. However, the convergence is absolute only when each $P_i$ is linear. Since we treat general polynomials, we have chosen to work with the truncated version to avoid problems related to the lack of absolute convergence.

The Bateman–Horn conjecture states that

$$\theta_{\mathbf{P}}(x) - \mathfrak{S}_{\mathbf{P}}(x)x = o(x).$$

Our next result shows that the estimate

$$\theta_{\mathbf{P}}(x) - \mathfrak{S}_{\mathbf{P}}(x)x = O\left(\frac{x}{\sqrt{\log x}}\right)$$

holds for 100% of $\mathbf{P} \in (\mathbb{Z}[t])^n$ in a certain range for $x$. Let

$$\mathscr{R}(x, H) = \frac{1}{\sharp \mathtt{Poly}(H)} \sum_{\mathbf{P} \in \mathtt{Poly}(H)} \left|\theta_{\mathbf{P}}(x) - \mathfrak{S}_{\mathbf{P}}(x)x\right|$$

be the average over all $n$-tuples $\mathbf{P}$ of the error terms in the Bateman–Horn conjecture.

**Theorem 1.9** *Let $n, d_1, \ldots, d_n, M$ be positive integers. Let $n_0 \in \mathbb{Z}$ and let $\mathbf{Q} = (Q_i(t)) \in (\mathbb{Z}[t])^n$. Fix arbitrary $A_1, A_2 \in \mathbb{R}$ with $n < A_1 < A_2$. Then for all $H \geqslant 3$ and all $x \geqslant 3$ with*

$$(\log H)^{A_1} < x \leqslant (\log H)^{A_2}$$

*we have*

$$\mathscr{R}(x, H) \ll \frac{x}{\sqrt{\log x}},$$

*where the implied constant depends only on $d_1, \ldots, d_n, M, n_0, \mathbf{Q}, A_1, A_2$.*

The necessity of $A_1 > n$ is addressed in Remark 4.2; one cannot expect typical polynomials to represent primes when the input is not large compared to the coefficients, and $m \approx (\log |\mathbf{P}|)^n$ seems to be a natural barrier.

From Theorem 1.9 and Markov's inequality one immediately deduces a form of the Bateman–Horn conjecture valid for almost all polynomials. For simplicity we state this result only in the case $n = M = n_0 = 1$.

**Corollary 1.10** *Let $d$ be a positive integer. Fix any $c \in \mathbb{R}$ with $0 < c < 1/2$ and any $A_1, A_2 \in \mathbb{R}$ with $1 < A_1 < A_2$. Then for all irreducible*

*$P \in \mathbb{Z}[t]$, $P > 0$, with $\deg(P) = d$ and all $x$ with $(\log|P|)^{A_1} < x \leqslant (\log|P|)^{A_2}$ we have*

$$\sum_{\substack{m\in\mathbb{N}\cap[1,x]\\ P(m)\text{ prime}}} \log P(m) = \left(\prod_{\substack{\ell \text{ prime}\\ \ell\leqslant \log x}} \frac{1-\ell^{-1}Z_P(\ell)}{1-\ell^{-1}}\right) x + O\left(\frac{x}{(\log x)^c}\right),$$

*with the exception of at most $O(H^{d+1}(\log\log H)^{c-1/2})$ of polynomials $P$ such that $|P| \leqslant H$.*

The asymptotic is meaningful, since $\mathfrak{S}_P(x) \gg (\log\log x)^{1-d}$ as long as $\mathfrak{S}_P(x) \neq 0$, see Lemma 4.11.

**Comparison with the literature**

Our main result, Theorem 1.9, is a vast generalisation of the well-known Barban–Davenport–Halberstam theorem on primes in arithmetic progressions, which gives a bound on

$$\sum_{\substack{1\leqslant q\leqslant Q\\ a\in(\mathbb{Z}/q\mathbb{Z})^*}} \left(\sum_{\substack{\text{prime } p\leqslant X\\ p\equiv a \,(\text{mod } q)}} \log p - \frac{X}{\varphi(q)}\right)^2.$$

To bring it to a form comparable to Theorem 1.9 we write $H = Q$, $x = X/Q$ and $P(t) = a + qt$, from which it becomes evident that the left hand side is essentially equal to

$$\sum_{\substack{P\in\mathbb{Z}[t]:\ \deg(P)=1\\ |P|\leqslant H}} \left(\sum_{\substack{m\leqslant x\\ P(m)\text{ prime}}} \log P(m) - \mathfrak{S}_P(x)x\right)^2.$$

While the Barban–Davenport–Halberstam theorem concerns a single linear polynomial, our work covers an arbitrary number of polynomials, each of arbitrary degree. Prior to our paper there has been a number of results on averaged forms of Bateman–Horn for special polynomials.

The work of Friedlander–Granville [30] has special interest in connection to our work as it shows that there are unexpectedly large fluctuations in the error term of the Bateman–Horn asymptotic; it would be interesting to understand analogous questions in the setting of Corollary 1.10. Furthermore, it would be

| $n$ | $P_1(t), \ldots, P_n(t)$ | Authors |
|---|---|---|
| $\geqslant 1$ | $t+b_1, \ldots, t+b_n$ | Lavrik [43] |
| 2 | $t, t+b$ | Lavrik [42], Mikawa [48], Wolke [59] |
| 1 | $at+b$ | Barban [5], Davenport–Halberstam [23] |
| $\geqslant 1$ | $a_1t+b_1, \ldots, a_nt+b_n$ | Balog [4] |
| 1 | $t^d+at+b$ | Friedlander–Granville [30] |
| 1 | $t^2+t+b$ and $t^2+b$ | Granville–Mollin [31] |
| 1 | $t^2+b$ | Baier–Zhao [2,3] |
| 1 | $t^3+b$ | Foo–Zhao [27] |
| 1 | $t^4+b$ | Yau [61] |
| 1 | $t^d+b$ | Zhou [63] |

interesting to investigate the case where one ranges over degree $d$ polynomials with a fixed coefficient; this corresponds to work of Friedlander–Goldston [29] where this is investigated for linear polynomials with fixed leading coefficient.

## Method of proof

Theorem 1.9 is a generalisation of Montgomery's proof of the Barban–Davenport–Halberstam theorem, which corresponds to the case $n = 1$ and $d_1 = 1$ of Theorem 1.9. By Cauchy–Schwarz we have

$$\mathscr{R}(x, H)^2 \leqslant \mathscr{V}(x, H) := \frac{1}{\sharp \texttt{Poly}(H)} \sum_{\mathbf{P} \in \texttt{Poly}(H)} (\theta_{\mathbf{P}}(x) - \mathfrak{S}_{\mathbf{P}}(x)x)^2, \tag{1.6}$$

which is the kind of second moment function studied in the BDH theorem. The original proof of the BDH theorem is a direct application of the large sieve; such an approach only applies to polynomials of very special shape, see [2,27]. The initial arguments in our paper are in fact closer to Montgomery's proof of the BDH theorem [50], which does not rely on the large sieve.

First, we open up the square in $\mathscr{V}(x, H)$ to get three terms: the second moments $\theta_{\mathbf{P}}(x)^2$ and $x^2\mathfrak{S}_{\mathbf{P}}(x)^2$, and the correlation $x\mathfrak{S}_{\mathbf{P}}(x)\theta_{\mathbf{P}}(x)$. The hardest term is $\theta_{\mathbf{P}}(x)^2$ and here Montgomery's approach relies exclusively on Lavrik's result on twin primes [42,43]. Lavrik's argument makes heavy use of the Hardy–Littlewood circle method and Vinogradov's estimates of exponential sums. In our work we need a suitable generalisation of Lavrik's result; this is provided by our Theorem 3.1. It produces an asymptotic for simultaneous prime values of two linear polynomials in an arbitrary number of variables, where the error term is uniform in the size of the coefficients. The difference between our work and that of Montgomery and Lavrik is that to prove Theorem 3.1 we do not use the circle method and we instead employ the

*Möbius randomness law*, see Sect. 3. This approach in the area of the averaged Bateman–Horn conjecture is new.

Next, we show that the three principal terms cancel out by constructing a probability space that models the behaviour of functions involving $Z$, see Sect. 2. This task inevitably leads to new complications of combinatorial nature, compared to the aforementioned papers on special polynomials where the Bateman–Horn singular series has a useful expression in terms of $L$-functions (see [2,27], for example). The final stages of the proof of Theorem 1.9 can be found in Sect. 4.4 and that of Theorem 1.5 in §4.5.

Applications to rational points, including the proofs of Theorems 1.3 and 1.4 , can be found in Sects. 5 and 6.

## Notation

The quantities $A_1, A_2, \delta_1, \delta_2, n, d_1, \ldots, d_n, \mathbf{Q}, n_0, M$, will be considered constant throughout. In particular, the dependence of implied constants in the big $O$ notation on these quantities will not be recorded. Any other dependencies of the implied constants on further parameters will be explicitly specified via the use of a subscript. Whenever we use iterated logarithm functions $\log t$, $\log\log t$, etc., we assume that $t$ is large enough to make the iterated logarithm well-defined.

## 2 Bernoulli models of Euler factors

In this section we study the $\ell$-factor $1 - \ell^{-1} Z_{P_1 \ldots P_n}(\ell)$ of the Euler product (1.5). We prove that if $P_1, \ldots, P_n$ are random polynomials of bounded degree in $\mathbb{F}_\ell[t]$, this factor is modelled by the arithmetic mean of $\ell$ pairwise independent, identically distributed Bernoulli random variables defined on a product of probability spaces. The results of this section are used in Sect. 4 to prove cancellation of principal terms. Proposition 2.8 is used to prove Theorem 1.5 in Sect. 4.5.

### 2.1 Bernoulli model

Let $\ell$ be a prime. Consider the probability space $(\Omega(d), \mathbb{P})$, where

$$\Omega(d) := \{P \in \mathbb{F}_\ell[t] : \deg(P) \leqslant d\}$$

and $\mathbb{P}$ is the uniform discrete probability. For every $m \in \mathbb{F}_\ell$ we define the Bernoulli random variable $Y_m : \Omega(d) \to \{0, 1\}$ by

$$Y_m = \begin{cases} 1, & \text{if } P(m) \neq 0 \text{ in } \mathbb{F}_\ell, \\ 0, & \text{otherwise.} \end{cases}$$

We have $Y_m = \chi(P(m))$, where $\chi$ is the principal Dirichlet character on $\mathbb{F}_\ell$.

**Lemma 2.1** *Let $\mathscr{J} \subset \mathbb{F}_\ell$ be a subset of cardinality $s \leqslant d + 1$. Then the variables $Y_m$ for $m \in \mathscr{J}$ are independent, and we have*

$$\mathbb{E}_{\Omega(d)} \prod_{m \in \mathscr{J}} Y_m = \prod_{m \in \mathscr{J}} \mathbb{E}_{\Omega(d)} Y_m = (1 - \ell^{-1})^s.$$

*Proof* It is enough to prove that

$$\begin{aligned} &\mathbb{E}_{\Omega(d)} \prod_{m \in \mathscr{J}} (1 - Y_m) \\ &= \frac{1}{\ell^{d+1}} \sharp \left\{ P \in \mathbb{F}_\ell[t] : \deg(P) \leqslant d,\, P(m) = 0 \text{ if } m \in \mathscr{J} \right\} = \frac{1}{\ell^s}. \end{aligned} \tag{2.1}$$

By the non-vanishing of the Vandermonde determinant this condition describes an $\mathbb{F}_\ell$-vector subspace of $\Omega(d)$ of codimension $s$, hence the result. □

Let $n \in \mathbb{N}$ and let $d_1, \ldots, d_n \in \mathbb{N}$. Consider $\Omega = \Omega(d_1) \times \ldots \times \Omega(d_n)$ as a Cartesian probability space equipped with the product measure

$$\mathbb{P}(A_1 \times \ldots \times A_n) := \mathbb{P}_1(A_1) \ldots \mathbb{P}_n(A_n), \quad \text{for all } \; A_i \subseteq \Omega(d_i), \tag{2.2}$$

where each $\mathbb{P}_i$ is the uniform discrete probability on $\Omega(d_i)$. For $m \in \mathbb{F}_\ell$ define the Bernoulli random variable $X_m : \Omega \to \{0, 1\}$ by

$$X_m = \begin{cases} 1, & \text{if } \prod_{i=1}^n P_i(m) \neq 0 \text{ in } \mathbb{F}_\ell, \\ 0, & \text{otherwise.} \end{cases}$$

It is clear that

$$X_1 + \ldots + X_\ell = \ell - Z_{P_1 \ldots P_n}(\ell). \tag{2.3}$$

**Lemma 2.2** *For all $m \in \mathbb{F}_\ell$ we have $\mathbb{E}_\Omega X_m = (1 - \ell^{-1})^n$.*

*Proof* This is immediate from Lemma 2.1. □

**Lemma 2.3** *For all $k \neq m \in \mathbb{F}_\ell$ the random variables $X_k$ and $X_m$ are independent.*

*Proof* Since $X_k$ and $X_m$ are Bernoulli random variables, it suffices to show that they are uncorrelated. Using Lemma 2.2 we write the covariance of $X_k$ and $X_m$ as

$$\mathbb{E}_\Omega\left[\left(\prod_{i=1}^{n}\chi(P_i(m)) - \left(1-\ell^{-1}\right)^n\right)\left(\prod_{j=1}^{n}\chi(P_j(k)) - \left(1-\ell^{-1}\right)^n\right)\right],$$

which equals

$$\begin{aligned}&\mathbb{E}_\Omega\left[\prod_{i=1}^{n}\chi(P_i(m))\chi(P_i(k))\right] - \left(1-\ell^{-1}\right)^{2n}\\ &= \left(\prod_{i=1}^{n}\mathbb{E}_{\Omega(d_i)}\left[\chi(P(m))\chi(P(k))\right]\right) - \left(1-\ell^{-1}\right)^{2n}\end{aligned}$$

by (2.2). Since $d_i \geqslant 1$ for all $i = 1, \ldots, n$, we conclude the proof by applying Lemma 2.1. □

For $d, s \in \mathbb{Z}_{\geqslant 0}$ define

$$G_\ell(d, s) := \sum_{r=0}^{s}\binom{s}{r}\frac{(-1)^r}{\ell^{\min\{r, 1+d\}}}. \tag{2.4}$$

**Lemma 2.4** *For a subset $\mathscr{J} \subset \mathbb{F}_\ell$ of cardinality $s$ we have*

$$\mathbb{E}_\Omega \prod_{m\in\mathscr{J}} X_m = \prod_{k=1}^{n} G_\ell(d_k, s).$$

*Proof* By multiplicativity of the principal Dirichlet character $\chi$ we have

$$\prod_{m\in\mathscr{J}} X_m = \prod_{m\in\mathscr{J}}\chi\left(\prod_{k=1}^{n} P_k(m)\right) = \prod_{k=1}^{n}\chi\left(\prod_{m\in\mathscr{J}} P_k(m)\right),$$

hence

$$\mathbb{E}_\Omega \prod_{m\in\mathscr{J}} X_m = \prod_{k=1}^{n}\mathbb{E}_{\Omega(d_k)}\prod_{m\in\mathscr{J}}\chi(P(m)).$$

For a fixed $k$ we have

$$\mathbb{E}_{\Omega(d_k)} \prod_{m\in\mathscr{J}} \chi(P(m)) = \mathbb{E}_{\Omega(d_k)} \prod_{m\in\mathscr{J}} Y_m$$
$$= \sum_{r=0}^{s} (-1)^{\sharp\mathscr{A}} \sum_{\mathscr{A}\subset\mathscr{J}} \mathbb{E}_{\Omega(d_k)} \prod_{m\in\mathscr{A}} (1-Y_m).$$

From the definition of the random variables $Y_m$ we get

$$\mathbb{E}_{\Omega(d_k)} \prod_{m\in\mathscr{A}} (1-Y_m)$$
$$= \ell^{-(d_k+1)} \sharp\left\{P \in \mathbb{F}_\ell[t] : \deg(P) \leqslant d_k,\, P(m) = 0 \text{ if } m \in \mathscr{A}\right\}.$$

If $\sharp\mathscr{A} \leqslant d_k + 1$, this equals $\ell^{-\sharp\mathscr{A}}$ by (2.1). If $\sharp\mathscr{A} \geqslant d_k + 1$, then $P$ has more than $\deg(P)$ roots in $\mathbb{F}_\ell$, hence $P$ is identically zero and the quantity above is $\ell^{-(d_k+1)}$. Thus

$$\mathbb{E}_{\Omega(d_k)} \prod_{m\in\mathscr{A}} (1-Y_m) = \ell^{-\min\{\sharp\mathscr{A}, d_k+1\}}.$$

This implies the lemma. □

**Lemma 2.5** (Joint distribution of Bernoulli variables) *For* $\gamma_1, \ldots, \gamma_\ell \in \{0, 1\}$ *we have*

$$\mathbb{P}\left[X_m = \gamma_m \text{ for all } m = 1, \ldots, \ell\right]$$
$$= (-1)^{\sharp\{i:\gamma_i=0\}} \sum_{\substack{\mathscr{J}\subset\mathbb{F}_\ell \\ i\notin\mathscr{J} \Rightarrow \gamma_i=0}} (-1)^{\ell-\sharp\mathscr{J}} \prod_{k=1}^{n} G_\ell(d_k, \sharp\mathscr{J}).$$

*Proof* The event $X_m = \gamma_m$ for $\gamma_m = 0$ (respectively, $\gamma_m = 1$) is detected by the function $1 - X_m$ (respectively, $X_m$). Therefore, writing $\beta_i = 1 - \gamma_i$ we obtain

$$\mathbb{P}\left[X_m = \gamma_m \text{ for all } m = 1, \ldots, \ell\right] = (-1)^{\sharp\{i:\,\gamma_i=0\}} \mathbb{E}_\Omega \prod_{m=1}^{\ell} (X_m - \beta_m).$$

The mean in the right hand side equals

$$\sum_{\mathscr{J}\subset\mathbb{F}_\ell} \left(\prod_{i\notin\mathscr{J}} (-\beta_i)\right) \mathbb{E}_\Omega \prod_{i\in\mathscr{J}} X_i = \sum_{\mathscr{J}\subset\mathbb{F}_\ell} (-1)^{\ell-\sharp\mathscr{J}} \prod_{k=1}^{n} G_\ell(d_k, \sharp\mathscr{J}) \prod_{i\notin\mathscr{J}} \beta_i$$

due to Lemma 2.4. In view of $\beta_i \in \{0, 1\}$ this proves the lemma. □

### 2.2 Consequences of the Bernoulli model

For $n \in \mathbb{N}$ and any prime $\ell$ define

$$\gamma_n(\ell) := 1 - \frac{1}{\ell} + \frac{\ell^{n-1}}{(\ell-1)^n}. \tag{2.5}$$

**Lemma 2.6** *We have*

$$\ell^{-(d+n)} \sum_{\substack{P_1 \in \mathbb{F}_\ell[t],\, \deg(P_1) \leqslant d_1 \\ \cdots \\ P_n \in \mathbb{F}_\ell[t],\, \deg(P_n) \leqslant d_n}} \left(1 - \frac{Z_{P_1 \ldots P_n}(\ell)}{\ell}\right)^2 = \gamma_n(\ell) \left(1 - \frac{1}{\ell}\right)^{2n}.$$

*Proof* We write the left hand side as $\ell^{-2}\mathbb{E}_\Omega[(X_1 + \ldots + X_\ell)^2]$, open up the square and use Lemmas 2.2 and 2.3. □

By considering $\ell^{-1}\mathbb{E}_{\mathbf{P} \in \Omega}[X_1 + \ldots + X_\ell]$ instead we obtain

$$\ell^{-(d+n)} \sum_{\substack{P_1 \in \mathbb{F}_\ell[t],\, \deg(P_1) \leqslant d_1 \\ \cdots \\ P_n \in \mathbb{F}_\ell[t],\, \deg(P_n) \leqslant d_n}} \left(1 - \frac{Z_{P_1 \ldots P_n}(\ell)}{\ell}\right) = \left(1 - \frac{1}{\ell}\right)^{n}.$$

**Lemma 2.7** *Fix any $m \in \mathbb{N}$. We have*

$$\ell^{-(d+n)} \sum_{\substack{P_1 \in \mathbb{F}_\ell[t],\, \deg(P_1) \leqslant d_1,\, P_1(m) \neq 0 \\ \cdots \\ P_n \in \mathbb{F}_\ell[t],\, \deg(P_n) \leqslant d_n,\, P_n(m) \neq 0}} \left(1 - \frac{Z_{P_1 \ldots P_n}(\ell)}{\ell}\right) = \gamma_n(\ell) \left(1 - \frac{1}{\ell}\right)^{2n}.$$

*Proof* By (2.3) and Lemma 2.3 the left hand side in our lemma equals

$$\mathbb{E}_\Omega\left[\left(\frac{X_1 + \ldots + X_\ell}{\ell}\right) X_m\right] = \frac{\mathbb{E}_\Omega[X_m]}{\ell} + \frac{\mathbb{E}_\Omega[X_m]}{\ell} \sum_{i \neq m} \mathbb{E}_\Omega[X_i].$$

The proof now concludes by using Lemma 2.2. □

### 2.3 Density of Schinzel $n$-tuples

For a prime $\ell$ define the set

$$\mathtt{T}_\ell := \{\mathbf{P} \in (\mathbb{F}_\ell[t])^n : Z_{P_1 \dots P_n}(\ell) \neq \ell,\ \deg(P_i) \leqslant d_i \text{ for all } \ i = 1, \dots, n\}.$$

By Lemma 2.5 with all $\gamma_i = 0$ we have $\sharp \mathtt{T}_\ell = (1 - c_\ell)\ell^{d+n}$, where

$$c_\ell := \sum_{\mathscr{J} \subset \mathbb{F}_\ell} (-1)^{\sharp \mathscr{J}} \prod_{k=1}^{n} G_\ell(d_k, \sharp \mathscr{J}). \tag{2.6}$$

When $\ell > d$ it is easy to see that $\sharp \mathtt{T}_\ell = \prod_{i=1}^n (\ell^{d_i+1} - 1)$, hence $1 - c_\ell = \prod_{i=1}^n (1 - \ell^{-(d_i+1)})$.

