ISRAEL JOURNAL OF MATHEMATICS **TBD** (2023), 1–31
DOI: 10.1007/s11856-023-2557-x

DISCRIMINANTS OF FIELDS GENERATED BY POLYNOMIALS OF GIVEN HEIGHT

BY

Rainer Dietmann

Department of Mathematics, Royal Holloway, University of London
Egham, Surrey TW20 0EX, United Kingdom
e-mail: rainer.dietmann@rhul.ac.uk

AND

Alina Ostafe and Igor E. Shparlinski

Department of Pure Mathematics, University of New South Wales
Sydney, NSW 2052, Australia
e-mail: alina.ostafe@unsw.edu.au, igor.shparlinski@unsw.edu.au

ABSTRACT

We obtain upper bounds for the number of monic irreducible polynomials over $\mathbb{Z}$ of a fixed degree n and a growing height H for which the field generated by one of its roots has a given discriminant. We approach it via counting square-free parts of polynomial discriminants via two complementing approaches. In turn, this leads to a lower bound on the number of distinct discriminants of fields generated by roots of polynomials of degree n and height at most H. We also give an upper bound for the number of trinomials of bounded height with given square-free part of the discriminant, improving previous results of I. E. Shparlinski (2010).

Received September 17, 2019 and in revised form January 4, 2022

1. Introduction

1.1. Motivation and background. For a positive integer H, we use $\mathcal{P}_n(H)$ to denote the set of polynomials

$$\mathcal{P}_n(H) = \{X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in \mathbb{Z}[X] : |a_0|, \ldots, |a_{n-1}| < H\}.$$

Furthermore, we use $\mathcal{I}_n(H)$ to denote the set of irreducible polynomials from $\mathcal{P}_n(H)$. It is useful to recall that

$$\#\mathcal{I}_n(H) = 2^n H^n + O(H^{n-1}),$$

which follows immediately from much more precise results of Chela [9], Dietmann [11, 12] and Zywina [44]. We also note that Bhargava [4] has recently established the celebrated van der Waerden conjecture about Galois groups of polynomials from $\mathcal{I}_n(H)$.

For an irreducible monic polynomial $f \in \mathbb{Z}[X]$ we use $\Delta(f)$ to denote the discriminant of the algebraic number field $\mathbb{Q}(\alpha)$, where α is a root of f (clearly, for any $f \in \mathcal{I}_n(H)$ all such fields $\mathbb{Q}(\alpha)$ are isomorphic and thus have the same discriminant).

For an integer Δ we denote by $N_n(H, \Delta)$ the number of polynomials $f \in \mathcal{I}_n(H)$ with $\Delta(f) = \Delta$.

We recall that various counting problems for discriminants of number fields have been studied in a number of works; see [3,5,13,20,22–24,29] and references therein. In particular, a remarkable result of Bhargava, Shankar and Wang [5] gives an asymptotic formula for the density of polynomials with square-free discriminants, however their model of counting is different from ours. In fact, it seems that the function $N_n(H, \Delta)$, which is our main object of study, has never been investigated before.

We derive our estimates from some counting results on square-free parts of discriminants of the polynomials from $\mathcal{P}_n(H)$. We recall that the square-free part u of an integer k is defined by $k = uv^2$ where v^2 is the largest perfect square dividing k. In particular, u has the same sign as k.

We remark that, despite the recent progress in [5], the problem of counting square-free discriminants of the polynomials from $\mathcal{P}_n(H)$ still remains open, unless one assumes the celebrated ABC-conjecture; see [26, 33]. So, one can consider our result as a first approximation to the desired goal.

Furthermore, some counting results about square-free parts of discriminants

$$\Delta_n(a,b) = (n-1)^{n-1}a^n + n^n b^{n-1} \tag{1.1}$$

of trinomials $X^n + aX + b$ with $n \equiv 1 \pmod 4$ have been given in [31] (conditionally under the ABC-conjecture) and in [39] (unconditionally). Here we obtain a new bound, improving that of [39] for a wide range of parameters.

In fact our our main result (Theorem 1.1 below) is a combination of two results, which we use depending on the relative sizes of parameters. One result is obtained via the determinant method of Bombieri and Pila [7], Heath-Brown [17] and Salberger [37], as in the work of Dietmann [12]. The other one is based on the square sieve of Heath-Brown [15], see Section 3.2, combined with bounds on character sums with discriminants, see Lemma 2.8, which are better than those directly implied by the Weil bound (see, for example, [21, Theorem 11.23]). We believe such bounds can be of independent interest.

1.2. Notation. We recall that the expressions $A \ll B$, $B \gg A$ and $A = O(B)$ are each equivalent to the statement that $|A| \leqslant cB$ for some positive constant c. We use $o(1)$ to denote any expression that tends to 0 for a fixed n and $H \to \infty$.

Throughout the paper, the implied constants in these symbols may depend on the degree n of the polynomials involved, and occasionally, when mentioned explicitly, on some other parameters.

The letters p and q always denote prime numbers.

1.3. Discriminants of general polynomials. Our main result is the following upper bound on $N_n(H,\Delta)$, which is obtained by a combination of various techniques.

Theorem 1.1: *Let Δ be a non-zero integer and $n \geqslant 3$. Then, uniformly over Δ, if for the square-free part u of Δ neither $|u|(n-1)^{n-1}$ nor $|u|n^n$ is a square, then*

$$N_n(H,\Delta) \leqslant H^{n-2+\sqrt{2}+o(1)}, \tag{1.2}$$

otherwise

$$N_n(H,\Delta) \ll \begin{cases} H^{n-2n/(3n+3)}(\log H)^{(5n+1)/(3n+3)} & \text{if } n \geqslant 5, \\ H^{n-n/(2n-1)}(\log H)^{(3n-2)/(2n-1)} & \text{if } n = 3,4, \end{cases} \tag{1.3}$$

for any Δ.

We note that the bound (1.2) is better (when it applies) than (1.3) only for $n \leqslant 7$.

Let

$$M_n(H, D) = \sum_{|\Delta| \leqslant D} N_n(H, \Delta).$$

Given a real parameter $D \geqslant 1$, using that there are $O(D^{1/2})$ values of $\Delta \leqslant D$ with the square-free part u satisfying $|u|(n-1)^{n-1}$ or $|u|n^n$ being a square, we immediately obtain that uniformly over D,

$$M_n(H, D) \leqslant H^{o(1)} \begin{cases} DH^{n-2n/(3n+3)} & \text{if } n \geqslant 8, \\ DH^{n-2+\sqrt{2}} + D^{1/2}H^{n-2n/(3n+3)} & \text{if } n = 5, 6, 7, \\ DH^{n-2+\sqrt{2}} + D^{1/2}H^{n-n/(2n-1)} & \text{if } n = 3, 4. \end{cases}$$

However, one can get a better result.

THEOREM 1.2: *Let $D \geqslant 1$ be an integer. Then, for $n \geqslant 5$, uniformly over D, we have*

$$M_n(H, D) \leqslant D^{(3n+2)/(3n+3)} H^{n(3n+1)/(3n+3)+o(1)}.$$

Clearly, Theorem 1.2 is nontrivial (that is, improves the trivial bound $M_n(H, D) \ll H^n$) provided that $D \leqslant H^{2n/(3n+2)-\varepsilon}$ for some fixed $\varepsilon > 0$. In particular, we see that almost all polynomials from $\mathcal{I}_n(H)$ generate fields with discriminants of size at least $H^{2n/(3n+2)+o(1)}$.

We also note very recent results of Anderson, Gafni, Lemke Oliver, Lowry-Duda, Shakan, and Zhang [1] about the arithmetic structure of discriminants of polynomials from $\mathcal{P}_n(H)$.