**Proposition 2.8** *For any $M \in \mathbb{N}$ we have*

$$\sharp\{\mathbf{P} \in \mathtt{Poly}(H) : Z_{P_1 \dots P_n}(\ell) \neq \ell \text{ for all } \ell \nmid M\} = 2^d \left( \prod_{\text{prime } \ell \nmid M} (1 - c_\ell) \right) \left( \frac{H}{M} \right)^{d+n} + O\left( \frac{H^{d+n}}{\log H} \right).$$

*The infinite product converges absolutely to a positive real number. In particular, the set of Schinzel $n$-tuples of given degrees has positive density in the set of all $n$-tuples of integer polynomials of the same degrees.*

*Proof* Let $\mathscr{W}$ be the product of all primes $\ell < \frac{1}{10} \log H$ such that $\ell \nmid M$. Define

$$K(H) = \sharp \left\{ \mathbf{P} \in \mathtt{Poly}(H) : Z_{P_1 \dots P_n}(\ell) \neq \ell \text{ for all primes } \ell | \mathscr{W} \right\}.$$

The counting function in the proposition is $K(H) + O(H^{d+n}(\log H)^{-1})$. Indeed, the number of $\mathbf{P} \in \mathtt{Poly}(H)$ such that for some $j = 1, \dots, n$ there is a prime $\ell > \frac{1}{10} \log H$ for which $P_j$ is identically zero on $\mathbb{F}_\ell$ is

$$\ll \sum_{\text{prime } \ell > \frac{1}{10} \log H} \left( \prod_{\substack{i=1 \\ i \neq j}}^{n} H^{1+d_i} \right) (H/\ell)^{1+d_j} \ll H^{d+n} \sum_{\text{prime } \ell > \frac{1}{10} \log H} \ell^{-2} \ll H^{d+n} (\log H)^{-1}.$$

We have

$$K(H)=\sum_{\mathbf{P}\in \mathtt{Poly}(H)}\prod_{\text{prime }\ell|\mathscr{W}}\mathbb{1}_{\mathtt{T}_\ell}(\mathbf{P})=2^{-n}\left(\frac{2H}{\mathscr{W}M}+O(1)\right)^{d+n}\prod_{\text{prime }\ell|\mathscr{W}}\sharp\mathtt{T}_\ell,$$

by the Chinese remainder theorem applied to the coefficients of the polynomials $P_i$. Taking into account that $\sharp\mathtt{T}_\ell=(1-c_\ell)\ell^{d+n}$ we rewrite this as

$$K(H)=2^d\left(\frac{H}{M}+O(1)\mathscr{W}\right)^{d+n}\prod_{\text{prime }\ell|\mathscr{W}}(1-c_\ell).$$

Note that $\log\mathscr{W}\leqslant\sum_{\ell\leqslant(\log H)/10}\log\ell\leqslant(\log H)/2$ for all sufficiently large $H$ by the prime number theorem. Hence $\mathscr{W}\leqslant H^{1/2}$, which implies

$$K(H)=2^d\left(\frac{H}{M}\right)^{n+d}\prod_{\text{prime }\ell|\mathscr{W}}(1-c_\ell)+O(H^{d+n-1/2}).$$

The estimate $\prod_{\text{prime }\ell>\frac{1}{10}\log H}\left(1-\ell^{-(d_i+1)}\right)=1+O((\log H)^{-d_i})$ concludes the proof.

The product converges absolutely because for all $\ell>d$ we have

$$1-c_\ell=\prod_{i=1}^{n}(1-\ell^{-(d_i+1)})=1+O(\ell^{-2}).$$

Since $\mathtt{T}_\ell\neq\varnothing$ we have $\sharp\mathtt{T}_\ell=(1-c_\ell)\ell^{d+n}>0$, so the infinite product is positive. □

**Corollary 2.9** *Fix $d,M\in\mathbb{N}$. Let $Q(t)\in\mathbb{Z}[t]$ be a polynomial of degree at most $d$. The number of degree $d$ polynomials $f(t)\in\mathbb{Z}[t]$ with positive leading coefficient and height at most $H$ such that $f\equiv Q\ (\mathrm{mod}\ M)$ and $Z_f(\ell)\neq\ell$ for each prime $\ell\nmid M$ is*

$$2^d\left(\prod_{\text{prime }\ell\nmid M}(1-\ell^{-\min\{\ell,d+1\}})\right)\frac{H^{d+1}}{M^{d+1}}+O\left(\frac{H^{d+1}}{\log H}\right).$$

*Proof* We apply Proposition 2.8 in the case $n=1$. For $\ell>d+1$ we have $c_\ell=\ell^{-(d+1)}$. If $s\leqslant d+1$ then (2.4) becomes $G_\ell(d,s)=(1-1/\ell)^s$. Hence for $\ell\leqslant d+1$, (2.6) gives $c_\ell=\ell^{-\ell}$. □

The case $M=1$ of Corollary 2.9 is particularly useful and is worth recording separately:

**Corollary 2.10** *The number of degree d Bouniakowsky polynomials of height at most H is*

$$2^d\left(\prod_{\text{prime } \ell}(1-\ell^{-\min\{\ell,d+1\}})\right)H^{d+1}+O\left(\frac{H^{d+1}}{\log H}\right).$$

## 3 Möbius randomness law

For any $d,k,m\in\mathbb{N}$ and $H\geqslant 1$ we let

$$\mathscr{G}_{k,m}(H;d):=\sum_{\substack{P\in\mathbb{Z}[t],\ \deg(P)=d\\ |P|\leqslant H,\ P>0}}\Lambda(P(k))\Lambda(P(m)),\tag{3.1}$$

where $\Lambda(n)$ is the von Mangoldt function. The main result of this section is the following asymptotic for $\mathscr{G}_{k,m}(H;d)$ as $H\to\infty$ that exhibits an effective dependence on $k$ and $m$.

**Theorem 3.1** *Fix any $d\in\mathbb{N}$ and $\delta>0$. Then for all $H\geqslant 1$, $A>0$, and all natural numbers $k,m\leqslant(\log H)^{\delta}$, $k\neq m$, we have*

$$\mathscr{G}_{k,m}(H;d)=2^dH^{d+1}\prod_{\substack{p\text{ prime}\\ p|k-m}}\frac{p}{p-1}+O_A\left(H^{d+1}(\log H)^{-A}\right),$$

*where the implied constant is independent of $k,m$ and $H$.*

### 3.1 Using Möbius randomness law

As usual, $\mu(r)$ is the Möbius function. In broad terms, the Möbius randomness law is a general principle which states that long sums containing the Möbius function should exhibit cancellation. An early example is the following result of Davenport, whose proof is based on bilinear sums techniques.

**Lemma 3.2** (Davenport) *Fix $A>0$. Then for all $y\geqslant 1$ we have*

$$\sup_{\alpha\in\mathbb{R}}\left|\sum_{r\in\mathbb{N}\cap[1,y]}\mu(r)\mathrm{e}^{ir\alpha}\right|\ll y(\log y)^{-A},$$

*where the implied constant depends only on A.*

*Proof* See [22] or [39, Thm. 13.10]. □

Recall that for $r \in \mathbb{N}$ we have $\Lambda(r) = -\sum_{d|r} \mu(d) \log d$. We define the truncated von Mangoldt function

$$\Lambda_z(r) := -\sum_{d \leqslant z,\, d|r} \mu(d) \log d, \quad \text{where} \quad z \geqslant 1,$$

which will give rise to the main term in Theorem 3.1 for suitably large $z$. The remainder

$$\mathscr{E}_z(r) := \Lambda(r) - \Lambda_z(r)$$

will contribute to the error term. When taking the sum over $r$, the variable $d$ in $\mathscr{E}_z(r) = -\sum_{z<d, d|r} \mu(d) \log d$ runs over a long segment, so the presence of $\mu(d)$ will give rise to cancellations. In particular, $\Lambda_z(r)$ is a good approximation to $\Lambda(r)$ for suitably large $z$ and when one sums over $r$. The advantage of this is that one can easily take care of various error terms in averages involving $\Lambda_z(r)$, due to truncation.

We shall use the following corollary of Lemma 3.2.

**Corollary 3.3** *Fix $A > 0$. Then for all $y, z \geqslant 1$ we have*

$$\sup_{\alpha \in \mathbb{R}} \left| \sum_{r \in \mathbb{N} \cap [1, y]} \mathscr{E}_z(r) \mathrm{e}^{ir\alpha} \right| \ll_A y (\log y)(\log z)^{-A},$$

*where the implied constant depends only on $A$.*

*Proof* See [39, Eq. (19.17)]. □

For a function $F : \mathbb{Z} \to \mathbb{R}$ we denote

$$S_F(\alpha) := \sum_{\substack{c \in \mathbb{Z} \\ |c| \leqslant (d+1)\mathscr{M}^d H}} F(c) \mathrm{e}^{ic\alpha},$$

where $\mathscr{M} = \max\{k, m\}$. Recall that for $t \in \mathbb{R}$, $H \in [1, \infty)$ the Dirichlet kernel is defined as

$$D_H(t) := \sum_{|c| \leqslant H} \mathrm{e}^{ict}.$$

We will also use $D_H^+(t) := \sum_{0<c \leqslant H} \mathrm{e}^{ict}$.

**Lemma 3.4** *For any integers $k, m$ and any functions $f, g : \mathbb{Z} \to \mathbb{R}$ we have*

$$\sum_{\substack{P \in \mathbb{Z}[t],\ P>0 \\ |P| \leqslant H,\ \deg(P)=d}} f(P(k))g(P(m)) = \frac{1}{4\pi^2} \int\limits_{(-\pi,\pi]^2} \overline{S_f(\alpha_1) S_g(\alpha_2)} D_H^+(k^d\alpha_1 + m^d\alpha_2) \times \prod_{j=0}^{d-1} D_H(k^j\alpha_1 + m^j\alpha_2)\, \mathrm{d}\boldsymbol{\alpha}.$$

Proof. Firstly, we write

$$\sum_{\substack{|P| \leqslant H \\ P>0}} f(P(k))g(P(m)) = \sum_{|k_1|,|k_2| \leqslant (d+1)\mathscr{M}^d H} f(k_1)g(k_2) \sum_{\substack{|P| \leqslant H \\ P>0}} \mathbb{1}(k_1 = P(k))\mathbb{1}(k_2 = P(m)).$$

The following identity holds for all integers $r$ and $s$:

$$\mathbb{1}(r=s) = \frac{1}{2\pi}\int_{-\pi}^{\pi} \mathrm{e}^{i(r-s)\alpha}\mathrm{d}\alpha.$$

Using it twice turns the sum into

$$\frac{1}{4\pi^2}\int_{-\pi}^{\pi}\int_{-\pi}^{\pi} \sum_{|k_1| \leqslant (d+1)\mathscr{M}^d H} f(k_1)\mathrm{e}^{-ik_1\alpha_1} \sum_{|k_2| \leqslant (d+1)\mathscr{M}^d H} g(k_2)\mathrm{e}^{-ik_2\alpha_2} \times \sum_{\substack{|P| \leqslant H \\ P>0}} \mathrm{e}^{i(P(k)\alpha_1 + P(m)\alpha_2)}\mathrm{d}\alpha_1\mathrm{d}\alpha_2.$$

The sums over $k_1$ and $k_2$ are equal to $\overline{S_f(\alpha_1)}$ and $\overline{S_g(\alpha_2)}$, respectively. To analyse the sum over $P$ we write $P(t) = \sum_{j=0}^d c_j t^j$ and recall that we have $c_d \in (0, H]$. We obtain

$$\sum_{\substack{|P| \leqslant H \\ P>0}} \mathrm{e}^{i(P(k)\alpha_1 + P(m)\alpha_2)} = D_H^+(k^d\alpha_1 + m^d\alpha_2) \prod_{j=0}^{d-1} D_H(k^j\alpha_1 + m^j\alpha_2).$$

□

Before proceeding we recall a well-known result of Lebesgue [62, Eq. (12.1), p. 67],

$$\int_{-\pi}^{\pi} |D_H(t)|\mathrm{d}t = O(\log H). \tag{3.2}$$

**Lemma 3.5** *For any integers $k \neq m$ and any functions $f, g : \mathbb{Z} \to \mathbb{R}$ we have*

$$\sum_{\substack{|P|\leqslant H \\ P>0}} f(P(k))g(P(m)) \ll \|S_f\|_\infty S_{|g|}(0) H^{d-1} \frac{\mathscr{M}(\log H)^2}{|k-m|},$$

*where $\|S_f\|_\infty := \max\{|S_f(\alpha)| : \alpha \in \mathbb{R}\}$, and the implied constant depends at most on $d$.*

*Proof* The bounds $|S_g(\alpha)| \leqslant S_{|g|}(0)$, $|D_H^+(\alpha)| \leqslant H$, $|D_H(\alpha)| \leqslant 1 + 2H$ and Lemma 3.4 give

$$\sum_{\substack{|P|\leqslant H \\ P>0}} f(P(k))g(P(m)) \ll \|S_f\|_\infty S_{|g|}(0) H^{d-1} \int_{(-\pi,\pi]^2} |D_H(\alpha_1+\alpha_2)||D_H(k\alpha_1+m\alpha_2)|\mathrm{d}\boldsymbol{\alpha}.$$

The change of variables $t_1 = \alpha_1 + \alpha_2$, $t_2 = k\alpha_1 + m\alpha_2$ shows that the integral is at most

$$\frac{1}{|k-m|} \int_{-2\pi}^{2\pi} \int_{-2\pi\mathscr{M}}^{2\pi\mathscr{M}} |D_H(t_1)||D_H(t_2)|\mathrm{d}\mathbf{t}.$$

The Dirichlet kernel $D_H(t)$ is an even and $2\pi$-periodic function of $t$, thus

$$\int_{-2\pi}^{2\pi} \int_{-2\pi\mathscr{M}}^{2\pi\mathscr{M}} |D_H(t_1)||D_H(t_2)|\mathrm{d}\mathbf{t} = 4\mathscr{M} \int_{-\pi}^{\pi} \int_{-\pi}^{\pi} |D_H(t_1)||D_H(t_2)|\mathrm{d}\mathbf{t}.$$

The proof concludes by invoking Lebesgue's result (3.2). □

*Remark 3.6* The proof of Lemma 3.5 makes clear that in order to prove Theorem 3.1 one needs to range over only two random coefficients and we are allowed to have the remaining $d-1$ coefficients fixed.

*Remark 3.7* It would be interesting to study the $N$-th moment $\sum_{\mathbf{P}} (\theta_{\mathbf{P}}(x) - \mathfrak{S}_{\mathbf{P}}(x)x)^N$ in (1.6) for $N \geqslant 3$. The proof of Lemma 3.5 can be adapted for this problem as long as $d$ is not too small compared to $N$. For example, when $n = 1$ one would need to take $d \geqslant N - 1$.

**Proposition 3.8** *Fix any $d \geqslant 1$, $A > 0$, and $\delta_1, \delta_2 > 0$ with $\delta_1 < 1$. Then for all $z, H \geqslant 1$ such that $H^{\delta_1} \leqslant z \leqslant H$ and all natural numbers $k \neq m$ satisfying*

$$k, m \leqslant (\log H)^{\delta_2}$$

*we have*

$$\mathscr{G}_{k,m}(H; d) = \sum_{\substack{P \in \mathbb{Z}[t],\, \deg(P)=d \\ |P| \leqslant H,\, P>0}} \Lambda_z(P(k))\Lambda_z(P(m)) + O_A\left(\frac{H^{d+1}}{(\log H)^A}\right),$$

*where the implied constant does not depend on $k, m, H$ and $z$.*

*Proof* For both choices $f = \mathscr{E}_z$ and $f = \Lambda_z$ we have $|f(t)| \leqslant \sum_{m|t} \log m \leqslant (\log t)\tau(t)$, where $\tau$ is the divisor function. In particular, we get $\sum_{t \leqslant y} |f(t)| \ll y(\log y)^2$, which shows that

$$S_{|f|}(0) \ll H(\log H)^2 \mathscr{M}^d \ll H(\log H)^{2+d\delta_2}.$$

Furthermore, by Corollary 3.3 we have

$$\|S_{\mathscr{E}_z}\|_\infty \ll_C \mathscr{M}^d H(\log H)(\log z)^{-C} \ll_{\delta_1} H(\log H)^{1+d\delta_2-C} \tag{3.3}$$

for every $C > 0$. Therefore, by Lemmas 3.4 and 3.5 we obtain

$$\left|\sum_{|P| \leqslant H, P>0} \mathscr{E}_z(P(k))\mathscr{E}_z(P(m))\right|, \left|\sum_{|P| \leqslant H, P>0} \mathscr{E}_z(P(k))\Lambda_z(P(m))\right| \ll \frac{\mathscr{M} H^{d+1}}{(\log H)^{C-2d\delta_2-5}}.$$

Using $\mathscr{M} \leqslant (\log H)^{\delta_2}$ and letting $A = C - (2d+1)\delta_2 - 5$ gives the required error term. The proof now concludes by recalling that $\Lambda = \Lambda_z + \mathscr{E}_z$. □

For later use we need a version of this result for one polynomial value instead of two but with the additional condition that the polynomial is in an arithmetic progression.

**Lemma 3.9** *Fix $d \geqslant 1$ and $\delta_1, \delta_2 > 0$ with $\delta_1 < 1$. Then for all $z, H \geqslant 1$, $A > 0$, all natural numbers $k$, $\Omega$, and all $R \in (\mathbb{Z}/\Omega)[t]$ of degree at most $d$ such that*

$$k \leqslant (\log H)^{\delta_2},\ \ H^{\delta_1} \leqslant z \leqslant H,\ \ \Omega \leqslant H$$

*we have*

$$\sum_{\substack{|P| \leqslant H,\ P > 0 \\ \deg(P) = d \\ P \equiv R \,(\mathrm{mod}\ \Omega)}} \Lambda(P(k)) - \sum_{\substack{|P| \leqslant H,\ P > 0 \\ \deg(P) = d \\ P \equiv R \,(mod\ \Omega)}} \Lambda_z(P(k)) = O_A\left(\frac{H^{d+1}}{(\log H)^A}\right),$$

*where the implied constant does not depend on $k$, $m$, $H$, $R$, $\Omega$ and $z$.*

The crucial point is that the estimate is uniform in the progression.

*Proof* Using that $\Lambda - \Lambda_z = \mathscr{E}_z$ turns the left hand side into

$$\Bigg(\sum_{\substack{0 < c_d \leqslant H \\ c_d \equiv r_d \,(\mathrm{mod}\ \Omega)}} \mathrm{e}^{ic_d k^d \alpha_1}\Bigg) \prod_{j=0}^{d-1} \Bigg(\sum_{\substack{|c_j| \leqslant H \\ c_j \equiv r_j \,(\mathrm{mod}\ \Omega)}} \mathrm{e}^{ic_j k^j \alpha_1}\Bigg).$$

Writing $P(t) = \sum_{j=0}^d c_j t^j$ and choosing integers $0 \leqslant r_j < \Omega$ such that $R(t) \equiv \sum_{j=0}^d r_j t^j \pmod{\Omega}$, converts the right hand sum over $P$ into

$$\Bigg(\sum_{\substack{0<c_d\leqslant H \\ c_d\equiv r_d (\mathrm{mod}\ \Omega)}} \mathrm{e}^{ic_d k^d \alpha_1}\Bigg) \prod_{j=0}^{d-1} \Bigg(\sum_{\substack{|c_j|\leqslant H \\ c_j\equiv r_j (\mathrm{mod}\ \Omega)}} \mathrm{e}^{ic_j k^j \alpha_1}\Bigg).$$

For each $j \neq 0$ we bound the sum over $c_j$ trivially by $O(H)$. Using (3.3) to bound $S_{\mathscr{E}_z}$ gives

$$\sum_{\substack{|P|\leqslant H,\, P>0 \\ \deg(P)=d \\ P\equiv R (\mathrm{mod}\ \Omega)}} \mathscr{E}_z(P(k)) \ll_{\delta_1} H(\log H)^{1+d\delta_2 - C} H^d \int_{-\pi}^{\pi} \Bigg| \sum_{\substack{|c_0|\leqslant H \\ c_0\equiv r_0 (\mathrm{mod}\ \Omega)}} \mathrm{e}^{ic_0\alpha_1} \Bigg| \mathrm{d}\alpha_1.$$

It suffices to prove that the integral is $O(\log H)$, since taking $C$ large enough compared to $d\delta_2$ will complete the proof.

Letting $c_0 = b\Omega + r_0$ makes the sum over $c_0$ equal to

$$\mathrm{e}^{ir_0\alpha_1} \sum_{|b+r_0/\Omega|\leqslant H/\Omega} \mathrm{e}^{ib\Omega\alpha_1}.$$

Since $|r_0| \leqslant \Omega$, the terms in the sum over $b$ that do not satisfy $|b| \leqslant H/\Omega$ are at most $O(1)$ with an absolute implied constant. Hence,

$$\int_{-\pi}^{\pi} \Bigg| \sum_{\substack{|c_0| \leqslant H \\ c_0 \equiv r_0 \pmod{\Omega}}} \mathrm{e}^{ic_0\alpha_1} \Bigg| \mathrm{d}\alpha_1$$
$$\ll 1 + \int_{-\pi}^{\pi} \Bigg| \sum_{|b| \leqslant H/\Omega} \mathrm{e}^{ib\Omega\alpha_1} \Bigg| \mathrm{d}\alpha_1 = 1 + \frac{1}{\Omega} \int_{-\pi\Omega}^{\pi\Omega} |D_{H/\Omega}(t)| \mathrm{d}t.$$

Since $|D_{H/\Omega}(t)|$ is even and has period $2\pi$ we can bound the integral by $\ll \int_{-\pi}^{\pi} |D_{H/\Omega}(t)| \mathrm{d}t$. Alluding to Lebesgue's result (3.2) is now sufficient to finish the proof. □

### 3.2 The main term

It now remains to estimate the sum involving $\Lambda_z$ in Proposition 3.8. This will be straightforward but somewhat involved because we need to keep track of the dependence of the error term on the parameters $k$ and $m$.