Remark 1.3: We note that the bound of Theorem 1.1 also implies an upper bound for the number $K_n(H, \delta)$ of polynomials $f \in \mathcal{I}_n(H)$ such that the discriminant $\delta(f)$ of the splitting field L_f of f is δ. Indeed, for a given $f \in \mathcal{I}_n(H)$, we have the divisibility $\Delta(f) \mid \delta(f)$. Thus, using $\delta(f) = H^{O(1)}$ for $f \in \mathcal{I}_n(H)$ and the classical bound $\tau(\delta) = \delta^{o(1)}$ for the divisor function τ, we obtain

$$K_n(H, \delta) \leqslant \sum_{\Delta \mid \delta} N_n(H, \Delta) \leqslant H^{o(1)} \begin{cases} H^{n-2n/(3n+3)} & \text{if } n \geqslant 5, \\ H^{n-n/(2n-1)} & \text{if } n = 3, 4. \end{cases}$$

Similarly, we also have an analogue of Theorem 1.2 for $K_n(H, \delta)$.

1.4. Discriminants of trinomials. Let $T_n(A,B,C,D;u)$ be the number of pairs of integers $(a,b) \in [C,C+A] \times [D,D+B]$ such that for the trinomial discriminant (1.1) we have $\Delta_n(a,b) = ur^2$, for some positive integer r.

For $n \equiv 1 \pmod 4$, $A \geqslant 1$, $B \geqslant 1$, $C \geqslant 0$, $D \geqslant 0$ and square-free u, Shparlinski [39, Theorem 1] has obtained the bound

$$T_n(A,B,C,D;u) \ll (AB)^{2/3}(\log(AB))^{4/3} + (A+B)(\log(AB))^2 + (AB)^{1/3}\Big(\frac{\log(ABCD)\log(AB)}{\log\log(ABCD)}\Big)^2,$$

using exponential sums and the square sieve. For $C \geqslant 1$ and $A \ll B^{2-\varepsilon}$ with an arbitrary fixed $\varepsilon > 0$, we can sharpen this as follows.

Theorem 1.4: *Let $n \equiv 1 \pmod 4$, $n \geqslant 2$, $A \geqslant 1$, $B \geqslant 1$, $C \geqslant 1$, $D \geqslant 0$, and let u be square-free. Then*

$$T_n(A,B,C,D;u) \leqslant A(A+B+C+D)^{o(1)}.$$

As in [39], from this we obtain the following two results:

Corollary 1.5: *In the notation of Theorem 1.4, let $S_n(A,B,C,D)$ be the number of distinct quadratic fields $\mathbb{Q}(\sqrt{\Delta_n(a,b)})$ taken for all pairs of integers $(a,b) \in [C,C+A] \times [D,D+B]$ such that $X^n + aX + b$ is irreducible over $\mathbb{Q}$. Then under the assumptions of Theorem 1.4, we have*

$$S_n(A,B,C,D) \geqslant B(A+B+C+D)^{o(1)}.$$

In fact, in Corollary 1.5, the lower bound holds for the number of distinct square-free parts of discriminants $\Delta_n(a,b)$. Thus, taking $C = D = 1$ and $A = B = H$ in Corollary 1.5, by Lemma 2.1 below, we also obtain the following:

Corollary 1.6: *For $n \geqslant 2$ with $n \equiv 1 \pmod 4$, the number of distinct discriminants of fields generated by a root of polynomials from*

$$\{X^n + aX + b : 1 \leqslant a, b \leqslant H\}$$

is at least $H^{1+o(1)}$.

Corollary 1.7: *Let $Q_n(\Delta)$ be the number of distinct quadratic fields $\mathbb{Q}(\sqrt{\Delta_n(a,b)})$ taken over all integers $a, b \geqslant 1$ such that $X^n + aX + b$ is irreducible over $\mathbb{Q}$ and $|\Delta_n(a,b)| \leqslant \Delta$. Then, for $n \equiv 1 \pmod 4$ we have*

$$Q_n(\Delta) \geqslant \Delta^{1/(n-1)+o(1)}.$$

Corollary 1.7 improves the bound

$$Q_n(\Delta) \gg \Delta^{\kappa_n/3}(\log \Delta)^{-1}$$

in [39], where

$$\kappa_n = \frac{1}{n} + \frac{1}{n-1},$$

by asymptotically a factor $3/2$ in the exponent.