**Lemma 3.10** *For all $z, H \geqslant 1$ with $z^2 \leqslant H$ and all distinct $k, m \in \mathbb{N}$ we have*

$$\sum_{\substack{P \in \mathbb{Z}[t] \\ |P| \leqslant H,\, P>0 \\ \deg(P)=d}} \Lambda_z(P(k))\Lambda_z(P(m))$$
$$= 2^d H^{d+1} \sum_{\substack{c, l_0 \in \mathbb{N} \\ cl_0 \leqslant z \\ \gcd(c,l_0)=1}} \frac{\mu(c)\mu(l_0)^2 \gcd(l_0, k-m)}{(cl_0)^2} \left( \sum_{\substack{t \in \mathbb{N} \\ cl_0 t \leqslant z \\ \gcd(t, cl_0)=1}} \frac{\mu(t)\log(cl_0 t)}{t} \right)^2$$
$$+ O(H^d z^3),$$

*where the implied constant depends only on $d$.*

*Proof* Write $\mathbf{c} = (c_0, \ldots, c_d)$ and $P(t) = P_{\mathbf{c}}(t) = \sum_{i=0}^{d} c_i t^i$. The left hand side becomes

$$\sum_{k_1, k_2 \leqslant z} \mu(k_1)\mu(k_2)\log(k_1)\log(k_2) \sum_{\substack{\mathbf{c} \in (\mathbb{Z} \cap [-H,H])^{d+1},\, c_d>0 \\ k_1 | P_{\mathbf{c}}(k),\, k_2 | P_{\mathbf{c}}(m)}} 1. \tag{3.4}$$

We only need to consider the terms corresponding to square-free $k_1$ and $k_2$. Then $l_0 = \gcd(k_1, k_2), l_1 = k_1/l_0, l_2 = k_2/l_0$ are square-free and pairwise coprime. The simultaneous conditions $k_1 \mid P_{\mathbf{c}}(k)$, $k_2 \mid P_{\mathbf{c}}(m)$ can be written equivalently as

$$P_{\mathbf{c}}(k) \equiv P_{\mathbf{c}}(m) \equiv 0 \,(\mathrm{mod}\, l_0)\,,\ l_1 \mid P_{\mathbf{c}}(k),\ l_2 \mid P_{\mathbf{c}}(m).$$

Then splitting the summation over each $c_i$ in arithmetic progressions modulo $l_0 l_1 l_2$ turns the sum over $\mathbf{c}$ into

$$\sum_{\substack{\mathbf{b}\in(\mathbb{Z}\cap[0,l_0l_1l_2))^{d+1}\\ P_{\mathbf{b}}(k)\equiv P_{\mathbf{b}}(m)\equiv 0 (\mathrm{mod}\, l_0)\\ l_1|P_{\mathbf{b}}(k),\, l_2|P_{\mathbf{b}}(m)}} \sharp\left\{\mathbf{c}\in(\mathbb{Z}\cap[-H,H])^{d+1} : c_d > 0, \mathbf{c}\equiv\mathbf{b}\,(\mathrm{mod}\, l_0l_1l_2)\right\}.$$

Since $z^2 \leqslant H$ we have $l_0 l_1 l_2 \leqslant k_1 k_2 \leqslant z^2 \leqslant H$. Therefore, the summand $\sharp\{\mathbf{c}\}$ is

$$\frac{1}{2}\left(\frac{2H}{l_0l_1l_2}\right)^{d+1} + O\left(\left(\frac{H}{l_0l_1l_2}\right)^{d}\right).$$

By the Chinese Remainder Theorem, the number of terms in the sum over $\mathbf{b}$ is

$$\prod_{\substack{p \text{ prime}\\ p|l_0}} \sharp\{\mathbf{b}\in\mathbb{F}_p^{d+1} : P_{\mathbf{b}}(k) = P_{\mathbf{b}}(m) = 0\} \prod_{\substack{p \text{ prime}\\ p|l_1}} \sharp\{\mathbf{b}\in\mathbb{F}_p^{d+1} : P_{\mathbf{b}}(k) = 0\}$$
$$\times \prod_{\substack{p \text{ prime}\\ p|l_2}} \sharp\{\mathbf{b}\in\mathbb{F}_p^{d+1} : P_{\mathbf{b}}(m) = 0\},$$

where we used that each $l_i$ is square-free and that $\gcd(l_i, l_j) = 1$ for all $i \neq j$. Fixing all $b_i$ except $b_0$ shows that

$$\sharp\{\mathbf{b}\in\mathbb{F}_p^{d+1} : P_{\mathbf{b}}(k) = 0\} = \sharp\{\mathbf{b}\in\mathbb{F}_p^{d+1} : P_{\mathbf{b}}(m) = 0\} = p^d.$$

Fixing all $b_i$ except $b_0$ and $b_1$ shows that $\sharp\{\mathbf{b}\in\mathbb{F}_p^{d+1} : P_{\mathbf{b}}(k) = P_{\mathbf{b}}(m) = 0\}$ equals $p^{d-1}$ if $p \nmid k-m$ and $p^d$ if $p \mid k-m$. Hence, the number of terms in the sum over $\mathbf{b}$ is

$$(l_1l_2)^d \prod_{\substack{\text{prime } p|l_0\\ p|k-m}} p^d \prod_{\substack{\text{prime } p|l_0\\ p\nmid k-m}} p^{d-1} = (l_1l_2)^d l_0^{d-1}\gcd(l_0, k-m).$$

Hence, (3.4) becomes

$$2^d H^{d+1} \sum_{\substack{l_0,l_1,l_2\in\mathbb{N}\\ \gcd(l_i,l_j)=1 \text{ for } i\neq j\\ l_0l_1,\, l_0l_2\leqslant z}} \mu(l_0)^2\mu(l_1)\mu(l_2)\log(l_0l_1)\log(l_0l_2)\frac{\gcd(l_0,k-m)}{l_0^2l_1l_2}$$

up to a quantity whose modulus is

$$\ll H^d \sum_{\substack{l_0,l_1,l_2\in\mathbb{N}\\ \gcd(l_i,l_j)=1 \text{ for } i\neq j\\ l_0l_1,\, l_0l_2\leqslant z}} \mu(l_0)^2\mu(l_1)^2\mu(l_2)^2\log(l_0l_1)\log(l_0l_2)\frac{\gcd(l_0,k-m)}{l_0}. \tag{3.5}$$

The condition $\gcd(l_1, l_2) = 1$ has indicator function given by

$$\sum_{\substack{c\in\mathbb{N}\\ c|\gcd(l_1,l_2)}} \mu(c) = \sum_{\substack{c,t_1,t_2\in\mathbb{N}\\ l_1=ct_1,\, l_2=ct_2}} \mu(c),$$

hence the sum over $l_0, l_1, l_2$ in the main term can be written as

$$\begin{aligned}&\sum_{\substack{c,l_0,t_1,t_2\in\mathbb{N}\\ \gcd(l_0,ct_1t_2)=1\\ l_0ct_1,\, l_0ct_2\leqslant z}} \mu(l_0)^2\mu(c)\mu(ct_1)\mu(ct_2)\log(l_0ct_1)\log(l_0ct_2)\frac{\gcd(l_0,k-m)}{l_0^2c^2t_1t_2}\\ &= \sum_{c\in\mathbb{N}\cap[1,z]}\frac{\mu(c)}{c^2}\sum_{\substack{l_0,t_1,t_2\in\mathbb{N}\\ \gcd(l_0,ct_1t_2)=1\\ \gcd(c,t_1t_2)=1\\ l_0ct_1,\, l_0ct_2\leqslant z}} \mu(l_0)^2\mu(t_1)\mu(t_2)\log(l_0ct_1)\log(l_0ct_2)\\ &\quad\times\frac{\gcd(l_0,k-m)}{l_0^2t_1t_2},\end{aligned}$$

where we used that the presence of $\mu(ct_1)\mu(ct_2)$ forces $\gcd(c, t_1t_2) = 1$ and $\mu(ct_1)\mu(ct_2) = \mu(c)^2\mu(t_1)\mu(t_2)$. The variables $t_1, t_2$ in the last sum are now independent hence we get the sum in the lemma. Turning to (3.5), we use

$\gcd(l_0, k-m) \leqslant l_0$ to bound it by

$$\ll H^d \sum_{\substack{l_0,l_1,l_2\in\mathbb{N}\\ l_0l_1,\, l_0l_2\leqslant z}} \mu(l_0)^2\mu(l_1)^2\mu(l_2)^2 \log(l_0l_1)\log(l_0l_2)$$

$$\ll H^d(\log z)^2 \left(\sum_{\substack{l_0,l_1\in\mathbb{N}\\ l_0l_1\leqslant z}} 1\right)^2 \ll H^d z^2(\log z)^4,$$

which completes the proof. □

Our aim is now to prove asymptotics for the sum over $t$ in the right hand side of the equation in Lemma 3.10. We need the following lemma.

**Lemma 3.11** *Fix any $A > 0$. Then for all $T \geqslant 1$ and $q \in \mathbb{N} \cap [1, T^{1/2}]$ we have*

$$\sum_{\substack{t\leqslant T/q\\ \gcd(t,q)=1}} \frac{\mu(t)\log(qt)}{t} = -\frac{q}{\varphi(q)} + O_A((\log T)^{-A}),$$

*where the implied constants depend only on $A$.*

*Proof* This can be deduced directly from

$$\sum_{\substack{t\leqslant T\\ \gcd(t,q)=1}} \frac{\mu(t)\log t}{t} = -\frac{q}{\varphi(q)} + O_A((\log T)^{-A}) \text{ and}$$

$$\sum_{\substack{t\leqslant T\\ \gcd(t,q)=1}} \frac{\mu(t)}{t} = O_A((\log T)^{-A}), \tag{3.6}$$

which are consequences of the prime number theorem, see [51, Ex. 17, p. 185]. □

Recall the following standard bounds from [51, Thm. 2.9, Thm. 2.11]:

$$\frac{1}{\varphi(n)} \ll \frac{\log\log n}{n}, \qquad \tau(n) \leqslant n^{O(\frac{1}{\log\log n})}. \tag{3.7}$$

**Lemma 3.12** *Keep the setting of Lemma 3.10 and fix an arbitrary positive constant A. Then the sum over the $c, l_0$ in Lemma 3.10 equals*

$$\prod_{\text{prime } p\mid k-m} \frac{p}{p-1} + O_A\left(\frac{|k-m|}{(\log z)^A}\right),$$

*where the implied constant does not depend on $k, m, z$ and $H$.*

*Proof* To apply Lemma 3.11 we must have $cl_0 \leqslant z^{1/2}$. Using the bound $\sum_{n\leqslant z} 1/n \ll \log z$ we see that the contribution of the terms failing this condition is in modulus at most

$$\sum_{\substack{c,l_0\in\mathbb{N}\\ cl_0>z^{1/2}}} \frac{|k-m|}{(cl_0)^2}\left(\sum_{t\leqslant z}\frac{\log z}{t}\right)^2 \ll |k-m|(\log z)^4 \sum_{s>z^{1/2}} \frac{\tau(s)}{s^2},$$

where we write $s = cl_0$. By (3.7) the sum over $s$ is $\ll \sum_{s>\sqrt{z}} s^{-3/2} \ll z^{-1/4}$, which is satisfactory. By Lemma 3.11 the remaining terms make the following contribution:

$$\sum_{\substack{c,l_0\in\mathbb{N}\\ cl_0\leqslant z^{1/2}\\ \gcd(c,l_0)=1}} \frac{\mu(c)\mu(l_0)^2\gcd(l_0,k-m)}{(cl_0)^2}\left(\frac{(cl_0)^2}{\varphi(cl_0)^2} + O_A\left(\frac{1}{(\log z)^A}\right)\right)^2.$$

The error term is

$$\ll \frac{1}{(\log z)^A}\sum_{c,l_0\in\mathbb{N}}\frac{|k-m|}{(cl_0)^2} \ll \frac{|k-m|}{(\log z)^A}.$$

The main term equals

$$\sum_{\substack{c,l_0\in\mathbb{N}\\ cl_0\leqslant z^{1/2}\\ \gcd(c,l_0)=1}} \frac{\mu(c)\mu(l_0)^2\gcd(l_0,k-m)}{\varphi(cl_0)^2}$$

$$= \sum_{\substack{c,l_0\in\mathbb{N}\\ \gcd(c,l_0)=1}} \frac{\mu(c)\mu(l_0)^2\gcd(l_0,k-m)}{\varphi(cl_0)^2} + O\left(\sum_{\substack{c,l_0\in\mathbb{N}\\ cl_0>z^{1/2}}}\frac{|k-m|}{\varphi(cl_0)^2}\right).$$

By (3.7) we have

$$\sum_{\substack{c,l_0\in\mathbb{N}\\ cl_0>z^{1/2}}}\frac{1}{\varphi(cl_0)^2}=\sum_{s>z^{1/2}}\frac{\tau(s)}{\varphi(s)^2}\ll\sum_{s>z^{1/2}}s^{-3/2}\ll z^{-1/4}.$$

The main term has Euler product

$$\sum_{\substack{c,l_0\in\mathbb{N}\\ \gcd(c,l_0)=1}}\frac{\mu(c)\mu(l_0)^2\gcd(l_0,k-m)}{\varphi(cl_0)^2}$$
$$=\prod_{p \text{ prime}}\left(1-\frac{1}{(p-1)^2}+\frac{\gcd(p,k-m)}{(p-1)^2}\right).$$

Only the primes dividing $k-m$ contribute. In particular, we get the product

$$\prod_{\text{prime } p|k-m}\left(1+\frac{1}{p-1}\right)=\prod_{\text{prime } p|k-m}\frac{p}{p-1},$$

which concludes the proof. □

Using Lemmas 3.10 and 3.12 with $z=H^{1/8}$ we obtain

**Lemma 3.13** *Fix any $\delta>0$. Then for all $H\geqslant 1$, $A>0$, and all pairs of distinct natural numbers $k,m\leqslant(\log H)^{\delta}$ we have*

$$\sum_{\substack{P\in\mathbb{Z}[t],\ \deg(P)=d\\ |P|\leqslant H,\ P>0}}\Lambda_z(P(k))\Lambda_z(P(m))$$
$$=2^dH^{d+1}\prod_{\text{prime } p|k-m}\frac{p}{p-1}+O_A\left(H^{d+1}(\log H)^{-A}\right),$$

*where $z=H^{1/8}$ and the implied constant does not depend on $k$, $m$, $z$ and $H$.*

Combining Proposition 3.8 with Lemma 3.13 proves Theorem 3.1.

### 3.3 A variant

We shall also need the following variant of Theorem 3.1.

**Lemma 3.14** *Fix any $d\geqslant 1$ and $\delta>0$. Then for all $H\geqslant 1$, $A>0$, all natural numbers $k,\Omega$, and all $R\in(\mathbb{Z}/\Omega)[t]$ such that $k\leqslant(\log H)^{\delta}$ and*

*$\Omega \leqslant H$ we have*

$$\sum_{\substack{|P|\leqslant H,\ P>0,\ \deg(P)=d \\ P(k)\text{ prime},\ P\equiv R(\bmod\ \Omega)}} \log P(k) = \frac{2^d H^{d+1}}{\Omega^d \varphi(\Omega)} \mathbb{1}(\gcd(R(k),\Omega)=1) + O_A\left(\frac{H^{d+1}}{(\log H)^A}\right),$$

*where the implied constant does not depend on $k$, $H$, $R$ and $\Omega$.*

*Proof* If $\gcd(R(k),\Omega)\neq 1$, then $P(k)$ is a prime divisor of $\Omega$. Since there are $O(H^d)$ polynomials $P(t)$ of degree $d$ with $|P|\leqslant H$ such that $P(k)$ is equal to a given integer, the sum in the lemma is $\ll \sharp\{\ell \text{ prime} : \ell \mid \Omega\} H^d \log H$. The number of prime divisors is $\ll \log\Omega \leqslant \log H$, thus the proof is complete when $\gcd(R(k),\Omega)\neq 1$.

Let us now assume that $\gcd(R(k),\Omega)=1$. We first transition to the von Mangoldt function by noting that

$$\sum_{\substack{|P|\leqslant H,\ P>0 \\ \deg(P)=d \\ P\equiv R(\bmod\ \Omega)}} \Lambda(P(k)) - \sum_{\substack{|P|\leqslant H,\ P>0,\ \deg(P)=d \\ P(k)\text{ prime} \\ P\equiv R(\bmod\ \Omega)}} \log P(k) \ll \sum_{2\leqslant\alpha\ll\log H} \sum_{\substack{\ell\text{ prime} \\ \ell^\alpha\leqslant(d+1)Hk^d}} (\log \ell) \sum_{\substack{|P|\leqslant H \\ \deg(P)=d \\ P(k)=\ell^\alpha}} 1.$$

The last sum over $P$ is $O(H^d)$, thus the error term is $\ll (\log H)^2 H^d (Hk^d)^{1/2}$, which is acceptable. To conclude the proof it therefore suffices to consider $\sum_P \Lambda(P(k))$. Define $z = H^{1/4}$. By Lemma 3.9 it is enough to estimate

$$\sum_{\substack{|P|\leqslant H,\ P>0 \\ \deg(P)=d,\ P\equiv R(\bmod\ \Omega)}} \Lambda_z(P(k)) = -\sum_{\substack{k_1\leqslant z \\ \gcd(k_1,\Omega)=1}} \mu(k_1)(\log k_1) \sum_{\substack{|P|\leqslant H,\ P>0 \\ k_1 | P(k),\ P\equiv R(\bmod\ \Omega)}} 1,$$

where $\gcd(k_1,\Omega)=1$ follows from $\gcd(R(k),\Omega)=1$. Hence the sum over $P$ is

$$2^d\left(\frac{H^{d+1}}{k_1^{d+1}\Omega^{d+1}} + O\left(1+\frac{H^d}{k_1^d\Omega^d}\right)\right) \sharp\{P\in(\mathbb{Z}/k_1)[t] : \deg(P)\leqslant d, P(k)\equiv 0 \,(\bmod\ k_1)\}.$$

Since $\sharp\{P\} = k_1^d$ and $k_1 \leqslant z \leqslant H$, the above becomes

$$\frac{2^d H^{d+1}}{\Omega^{d+1}} \frac{1}{k_1} + O(H^d).$$

The error term contribution is

$$\ll H^d \sum_{k_1 \leqslant z} \log k_1 \ll H^d z \log z \ll H^{d+1/2}.$$

The main term contribution is

$$-\frac{2^d H^{d+1}}{\Omega^{d+1}} \sum_{\substack{k_1 \leqslant z \\ \gcd(k_1,\Omega)=1}} \frac{\mu(k_1) \log k_1}{k_1} = \frac{2^d H^{d+1}}{\Omega^d \varphi(\Omega)} + O_A\left(\frac{H^{d+1}}{\log^A z}\right),$$

where we used (3.6). □

## 4 Dispersion

Recall that $\mathscr{V}(x, H)$ was defined in (1.6). In this section we prove $\mathscr{V}(x, H) \ll x^2/(\log x)^{-1}$ via Linnik's dispersion method [45]. Theorem 1.9 then follows by the Cauchy–Schwarz inequality $\mathscr{R}(x, H)^2 \leqslant \mathscr{V}(x, H)$. Removing the condition $P_i \equiv Q_i \pmod M$ can only increase $\sharp\texttt{Poly}(H)\mathscr{V}(x, H)$, thus

$$\begin{aligned} &\sharp\texttt{Poly}(H)\mathscr{V}(x, H) \\ &\leqslant \sum_{\substack{\mathbf{P} \in \mathbb{Z}[t]^n,\ |\mathbf{P}| \leqslant H \\ \deg(P_i) = d_i,\ P_i > 0}} \theta_{\mathbf{P}}(x)^2 - 2x \sum_{\substack{\mathbf{P} \in \mathbb{Z}[t]^n,\ |\mathbf{P}| \leqslant H \\ \deg(P_i) = d_i,\ P_i > 0}} \mathfrak{S}_{\mathbf{P}}(x)\theta_{\mathbf{P}}(x) \\ &\quad + x^2 \sum_{\substack{\mathbf{P} \in \mathbb{Z}[t]^n,\ |\mathbf{P}| \leqslant H \\ \deg(P_i) = d_i,\ P_i > 0}} \mathfrak{S}_{\mathbf{P}}(x)^2. \end{aligned} \tag{4.1}$$

The term $\sum_{\mathbf{P}} \theta_{\mathbf{P}}(x)^2$ is studied in §4.1 using Theorem 3.1. The terms $\sum_{\mathbf{P}} \mathfrak{S}_{\mathbf{P}}(x)^2$ and $\sum_{\mathbf{P}} \mathfrak{S}_{\mathbf{P}}(x)\theta_{\mathbf{P}}(x)$ are estimated in §4.2 and §4.3, respectively.

Throughout this section $d = d_1 + \ldots + d_n$. We write $P_i(t) = \sum_{j=0}^{d_i} c_{ij} t^j$ for each $i = 1, \ldots, n$.

### 4.1 The term $\sum_{\mathbf{P}} \theta_{\mathbf{P}}(x)^2$

Recall that $\mathscr{G}_{k,m}(H; d_i)$ is defined in (3.1).

**Lemma 4.1** *Fix any $\delta > 0$. For all $x$, $H$ with $1 \leqslant x \leqslant (\log H)^\delta$ we have*

$$\sum_{\substack{\mathbf{P} \in \mathbb{Z}[t]^n,\ |\mathbf{P}| \leqslant H \\ \deg(P_i) = d_i,\ P_i > 0}} \theta_{\mathbf{P}}(x)^2$$

$$= 2 \sum_{\substack{1 \leqslant m < k \leqslant x \\ k \equiv m \equiv n_0 \,(mod\ M)}} \prod_{i=1}^{n} \mathcal{G}_{k,m}(H; d_i) + O\left(x H^{d+n} (\log H)^n\right),$$

*where the implied constant depends only on $\delta$ and $d_i$.*

*Proof* First, note that for all $j \in \mathbb{N}$ we have $\mathbb{1}_{\text{primes}}(j) \log j \leqslant \Lambda(j)$, where $\Lambda$ is the von Mangoldt function. Therefore, the sum over the $P_i$ in our lemma is at most

$$\sum_{\substack{P_1, \ldots, P_n \\ |P_i| \leqslant H,\ P_i > 0}} \left( \sum_{\substack{m \leqslant x \\ m \equiv n_0 \,(\mathrm{mod}\ M)}} \Lambda(P_1(m)) \ldots \Lambda(P_n(m)) \right)^2$$

$$= \sum_{\substack{1 \leqslant k,\ m \leqslant x \\ k \equiv m \equiv n_0 \,(\mathrm{mod}\ M)}} \prod_{i=1}^{n} \mathcal{G}_{k,m}(H; d_i).$$

The contribution of the diagonal terms $k = m$ is at most

$$\sum_{1 \leqslant m \leqslant x} \prod_{i=1}^{n} \sum_{\substack{|P_i| \leqslant H,\ P_i > 0 \\ \deg(P_i) = d_i}} \Lambda(P_i(m))^2.$$

Using $0 \leqslant \Lambda(h) \leqslant \log h$ gives the bound

$$\ll (\log H)^n \sum_{1 \leqslant m \leqslant x} \prod_{i=1}^{n} \sum_{\substack{|P_i| \leqslant H,\ P_i > 0 \\ \deg(P_i) = d_i}} \Lambda(P_i(m)).$$

We can now apply Lemma 3.14 with $\Omega = 1$ and $d = d_i$. It shows that the sum over the $P_i$ is $O(H^{1+d_i})$, hence

$$(\log H)^n \sum_{1 \leqslant m \leqslant x} \prod_{i=1}^{n} \sum_{\substack{|P_i| \leqslant H,\ P_i > 0 \\ \deg(P_i) = d_i}} \Lambda(P_i(m)) \ll (\log H)^n x H^{d+n},$$

which is sufficient for the proof. □

*Remark 4.2* Lemma 4.1 shows why we need to have $x/(\log H)^n \to +\infty$: if $x$ is not this large compared to the typical size of the coefficients of the polynomials, then the diagonal terms in the second moment dominate; using Lemmas 4.4, 4.7, 4.9 it is then easy to see that the three principal terms do not cancel. In particular, one has

$$\mathscr{V}(x, H) \asymp x(\log H)^n \gg x^2,$$

which is not sufficient for proving Theorem 1.5.

Our next step is to use Theorem 3.1 to estimate the sum over $m, k$ in Lemma 4.1. This will give rise to an average of the multiplicative function

$$\prod_{\text{prime } p|t} \left(1 + \frac{1}{p-1}\right)^n.$$

For this we need the following lemma.