We conclude the paper with an appendix where we take the opportunity to correct an error in [12, Lemmas 5 and 6] (and consequently [12, Lemma 8]) which are not correct as stated if the degree n is of the form $n = m^2$ or $n = m^2 + 1$ for some odd m; see Section 7.

2. Preparations

2.1. Polynomials and discriminants. We recall that for an arbitrary field $\mathbb{K}$ and $f = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in \mathbb{K}[X]$, the discriminant of f is defined by

$$\mathrm{Disc}(f) = (-1)^{n(n-1)/2} \mathrm{Res}(f, f'), \tag{2.1}$$

where $\mathrm{Res}(g, h)$ denotes the resultant of $g, h \in \mathbb{K}[X]$.

Throughout we treat $\mathrm{Disc}(f)$ as a polynomial in formal variables $a_0, \ldots, a_{n-1}$.

It is well-known, see [28, Section 3.3], that $\mathrm{Disc}(f)$ and $\Delta(f)$ are related via an integer square.

Lemma 2.1: *Let $f \in \mathbb{Q}[X]$ be a monic irreducible polynomial. Then*

$$\mathrm{Disc}(f)/\Delta(f) = r^2$$

for some integer $r \geqslant 1$.

We also recall that the question about the number of polynomials $f \in \mathcal{I}_n(H)$ with $\Delta(f) = \mathrm{Disc}(f)$ remains unanswered. Ash, Brakenhoff and Zarrabi [2] give some heuristic and numerical evidence towards the conjecture, attributed in [2] to Hendrik Lenstra, that the density of such polynomials is $6/\pi^2$. We remark that this density is higher than the expected density of square-free discriminants $\mathrm{Disc}(f)$ (in which case we immediately obtain $\Delta(f) = \mathrm{Disc}(f)$ by Lemma 2.1); see [2] for a discussion of this phenomenon.

We now need several results about the irreducibility of some polynomials involving polynomial discriminants. For the rest of the paper the discriminant $\mathrm{Disc}(F)$ of a polynomial F always means the discriminant with respect to the variable X, even if the polynomial F may depend on other variables.

LEMMA 2.2: *Let $n \geqslant 3$, let $a_2, \dots, a_{n-1} \in \mathbb{Z}$ and let $c_0, c_1 \in \mathbb{Q}$. Moreover, let $u \in \mathbb{Z}$ be square-free such that neither $|u|(n-1)^{n-1}$ nor $|u|n^n$ is a square. Then the polynomial*

$$Z^2 - u\,\mathrm{Disc}(X^n + a_{n-1}X^{n-1} + \cdots + a_2X^2 + (c_0A_0 + c_1)X + A_0) \in \mathbb{Q}[A_0, Z]$$

is irreducible in $\mathbb{Q}[A_0, Z]$.

Proof. We closely follow the proof of [12, Lemma 5]; see also Section 7. Writing

$$D(A_0) = u\,\mathrm{Disc}(X^n + a_{n-1}X^{n-1} + \cdots + a_2X^2 + (c_0A_0 + c_1)X + A_0),$$

it is enough to show that $D(A_0)$ is no square in $\mathbb{Q}[A_0]$.

For $c_0 \neq 0$, by [12, Lemma 4], we find that the monomial in $D(A_0)$ with biggest degree is

$$u(-1)^{(n-1)(n-2)/2}(n-1)^{n-1}c_0^nA_0^n,$$

which cannot be a square in $\mathbb{Q}[A_0]$. Indeed, if n is odd this is obvious. If n is even this is true since $|u|(n-1)^{n-1}$ is not a square but c_0^n is.

For $c_0 = 0$, by [12, Lemma 3], one finds that the monomial in $D(A_0)$ with biggest degree is

$$u(-1)^{n(n-1)/2}n^nA_0^{n-1}.$$

Again, since $|u|n^n$ is no square, this cannot be a square in $\mathbb{Q}[A_0]$. ∎

In the same way one proves the following analogue of [12, Lemma 6].

LEMMA 2.3: *Let $n \geqslant 3$, let $a_2, \dots, a_{n-1} \in \mathbb{Z}$ and $c \in \mathbb{Q}$. Moreover, let $u \in \mathbb{Z}$ be square-free such that $|u|(n-1)^{n-1}$ is not a square. Then the polynomial*

$$Z^2 - u\,\mathrm{Disc}(X^n + a_{n-1}X^{n-1} + \cdots + a_2X^2 + A_1X + c) \in \mathbb{Q}[A_1, Z]$$

is irreducible in $\mathbb{Q}[A_1, Z]$.

The argument below is modelled from that of the proof of [38, Lemma 4].

For a monic polynomial $f(X) \in \mathbb{K}[X]$ and $(u, v) \in \mathbb{K}^* \times \mathbb{K}$, we define the polynomial

$$f_{u,v}(X) = u^n f(u^{-1}(X + v)) \in \mathbb{K}[X],$$

which we write as

$$f_{u,v}(X) = X^n + \sum_{j=1}^{n} A_{f,j}(u,v)X^{n-j}. \tag{2.2}$$

One easily verifies that by the Taylor formula

$$A_{f,j}(u,v) = u^j \frac{f^{(n-j)}(u^{-1}v)}{(n-j)!}, \quad j = 1, \ldots, n. \tag{2.3}$$

We need some simple properties of the polynomials $f_{u,v}(X)$. First we relate $\mathrm{Disc}(f_{u,v})$ to $\mathrm{Disc}(f)$. The following statement is shown in the proof of [40, Theorem 1]; it follows easily via the standard expression of the discriminant via the roots of the corresponding polynomial and the relation between the roots of f and $f_{u,v}$.

LEMMA 2.4: *For any field $\mathbb{K}$ and a monic polynomial $f(X) \in \mathbb{K}[X]$ of degree n, we have*

$$\mathrm{Disc}(f_{u,v}) = u^{n(n-1)} \mathrm{Disc}(f), \quad (u,v) \in \mathbb{K}^* \times \mathbb{K}.$$

Let $\mathbb{F}_p$ denote the finite field of p elements.

We now show that the map $f \mapsto f_{u,v}$ is almost a permutation on the set of monic polynomials $f(X) \in \mathbb{F}_p[X]$ of fixed degree.

LEMMA 2.5: *For a prime $p > n$, for all but at most $O(p^{\lfloor n/2 \rfloor + 1})$ monic polynomials $f(X) \in \mathbb{F}_p[X]$ of degree n, the polynomials $f_{u,v}(X)$, $(u,v) \in \mathbb{F}_p^* \times \mathbb{F}_p$, are pairwise distinct.*

Proof. Let $\mathcal{A}$ be the set of $m \leqslant n$ distinct roots of f. Then the non-uniqueness condition

$$f_{s,t}(X) = f_{u,v}(X)$$

with $(s,t) \neq (u,v)$ means that for any $\alpha \in \mathcal{A}$ there is $\beta \in \mathcal{A}$ with $s\alpha - t = u\beta - v$. Hence there is a nontrivial linear transformation $\mathcal{A} \mapsto a\mathcal{A} + b$, sending each element $\alpha \in \mathcal{A}$ to $a\alpha + b$, which fixes the set $\mathcal{A}$, that is,

$$\mathcal{A} = a\mathcal{A} + b.$$

If $a = 1$ then $b \neq 0$ and examining the orbit

$$\alpha \mapsto \alpha + b \mapsto \alpha + 2b \mapsto \cdots$$

of any element $\alpha \in \mathcal{A}$ we see that for some $k \leqslant n$ we must have $\alpha = \alpha + kb$ which is impossible since $p > n$.