**Lemma 4.3** *Fix any $n \in \mathbb{N}$ and $c > 0$. Let $f$ be a function defined on the primes such that $|f(p)| \leqslant c/p$ for all $p$. Then for all $x, T \geqslant 1$ we have*

$$\sum_{\substack{t \in \mathbb{N} \\ t \leqslant x}} \prod_{\text{prime } p|t} (1 + f(p))^n = O(x)$$

*and*

$$\int_0^T \sum_{\substack{t \in \mathbb{N} \\ t \leqslant x}} \prod_{\text{prime } p|t} (1 + f(p))^n \mathrm{d}x = \frac{T^2}{2} \prod_{\text{prime } p} \left(1 + \frac{(1 + f(p))^n - 1}{p}\right) + O(T^{3/2}),$$

*where the implied constants depend only on $n$ and $c$.*

*Proof* Wintner's theorem (as generalised by Iwaniec–Kowalski [39, Eq. (1.72)]) states that for any arithmetic function $g$ and any monotonic and bounded $h : [0, \infty) \to \mathbb{R}$, one has

$$\sum_{t \leqslant x} (g * h)(t) = \int_0^x \left( \sum_{t \leqslant y} \frac{g(t)}{t} h\left(\frac{y}{t}\right) \right) \mathrm{d}y + O\left( \sum_{t \leqslant x} |g(t)| \right) \qquad (4.2)$$

for all $x \geqslant 1$. Here $g * h$ is the Dirichlet convolution. Letting $h = 1$ and

$$g(t) = |\mu(t)| \prod_{\text{prime } p|t} \big((1+f(p))^n - 1\big)$$

gives $(g * h)(t) = \prod_{p|t}(1+f(p))^n$, hence, by (4.2), we obtain

$$\sum_{\substack{t\in\mathbb{N}\\ t\leqslant x}} \prod_{\text{prime } p|t} (1+f(p))^n = \int_0^x \sum_{t\leqslant y} \frac{g(t)}{t} \mathrm{d}y + O\left(\sum_{t\leqslant x} |g(t)|\right). \quad (4.3)$$

For a prime $p$ we have

$$|g(p)| = \left|\sum_{j=1}^n \binom{n}{j} f(p)^j\right| \leqslant \sum_{j=1}^n \binom{n}{j} \frac{c^j}{p^j} \leqslant \frac{2^\alpha}{p}$$

for some positive constant $\alpha$ that depends only on $n$ and $c$. Therefore, by (3.7) we obtain

$$t|g(t)| \leqslant |\mu(t)|\tau(t)^\alpha = O(t^{1/2}).$$

This implies that for all $x, y \geqslant 1$ one has

$$\sum_{t\leqslant x} |g(t)| \ll \sum_{t\leqslant x} t^{-1/2} \ll x^{1/2} \quad \text{and} \quad \sum_{t>y} \frac{|g(t)|}{t} \ll \sum_{t>y} t^{-3/2} \ll y^{-1/2}.$$

Therefore,

$$\sum_{t\leqslant y} \frac{g(t)}{t} = \sum_{t\in\mathbb{N}} \frac{g(t)}{t} + O(y^{-1/2}) = \prod_p \left(1 + \frac{g(p)}{p}\right) + O(y^{-1/2}).$$

Using $1 + g(p) = (1+f(p))^n$ in the product and alluding to (4.3), we obtain

$$\sum_{\substack{t\in\mathbb{N}\\ t\leqslant x}} \prod_{\text{prime } p|t} (1+f(p))^n = x \prod_{\text{prime } p} \left(1 + \frac{(1+f(p))^n - 1}{p}\right) + O(x^{1/2}).$$

Clearly this is $O(x)$, which proves the first claim in the lemma. The second claim follows by integrating over the range $0 \leqslant x \leqslant T$. □

Recall that $\gamma_n(\ell)$ was defined in (2.5).

**Lemma 4.4** *Fix any $\delta > 0$. For all $x$, $H$ with $1 \leqslant x \leqslant (\log H)^\delta$ we have*

$$\sum_{\substack{\mathbf{P} \in \mathbb{Z}[t]^n,\ |\mathbf{P}| \leqslant H \\ \deg(P_i) = d_i,\ P_i > 0}} \theta_{\mathbf{P}}(x)^2 = \frac{x^2 M^{n-2}}{\varphi(M)^n} 2^d H^{d+n} \prod_{\text{prime } \ell \nmid M} \gamma_n(\ell) + O\left(x H^{d+n} (\log H)^n + x^{3/2} H^{d+n}\right),$$

*where the implied constant depends only on $\delta$, $n$, $M$ and $d_i$.*

*Proof* Taking sufficiently large $A$ in Theorem 3.1 and using Lemma 4.1 yields

$$\sum_{\substack{P_1,\dots,P_n \\ |P_i| \leqslant H,\ P_i > 0}} \theta_{\mathbf{P}}(x)^2 = 2^{d+1} H^{d+n} T_0(x) + O_A\left(x H^{d+n} (\log H)^n + H^{d+n} (\log H)^{-A}\right),$$

where

$$T_0(x) := \sum_{\substack{1 \leqslant m < k \leqslant x \\ k \equiv m \equiv n_0 \pmod{M}}} \prod_{\text{prime } p \mid k-m} \frac{p^n}{(p-1)^n}.$$

We have $k - m = tM$ for some integer $t$. Hence, $T_0(x)$ equals

$$\sum_{\substack{t \in \mathbb{N} \\ 1 < tM \leqslant x}} \left( \prod_{p \mid tM} \frac{p^n}{(p-1)^n} \right) \sum_{\substack{m \in \mathbb{N} \\ m < x - tM \\ m \equiv n_0 \pmod{M}}} 1$$

$$= \sum_{\substack{t \in \mathbb{N} \\ 1 < tM \leqslant x}} \left( \prod_{p \mid tM} \frac{p^n}{(p-1)^n} \right) \left( \frac{x}{M} - t + O(1) \right). \tag{4.4}$$

Define a function $f$ on the primes such that $f(p) = 1/(p-1)$ if $p \nmid M$, and $f(p) = 0$ if $p \mid M$. Then

$$\prod_{\text{prime } p \mid tM} \frac{p^n}{(p-1)^n} = \frac{M^n}{\varphi(M)^n} \prod_{\text{prime } p \mid t} (1 + f(p))^n,$$

hence the right hand side of (4.4) is

$$\frac{M^n}{\varphi(M)^n} \sum_{t \leqslant x/M} \left( \prod_{\text{prime } p \mid t} (1 + f(p))^n \right) \left( \frac{x}{M} - t \right) + O(x),$$

where we used the first part of Lemma 4.3 to bound the contribution of the $O(1)$ term. Using $\int_t^{x/M} 1\mathrm{d}y = x/M - t$ we can write the sum over $t$ as

$$\int_0^{x/M} \sum_{t\leqslant y} \prod_{p|t} (1+f(p))^n \mathrm{d}y.$$

Invoking the second part of Lemma 4.3 shows that this is

$$\frac{x^2}{2M^2} \prod_{\text{prime } p\nmid M} \gamma_n(p) + O(x^{3/2}),$$

which concludes the proof. □

It is convenient to truncate the product over $\ell$ in Lemma 4.4 now, as it will make it easier to compare $\sum_{\mathbf{P}} \theta_{\mathbf{P}}(x)^2$ to $\sum_{\mathbf{P}} \theta_{\mathbf{P}}(x)\mathfrak{S}_{\mathbf{P}}(x)$ and $\sum_{\mathbf{P}} \mathfrak{S}_{\mathbf{P}}(x)^2$.

**Lemma 4.5** *Fix $n \in \mathbb{N}$. Then for all $x \geqslant 1$ we have*

$$\prod_{\text{prime } \ell > \log x} \gamma_n(\ell) = 1 + O\left(\frac{1}{\log x}\right).$$

Proof. The bound $(1+\psi)^n \leqslant 1 + n\psi + n2^n\psi^2$, valid for all $0 < \psi < 1$, can be used for $\psi = 1/(\ell-1)$ to show that

$$\begin{aligned}\gamma_n(\ell) &= 1 - \frac{1}{\ell} + \frac{1}{\ell}\left(1 + \frac{1}{\ell-1}\right)^n \\ &\leqslant 1 - \frac{1}{\ell} + \frac{1}{\ell}\left(1 + \frac{n}{\ell-1} + \frac{n2^n}{(\ell-1)^2}\right) \\ &\leqslant 1 + \frac{n2^{n+1}}{\ell(\ell-1)}.\end{aligned}$$

In particular, $\log \gamma_n(\ell) \leqslant \frac{n2^{n+1}}{\ell(\ell-1)}$. We obtain

$$\begin{aligned}\log\left(\prod_{\substack{\text{prime } \ell \\ \ell > \log x}} \gamma_n(\ell)\right) &\leqslant \sum_{\substack{\text{prime } \ell \\ \ell > \log x}} \frac{n2^{n+1}}{\ell(\ell-1)} \leqslant n2^{n+1} \sum_{\substack{k\in\mathbb{N} \\ k > \log x}} \frac{1}{k(k-1)} \\ &\leqslant \frac{n2^{n+1}}{-1+\log x}.\end{aligned}$$

Exponentiating gives

$$\prod_{\substack{\text{prime } \ell \\ \ell > \log x}} \gamma_n(\ell) \leqslant \exp\left(\frac{n2^{n+2}}{-1+\log x}\right) = 1 + O\left(\frac{1}{\log x}\right).$$

□

Combining Lemma 4.5 with Lemma 4.4 gives

$$\sum_{\substack{\mathbf{P}\in(\mathbb{Z}[t])^n, |\mathbf{P}|\leqslant H \\ \deg(P_i)=d_i, P_i>0}} \theta_{\mathbf{P}}(x)^2 = \frac{x^2 M^{n-2}}{\varphi(M)^n} 2^d H^{d+n} \prod_{\substack{\ell \nmid M \\ \ell \leqslant \log x}} \gamma_n(\ell) + O\left(\frac{x^2 H^{d+n}}{\log x} + x H^{d+n} (\log H)^n\right). \tag{4.5}$$

## 4.2 The term $\sum_{\mathbf{P}} \mathfrak{S}_{\mathbf{P}}(x)^2$

Let

$$W = \prod_{\substack{\text{prime } \ell \\ \ell \nmid M,\ \ell \leqslant \log x}} \ell.$$

The prime number theorem implies that

$$\log W \leqslant \sum_{\text{prime } \ell \leqslant \log x} \log \ell \leqslant 2 \log x,$$

whence we obtain

$$W \leqslant x^2. \tag{4.6}$$

**Lemma 4.6** *For every square-free $m \in \mathbb{N}$ we have*

$$\sum_{\substack{R_1,\ldots,R_n \in (\mathbb{Z}/m)[t] \\ \deg(R_i) \leqslant d_i}} \prod_{\text{prime } \ell | m} \left(\frac{1-\ell^{-1} Z_{R_1\ldots R_n}(\ell)}{(1-\ell^{-1})^n}\right)^2 = m^{n+d} \prod_{\text{prime } \ell | m} \gamma_n(\ell).$$

*Proof* A standard argument based on the Chinese remainder theorem shows that the left hand side is a multiplicative function of $m$. Invoking Lemma 2.6 concludes the proof. □

**Lemma 4.7** *For* $1 \leqslant x \leqslant H^{1/4}$ *we have*

$$\sum_{\substack{\mathbf{P}\in\mathbb{Z}[t]^n,\ |\mathbf{P}|\leqslant H \\ \deg(P_i)=d_i,\ P_i>0}} \mathfrak{S}_{\mathbf{P}}(x)^2 = \frac{2^d H^{d+n} M^{n-2}}{\varphi(M)^n} \prod_{\substack{\text{prime } \ell\nmid M \\ \ell\leqslant \log x}} \gamma_n(\ell) + O(H^{d+n-1/2}),$$

*where the implied constant depends only on* $n$, $M$ *and* $d_1, \ldots, d_n$.

*Proof* By (1.5) our sum can be rewritten as

$$\frac{M^{2n-2}}{\varphi(M)^{2n}} \sum_{\substack{\mathbf{P}\in(\mathbb{Z}[t])^n,\ |\mathbf{P}|\leqslant H \\ \deg(P_i)=d_i,\ P_i>0 \\ \gcd(M,\prod_{i=1}^n P_i(n_0))=1}} B_{\mathbf{P}}(x)^2, \text{ where}$$

$$B_{\mathbf{P}}(x) := \prod_{\substack{\text{prime } \ell\nmid M \\ \ell\leqslant \log x}} \frac{1-\ell^{-1} Z_{P_1\ldots P_n}(\ell)}{\left(1-\ell^{-1}\right)^n}. \tag{4.7}$$

If the coefficients of $P$ and $R$ in $\mathbb{Z}[t]$ are congruent modulo $\ell$, then $Z_P(\ell) = Z_R(\ell)$. Hence, denoting the reduction of $P_i(t)$ in $(\mathbb{Z}/W)[t]$ by $R_i(t)$, the sum over the $P_i$ in (4.7) becomes

$$\sum_{\substack{R_1,\ldots,R_n\in(\mathbb{Z}/W)[t] \\ \deg(R_i)\leqslant d_i}} B_{\mathbf{R}}(x)^2 \,\sharp \left\{ P_1, \ldots, P_n \in \mathbb{Z}[t] : \begin{array}{l} |P_i| \leqslant H,\ P_i > 0 \\ \deg(P_i) = d_i, \\ P_i \equiv R_i \ (\mathrm{mod}\ W) \\ \gcd(M, P_i(n_0)) = 1 \end{array} \right\}.$$

By Möbius inversion we have

$$\sum_{\substack{k_i\in\mathbb{N} \\ k_i|M,\ k_i|P_i(n_0)}} \mu(k_i) = \begin{cases} 1, & \text{if } \gcd(M, P_i(n_0)) = 1, \\ 0, & \text{otherwise.} \end{cases}$$

Hence, denoting the reduction of $P_i(t)$ in $(\mathbb{Z}/k_i)[t]$ by $F_i(t)$, we obtain

$$\sum_{R_1,\ldots,R_n\in(\mathbb{Z}/W)[t]} B_{\mathbf{R}}(x)^2 \sum_{\mathbf{k}\in\mathbb{N}^n,\, k_i|M} \left(\prod_{i=1}^n \mu(k_i)\right) \times \sum_{\substack{F_1\in(\mathbb{Z}/k_1)[t],\ldots,F_n\in(\mathbb{Z}/k_n)[t]\\ F_i(n_0)\equiv 0 \,(\mathrm{mod}\, k_i)}} \sum_{\substack{P_1,\ldots,P_n\in\mathbb{Z}[t]\\ |P_i|\leqslant H,\ P_i>0\\ P_i\equiv R_i\,(\mathrm{mod}\, W)\\ P_i\equiv F_i\,(\mathrm{mod}\, k_i)}} 1,$$

where $\deg(P_i)=d_i$, $\max\{\deg(R_i),\deg(F_i)\}\leqslant d_i$. Viewing the sum over the $P_i$ as a sum over $1+d_i$ integers in arithmetic progressions modulo $k_iW$ we obtain

$$\sum_{\substack{\mathbf{R}\in(\mathbb{Z}/W)[t]^n\\ \deg(R_i)\leqslant d_i}} B_{\mathbf{R}}(x)^2 \sum_{\mathbf{k}\in\mathbb{N}^n,\, k_i|M} \left(\prod_{i=1}^n \mu(k_i)\right) \times \sum_{\substack{F_i\in(\mathbb{Z}/k_i)[t]\\ F_i(n_0)\equiv 0(\mathrm{mod}\ k_i)\\ \deg(F_i)\leqslant d_i}} \prod_{i=1}^n \left(\frac{2^{d_i}H^{1+d_i}}{(k_iW)^{1+d_i}} + O\left(1+\frac{H^{d_i}}{W^{d_i}}\right)\right).$$

Now note that $W\leqslant H^{1/2}$ due to $x\leqslant H^{1/4}$ and (4.6). The sum over $F_1,\ldots,F_n$ has $\prod_{i=1}^n k_i^{d_i}$ terms because the condition $F_i(n_0)\equiv 0\,(\mathrm{mod}\, k_i)$ determines uniquely the constant term of every $F_i$ by $n_0$ and the other coefficients of $F_i$. This gives

$$\sum_{\substack{\mathbf{R}\in(\mathbb{Z}/W)[t]^n\\ \deg(R_i)\leqslant d_i}} B_{\mathbf{R}}(x)^2 \sum_{\mathbf{k}\in\mathbb{N}^n,\, k_i|M} \left(\prod_{i=1}^n \frac{\mu(k_i)}{k_i}\right) \left(1+O(H^{-1/2})\right) \frac{2^d H^{d+n}}{W^{d+n}}$$

and the identity $\sum_{k|M}\mu(k)k^{-1} = \varphi(M)M^{-1}$ shows that the sum over $\mathbf{P}$ in (4.7) is

$$\frac{\varphi(M)^n}{M^n}\frac{2^d H^{d+n}}{W^{d+n}}\left(1+O(H^{-1/2})\right) \sum_{\substack{\mathbf{R}\in(\mathbb{Z}/W)[t]^n\\ \deg(R_i)\leqslant d_i}} \prod_{\substack{\text{prime } \ell\nmid M\\ \ell\leqslant \log x}} \left(\frac{1-\ell^{-1}Z_{P_1\ldots P_n}(\ell)}{(1-\ell^{-1})^n}\right)^2.$$

By Lemma 4.6 applied to $W$, the quantity in (4.7) becomes

$$\frac{2^d H^{d+n} M^{n-2}}{\varphi(M)^n} \left(1 + O(H^{-1/2})\right) \prod_{\substack{\ell \nmid M \\ \ell \leqslant \log x}} \gamma_n(\ell) = \frac{2^d H^{d+n} M^{n-2}}{\varphi(M)^n} \prod_{\substack{\ell \nmid M \\ \ell \leqslant \log x}} \gamma_n(\ell) + O(H^{d+n-1/2})$$

because $\prod_\ell \gamma_n(\ell)$ converges. □

*Remark 4.8* It would be interesting to study moments higher than the second moment in the setting of Lemma 4.7. This has been studied previously by Kowalski [41].

### 4.3 The term $\sum_{\mathbf{P}} \mathfrak{S}_{\mathbf{P}}(x)\theta_{\mathbf{P}}(x)$

**Lemma 4.9** *Fix any* $A_2 > 0$. *Then for all* $x, H \geqslant 1$ *such that* $1 \leqslant x \leqslant (\log H)^{A_2}$ *we have*

$$\sum_{\substack{\mathbf{P} \in (\mathbb{Z}[t])^n,\, |\mathbf{P}| \leqslant H \\ \deg(P_i)=d_i,\, P_i>0}} \mathfrak{S}_{\mathbf{P}}(x)\theta_{\mathbf{P}}(x) = x 2^d H^{d+n} \frac{M^{n-2}}{\varphi(M)^n} \prod_{\substack{\text{prime } \ell \nmid M \\ \ell \leqslant \log x}} \gamma_n(\ell) + O\left(H^{d+n}\right).$$

Proof. Using the definition of $\theta_{\mathbf{P}}$ in (1.4) and changing the order of summation turns the sum over $\mathbf{P}$ in our lemma into

$$\sum_{\substack{m \in \mathbb{N} \cap [1,x] \\ m \equiv n_0 (\mathrm{mod}\ M)}} \sum_{\substack{\mathbf{P} \in (\mathbb{Z}[t])^n,\, |\mathbf{P}| \leqslant H \\ \deg(P_i)=d_i,\, P_i>0 \\ P_i(m) \text{ prime for } i=1,\dots,n}} \mathfrak{S}_{\mathbf{P}}(x) \prod_{i=1}^n \log P_i(m).$$

By (1.5) and (4.7) we can write this as

$$\frac{M^{n-1}}{\varphi(M)^n} \sum_{\substack{m \in \mathbb{N} \cap [1,x] \\ m \equiv n_0 (\mathrm{mod}\ M)}} \sum_{\substack{\mathbf{P} \in (\mathbb{Z}[t])^n,\, |\mathbf{P}| \leqslant H \\ \deg(P_i)=d_i,\, P_i>0 \\ \gcd(M, P_i(n_0))=1 \\ P_i(m) \text{ prime for } i=1,\dots,n}} \left(\prod_{i=1}^n \log P_i(m)\right) B_{\mathbf{P}}(x).$$

Letting $R_i$ denote the reduction of $P_i$ in $(\mathbb{Z}/W)[t]$ we note that $B_{\mathbf{P}}(x) = B_{\mathbf{R}}(x)$, hence we obtain

$$\frac{M^{n-1}}{\varphi(M)^n} \sum_{\substack{1 \leqslant m \leqslant x \\ m \equiv n_0 (\mathrm{mod}\ M)}} \sum_{\substack{\mathbf{R} \in (\mathbb{Z}/W)[t]^n \\ \deg(R_i) \leqslant d_i}} B_{\mathbf{R}}(x) \prod_{i=1}^{n} \left( \sideset{}{^*}\sum_{\substack{|P| \leqslant H \\ P \equiv R_i (\mathrm{mod}\ W)}} \log P(m) \right), \tag{4.8}$$

where $\sum^*$ has the extra conditions $\deg(P) = d_i$, $\gcd(P(n_0), M) = 1$, and $P(m)$ is prime. The polynomials $P$ with $\gcd(P(n_0), M) \neq 1$ contribute $O(H^{d_i} \log H)$ towards $\sum^*$ because $P(m)$ must be a prime divisor of $M$. Hence, ignoring the condition $\gcd(P(n_0), M) = 1$, brings $\sum^*$ to a shape suitable for the application of Lemma 3.14. Thus for all $A > 0$ we have

$$\sideset{}{^*}\sum_{\substack{|P| \leqslant H \\ P \equiv R (\mathrm{mod}\ W)}} \log P(m) = \frac{2^{d_i} H^{d_i+1}}{W^{d_i} \varphi(W)} \mathbb{1}(\gcd(R_i(m), W) = 1) + O_A\left( \frac{H^{d_i+1}}{(\log H)^A} \right).$$

To study the contribution of the error term towards (4.8) we bound every other $\sum^*$ trivially by $O(H^{1+d_i} \log H)$, hence we obtain

$$\ll \frac{H^{d+n}}{(\log H)^{A-n}} x \sum_{\substack{\mathbf{R} \in (\mathbb{Z}/W)[t]^n \\ \deg(R_i) \leqslant d_i}} B_{\mathbf{R}}(x) \ll \frac{H^{d+n}}{(\log H)^{A-n}} x W^{d+n} (\log\log x)^n,$$

where we used

$$B_{\mathbf{R}}(x) = \prod_{\substack{\text{prime } \ell \nmid M \\ \ell \leqslant \log x}} \frac{1 - \ell^{-1} Z_{R_1 \ldots R_n}(\ell)}{\left(1 - \ell^{-1}\right)^n} \leqslant \prod_{\ell \leqslant \log x} \left(1 - \ell^{-1}\right)^{-n} \ll (\log\log x)^n$$

which follows from Mertens' theorem. Using (4.6), $x \leqslant (\log H)^{A_2}$ and enlarging $A$ we see that the contribution towards (4.8) is $O(H^{d+n} (\log H)^{-A})$. The main term is

$$\frac{2^d H^{d+n}}{W^{d+n} \varphi(W)^n} \frac{M^{n-1}}{\varphi(M)^n} \sum_{\substack{1 \leqslant m \leqslant x \\ m \equiv n_0 (\mathrm{mod}\ M)}} \sum_{\substack{\mathbf{R} \in (\mathbb{Z}/W)[t]^n,\, \deg(R_i) \leqslant d_i \\ \gcd(R_i(m), W) = 1}} B_{\mathbf{R}}(x).$$

By Lemma 2.7 and a factorisation argument this becomes

$$2^d H^{d+n} \frac{M^{n-1}}{\varphi(M)^n} (x/M + O(1)) \prod_{\ell|W} \gamma_n(\ell)$$
$$= 2^d H^{d+n} \frac{x M^{n-2}}{\varphi(M)^n} \prod_{\ell|W} \gamma_n(\ell) + O\left(H^{d+n}\right).$$

□

### 4.4 The proof of Theorem 1.9

Recall that $A_1, A_2$ are fixed constants with $n < A_1 < A_2$ and that $(\log H)^{A_1} < x \leqslant (\log H)^{A_2}$. Then (4.5), together with Lemmas 4.7 and 4.9 , shows that the right hand side of (4.1) is $\ll x^2 H^{d+n} (\log x)^{-1}$. The reason behind this is that the main terms compensate each other. Since $H^{d+n} \ll \sharp\texttt{Poly}(H)$, this concludes the proof of Theorem 1.9.

### 4.5 The proof of Theorem 1.5

To study the numerator in the left hand side of (1.3) we use Theorem 1.9 to see that for almost all Schinzel $n$-tuples $\mathbf{P}$ the prime counting function $\theta_{\mathbf{P}}(x)$ is closely approximated by $\mathfrak{S}_{\mathbf{P}}(x)x$.