Assume now that $a \neq 1$. Hence for $\mathcal{B} = \mathcal{A} + b(a-1)^{-1}$ we have

$$\mathcal{B} = a\mathcal{B}. \tag{2.4}$$

Examining the orbit

$$\beta \mapsto a\beta \mapsto a^2\beta \mapsto \cdots$$

of any non-zero element $\beta \in \mathcal{B}$ we see that a is of multiplicative order at most m and thus takes at most $m(m+1)/2$ possible values.

Finally, when $a \neq 1$ is fixed, there are at most $O(p^{\lfloor n/2 \rfloor})$ possibilities for the set $\mathcal{B}$. Indeed, we see from (2.4) that $\mathcal{B}$ is a union of cosets of the multiplicative group $\langle a \rangle \subseteq \mathbb{F}_p^*$ generated by a, and possibly of $\{0\}$. Since $a \neq 1$ we see that $\#\langle a \rangle \geqslant 2$ so each such coset if of size at least 2, and thus there are at most $\lfloor m/2 \rfloor$ such cosets in $\mathcal{B}$. We now observe that, for a fixed a, any such coset is defined by any of its elements. Hence the number of possibilities for the set $\mathcal{B}$ does not exceed the number of choices of $\lfloor m/2 \rfloor$ distinct elements of $\mathbb{F}_p$.

When the set $\mathcal{B}$ is fixed, there are p possibilities for $b \in \mathbb{F}_p$. Therefore we conclude that there are $O(p^{\lfloor m/2 \rfloor + 1})$ possibilities for the set of roots $\mathcal{A}$. Since there are $O(1)$ choices for the multiplicities of these roots, and $m \leqslant n$, the result follows. ∎

2.2. Character sums with discriminants. We remark that the values of the quadratic character χ of discriminants are polynomial analogues of the Möbius functions for integers, since by the Stickelberger theorem [10, 42], for a square-free polynomial $f \in \mathbb{F}_p[X]$ of degree n, where p is odd,

$$\Big(\frac{\mathrm{Disc}(f)}{p}\Big) = (-1)^{n-r}, \tag{2.5}$$

where (u/p) is the Legendre symbol of u modulo p and r is the number of distinct irreducible factors of f and, of course,

$$\Big(\frac{\mathrm{Disc}(f)}{p}\Big) = 0$$

if f is not square-free. In particular, this interpretation has motivated the work of Carmon and Rudnick [8]. Here we also need some simple estimates.

Let $\mathcal{M}_{n,p}$ be the set of monic polynomials of degree n over $\mathbb{F}_p$.

Lemma 2.6: *For a prime $p \geqslant 3$,*

$$\sum_{f \in \mathcal{M}_{n,p}} \Big(\frac{\mathrm{Disc}(f)}{p}\Big) = 0.$$

Proof. Let $\mathcal{J}(p)$ be the set of all monic irreducible polynomials over $\mathbb{F}_p$. We consider the zeta function $\zeta(T)$ of the affine line over $\mathbb{F}_p$, which is given by the product

$$\zeta(T) = \prod_{g \in \mathcal{J}(p)} \Big(\frac{1}{1 - T^{\deg g}}\Big) = \frac{1}{1 - pT},$$

that is absolutely converging for $|T| < 1$; see [36, Equations (1) and (2)]. Taking the inverse, we derive

$$\zeta(T)^{-1} = (1 - pT) = \prod_{g \in \mathcal{J}(p)} (1 - T^{\deg g}) = \sum_{f \in \mathcal{S}(p)} (-1)^{\omega(f)} T^{\deg f}, \tag{2.6}$$

where $\mathcal{S}(p)$ is the set of all monic square-free polynomials over $\mathbb{F}_p$ and $\omega(f)$ denotes the number of distinct irreducible factors of f.