**Lemma 4.10** *Let* $\varepsilon : \mathbb{R} \to (0, \infty)$ *be a function. Fix any* $A_1, A_2$ *with* $n < A_1 < A_2$. *Then for any* $x, H \geqslant 2$ *such that* $(\log H)^{A_1} < x < (\log H)^{A_2}$ *we have*

$$\frac{\sharp\{\mathbf{P} \in \texttt{Poly}(H) : \mathbf{P} \text{ is Schinzel}, |\theta_{\mathbf{P}}(x) - \mathfrak{S}_{\mathbf{P}}(x)x| \leqslant \varepsilon(x)x\}}{\sharp\{\mathbf{P} \in \texttt{Poly}(H) : \mathbf{P} \text{ is Schinzel}\}}$$
$$= 1 + O\left(\frac{1}{\varepsilon(x)(\log x)^{1/2}}\right).$$

*Proof* It is enough to show that

$$\frac{\sharp\{\mathbf{P} \in \texttt{Poly}(H) : \mathbf{P} \text{ is Schinzel}, |\theta_{\mathbf{P}}(x) - \mathfrak{S}_{\mathbf{P}}(x)x| > \varepsilon(x)x\}}{\sharp\{\mathbf{P} \in \texttt{Poly}(H) : \mathbf{P} \text{ is Schinzel}\}}$$
$$\ll \frac{1}{\varepsilon(x)(\log x)^{1/2}}. \tag{4.9}$$

The values of the function $|\theta_{\mathbf{P}}(x) - \mathfrak{S}_{\mathbf{P}}(x)x|\varepsilon(x)^{-1}x^{-1}$ are non-negative, and greater than 1 when $|\theta_{\mathbf{P}}(x) - \mathfrak{S}_{\mathbf{P}}(x)x| > \varepsilon(x)x$. Thus the left hand side of (4.9) is at most

$$\frac{1}{\sharp\{\mathbf{P}\in\texttt{Poly}(H):\mathbf{P}\text{ is Schinzel}\}}\sum_{\substack{\mathbf{P}\in\texttt{Poly}(H)\\ \mathbf{P}\text{ is Schinzel}}}\frac{|\theta_{\mathbf{P}}(x)-\mathfrak{S}_{\mathbf{P}}(x)x|}{\varepsilon(x)x}.$$

Using Theorem 1.9 we see that this is

$$\ll\frac{\sharp\texttt{Poly}(H)}{\sharp\{\mathbf{P}\in\texttt{Poly}(H):\mathbf{P}\text{ is Schinzel}\}}\varepsilon(x)^{-1}(\log x)^{-1/2}.$$

An application of Proposition 2.8 concludes the proof. □

We next show that if $\mathbf{P}$ is Schinzel, then $\mathfrak{S}_{\mathbf{P}}(x)$ stays at a safe distance from zero. Thus, $\mathfrak{S}_{\mathbf{P}}(x)$ may be thought of as a 'detector' of Schinzel $n$-tuples.

**Lemma 4.11** *Let* $\mathbf{P}$ *be a Schinzel* $n$*-tuple such that* $\prod_{i=1}^n P_i(n_0)$ *and* $M$ *are coprime. Then there exists a positive constant* $\beta_0=\beta_0(n,n_0,M,d_1,\dots,d_n)$ *such that for all sufficiently large* $x$ *we have* $\mathfrak{S}_{\mathbf{P}}(x)>\beta_0(\log\log x)^{n-d}$.

*Proof* Our assumption implies that

$$\mathfrak{S}_{\mathbf{P}}(x)\gg\prod_{\substack{\text{prime }\ell\nmid M\\ \ell\leqslant d}}\frac{1-\ell^{-1}Z_{P_1\dots P_n}(\ell)}{\left(1-\ell^{-1}\right)^n}\prod_{\substack{\text{prime }\ell\nmid M\\ d<\ell\leqslant\log x}}\frac{1-\ell^{-1}Z_{P_1\dots P_n}(\ell)}{\left(1-\ell^{-1}\right)^n}.$$

To deal with the product over $\ell\leqslant d$, we note that $Z_{P_1\dots P_n}(\ell)\neq\ell$ gives $Z_{P_1\dots P_n}(\ell)\leqslant\ell-1$. In particular,

$$\prod_{\substack{\text{prime }\ell\nmid M\\ \ell\leqslant d}}\frac{1-\ell^{-1}Z_{P_1\dots P_n}(\ell)}{\left(1-\ell^{-1}\right)^n}\geqslant\prod_{\substack{\text{prime }\ell\nmid M\\ \ell\leqslant d}}\frac{\ell^{-1}}{\left(1-\ell^{-1}\right)^n}\gg 1.$$

To deal with the product over $\ell>d$ we observe that $Z_{P_1\dots P_n}(\ell)\neq\ell$ implies that $P_1\dots P_n$ is not identically zero in $\mathbb{F}_\ell$, thus $Z_{P_1\dots P_n}(\ell)\leqslant d$. This shows that

$$\prod_{\substack{\text{prime }\ell\nmid M\\ d<\ell\leqslant\log x}}\frac{1-\ell^{-1}Z_{P_1\dots P_n}(\ell)}{\left(1-\ell^{-1}\right)^n}\geqslant\prod_{\substack{\text{prime }\ell\nmid M\\ d<\ell\leqslant\log x}}\frac{1-d\ell^{-1}}{\left(1-\ell^{-1}\right)^n}\gg\prod_{d<\ell\leqslant\log x}\frac{1-d\ell^{-1}}{\left(1-\ell^{-1}\right)^n}.$$

For each fixed $d\in\mathbb{N}$ we have

$$\lim_{\psi\to 0}\psi^{-2}\left(\frac{1-d\psi}{(1-\psi)^d}-1\right)=-\frac{d(d-1)}{2}.$$

In particular, for each $d, n \in \mathbb{N}$ there exist constants $\psi_{d,n} > 0$, $K_{d,n} > 0$, such that

$$\frac{1-d\psi}{(1-\psi)^n} \geqslant (1-\psi)^{d-n}\left(1-K_{d,n}\psi^2\right)$$

for all $\psi \in (0, \psi_{d,n})$. We obtain

$$\prod_{d<\ell\leqslant \log x} \frac{1-d\ell^{-1}}{\left(1-\ell^{-1}\right)^n} \gg_{d,n} \prod_{\max\{d,\psi_{d,n}^{-1},K_{d,n}\}<\ell\leqslant \log x} \frac{1-d\ell^{-1}}{\left(1-\ell^{-1}\right)^n}$$
$$\geqslant \prod_{\max\{d,\psi_{d,n}^{-1},K_{d,n}\}<\ell\leqslant \log x} \left(1-\ell^{-1}\right)^{d-n}\left(1-K_{d,n}\ell^{-2}\right).$$

By Mertens' estimate this is $\gg_{d,n} (\log\log x)^{-n+d}$. □

**End of proof of Theorem 1.5**. Take $A_1 = n + A/2$, $A_2 = n + 3A/4$ and let $x$, $H$, $\varepsilon(x)$ be as in Lemma 4.10. By Lemma 4.11, $|\theta_{\mathbf{P}}(x) - \mathfrak{S}_{\mathbf{P}}(x)x| \leqslant \varepsilon(x)x$ implies

$$\theta_{\mathbf{P}}(x) \geqslant \mathfrak{S}_{\mathbf{P}}(x)x - \varepsilon(x)x \geqslant \beta_0(\log\log x)^{n-d}x - \varepsilon(x)x.$$

Hence Lemma 4.10 gives

$$\frac{\sharp\{\mathbf{P} \in \texttt{Poly}(H) : \mathbf{P} \text{ is Schinzel}, \theta_{\mathbf{P}}(x) \geqslant (\beta_0(\log\log x)^{n-d} - \varepsilon(x))x\}}{\sharp\{\mathbf{P} \in \texttt{Poly}(H) : \mathbf{P} \text{ is Schinzel}\}}$$
$$= 1 + O\left(\frac{1}{\varepsilon(x)(\log x)^{1/2}}\right).$$

The choice $\varepsilon(x) = \frac{1}{2}\beta_0(\log\log x)^{n-d}$ gives

$$\frac{\sharp\{\mathbf{P} \in \texttt{Poly}(H) : \mathbf{P} \text{ is Schinzel}, \theta_{\mathbf{P}}(x) \geqslant \frac{\beta_0}{2}(\log\log x)^{n-d}x\}}{\sharp\{\mathbf{P} \in \texttt{Poly}(H) : \mathbf{P} \text{ is Schinzel}\}}$$
$$= 1 + O\left(\frac{(\log\log x)^{d-n}}{\sqrt{\log x}}\right).$$

Since $(\log H)^{A_1} < x \leqslant (\log H)^{A_2}$, the error term is $\ll (\log\log\log H)^{d-n} \times (\log\log H)^{-1/2}$, thus,

$$\frac{\sharp\left\{\mathbf{P} \in \texttt{Poly}(H) : \mathbf{P} \text{ is Schinzel}, \theta_{\mathbf{P}}(x) \geqslant \frac{\beta_0 x}{2(\log\log x)^{d-n}}\right\}}{\sharp\{\mathbf{P} \in \texttt{Poly}(H) : \mathbf{P} \text{ is Schinzel}\}} = 1 + O\left(\frac{(\log\log\log H)^{d-n}}{\sqrt{\log\log H}}\right). \tag{4.10}$$

It remains to find a lower bound for $\sharp S_{n+A}(\mathbf{P})$. Observing that for all, except $O(H^{n+d-1/2})$, $n$-tuples $\mathbf{P}$ with $|\mathbf{P}| \leqslant H$ one has $|\mathbf{P}| > H^{1/2}$, we see that $x \leqslant (\log H)^{A_2} \ll (\log|\mathbf{P}|)^{A_2} \leqslant (\log|\mathbf{P}|)^{n+A}$, hence

$$\theta_{\mathbf{P}}(x) = \sum_{\substack{m\in\mathbb{N}\cap[1,x],\, m\equiv n_0 (\mathrm{mod}\ M) \\ P_i(m) \text{ prime for } i=1,\ldots,n}} \prod_{i=1}^{n} \log P_i(m) \leqslant \sharp S_{n+A}(\mathbf{P}) \prod_{i=1}^{n} \log((d_i+1)Hx^{d_i})$$

due to $m \leqslant x$ and $|\mathbf{P}| \leqslant H$. From $x \leqslant (\log H)^{A_2}$ we obtain $\theta_{\mathbf{P}}(x) \ll \sharp S_{n+A}(\mathbf{P})(\log H)^n$. By (4.10) all, except

$$O(H^{n+d}(\log\log\log H)^{d-n}(\log\log H)^{-1/2})$$

Schinzel $n$-tuples $\mathbf{P} \in \texttt{Poly}(H)$ fulfil $\theta_{\mathbf{P}}(x) \geqslant \frac{\beta_0}{2}(\log\log x)^{n-d}x$. For these $\mathbf{P}$ we use the upper and the lower bound for $\theta_{\mathbf{P}}(x)$ in conjunction with $x \geqslant (\log H)^{A_1}$ to get the following when $H \gg_{d,n,A} 1$:

$$(\log H)^{n+A/3} \leqslant \frac{(\log H)^{A_1}}{(\log\log\log H)^{n-d}} \ll \frac{\beta_0 x}{2(\log\log x)^{n-d}} \leqslant \theta_{\mathbf{P}}(x) \ll \sharp S_{n+A}(\mathbf{P})(\log H)^n.$$

Together with $|\mathbf{P}| > H^{1/2}$, this gives $\sharp S_{n+A}(\mathbf{P}) \geqslant (\log|\mathbf{P}|)^{A/3}$. □

## 5 Random Châtelet varieties

### 5.1 Irreducible polynomials

Let $K$ be a finite field extension of $\mathbb{Q}$ of degree $r = [K : \mathbb{Q}]$. Let $\mathrm{N}_{K/\mathbb{Q}} : K \to \mathbb{Q}$ be the norm. Choose a $\mathbb{Z}$-basis $\omega_1, \ldots, \omega_r$ of the ring of integers $\mathscr{O}_K \subset K$.

For $\mathbf{z} = (z_1, \ldots, z_r)$ we define a norm form

$$\mathrm{N}_{K/\mathbb{Q}}(\mathbf{z}) = \mathrm{N}_{K/\mathbb{Q}}(z_1\omega_1 + \ldots + z_r\omega_r).$$

For a positive integer $d$ consider the affine $\mathbb{Z}$-space $\mathbb{A}_{\mathbb{Z}}^{d+2} = \mathbb{A}_{\mathbb{Z}}^1 \times \mathbb{A}_{\mathbb{Z}}^{d+1}$, where $\mathbb{A}_{\mathbb{Z}}^{d+1} = \mathrm{Spec}(\mathbb{Z}[x_0, \ldots, x_d])$ and $\mathbb{A}_{\mathbb{Z}}^1 = \mathrm{Spec}(\mathbb{Z}[t])$. Let $V$ be the open subscheme of $\mathbb{A}_{\mathbb{Z}}^{d+2}$ given by

$$P(t, \mathbf{x}) := x_d t^d + x_{d-1} t^{d-1} + \ldots + x_1 t + x_0 \neq 0,$$

where $\mathbf{x} = (x_0, \ldots, x_d)$. Let $U$ be the affine scheme given by

$$P(t, \mathbf{x}) = \mathrm{N}_{K/\mathbb{Q}}(\mathbf{z}) \neq 0,$$

and let $f : U \to V$ be the natural morphism. Note that $U_\mathbb{Q}$ is smooth over $V_\mathbb{Q}$ with geometrically integral fibres. Let $g : U \to \mathbb{A}_{\mathbb{Z}}^1$ be the projection to the variable $t$, and let $h : U \to \mathbb{A}_{\mathbb{Z}}^{d+1}$ be the projection to the variable $\mathbf{x}$.

For a ring $R$ and a point $\mathbf{m} = (m_0, \ldots, m_d) \in R^{d+1}$ of $\mathbb{A}_{\mathbb{Z}}^{d+1}$ define $U_\mathbf{m} = h^{-1}(\mathbf{m})$. Then $g : U_\mathbf{m} \to \mathbb{A}_R^1 \setminus \{P(t, \mathbf{m}) = 0\}$ is a morphism given by coordinate $t$. For $\nu \in R$ we define $U_{\nu,\mathbf{m}} = f^{-1}(\nu, \mathbf{m})$.

For a prime $p$, a point $(\nu, \mathbf{m}) \in \mathbb{Z}_p^{d+2}$ belongs to $V(\mathbb{Z}_p)$ if and only if $P(\nu, \mathbf{m}) \in \mathbb{Z}_p^*$. Similarly, $U(\mathbb{Z}_p)$ in $\mathbb{Z}_p^{d+2} \times (\mathscr{O}_K \otimes \mathbb{Z}_p)$ is given by $P(\nu, \mathbf{m}) = \mathrm{N}_{K/\mathbb{Q}}(\mathbf{z}) \in \mathbb{Z}_p^*$.

**Lemma 5.1** *Let $S$ be the set of primes where $K/\mathbb{Q}$ is ramified. Then for any $p \notin S$ and any $(\nu, \mathbf{m}) \in V(\mathbb{Z}_p)$ the fibre $U_{\nu,\mathbf{m}}$ has a $\mathbb{Z}_p$-point.*

*Proof* This follows from the fact that for any finite unramified extension $\mathbb{Q}_p \subset K_v$ any element of $\mathbb{Z}_p^*$ is the norm of an integer in $K_v$, see [13, Ch. 1, §7]. □

**Lemma 5.2** *Let $p$ be a prime and let $N \in U(\mathbb{Q}_p)$. There is a positive integer $M$ such that if $\nu \in \mathbb{Q}_p$ and $\mathbf{m} \in (\mathbb{Q}_p)^{d+1}$ satisfy*

$$\max\left(|\nu - g(N)|_p, |\mathbf{m} - h(N)|_p\right) \leqslant p^{-M},$$

*then $U_{\nu,\mathbf{m}}(\mathbb{Q}_p) \neq \varnothing$.*

*Proof* We note that $U_\mathbb{Q}$ is smooth, so every $\mathbb{Q}_p$-point of $U_\mathbb{Q}$ has an open neighbourhood $\mathscr{U}$ homeomorphic to an open $p$-adic ball. Since $f : U_\mathbb{Q} \to V_\mathbb{Q}$, $V_\mathbb{Q} \to \mathbb{A}_\mathbb{Q}^1$ and $V_\mathbb{Q} \to \mathbb{A}_\mathbb{Q}^{d+1}$ are smooth morphisms, $g$ and $h$ are also smooth. This implies that the maps of topological spaces $g : U(\mathbb{Q}_p) \to \mathbb{Q}_p$ and $h : U(\mathbb{Q}_p) \to (\mathbb{Q}_p)^{d+1}$ are open, cf. [21, p. 80]. Thus there exist open $p$-adic balls $\mathscr{U}_1 \subset \mathbb{Q}_p$ with centre $g(N)$ and $\mathscr{U}_2 \subset (\mathbb{Q}_p)^{d+1}$ with centre $h(N)$ such that $\mathscr{U}_1 \times \mathscr{U}_2 \subset f(\mathscr{U})$. □

**Theorem 5.3** *Let $K$ be a cyclic extension of $\mathbb{Q}$ and let $S$ be the set of primes where $K/\mathbb{Q}$ is ramified. Let $\mathscr{P}$ be the set of $\mathbf{m} \in \mathbb{Z}^{d+1}$ such that $P(t, \mathbf{m})$ is a Bouniakowsky polynomial. Let $\mathscr{M}$ be the set of $\mathbf{m} \in \mathscr{P}$ such that $U_{\mathbf{m}}(\mathbb{Z}_p) \neq \varnothing$ for each $p \in S$. When $\mathscr{P}$ is ordered by height, there is a subset $\mathscr{M}' \subset \mathscr{M}$ of density 1 such that $U_{\mathbf{m}}(\mathbb{Q}) \neq \varnothing$ for every $\mathbf{m} \in \mathscr{M}'$. The set $\mathscr{M}'$ has positive density in $\mathbb{Z}^{d+1}$ ordered by height.*

*Remark 5.4* (1) The Bouniakowsky condition at $p \notin S$ implies that $U_{\mathbf{m}}(\mathbb{Z}_p) \neq \varnothing$. Indeed, for $\mathbf{m} \in \mathscr{P}$ the reduction of $P(t, \mathbf{m})$ modulo $p$ is a non-zero function $\mathbb{F}_p \to \mathbb{F}_p$. Hence we can find a $t_p \in \mathbb{Z}_p$ such that $P(t_p, \mathbf{m}) \in \mathbb{Z}_p^*$ and apply Lemma 5.1. Likewise, the positivity of the leading term of $P(t, \mathbf{m})$, which is the 'Bouniakowsky condition at infinity', implies that $U_{\mathbf{m}}$ has real points over large real values of $t$. Thus in our setting the condition that $U_{\mathbf{m}}(\mathbb{Z}_p) \neq \varnothing$ for each $p \in S$ implies that $U_{\mathbf{m}}$ is everywhere locally soluble.

(2) The existence of a subset $\mathscr{M}' \subset \mathscr{M}$ of density 1 can be linked to the triviality of the unramified Brauer group of $U_{\mathbf{m}}$ when $K/\mathbb{Q}$ is cyclic and $P(t, \mathbf{m})$ is an irreducible polynomial, as follows from [19, Cor. 2.6 (c)], see also [58, Prop. 2.2 (b), (d)].

*Proof* Since $\mathbb{Z}_p^*$ is closed in $\mathbb{Z}_p$ and $P(t, \mathbf{x})$ is a continuous function, $V(\mathbb{Z}_p)$ is closed in $\mathbb{Z}_p^{d+2}$, hence compact. For the same reason $U(\mathbb{Z}_p)$ is compact, thus $h(U(\mathbb{Z}_p))$ is compact as a continuous image of a compact set. Therefore, $\prod_{p\in S} h(U(\mathbb{Z}_p))$ is compact.

Take any $(N_p) \in \prod_{p\in S} U(\mathbb{Z}_p)$. For each $p \in S$ there is a positive integer $M_p$ such that the $p$-adic ball $\mathscr{B}_{N_p} \subset \mathbb{Z}_p^{d+1}$ of radius $p^{-M_p}$ around $h(N_p)$ satisfies the conclusion of Lemma 5.2. Thus the open sets $\prod_{p\in S} \mathscr{B}_{N_p}$, where $(N_p) \in \prod_{p\in S} U(\mathbb{Z}_p)$, cover $\prod_{p\in S} h(U(\mathbb{Z}_p))$. By compactness, there exist finitely many points $(N_p^{(i)}) \in \prod_{p\in S} U(\mathbb{Z}_p)$, $i = 1, \ldots, n$, such that the corresponding open sets $\prod_{p\in S} \mathscr{B}_{N_p^{(i)}}$ cover $\prod_{p\in S} h(U(\mathbb{Z}_p))$.

It follows that $\mathscr{M} = \cup_{i=1}^n \mathscr{M}_i$, where $\mathscr{M}_i = \mathscr{M} \cap \prod_{p\in S} \mathscr{B}_{N_p^{(i)}}$ for all $i$. Thus it is enough to prove that for 100% of $\mathbf{m} \in \mathscr{M}_i$ we have $U_{\mathbf{m}}(\mathbb{Q}) \neq \varnothing$.

In the rest of proof we write $\mathscr{M} = \mathscr{M}_i$ and $N_p = N_p^{(i)}$, where $p \in S$. Write $n_p = g(N_p)$ and $\mathbf{m}_p = h(N_p)$, where $p \in S$. Note that $P(n_p, \mathbf{m}_p) \in \mathbb{Z}_p^*$ for each $p \in S$. Write $M = \prod_{p\in S} p^{M_p}$. By the Chinese remainder theorem we can find $n_0 \in \mathbb{Z}$ and $\mathbf{m}_0 \in \mathbb{Z}^{d+1}$ such that $n_0 \equiv n_p \pmod{p^{M_p}}$ and $\mathbf{m}_0 \equiv \mathbf{m}_p \pmod{p^{M_p}}$ for each $p \in S$. Our new set $\mathscr{M}$ consists of all $\mathbf{m} \in \mathscr{P}$ such that $\mathbf{m} \equiv \mathbf{m}_0 \pmod{M}$. Since $P(n_p, \mathbf{m}_p) \in \mathbb{Z}_p^*$ for each $p \in S$, we obtain that $P(n_0, \mathbf{m}_0)$ is coprime to $M$.

Thus we can apply Theorem 1.2 to our $n_0, M$, with $Q(t) = P(t, \mathbf{m}_0)$. It gives that for 100% of $\mathbf{m} \in \mathscr{M}$, ordered by height, one can choose $\nu \equiv n_0 \pmod{M}$ such that $P(\nu, \mathbf{m})$ is a prime. Call this prime $q$.

We claim that $q = \mathrm{N}_{K/\mathbb{Q}}(\xi)$ for some $\xi \in K^*$, so that $U_{\nu,\mathbf{m}}(\mathbb{Q}) \neq \varnothing$. Since $K$ is a cyclic extension of $\mathbb{Q}$, it is enough to show that for all places $v$ of $\mathbb{Q}$, except possibly the place corresponding to the prime $q$, we have $U_{\nu,\mathbf{m}}(\mathbb{Q}_v) \neq \varnothing$, see, e.g., [20, Cor. 13.1.10] and references there. Indeed, the prime $q$ is a local norm at $\mathbb{Q}_v = \mathbb{R}$, since any positive real number is a norm for any finite extension. Next, $q$ is a local norm at $\mathbb{Q}_p$ for $p \in S$, by the definition of $\mathscr{M}$ and Lemma 5.2. Finally, $q$ is a local norm at $\mathbb{Q}_p$ for $p \notin S$, $p \neq q$, since $q \in \mathbb{Z}_p^*$ implies $(\nu, \mathbf{m}) \in V(\mathbb{Z}_p)$, so we can apply Lemma 5.1.

Proving that $\mathscr{M}'$ has positive density in $\mathbb{Z}^{d+1}$ is equivalent to proving the same for $\mathscr{M}$. We have $\mathscr{M} = \cup_{i=1}^n \mathscr{M}_i$, where each $\mathscr{M}_i$ consists of all Bouniakowsky polynomials $P(t)$ of degree $d$ satisfying $P(t) \equiv Q(t) \pmod{M}$ with $(Q(n_0), M) = 1$. Corollary 2.9 implies that any such set has positive density. Similarly, any non-empty intersection of some of the sets $\mathscr{M}_i$ also has positive density. By inclusion-exclusion $\mathscr{M}$ has positive density in $\mathbb{Z}^{d+1}$. □

*Remark 5.5* It is not clear to us if $U_{\nu,\mathbf{m}}(\mathbb{Z}) \neq \varnothing$.

*Example 5.6* Let $K = \mathbb{Q}(\sqrt{-1})$. Then $S = \{2\}$. Fix a positive integer $m \geqslant 2$. Let $s = |(\mathbb{Z}/2^m)^*| = 2^{m-1}$. Consider

$$P(t) = 3 + (2^m - 3)t^s + 2^{m+2}Q(t), \quad \text{where} \quad Q(t) \in \mathbb{Z}[t].$$

If $n \in \mathbb{Z}$ is even, then $P(n) \equiv 3 \pmod 4$ so $P(n)$ is not a sum of two squares in $\mathbb{Q}_2$. If $n$ is odd, then $n^s \equiv 1 \pmod{2^m}$, hence $P(n)$ is divisible by $2^m$. Since $P(1) = 2^m(1+4k)$ is a sum of two squares in $\mathbb{Z}_2$, our equation $x^2 + y^2 = P(t)$ is solvable in $\mathbb{Z}_2$, but for *any* 2-adic solution the 2-adic valuation of the right hand side is divisible by $2^m$. This example shows that the set of $\mathbf{m} \in \mathbb{Z}^{d+1}$ such that $U_{\mathbf{m}}(\mathbb{Z}_2) = \varnothing$ while $U_{\mathbf{m}}(\mathbb{Q}_2) \neq \varnothing$ has positive density.

Let us now give a simpler version of Theorem 5.3 applicable to some non-cyclic abelian extensions $K/\mathbb{Q}$. Let $K^{(1)}$ be the Hilbert class field of $K$ and let $K^{(+)}$ be the *extended Hilbert class field* of $K$, see [40, p. 241] (it is also called the strict Hilbert class field [14, Def. 15.32]). By definition, $K^{(+)}$ is the ray class field whose modulus is the union of all real places of $K$. Thus $K^{(+)}$ is a maximal abelian extension of $K$ unramified at all the *finite* places of $K$, so that $K^{(1)} \subset K^{(+)}$. By class field theory a prime $\mathfrak{p}$ of $K$ splits in $K^{(+)}$ if and only if $\mathfrak{p} = (x)$ is a principal prime ideal with a totally positive generator $x \in K$.

**Theorem 5.7** *Let $d$ be a positive integer. Let $K$ be a finite abelian extension of $\mathbb{Q}$ such that $K^{(+)}$ is abelian over $\mathbb{Q}$. Then for a positive proportion of polynomials $P(t) \in \mathbb{Z}[t]$ of degree $d$ ordered by height the equation (1.1) is soluble in $\mathbb{Z}$.*

*Proof* Since $K^{(+)}$ is abelian over $\mathbb{Q}$, by the Kronecker–Weber theorem there is a positive integer $M$ such that $K^{(+)} \subset \mathbb{Q}(\zeta_M)$. Thus if a prime number $p$ is 1 (mod $M$) then $p$ splits in $K^{(+)}$. This implies that $p$ splits in $K$ so that every prime $\mathfrak{p}$ of $K$ over $p$ has norm $p$; moreover, $\mathfrak{p}$ splits in $K^{(+)}$ and so $\mathfrak{p} = (x)$ where $x \in \mathscr{O}_K$ is totally positive. Then the ideal $(p) \subset \mathbb{Z}$ is the norm of the ideal $(x) \subset \mathscr{O}_K$, hence $(p) = (\mathrm{N}_{K/\mathbb{Q}}(x))$. Since $x$ is totally positive, we have $\mathrm{N}_{K/\mathbb{Q}}(x) > 0$, so $p = \mathrm{N}_{K/\mathbb{Q}}(x)$.

A positive proportion of polynomials of degree $d$ are Bouniakowsky polynomials, and a positive proportion of these are congruent to the constant polynomial $Q(t) = 1$ modulo $M$, by Proposition 2.8. Taking $n_0 = 0$ in Theorem 1.2 we see that for 100 % of such polynomials $P(t)$ there is an integer $m$ such that $P(m)$ is a prime number $p \equiv 1 \pmod{M}$. Then $p = \mathrm{N}_{K/\mathbb{Q}}(x)$ for some $x \in \mathscr{O}_K$. □

If $K$ is a totally imaginary abelian extension of $\mathbb{Q}$ of class number 1, then $K = K^{(1)} = K^{(+)}$ so that Theorem 5.7 can be applied. For example, this holds for $K = \mathbb{Q}(\sqrt{-1}, \sqrt{2})$, which is one of 47 biquadratic extensions of $\mathbb{Q}$ with class number 1, see [9]. If $K$ is an imaginary quadratic field, then $K^{(1)}$ is abelian over $\mathbb{Q}$ if and only if the class group of $K$ is an elementary 2-group [40, Cor. VI.3.4].

### 5.2 Reducible polynomials

Let $d_1, \ldots, d_n$ be positive integers. In this section we let $U$ be the affine $\mathbb{Z}$-scheme given by

$$\prod_{i=1}^{n} P_i(t, \mathbf{x}_i) = \mathrm{N}_{K/\mathbb{Q}}(\mathbf{z}) \neq 0, \tag{5.1}$$

where $\mathbf{x}_i = (x_{i,0}, \ldots, x_{i,d_i})$ and

$$P_i(t, \mathbf{x}_i) = x_{i,d_i} t^{d_i} + x_{i,d_i-1} t^{d_i-1} + \ldots + x_{i,1} t + x_{i,0}, \qquad i = 1, \ldots, n.$$

Write $d = d_1 + \ldots + d_n$ and $\mathbf{x} = (\mathbf{x}_1, \ldots, \mathbf{x}_n)$. Consider the affine space $\mathbb{A}_{\mathbb{Z}}^{d+n+1}$ with coordinates $t$ and $x_{ij}$ for all pairs $(i, j)$, where $1 \leqslant i \leqslant n$ and $0 \leqslant j \leqslant d_i$. Define $V$ as the open subscheme of $\mathbb{A}_{\mathbb{Z}}^{d+n+1}$ given by $\prod_{i=1}^n P_i(t, \mathbf{x}_i) \neq 0$. The morphism $f : U \to V$ is the product of the morphism $g$ (the projection to $t$) and the morphisms $h_i$ (the projection to $\mathbf{x}_i$), for $i = 1, \ldots, n$.

**Theorem 5.8** *Let $K$ be a cyclic extension of $\mathbb{Q}$ of degree $r = [K : \mathbb{Q}]$ with character*

$$\chi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathbb{Z}/r.$$

*Let $S$ be the set of primes where $K/\mathbb{Q}$ ramifies. Let $\mathscr{P}$ be the set of $\mathbf{m} = (\mathbf{m}_1, \ldots, \mathbf{m}_n) \in \mathbb{Z}^{d+n}$ such that $P_1(t, \mathbf{m}_1), \ldots, P_n(t, \mathbf{m}_n)$ is a Schinzel $n$-tuple. Let $\mathscr{M} \subset \mathscr{P}$ be the subset whose elements $\mathbf{m}$ satisfy the following condition:*

for each $p \in S$ there is a point $(t_p, \mathbf{z}_p) \in U_{\mathbf{m}}(\mathbb{Z}_p)$ such that for each $i = 1, \ldots, n$ we have

$$\sum_{p \in S} \mathrm{inv}_p(\chi, P_i(t_p, \mathbf{m}_i)) = 0. \tag{5.2}$$

*Then there is a subset $\mathscr{M}' \subset \mathscr{M}$ of density 1 such that $U_{\mathbf{m}}(\mathbb{Q}) \neq \varnothing$ for every $\mathbf{m} \in \mathscr{M}'$. The set $\mathscr{M}'$ has positive density in $\mathbb{Z}^{d+n}$ ordered by height.*

Let us explain the notation used in this statement. For a place $v$ of $\mathbb{Q}$ and $a \in \mathbb{Q}_v^*$ we denote by $(\chi, a_v)$ the element of the Brauer group $\mathrm{Br}(\mathbb{Q}_v)$ which is the class of the cyclic algebra over $\mathbb{Q}_v$ of degree $r$ defined by $\chi$ and $a_v$, see [20, §1.3.4]. We have $(\chi, a_v) = 0$ if and only if $a_v$ is a local norm for the extension $K/\mathbb{Q}$. The local invariant $\mathrm{inv}_v$ is an injective homomorphism

$$\mathrm{inv}_v\colon \mathrm{Br}(\mathbb{Q}_v) \to \mathbb{Q}/\mathbb{Z},$$

which is surjective if $v$ is a finite place, and has image $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$ if $\mathbb{Q}_v = \mathbb{R}$. The sum of maps $\mathrm{inv}_v$ for all places $v$ of $\mathbb{Q}$ fits into the exact sequence

$$0 \longrightarrow \mathrm{Br}(\mathbb{Q}) \longrightarrow \oplus_v \mathrm{Br}(\mathbb{Q}_v) \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0, \tag{5.3}$$

where each map $\mathrm{Br}(\mathbb{Q}) \to \mathrm{Br}(\mathbb{Q}_v)$ is the natural restriction, see [20, §13.1.2].

*Remark 5.9* (1) For $n = 1$ condition (5.2) is automatically satisfied, so we recover Theorem 5.3 as a particular case of Theorem 5.8.

(2) Since each $P_i(t, \mathbf{m}_i)$ is a Bouniakowsky polynomial, for each $p \notin S$ we can find a $t_p \in \mathbb{Z}_p$ such that $P_i(t_p, \mathbf{m}_i) \in \mathbb{Z}_p^*$ and hence $\mathrm{inv}_p(\chi, P_i(t_p, \mathbf{m}_i)) = 0$. Taking the product over $i = 1, \ldots, n$ we see that $U_{\mathbf{m}}$ has a $\mathbb{Z}_p$-point over $t_p$. Similarly, each $P_i(t, \mathbf{m}_i)$ takes positive values when $t_0 \in \mathbb{R}$ is large, so $\mathrm{inv}_{\mathbb{R}}(\chi, P_i(t_0, \mathbf{m}_i)) = 0$. Thus $U_{\mathbf{m}}$ has a real point over $t_0$. Thus (5.2) implies that $U_{\mathbf{m}}$ has $\mathbb{Z}_p$-points $(t_p, \mathbf{z}_p)$ for all $p$ and a real point $(t_0, \mathbf{z}_0)$ such that

$$\sum \mathrm{inv}_p(\chi, P_i(t_p, \mathbf{m}_i)) = 0$$

for $i = 1, \dots, n$, where the sum is over all places of $\mathbb{Q}$. Since $K/\mathbb{Q}$ is cyclic, from [19, Cor. 2.6 (c)] we know that the unramified Brauer group of $U_{\mathbf{m}}$ is contained in the subgroup of $\mathrm{Br}(\mathbb{Q}(U_{\mathbf{m}}))$ generated by $\mathrm{Br}(\mathbb{Q})$ and the classes $(\chi, P_i(t, \mathbf{m}_i))$, for $i = 1, \dots, n$. We conclude that when each $P_i(t, \mathbf{m}_i)$ is irreducible, for any smooth and proper model $X$ of $U_{\mathbf{m}}$, the Brauer group $\mathrm{Br}(X)$ does not obstruct the Hasse principle on $X$.

*Proof* We follow the proof of Theorem 5.3 with necessary adjustments. The analogue of Lemma 5.2 says that for $p \in S$ and $N_p \in U(\mathbb{Q}_p)$ there is a positive integer $M_p$ such that if $\nu \in \mathbb{Q}_p$ and $\mathbf{m} \in (\mathbb{Q}_p)^{d+n}$ satisfy

$$\max\left(|\nu - g(N_p)|_p, |\mathbf{m}_i - h_i(N_p)|_p\right) \leqslant p^{-M_p}, \text{ for } i = 1, \dots, n, \quad (5.4)$$

then $\mathrm{inv}_p(\chi, P_i(\nu, \mathbf{m}_i))$ is constant and equal to $\mathrm{inv}_p(\chi, P_i(g(N_p), h_i(N_p)))$. This implies

$$\mathrm{inv}_p(\chi, \prod_{i=1}^{n} P_i(\nu, \mathbf{m}_i)) = \sum_{i=1}^{n} \mathrm{inv}_p(\chi, P_i(\nu, \mathbf{m}_i))$$
$$= \mathrm{inv}_p(\chi, \prod_{i=1}^{n} P_i(g(N_p), h_i(N_p))) = 0, \quad (5.5)$$

in particular, $U_{\nu,\mathbf{m}}(\mathbb{Q}_p) \neq \varnothing$.

Let $Z \subset \prod_{p\in S} U(\mathbb{Z}_p)$ be the subset consisting of the points $(N_p)$ subject to the condition

$$\sum_{p\in S} \mathrm{inv}_p(\chi, P_i(g(N_p), h_i(N_p))) = 0, \text{ for } i = 1, \dots, n. \quad (5.6)$$

The left hand side of (5.6), for a fixed $i$, takes values in $\mathbb{Z}/r$ and each level set is open, hence also closed. We know that $\prod_{p\in S} U(\mathbb{Z}_p)$ is compact, hence $Z$ is compact. Thus $f(Z)$ is compact, so $f(Z)$ can be covered by finitely many open subsets given by congruence conditions on $\nu$ and $\mathbf{m}$ as in (5.4) such that (5.6) holds.

The condition (5.2) in the theorem implies that $\mathscr{M} \subset h(Z)$. As a consequence, using the Chinese remainder theorem, we represent $\mathscr{M}$ as a finite union of subsets $\mathscr{M}_j$, each of which consists of all Schinzel $n$-tuples satisfying a congruence condition of the form $\mathbf{m} \equiv \mathbf{m}_0 \pmod{M}$, where $\mathbf{m}_0 \in \mathbb{Z}^{d+n}$ and $M = \prod_{p\in S} p^{M_p}$. Moreover, there exists an $n_0 \in \mathbb{Z}$ with $(\prod_{i=1}^{n} P_i(n_0, \mathbf{m}_{0,i}), M) = 1$ such that the following holds: if $\nu \equiv n_0 \pmod{M}$, then for all $\mathbf{m} \in \mathscr{M}_j$ we have

$$\sum_{p\in S} \mathrm{inv}_p(\chi, P_i(\nu, \mathbf{m}_i)) = 0, \text{ for } i = 1, \dots, n, \tag{5.7}$$

and

$$\sum_{i=1}^{n} \mathrm{inv}_p(\chi, P_i(\nu, \mathbf{m}_i)) = 0, \text{ for } p \in S, \tag{5.8}$$

which follow from (5.6) and (5.5), respectively. It is enough to prove that for 100% of $\mathbf{m} \in \mathscr{M}_j$ we have $U_{\mathbf{m}}(\mathbb{Q}) \neq \varnothing$.

We apply Theorem 1.2 to our $n_0$ and $M$, with $Q_i(t) = P_i(t, \mathbf{m}_{0,i})$. It gives that for 100% of $\mathbf{m}$ there is an integer $\nu \equiv n_0 \pmod M$ such that each $q_i = P_i(\nu, \mathbf{m}_i)$ is a prime. We have

$$\mathrm{inv}_p(\chi, q_i) = \mathrm{inv}_p(\chi, P_i(\nu, \mathbf{m}_i)) = 0 \tag{5.9}$$

for every prime $p \notin S \cup \{q_i\}$ and also for the real place. The real condition trivially holds since $q_i > 0$. A prime $p \notin S \cup \{q_i\}$ does not divide $q_i$ and is unramified in $K$, so the condition holds for such $p$. Therefore, by global reciprocity we have

$$\begin{aligned} \mathrm{inv}_{q_i}(\chi, q_i) &= -\sum_{p\neq q_i} \mathrm{inv}_p(\chi, q_i) \\ &= -\sum_{p\in S} \mathrm{inv}_p(\chi, q_i) = 0, \text{ for } i = 1, \dots, n, \end{aligned} \tag{5.10}$$

where the last equality follows from (5.7). We claim that

$$\mathrm{inv}_p(\chi, q_1 \dots q_n) = 0$$

for every prime $p$ (and also for the real place). This is clear for $p \notin S \cup \{q_1, \dots, q_n\}$ and for the real place, but this is also clear for $p = q_i$ by (5.10) and (5.9). Using (5.8) we obtain the vanishing for $p \in S$, thus proving the claim.

The class $(\chi, q_1 \dots q_n) \in \mathrm{Br}(\mathbb{Q})[r]$ has all local invariants equal to 0, so it is zero due to the exactness of (5.3). Thus $\prod_{i=1}^{n} P(\nu, \mathbf{m}_i) = q_1 \dots q_n$ is a global norm for the extension $K/\mathbb{Q}$, so $U_{\nu,\mathbf{m}}(\mathbb{Q}) \neq \varnothing$.

The last statement of the theorem is proved in the same way as the last statement of Theorem 5.3, using Proposition 2.8. □

## 6 Random conic bundles

The classification of Enriques–Manin–Iskovskikh [38, Thm. 1] states that smooth projective geometrically rational surfaces over a field, up to birational equivalence, fall into finitely many exceptional families (del Pezzo surfaces of degree $1 \leqslant d \leqslant 9$) and infinitely many families of conic bundles $X \to \mathbb{P}^1$. The generic fibre of a conic bundle over $\mathbb{Q}$ is a projective conic over the field $\mathbb{Q}(t)$ which can be described as the zero set of a diagonal quadratic form of rank 3. We consider the equation

$$a_1 \prod_{j=1}^{n_1} P_{1,j}(t)\, x^2 + a_2 \prod_{k=1}^{n_2} P_{2,k}(t)\, y^2 + a_3 \prod_{l=1}^{n_3} P_{3,l}(t)\, z^2 = 0, \tag{6.1}$$

where $a_1, a_2, a_3$ are fixed non-zero integers and $P_{ij} \in \mathbb{Z}[t]$ is a polynomial of fixed degree $d_{ij}$, for $i = 1, 2, 3$ and $j = 1, \ldots, n_i$, where $n_1 > 0$, $n_2 > 0$ and $n_3 \geqslant 0$. Let $d = \sum_{i,j} d_{ij}$. We write $P_{ij}(t, \mathbf{m}_{ij})$ for the polynomial of degree $d_{ij}$ with coefficients $\mathbf{m}_{ij} \in \mathbb{Z}^{d_{ij}+1}$, and write $\mathbf{m} = (\mathbf{m}_{ij}) \in \mathbb{Z}^{d+n}$. Let $U_{\mathbf{m}} \subset \mathbb{P}^2_{\mathbb{Z}} \times \mathbb{A}^1_{\mathbb{Z}}$ be the scheme given by equation (6.1) together with the condition $\prod_{i,j} P_{ij}(t, \mathbf{m}_{ij}) \neq 0$. The proof of the following theorem is given in §6.3.

**Theorem 6.1** *Let $n_1, n_2, n_3$ be integers such that $n_1 > 0$, $n_2 > 0$, and $n_3 \geqslant 0$, and let $n = n_1 + n_2 + n_3$. Let $a_1, a_2, a_3$ be non-zero integers not all of the same sign and such that $a_1a_2a_3$ is square-free. Let $S$ be the set of prime factors of $2a_1a_2a_3$. Let $d_{ij}$ be natural numbers, for $i = 1, 2, 3$ and $j = 1, \ldots, n_i$, and let $d = \sum_{i,j} d_{ij}$. Let $\mathscr{P}$ be the set of $\mathbf{m} = (\mathbf{m}_{ij}) \in \mathbb{Z}^{d+n}$ such that the $n$-tuple $(P_{ij}(t, \mathbf{m}_{ij}))$ is Schinzel. Let $\mathscr{M}$ be the set of $\mathbf{m} \in \mathscr{P}$ such that $U_{\mathbf{m}}(\mathbb{Z}_p) \neq \varnothing$ for each $p \in S$. Then there is a subset $\mathscr{M}' \subset \mathscr{M}$ of density 1 such that $U_{\mathbf{m}}(\mathbb{Q}) \neq \varnothing$ for every $\mathbf{m} \in \mathscr{M}'$. The set $\mathscr{M}'$ has positive density in $\mathbb{Z}^{d+n}$ ordered by height.*

*Remark 6.2* Let $\mathbf{x} = (x_{ij})$, for $i = 1, 2, 3$ and $j = 1, \ldots, n_i$, be independent variables. We expect that for the generic polynomials $(P_{ij}(t, \mathbf{x}_{ij}))$ the unramified Brauer group of the conic bundle (6.1) over $\mathbb{Q}(\mathbf{x})$ is reduced to $\mathrm{Br}(\mathbb{Q}(\mathbf{x}))$. This explains the absence of extra conditions like (5.2) in Theorem 6.1.

### 6.1 Correlations between prime values of polynomials and quadratic characters

When $a$ and $b$ are integers such that $b > 0$ we write $\left(\frac{a}{b}\right)$ for the Legendre–Jacobi quadratic symbol. We allow $b$ to be even, so that $\left(\frac{a}{2}\right)$ is 0 or 1 when $a$ is even and odd, respectively.

A new analytic input in this section is the following result of Heath-Brown.

**Lemma 6.3** (Heath-Brown) *Let $(a_k)_{k\in\mathbb{N}}$ and $(b_l)_{l\in\mathbb{N}}$ be sequences of complex numbers such that $a_k = 0$ for $k > K$ and $b_l = 0$ for $l > L$. Then for any $\varepsilon > 0$ we have*

$$\sum_{\text{primes}\, k,l} a_k b_l \left(\frac{k}{l}\right) \ll_\varepsilon \max\{|a_k|\} \max\{|b_l|\} \left((KL)^{1+\varepsilon} (\min\{K, L\})^{-1/2} + K\right),$$

*where the implied constant depends only on $\varepsilon$.*

*Proof* We write the sum as

$$\sum_{\substack{k,l\in\mathbb{N}\\ l \text{ odd}}} \left(a_k \mathbb{1}_{\text{primes}}(k)\right) \left(b_l \mathbb{1}_{\text{primes}}(l)\right) \left(\frac{k}{l}\right) + \sum_{k \text{ prime}} a_k b_2 \left(\frac{k}{2}\right).$$

By [35, Cor. 4] the first sum is $\ll \max\{|a_k|\} \max\{|b_l|\}(KL)^{1+\varepsilon} (\min\{K, L\})^{-1/2}$ The second sum is trivially bounded by $\max\{|a_k|\}|b_2|K$, which is enough. □

The following definition introduces a class of character sums to which Heath-Brown's estimate will be applied.

**Definition 6.4** Let $n \geqslant 2$. Let $\mathscr{F}_1, \mathscr{F}_2, \mathscr{G}$ be functions

$$\mathscr{F}_1, \mathscr{F}_2 : \mathbb{Z}^{n-1} \to \{z \in \mathbb{C} : |z| \leqslant 1\}, \quad \mathscr{G} : \mathbb{Z}^{n-2} \to \{z \in \mathbb{C} : |z| \leqslant 1\},$$

where $\mathscr{G}$ is the constant function 1 when $n = 2$. Let $\mathbf{P} = (P_i) \in (\mathbb{Z}[t])^n$ be an $n$-tuple such that each $P_i$ has positive leading coefficient. For any integers $h \neq k$ such that $1 \leqslant h, k \leqslant n$ and any $n_0 \in \mathbb{N}$, $M \in \mathbb{N}$, we define

$$\eta_{\mathbf{P}}(x; h, k) := \sum_{\substack{m\in\mathbb{N}\cap[1,x]\\ m\equiv n_0 (\text{mod } M)\\ P_i(m) \text{ prime}, i=1,\ldots,n}} \left(\prod_{i=1}^n \log P_i(m)\right)\left(\frac{P_h(m)}{P_k(m)}\right)$$
$$\times \mathscr{F}_1(P_a(m)_{a\neq k}) \mathscr{F}_2(P_b(m)_{b\neq h}) \mathscr{G}(P_c(m)_{\substack{c\neq h\\ c\neq k}}).$$

Here the functions $\mathscr{F}_1, \mathscr{F}_2, \mathscr{G}$ are applied to $P_1(m), \ldots, P_n(m)$, where $P_k(m)$ is omitted in $\mathscr{F}_1$, $P_h(m)$ is omitted in $\mathscr{F}_2$, and $P_h(m)$ and $P_k(m)$ are omitted in $\mathscr{G}$.

Our work in previous sections shows that $\theta_{\mathbf{P}}(x)$ is typically of size $x$. We now prove that for 100% of $\mathbf{P} \in (\mathbb{Z}[t])^n$ one has $\eta_{\mathbf{P}}(x; h, k) = O(x^\delta)$ for some constant $\delta < 1$.

**Proposition 6.5** *Let $n, d_1, \dots, d_n, M$ be positive integers and let $\mathscr{F}_1, \mathscr{F}_2, \mathscr{G}, h, k$ be as in Definition 6.4. Let $n_0 \in \mathbb{N}$ and $\mathbf{Q} \in (\mathbb{Z}[t])^n$ be such that $\gcd(Q_i(n_0), M) = 1$ for all $i = 1, \dots, n$. Fix $A_1, A_2 \in \mathbb{R}$ with $n < A_1 < A_2$. Then for all $H \geqslant 3$ and all $x$ with $(\log H)^{A_1} < x \leqslant (\log H)^{A_2}$ we have*

$$\frac{1}{\sharp\texttt{Poly}(H)} \sum_{\mathbf{P}\in\texttt{Poly}(H)} |\eta_{\mathbf{P}}(x; h, k)| \ll x^{\frac{1}{2}+\frac{n}{2A_1}},$$

*where the implied constant depends only on $d_1, \dots, d_n, M, n_0, \mathbf{Q}, A_1, A_2$.*

*Proof* By the Cauchy–Schwarz inequality it is enough to prove

$$\frac{1}{\sharp\texttt{Poly}(H)} \sum_{\mathbf{P}\in\texttt{Poly}(H)} |\eta_{\mathbf{P}}(x; h, k)|^2 \ll x^{1+\frac{n}{A_1}}. \tag{6.2}$$

Without loss of generality we assume that $h = 1, k = 2$ and write $\eta_{\mathbf{P}}(x)$ for $\eta_{\mathbf{P}}(x; 1, 2)$. Using $|\eta_{\mathbf{P}}(x)|^2 = \eta_{\mathbf{P}}(x)\overline{\eta_{\mathbf{P}}(x)}$ and changing the order of summation we write $\sum_{\mathbf{P}\in\texttt{Poly}(H)} |\eta_{\mathbf{P}}(x)|^2$ as

$$\begin{aligned}
&\sum_{\substack{m_1, m_2 \in \mathbb{N}\cap[1,x] \\ m_1, m_2 \equiv n_0 \ (\mathrm{mod}\ M)}} \ \sum_{\substack{\mathbf{P}\in\texttt{Poly}(H) \\ P_i(m_j) \text{ prime for } i=1,\dots,n,\ j=1,2}} \left(\frac{P_1(m_1)}{P_2(m_1)}\right)\left(\frac{P_1(m_2)}{P_2(m_2)}\right) \\
&\times \left(\prod_{1\leqslant i\leqslant n} \log P_i(m_1) \log P_i(m_2)\right) \\
&\times \mathscr{F}_1(P_i(m_1)_{i\neq 2})\mathscr{F}_2(P_i(m_1)_{i\neq 1})\mathscr{G}(P_i(m_1)_{i\notin\{1,2\}}) \\
&\times \overline{\mathscr{F}_1(P_i(m_2)_{i\neq 2})}\,\overline{\mathscr{F}_2(P_i(m_2)_{i\neq 1})}\,\overline{\mathscr{G}(P_i(m_2)_{i\notin\{1,2\}})}.
\end{aligned}$$

Ignoring the congruence conditions modulo $M$ and using $|\mathscr{F}_i|, |\mathscr{G}| \leqslant 1$ we see that the modulus of the contribution of the diagonal terms $m_1 = m_2$ is at most

$$\sum_{1\leqslant m_1\leqslant x} \prod_{i=1}^{n} \sum_{|P_i|\leqslant H,\ P_i>0} \Lambda(P_i(m_1))^2,$$

which is $\ll xH^{d+n}(\log H)^n$ as in the proof of Lemma 4.1. This is sufficient because

$$\begin{aligned}
xH^{d+n}(\log H)^n &= xH^{d+n}((\log H)^{A_1})^{n/A_1} \\
&\leqslant xH^{d+n}x^{n/A_1} \ll \sharp\texttt{Poly}(H)x^{1+n/A_1}.
\end{aligned}$$

To study the remaining terms we introduce the variables

$$k_1 := P_1(m_1), k_2 := P_2(m_1) \text{ and } l_1 := P_1(m_2), l_2 := P_2(m_2)$$

and sum over all values of $l_i, k_i$. Take any $\varepsilon > 0$. For any integer polynomial $P$ of degree at most $d_i$ satisfying $|P| \leqslant H$ and for any $m \leqslant x$ with $P_i(m)$ prime one has $\log P_i(m) = O_{\varepsilon,d_i}(H^\varepsilon)$. Using this we bound the modulus of the remaining sum by $O(\Xi)$, where

$$\begin{aligned}\Xi := &\sum_{\substack{l_1, l_2 \in \mathbb{N} \\ 1 \leqslant m_1 \neq m_2 \leqslant x}} (\log l_1)(\log l_2) \\ &\times \sum_{\substack{P_3, \dots, P_n \in \mathbb{Z}[t] \\ P_i > 0,\ \deg(P_i) = d_i,\ |P_i| \leqslant H}} \\ &\times H^\varepsilon \left| \sum_{k_1, k_2 \text{ primes}} \left(\frac{k_1}{k_2}\right) F_1(k_1, l_1) F_2(k_2, l_2) \right|,\end{aligned}$$

where for $i = 1, 2$ and $k, l \in \mathbb{N}$ we let

$$F_i(k,l) := (\log k) N_i(k,l) \mathscr{F}_i(k, (P_j(m_1))_{j \notin \{1,2\}}) \overline{\mathscr{F}_i(l, (P_j(m_2))_{j \notin \{1,2\}})},$$

and denote by $N_i(k,l)$ the number

$$\begin{aligned}\sharp\{P \in \mathbb{Z}[t] : P > 0, \deg(P) = d_i, |P| \leqslant H, \\ P \equiv Q_i \pmod{M}, P(m_1) = k, P(m_2) = l\}.\end{aligned}$$

To complete the proof of (6.2) it is now sufficient to prove

$$\Xi \ll \texttt{Poly}(H)\, x^{1+\frac{n}{A_1}}. \tag{6.3}$$

The conditions $P(m_1) = k$, $P(m_2) = l$ define an affine subspace of codimension 2 in the vector space of polynomials of degree $d_i$, hence $N_i(k,l) \ll H^{d_i - 1}$. (This uses $m_1 \neq m_2$, which explains the precursory manoeuvre of separating the diagonal terms $m_1 = m_2$.) We obtain the estimate $F_i(k,l) \ll (\log H) H^{d_i-1}$ with an implied constant depending only on $n$ and $d_i$. Since we have $|P_i(m_1)| \leqslant (1 + d_i) H x^{d_i}$, we can see that $N_i(k,l) = 0$ unless $k, l \leqslant (1 + d_i) H x^{d_i}$, so we can apply Lemma 6.3 with $K = (1 + d_1) H x^{d_1}$ and $L = (1 + d_2) H x^{d_2}$. Hence the sum over $k_1, k_2$ in the definition of $\Xi$ is

$\ll H^{d_1+d_2-1/2+\varepsilon}$, where we used that $x \leqslant (\log H)^{A_2} \ll H^{\varepsilon}$. Therefore,

$$\Xi \ll H^{d_1+d_2-1/2+\varepsilon} \sum_{\substack{l_1 \leqslant K, l_2 \leqslant L \\ 1 \leqslant m_1 \neq m_2 \leqslant x}} (\log l_1)(\log l_2) \sum_{\substack{P_3,\dots,P_n \in \mathbb{Z}[t] \\ P_i>0,\, \deg(P_i)=d_i,\, |P_i| \leqslant H}} H^{\varepsilon}.$$

The number of terms in the sum over the $P_i$ is $\ll H^{d+n-d_1-d_2-2}$ and the sum over $l_1, l_2, m_1, m_2$ is $\ll KLx^2(\log K)(\log L) \ll H^{2+\varepsilon}$. This proves that

$$\Xi \ll H^{d+n-1/2+3\varepsilon} \ll \sharp\mathtt{Poly}(H) H^{-1/2+3\varepsilon},$$

which immediately implies (6.3) by choosing $\varepsilon = 1/6$. □

### 6.2 Indicator function of solvable conics

Recall that for $a, b, c \in \mathbb{Q}_p^*$ the projective conic

$$ax^2 + by^2 + cz^2 = 0$$

has a $\mathbb{Q}_p$-point if and only if the Hilbert symbol $(-ac, -bc)_p$ is 1. We refer to [54, Ch. III, §1] for the standard formulae for the calculation of the Hilbert symbol.

Let $a_1, a_2, a_3$ be non-zero integers. Let $p_{ij}$, where $i = 1, 2, 3$ and $j = 1, \dots, n_i$, be distinct primes not dividing $2a_1a_2a_3$. (If $n_3 = 0$, then $i = 1, 2$.) For $k \in \mathbb{N}$ write $[k] = \{1, \dots, k\}$. Let $S_i$ be a subset of $[n_i]$. Define $\pi(S_i) = \prod_{j \in S_i} p_{ij}$ and abbreviate $\pi([n_i])$ to $\pi_i$. We denote by $S_i^c = [n_i] \setminus S_i$ the complement to $S_i$ in $[n_i]$. Let

$$Q = 2^{-n} \left( 2 + \sum_{S_1,S_2,S_3}^{*} \left( \frac{-a_2a_3\pi_2\pi_3}{\pi(S_1)} \right) \left( \frac{-a_1a_3\pi_1\pi_3}{\pi(S_2)} \right) \left( \frac{-a_1a_2\pi_1\pi_2}{\pi(S_3)} \right) \right),$$

where the sum is over all subsets $S_i \subset [n_i], i = 1, 2, 3,$ such that $(S_1, S_2, S_3) \neq (\varnothing, \varnothing, \varnothing)$ and $(S_1, S_2, S_3) \neq ([n_1], [n_2], [n_3])$.

**Lemma 6.6** *Let $n_1, n_2, n_3$ be integers such that $n_1 > 0$, $n_2 > 0$, $n_3 \geqslant 0$. Let $a_1, a_2, a_3$ be non-zero integers not all of the same sign such that $a_1a_2a_3$ is square-free. Suppose that $p_{ij}$, for $i = 1, 2, 3$ and $j = 1, \dots, n_i$, are distinct primes not dividing $2a_1a_2a_3$ such that the conic $C$ given by*

$$a_1\pi_1x^2 + a_2\pi_2y^2 + a_3\pi_3z^2 = 0, \tag{6.4}$$

*has a $\mathbb{Q}_p$-point for all $p | 2a_1a_2a_3$. Then $C(\mathbb{Q}) \neq \varnothing$ if and only if $Q = 1$, otherwise $Q = 0$.*

*Proof* The condition concerning the signs of the $a_i$ guarantees that $C(\mathbb{R}) \neq \varnothing$. Therefore, $C(\mathbb{Q}) \neq \varnothing$ if and only if for every $i, j$ we have

$$\left(\frac{-a_{i'}a_{i''}\pi_{i'}\pi_{i''}}{p_{ij}}\right) = 1,$$

where $\{i, i', i''\} = \{1, 2, 3\}$. Thus the following is $2^n$ when $C(\mathbb{Q}) \neq \varnothing$, and 0 when $C(\mathbb{Q}) = \varnothing$:

$$\prod_{i=1}^{3}\prod_{j=1}^{n_i}\left(1 + \left(\frac{-a_{i'}a_{i''}\pi_{i'}\pi_{i''}}{p_{ij}}\right)\right)$$
$$= \sum_{S_1,S_2,S_3}\left(\frac{-a_2a_3\pi_2\pi_3}{\pi(S_1)}\right)\left(\frac{-a_1a_3\pi_1\pi_3}{\pi(S_2)}\right)\left(\frac{-a_1a_2\pi_1\pi_2}{\pi(S_3)}\right),$$

where the sum is over all subsets $S_i \subset \{1, \ldots, n_i\}$, $i = 1, 2, 3$. We separate the term 1 corresponding to the case when $S_i = \varnothing$ for $i = 1, 2, 3$. The term corresponding to the case when $S_i = [n_i]$ for $i = 1, 2, 3$ is

$$\mathscr{R}(x, H)^2 \leqslant \mathscr{V}(x, H) := \frac{1}{\sharp\texttt{Poly}(H)} \sum_{\mathbf{P} \in \texttt{Poly}(H)} (\theta_{\mathbf{P}}(x) - \mathfrak{S}_{\mathbf{P}}(x)x)^2,$$

This equals $(-1)^r$, where $r$ is the number of pairs $(i, j)$ such that $C(\mathbb{Q}_{p_{ij}}) = \varnothing$. Since $C$ is locally soluble everywhere except, perhaps, at the primes $p_{ij}$, the product formula for the Hilbert symbol implies that $r$ is even. Hence the above term is 1. □

**Proposition 6.7** *Let $n_1, n_2, n_3$ be integers such that $n_1 > 0$, $n_2 > 0$, $n_3 \geqslant 0$, and let $n = n_1+n_2+n_3$. Let $a_1, a_2, a_3$ be non-zero integers not all of the same sign such that $a_1a_2a_3$ is square-free. Let $M$ be a multiple of $8a_1a_2a_3$. Let $n_0$ be an integer. Let $Q_{ij}(t) \in \mathbb{Z}[t]$ be a polynomial of degree at most $d_{ij}$ such that $(Q_{ij}(n_0), M) = 1$, for $i = 1, 2, 3$ and $j = 1, \ldots, n_i$, satisfying the following condition: for any integer $m \equiv n_0 \pmod M$ and any $n$-tuple of polynomials $\mathbf{P} = (P_{ij}(t)) \in (\mathbb{Z}[t])^n$ with $\deg P_{ij} = d_{ij}$ such that $\mathbf{P} \equiv \mathbf{Q} \pmod M$ the conic (6.1) with $t = m$ has a $\mathbb{Q}_p$-point, for any $p|M$. Then for 100% of Schinzel $n$-tuples $\mathbf{P} \equiv \mathbf{Q} \pmod M$ with $\deg P_{ij} = d_{ij}$, ordered by height, the conic bundle surface (6.1) has a $\mathbb{Q}$-point.*

*Proof* For $\mathbf{P} \in (\mathbb{Z}[t])^n$ such that $\mathbf{P} \equiv \mathbf{Q} \pmod{M}$ define the following counting function

$$C_{\mathbf{P}}(x) := \sum_{\substack{m \in \mathbb{N} \cap [1,x] \\ m \equiv n_0 (\text{mod } M) \\ P_{ij}(m) \text{ prime for all } i,j \\ P_{ij}(m) \neq P_{rs}(m) \text{ if } (i,j) \neq (r,s)}} \left( \prod_{i=1}^{3} \prod_{j=1}^{n_i} \log P_{ij}(m) \right) \mathbb{1}(m),$$

where $\mathbb{1}$ is the indicator function of those $m$ for which the conic (6.1) with $t = m$ has a $\mathbb{Q}$-point. Define

$$\widetilde{\theta}_{\mathbf{P}}(x) = \sum_{\substack{m \in \mathbb{N} \cap [1,x] \\ m \equiv n_0 \ (\text{mod } M) \\ P_i(m) \text{ prime for } i = 1,\ldots,n \\ P_{ij}(m) \neq P_{rs}(m) \text{ if } (i,j) \neq (r,s)}} \prod_{i=1}^{3} \prod_{j=1}^{n_i} \log P_{ij}(m).$$

By the condition in the proposition and Lemma 6.6 we have

$$C_{\mathbf{P}}(x) = \frac{1}{2^{n-1}} \widetilde{\theta}_{\mathbf{P}}(x) + \frac{1}{2^n} \sum_{\mathbf{S}}{}^{*} T_{\mathbf{S},\mathbf{P}}(x). \tag{6.5}$$

Here $\sum^*$ is the sum over $\mathbf{S} = (S_1, S_2, S_3)$, where $S_i \subset [n_i]$ for $i = 1, 2, 3$ are such that at least one $S_i$ is non-empty and at least one complement $S_j^c = [n_j] \setminus S_j$ is non-empty, and

$$T_{\mathbf{S},\mathbf{P}}(x) := \sum_{\substack{m \in \mathbb{N} \cap [1,x] \\ m \equiv n_0 \ (\text{mod } M) \\ P_{ij}(m) \text{ prime for all } i,j \\ P_{ij}(m) \neq P_{rs}(m) \text{ if } (i,j) \neq (r,s)}} \times \prod_{i=1}^{3} \left( \frac{-a_{i'} a_{i''} \prod_k P_{i'k}(m) \prod_l P_{i''l}(m)}{\prod_{j \in S_i} P_{ij}(m)} \right) \prod_{j=1}^{n_i} \log P_{ij}(m), \tag{6.6}$$

where $\{i, i', i''\} = \{1, 2, 3\}$. The bound $P_{ij}(m) = O_{d_{ij}}(Hx^{d_{ij}})$ yields $\log P_{ij}(m) = O_{d_{ij}}(\log(Hx))$, hence

$$0 \leqslant \theta_{\mathbf{P}}(x) - \widetilde{\theta}_{\mathbf{P}}(x) \ll_{n,d_{ij}} (\log(Hx))^n. \tag{6.7}$$

We claim that for all $x$ and $H \geqslant 3$ with $(\log H)^{2n} < x \leqslant (\log H)^{3n}$ and all $\mathbf{S}$ as above we have

$$\frac{1}{\sharp\texttt{Poly}(H)} \sum_{\mathbf{P}\in\texttt{Poly}(H)} |T_{\mathbf{S},\mathbf{P}}(x)| \ll x^{3/4}. \tag{6.8}$$

Assuming this, we see from (6.5) and (6.7) that

$$\frac{1}{\sharp\texttt{Poly}(H)} \sum_{\mathbf{P}\in\texttt{Poly}(H)} |C_{\mathbf{P}}(x) - 2^{-n+1}\theta_{\mathbf{P}}(x)| \ll x^{3/4} + (\log H)^n \ll x^{3/4}$$

due to $(\log H)^n \leqslant x^{1/2}$. Therefore,

$$\frac{\sharp\{\mathbf{P}\in\texttt{Poly}(H) : |C_{\mathbf{P}}(x) - 2^{-n+1}\theta_{\mathbf{P}}(x)| > x^{4/5}\}}{\sharp\texttt{Poly}(H)} \leqslant \frac{1}{\sharp\texttt{Poly}(H)} \sum_{\mathbf{P}\in\texttt{Poly}(H)} \frac{|C_{\mathbf{P}}(x) - 2^{-n+1}\theta_{\mathbf{P}}(x)|}{x^{4/5}},$$

is $\ll x^{-1/20} \ll (\log H)^{-2n/20}$. Schinzel $n$-tuples $\mathbf{P} \equiv \mathbf{Q} \pmod M$ have positive density within $\texttt{Poly}(H)$ by Proposition 2.8, hence, for 100% of them one has

$$C_{\mathbf{P}}(x) \geqslant 2^{-n+1}\theta_{\mathbf{P}}(x) - x^{4/5} \geqslant 2^{-n+1}\frac{\beta_0 x}{2(\log\log x)^{d-n}} - x^{4/5},$$

where we used (4.10) in the second inequality. (The constant $\beta_0$ was introduced in Lemma 4.11.) Since $x \geqslant (\log H)^n$, we see that for all sufficiently large $H$ one has $C_{\mathbf{P}}(x) > 0$.

To verify (6.8) we check that $T_{\mathbf{S},\mathbf{P}}(x)$ is a particular case of the sum introduced in Definition 6.4. (This crucially uses the assumptions $n_1 > 0$ and $n_2 > 0$.) Using quadratic reciprocity and the identities $\pi_i = \pi(S_i)\pi(S_i^c)$, $i = 1, 2, 3$, we rewrite each summand in (6.6) as the product of $\prod_{i,j} \log P_{ij}(m)$ and

$$\left(\frac{-a_2a_3\pi(S_2^c)\pi(S_3^c)}{\pi(S_1)}\right)\left(\frac{-a_1a_3\pi(S_1^c)\pi(S_3^c)}{\pi(S_2)}\right)\left(\frac{-a_1a_2\pi(S_1^c)\pi(S_2^c)}{\pi(S_3)}\right)$$

multiplied by the product of $(-1)^{(p-1)(q-1)/4}$ for all primes $p \in S_i$ and $q \in S_{i'}$, where $i \neq i'$. Without loss of generality we can assume that $S_1 \neq \varnothing$. Take any $k \in S_1$. If $S_2^c$ or $S_3^c$ is non-empty, say $S_2^c \neq \varnothing$, choose any $h \in S_2^c$ and separate the term $(\frac{P_h(m)}{P_k(m)})$ in the first quadratic symbol above. If $S_2^c$ or $S_3^c$ are both empty, then $S_1^c \neq \varnothing$ and $S_2 \neq \varnothing$. Hence there exist $h \in S_1^c$ and $k \in S_2$ so that we can separate the term $(\frac{P_h(m)}{P_k(m)})$ in the second quadratic symbol above. Let $\mathscr{F}_1$ be the product of all the terms involving $h$ but not $k$, let $\mathscr{F}_2$ be the product of all the terms involving $k$ but not $h$, and let $\mathscr{G}$ be the product of all the terms that depend neither on $k$ nor on $h$. We conclude by applying Proposition 6.5 with $A_1 = 2n$ so that $\frac{n}{2A_1} = \frac{1}{4}$. □

### 6.3 Proof of Theorem 6.1

Recall that $\mathbf{m}_{ij} \in \mathbb{Z}^{d_{ij}+1}$ are the coefficients of the polynomial $P_{ij}(t) \in \mathbb{Z}[t]$ of degree $d_{ij}$, where $i = 1, 2, 3$ and $j = 1, \ldots, n_i$. Let $\mathbf{x}_{ij} = (x_{i,j,0}, \ldots, x_{i,j,d_{ij}})$ be variables and let $P_{ij}(t, \mathbf{x}_{ij}) = \sum_{k=0}^{d_{ij}} x_{ijk}t^k$ be the generic polynomial of degree $d_{ij}$. Let $V$ be the open subscheme of $\mathbb{A}_{\mathbb{Z}}^{d+n+1}$ given by the condition $\prod_{i,j} P_{ij}(t, \mathbf{x}_{ij}) \neq 0$. Let $U$ be the subscheme of $\mathbb{P}_{\mathbb{Z}}^2 \times \mathbb{A}_{\mathbb{Z}}^{d+n+1}$ given by (6.1) and $\prod_{i,j} P_{ij}(t, \mathbf{x}_{ij}) \neq 0$. Assigning the value $\mathbf{m}_{ij} \in \mathbb{Z}^{d_{ij}+1}$ to the variable $\mathbf{x}_{ij}$ we obtain a conic bundle $U_{\mathbf{m}} \subset \mathbb{P}_{\mathbb{Z}}^2 \times \mathbb{A}_{\mathbb{Z}}^1$ given by (6.1) together with the condition $\prod_{i,j} P_{ij}(t, \mathbf{m}_{ij}) \neq 0$.

Let $f : U \to V$ be the projection to the coordinates $t$ and $\mathbf{x}$. As in Sect. 5 we denote by $g$ (respectively, by $h$) the projection to the coordinate $t$ (respectively, to the coordinate $\mathbf{x}$).

We follow the scheme of proof of Theorem 5.3. Let $S$ be the set of prime factors of $2a_1a_2a_3$. The analogue of Lemma 5.1 says that the fibre of the projective morphism $f : U \to V$ at any $\mathbb{Z}_p$-point of $V$ has a $\mathbb{Q}_p$-point when $p \notin S$. Indeed, this fibre is a conic with good reduction.

Since $f : U \to V$ is proper, the induced map $f : U(\mathbb{Q}_p) \to V(\mathbb{Q}_p)$ is topologically proper [21, p. 79]. As $V(\mathbb{Q}_p)$ is locally compact and Hausdorff, $f : U(\mathbb{Q}_p) \to V(\mathbb{Q}_p)$ is a closed map. We have $f(U(\mathbb{Z}_p)) = f(U(\mathbb{Q}_p)) \cap V(\mathbb{Z}_p)$, hence $f(U(\mathbb{Z}_p))$ is closed in $V(\mathbb{Z}_p)$. Since $V(\mathbb{Z}_p)$ is compact, $f(U(\mathbb{Z}_p))$ and $h(U(\mathbb{Z}_p))$ are compact too. Thus $\prod_{p\in S} h(U(\mathbb{Z}_p))$ is compact.

Lemma 5.2 only uses the smoothness of $g\colon U_{\mathbb{Q}} \to \mathbb{A}_{\mathbb{Q}}^1$ and $h\colon U_{\mathbb{Q}} \to \mathbb{A}_{\mathbb{Q}}^{d+n}$, so it also holds in our case. It implies that for $p \in S$ and $N_p \in U(\mathbb{Z}_p)$ there is a positive integer $M_p$ such that if $\nu \in \mathbb{Z}_p$ and $\mathbf{m} \in (\mathbb{Z}_p)^{d+n}$ satisfy

$$\max\left(|\nu - g(N_p)|_p, |\mathbf{m} - h(N_p)|_p\right) \leqslant p^{-M_p}, \tag{6.9}$$

then $U_{\nu,\mathbf{m}}(\mathbb{Z}_p) \neq \varnothing$. Let $\mathscr{B}_{N_p} \subset \mathbb{Z}_p^{d+n}$ be the $p$-adic ball of radius $p^{-M_p}$ around $h(N_p)$. The open sets $\prod_{p\in S} \mathscr{B}_{N_p}$, where $(N_p) \in \prod_{p\in S} U(\mathbb{Z}_p)$, cover $\prod_{p\in S} h(U(\mathbb{Z}_p))$. By compactness, finitely many such open sets cover $\prod_{p\in S} h(U(\mathbb{Z}_p))$. Hence $\mathscr{M} = \cup_{i=1}^{n} \mathscr{M}_i$, where $\mathscr{M}_i = \mathscr{M} \cap \prod_{p\in S} \mathscr{B}_{N_p}$ for one of these finitely many choices of $(N_p) \in \prod_{p\in S} U(\mathbb{Z}_p)$. Thus it is enough to prove that for 100% of $\mathbf{m} \in \mathscr{M}_i$ we have $U_{\mathbf{m}}(\mathbb{Q}) \neq \varnothing$.

In the rest of proof we write $\mathscr{M} = \mathscr{M}_i$. Write $n_p = g(N_p)$ and $\mathbf{m}_p = h(N_p)$, where $p \in S$. Note that $N_p \in U(\mathbb{Z}_p)$ implies $P_{ij}(n_p, \mathbf{m}_p) \in \mathbb{Z}_p^*$ for each $p \in S$. Write $M = \prod_{p \in S} p^{M_p}$. By the Chinese remainder theorem we can find $n_0 \in \mathbb{Z}$ and $\mathbf{m}_0 \in \mathbb{Z}^{d+1}$ such that $n_0 \equiv n_p \pmod{p^{M_p}}$ and $\mathbf{m}_0 \equiv \mathbf{m}_p \pmod{p^{M_p}}$ for each $p \in S$. Our new set $\mathscr{M}$ consists of all $\mathbf{m} \in \mathscr{P}$ such that $\mathbf{m} \equiv \mathbf{m}_0 \pmod{M}$. Since $P_{ij}(n_p, \mathbf{m}_p) \in \mathbb{Z}_p^*$ for each $p \in S$, we see that $P_{ij}(n_0, \mathbf{m}_0)$ is coprime to $M$.

We now apply Proposition 6.7 to our $n_0$ and $M$, with $Q_{ij}(t) = P_{ij}(t, \mathbf{m}_0)$ for all $i$ and $j$. This is legitimate because $P_{ij}(n_0, \mathbf{m}_0)$ is coprime to $M$ and for any integer $\nu \equiv n_0 \pmod{M}$ and any $\mathbf{m} \equiv \mathbf{m}_0 \pmod{M}$ we have $U_{\nu,\mathbf{m}}(\mathbb{Z}_p) \neq \varnothing$ whenever $p \in S$. Thus for 100% of $\mathbf{m} \in \mathscr{M}$ we have $U_{\mathbf{m}}(\mathbb{Q}) \neq \varnothing$.

The last statement of Theorem 6.1 is proved in the same way as in Theorems 5.3 and 5.8 .

### 6.4 The proof of Theorem 1.4

We can ensure that $a_1, a_2, a_3$ are not all of the same sign by replacing $P_{1,1}(x)$ by $-P_{1,1}(x)$, if necessary. We can also ensure that $a_1a_2a_3$ is square-free. (If $p$ is a prime such that $p^2|a_1$, we absorb $p$ into $x$; if $p|a_1$ and $p|a_2$, then we multiply (6.1) by $p$ and absorb $p$ into $x$ and $y$.) It remains to apply Theorem 6.1.

## 7 Explicit probabilities

In this section we obtain an explicit estimate for the probability that random affine Châtelet surfaces have integer points, following the method of Theorem 5.7. We prove that this probability exceeds 56% for a family that has attracted much attention in the literature, namely,

$$x^2 + y^2 = f(t), \tag{7.1}$$

where $f$ is a polynomial of fixed degree $d$ with positive leading coefficient. V.A. Iskovskikh [38] gave a first counter-example to the Hasse principle with $d = 4$; the density of such counterexamples was studied in [24] and [52]. Little is known about the arithmetic of (7.1) when $d > 6$ and $f(t)$ is irreducible. Let

$$P_d(H) := \{f \in \mathbb{Z}[t] : \deg(d) = d, |f| \leqslant H, \text{the leading coefficient of } f \text{ is positive}\}.$$

**Theorem 7.1** *For all $d \geqslant 2$, $\varepsilon > 0$ and all sufficiently large $H$ we have*

$$\frac{\sharp\{f \in P_d(H) : x^2 + y^2 = f(t) \textit{ is soluble in } \mathbb{Z}\}}{\sharp P_d(H)} \\ \geqslant (1-\varepsilon)\frac{(38 + \mathbb{1}(d \geqslant 3))}{64} \prod_{p \geqslant 3}\left(1 - \frac{1}{p^{\min\{p,d+1\}}}\right).$$

The infinite product is a strictly increasing function of $d$. For $d = 2$ it equals $0.95\ldots$ and as $d \to \infty$ the limit of the product is $\prod_{p\geqslant 3}(1-p^{-p}) = 0.962\ldots$.

**Corollary 7.2** *For every $d \geqslant 2$ and all sufficiently large $H$ we have*

$$\frac{\sharp\{f \in P_d(H) : x^2 + y^2 = f(t) \textit{ is soluble in } \mathbb{Z}\}}{\sharp P_d(H)} > \frac{56}{100}.$$

To prove Theorem 7.1 we apply Theorem 1.2 with $n = 1$, $M = 4$, $n_0 \in \{0, 1, 2, 3\}$ and arbitrary $Q_1(t)$ of degree at most $d$ such that $Q_1(n_0)$ is 1 modulo 4. It shows that for 100% of Bouniakowsky polynomials $f(t)$ of degree $d$ such that $f(n_0)$ is 1 modulo 4, there exists an integer $m$ such that $f(m)$ is a prime congruent to 1 modulo 4. In this case (7.1) has an integer solution. Thus, for all $\varepsilon > 0$ and all sufficiently large $H$ we have

$$\frac{\sharp\{f \in P_d(H) : x^2 + y^2 = f(t) \text{ is soluble in } \mathbb{Z}\}}{\sharp P_d(H)} \geqslant R_d(H) - \varepsilon,$$

where

$$R_d(H) := \frac{\sharp\{f \in P_d(H) : f \text{ is Bouniakowsky, } \exists\, n_0 \in \{0,1,2,3\} \text{ such that } f(n_0) \equiv 1 \pmod 4\}}{\sharp P_d(H)}.$$

It is therefore sufficient to show that $\lim_{H\to\infty} R_d(H)$ exists and find its value. For this we partition the coefficients of $f$ according to their values modulo 4 as follows:

$$R_d(H)\sharp P_d(H) \\ = \sum_{\substack{Q\in(\mathbb{Z}/4\mathbb{Z})[t], \deg(Q)\leqslant d \\ \exists n_0\in\mathbb{Z}/4\mathbb{Z}:\ Q(n_0)\equiv 1 \pmod 4}} \sharp\{f \in P_d(H) : f \equiv Q \pmod 4,\ Z_f(p) \neq p,\ \forall p \geqslant 3\}.$$

By Corollary 2.9 with $M = 4$ and the fact that $\sharp P_d(H)$ is asymptotic to $2^d H^{d+1}$ we obtain

$$\lim_{H\to\infty} R_d(H) = r_d \prod_{p\geqslant 3}\left(1 - \frac{1}{p^{\min\{p,d+1\}}}\right),$$

where

$$r_d := \frac{1}{4^{d+1}}\, \sharp\{Q \in (\mathbb{Z}/4\mathbb{Z})[t] : \deg(Q) \leqslant d, \exists\, n_0 \in \{0,1,2,3\} \text{ such that } Q(n_0) \equiv 1 \pmod 4\}.$$

A straightforward listing shows that $r_2 = 19/32$. For the remaining case $d \geqslant 3$ we write $f(t) = \sum_{i=0}^{d} c_i t^i$, thus

$$1 - r_d = \frac{1}{4^{d+1}} \sum_{(v_0,v_1,v_2,v_3)\in\{0,2,3\}^4} \sharp\left\{\mathbf{c} \in (\mathbb{Z}/4\mathbb{Z})^{d+1} : \sum_{i=0}^{d} c_i j^i \equiv v_j \pmod 4,\ \forall j = 0,1,2,3\right\}.$$

The system of four equations corresponding to $j = 0, 1, 2, 3$ is equivalent to

$$c_0 \equiv v_0 \pmod 4,\ 2c_1 \equiv v_2 - v_0 \pmod 4,\ \sum_{0\leqslant i\leqslant d} c_i \equiv v_1 \pmod 4,$$
$$2 \sum_{0\leqslant i\leqslant d/2} c_{2i} \equiv v_1 + v_3 \pmod 4.$$

This system has at least four unknowns $c_i$ due to $d \geqslant 3$. It is soluble if and only if both $v_0 \equiv v_2 \pmod 2$ and $v_1 \equiv v_3 \pmod 2$ hold; this happens for exactly 25 vectors $(v_i) \in \{0,2,3\}^4$. For each of these vectors, the first equation determines $c_0$ uniquely and the second equation gives two values of $c_1$. For any such $c_0, c_1$ and any $c_4, c_5, \ldots, c_d$ the last equation gives two values of $c_2$. The third equation determines $c_3$ uniquely. Thus we obtain

$$1 - r_d = \frac{1}{4^{d+1}} \times 25 \times (1 \times 2 \times 1 \times 2 \times 4^{d+1-4}) = \frac{25}{64}.$$

**Acknowledgements** The work on this paper started during the research trimester "À la redécouverte des points rationnels" at the Institut Henri Poincaré in Paris, whose support is gratefully acknowledged. The authors would like to thank Andrew Granville for his interest in this paper, his enthusiasm and useful discussions. We are very grateful to the referee for careful reading of the paper and many helpful comments.

## References

1. Adleman, L.M., Odlyzko, A.M.: Irreducibility testing and factorization of polynomials. Math. Comput. **41**, 699–709 (1983)
2. Baier, S., Zhao, L.: Primes in quadratic progressions on average. Math. Ann. **338**, 963–982 (2007)
3. Baier, S., Zhao, L.: On primes in quadratic progressions. Int. J. Number Theory **5**, 1017–1035 (2009)
4. Balog, A.: The prime $k$-tuplets conjecture on average. Analytic Number Theory. Progr. Math. vol. 85. Birkhäuser (1990)
5. Barban, M.B.: Analogues of the divisor problem of Titchmarsh. Vestnik Leningrad Univ. Mat. Meh. Astronom. **18**, 5–13 (1963). (**Russian**)
6. Bateman, P., Horn, R.A.: A heuristic asymptotic formula concerning the distribution of prime numbers. Math. Comput. **16**, 363–367 (1962)
7. Bouniakowsky, V.: Sur les diviseurs numériques invariables des fonctions rationnelles entières. (Lu le 4 août), Mém. Acad. Impériale Sci. de Saint-Pétersbourg, 6-ème série. Sciences math. phys. VI, 305–329 (1857)
8. Bright, M.J., Browning, T.D., Loughran, D.: Failures of weak approximation in families. Compositio Math. **152**, 1435–1475 (2016)
9. Brown, E., Parry, C.J.: The imaginary bicyclic biquadratic fields with class-number 1. J. reine angew. Math. **266**, 118–120 (1974)
10. Browning, T.D., Heath-Brown, D.R.: Quadratic polynomials represented by norm forms. GAFA **22**, 1124–1190 (2012)
11. Browning, T.D., Matthiesen, L., Skorobogatov, A.N.: Rational points on pencils of conics and quadrics with many degenerate fibres. Ann. Math. **180**, 381–402 (2014)
12. Cassels, J.W.S.: Bounds for the least solutions of homogeneous quadratic equations. Proc. Camb. Philos. Soc. **51**, 262–264 (1955)
13. Cassels, J.W.S., Fröhlich, A. (eds.): Algebraic Number Theory. Academic Press, New York (1967)
14. Cohn, H.: A Classical Invitation to Algebraic Numbers and Class Fields. Springer, Berlin (1978)
15. Colliot-Thélène, J.-L.: Surfaces rationnelles fibrées en coniques de degré 4. Sém. théorie des nombres Paris 1988–89. Progress in Mathematics, vol. 91. Birkhäuser, pp. 43–55 (1990)
16. Colliot-Thélène, J.-L., Salberger, P.: Arithmetic on some singular cubic hypersurfaces. Proc. Lond. Math. Soc. **58**, 519–549 (1989)
17. Colliot-Thélène et, J.-L., Sansuc, J.-J.: Sur le principe de Hasse et l'approximation faible, et sur une hypothèse de Schinzel. Acta Arith. **41**, 33–53 (1982)
18. Colliot-Thélène, J.-L., Sansuc, J.-J., Swinnerton-Dyer, Sir Peter: Intersections of two quadrics and Châtelet surfaces, I. J. reine angew. Math. **373**, 37–107 (1987); II, ibid. **374**, 72–168 (1987)

19. Colliot-Thélène, J.-L., Harari et, D. Skorobogatov, A.N.: Valeurs d'un polynôme à une variable représentées par une norme. Number Theory and Algebraic Geometry. In: Reid, M., Skorobogatov, A. (eds.) London Math. Soc. Lecture Note Series, vol. 303, pp. 69–89. Cambridge University Press, Cambridge (2003)
20. Colliot-Thélène, J.-L., Skorobogatov, A.N.: The Brauer–Grothendieck group. Ergebnisse der Mathematik und ihrer Grenzgebiete, 3. Folge, Band 71. Springer, Berlin (2021)
21. Conrad, B.: Weil and Grothendieck approaches to adelic points. Enseign. Math. **58**, 61–97 (2012)
22. Davenport, H.: On some infinite series involving arithmetical functions. II. Quart. J. Math. **8**, 313–320 (1937)
23. Davenport, H., Halberstam, H.: Primes in arithmetic progressions. Michigan Math. J. **13**, 485–489 (1966)
24. de la Bretèche, R., Browning, T.D.: Density of Châtelet surfaces failing the Hasse principle. Proc. Lond. Math. Soc. **108**, 1030–1078 (2014)
25. Derenthal, U., Smeets, A., Wei, D.: Universal torsors and values of quadratic polynomials represented by norms. Math. Ann. **361**, 1021–1042 (2015)
26. Filaseta, M.: Prime values of irreducible polynomials. Acta Arith. **50**, 133–145 (1988)
27. Foo, T., Zhao, L.: On primes represented by cubic polynomials. Math. Z. **274**, 323–340 (2013)
28. Freeman, D., Scott, M., Teske, E.: A taxonomy of pairing-friendly elliptic curves. J. Cryptol. **23**, 224–280 (2010)
29. Friedlander, J., Goldston, D.A.: Variance of distribution of primes in residue classes. Quart. J. Math. **47**, 313–336 (1996)
30. Friedlander, J., Granville, A.: Limitations to the equi-distribution of primes. IV. Proc. R. Soc. Lond. Ser. A. **435**, 197–204 (1991)
31. Granville, A., Mollin, R.A.: Rabinowitsch revisited. Acta Arith. **96**, 139–153 (2000)
32. Green, B., Tao, T., Ziegler, T.: An inverse theorem for the Gowers $U^{s+1}[N]$-norm. Ann. Math. **176**, 1231–1372 (2012)
33. Harpaz, Y., Skorobogatov, A.N., Wittenberg, O.: The Hardy-Littlewood conjecture and rational points. Compositio Math. **150**, 2095–2111 (2014)
34. Harpaz, Y., Wittenberg, O.: On the fibration method for zero-cycles and rational points. Ann. Math. **183**, 229–295 (2016)
35. Heath-Brown, D.R.: A mean value estimate for real character sums. Acta Arith. **72**, 235–275 (1995)
36. Heath-Brown, D.R., Skorobogatov, A.N.: Rational solutions of certain equations involving norms. Acta Math. **189**, 161–177 (2002)
37. Holzer, L.: Minimal solutions of Diophantine equations. Can. J. Math. **2**, 238–244 (1950)
38. Iskovskikh, V.A.: Minimal models of rational surfaces over arbitrary fields. Izv. Akad. Nauk SSSR Ser. Mat. **43**, 19–43 (1979)
39. Iwaniec, H., Kowalski, E.: Analytic Number Theory. American Mathematical Society Colloquium Publications, vol. 53. Amer. Math. Soc. (2004)
40. Janusz, G.: Algebraic Number Fields, 2nd edn. Graduate Studies in Mathematics, vol. 7. Amer. Math. Soc. (1996)
41. Kowalski, E.: Averages of Euler products, distribution of singular series and the ubiquity of Poisson distribution. Acta Arith. **148**, 153–187 (2011)
42. Lavrik, A.F.: On the distribution of $k$-twin primes. Dokl. Akad. Nauk SSSR **132**, 1258–1260 (1960). (**Russian**)
43. Lavrik, A.F.: On the theory of distribution of primes based on I.M. Vinogradov's method of trigonometric sums. Trudy Mat. Inst. Steklov **64**, 90–125 (1961) (**Russian**)
44. Li, J., Pratt, K., Shakan, G.: A lower bound for the least prime in an arithmetic progression. Quart. J. Math. **68**, 729–758 (2017)
45. Linnik, J.V.: The Dispersion Method in Binary Additive Problems. Amer. Math. Soc. (1963)

46. Loughran, D., Smeets, A.: Fibrations with few rational points. GAFA **26**, 1449–1482 (2016)
47. McCurley, K.S.: The smallest prime value of $x^n + a$. Can. J. Math. **38**, 925–936 (1986)
48. Mikawa, H.: On prime twins. Tsukuba J. Math. **15**, 19–29 (1991)
49. Mollin, R.A.: Prime-producing quadratics. Amer. Math. Mon. **104**, 529–544 (1997)
50. Montgomery, H.L.: Primes in arithmetic progressions. Michigan Math. J. **15**, 33–39 (1970)
51. Montgomery, H.L., Vaughan, R.C.: Multiplicative Number Theory. I. Classical theory. Cambridge Studies in Advanced Mathematics, vol. 97. Cambridge University Press, (2007)
52. Rome, N.: A positive proportion of Hasse principle failures in a family of Châtelet surfaces. Int. J. Number Theory **15**, 1237–1249 (2019)
53. Schinzel et, A., Sierpiński, W.: Sur certaines hypothèses concernant les nombres premiers. Acta Arith. **4**, 185–208 (1958); Errata, ibid. **5**, 259 (1959)
54. Serre, J.-P.: Cours d'arithmétique. Presses Universitaires de France, Paris (1970)
55. Skorobogatov, A.N.: Torsors and Rational Points. Cambridge Tracts in Mathematics, vol. 144. Cambridge University Press, Cambridge (2001)
56. Swinnerton-Dyer, P.: Rational points on some pencils of conics with 6 singular fibres. Ann. Fac. Sci. Toulouse Math. **8**, 331–341 (1999)
57. Tschinkel, Y.: Algebraic varieties with many rational points, Arithmetic Geometry, Clay Math. Proc., vol. 8. Amer. Math. Soc. (2009)
58. Wei, D.: On the equation $N_{K/k}(\Xi) = P(t)$. Proc. Lond. Math. Soc. **109**, 1402–1434 (2014)
59. Wolke, D.: Über das Primzahl-Zwillingsproblem. Math. Ann. **283**, 529–537 (1989)
60. Xylouris, T.: Über die Nullstellen der Dirichletschen L-Funktionen und die kleinste Primzahl in einer arithmetischen Progression. Bonner Mathematische Schriften **404** (2011)
61. Yau, K.H.: On primes represented by quartic polynomials on average. arXiv:1908.09439
62. Zygmund, A.: Trigonometric Series. I. Classical Theory. Cambridge University Press (2002)
63. Zhou, N.H.: Primes in higher-order progressions on average. Int. J. Number Theory **14**, 1943–1959 (2018)