Using (2.5) and comparing the coefficient of T^n in the equation (2.6), we obtain the claimed result. ∎

Now, for a vector

$$\boldsymbol{\lambda} = (\lambda_1, \ldots, \lambda_n) \in \mathbb{F}_p^n$$

and a polynomial

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \in \mathcal{M}_{n,p}$$

we define

$$\langle \boldsymbol{\lambda} \circ f \rangle = \lambda_1 a_{n-1} + \cdots + \lambda_n a_0. \tag{2.7}$$

For an integer $m \geqslant 1$, we denote

$$\mathbf{e}_m(z) = \exp(2\pi i z/m),$$

and consider certain mixed exponential and character sums with polynomials. Bounds of these sums underly our approach via the square-sieve method.

We emphasise that our bounds in Lemmas 2.7 and 2.8 below save $\max\{p^{(n-1)/4}, p\}$ against the trivial bound, while an immediate application of the classical Weil bound (see, for example, [21, Theorem 11.23]) saves only $p^{1/2}$. The existence of such a bound is quite remarkable since the discriminant $\mathrm{Disc}(f)$, as a polynomial in the coefficients of f, is highly singular: its locus of singularity is of co-dimension one, see [40, Section 4]. In particular, this means that the result of Katz [25] does not apply, while the result of Rojas-León [35] does not give any advantage over the direct application of the Weil bound [21, Theorem 11.23], which saves $p^{1/2}$ over the trivial bound. Instead we recall the

following bound obtained independently by Bienvenu and Lê [6, Theorem 1] and Porritt [34, Theorem 1].

LEMMA 2.7: *Let $p \geqslant 3$ be a prime. Then, for $n \geqslant 3$ and any $\boldsymbol{\lambda} \in \mathbb{F}_p^n$, in the notation* (2.7)*, we have*

$$\sum_{f \in \mathcal{M}_{n,p}} \Big(\frac{\mathrm{Disc}(f)}{p}\Big) \mathbf{e}_p(\langle \boldsymbol{\lambda} \circ f \rangle) \ll p^{(3n+1)/4}.$$

We now use a different argument, which stems from [38], to get a larger saving for small values of n.

LEMMA 2.8: *Let $p \geqslant 3$ be a prime. Then, for $n \geqslant 3$ and any $\boldsymbol{\lambda} \in \mathbb{F}_p^n$, in the notation* (2.7)*, we have*

$$\sum_{f \in \mathcal{M}_{n,p}} \Big(\frac{\mathrm{Disc}(f)}{p}\Big) \mathbf{e}_p(\langle \boldsymbol{\lambda} \circ f \rangle) \ll p^{n-1}.$$

Proof. By Lemma 2.6 we can assume that $\boldsymbol{\lambda}$ is not identical to zero.

Let $\mathcal{E}_{n,p}$ be the exceptional set of polynomials which are described in Lemma 2.5, that is, the set of monic polynomials $f(X) \in \mathbb{F}_p[X]$ of degree n, such that the polynomials $f_{u,v}(X)$, $(u,v) \in \mathbb{F}_p^* \times \mathbb{F}_p$, are not pairwise distinct.

Thus, by Lemma 2.5, for $n \geqslant 3$, we have

$$\#\mathcal{E}_{n,p} = O(p^{\lfloor n/2 \rfloor + 1}) = O(p^{n-1}). \tag{2.8}$$

For $f \in \mathcal{M}_{n,p}$ we define the quantity $R(f)$ as the following product of the resultants of the consecutive derivatives of f:

$$R(f) = \prod_{j=0}^{n-1} \mathrm{Res}(f^{(j)}, f^{(j+1)}).$$

Let $\mathcal{F}_{n,p}$ be the set of $f \in \mathcal{M}_{n,p}$ with $R(f) = 0$. Clearly

$$\#\mathcal{F}_{n,p} = O(p^{n-1}). \tag{2.9}$$

Define

$$\mathcal{L}_{n,p} = \mathcal{M}_{n,p} \setminus (\mathcal{E}_{n,p} \cup \mathcal{F}_{n,p}).$$

We now see from (2.8) and (2.9) that for any $(u,v) \in \mathbb{F}_p^* \times \mathbb{F}_p$ we have

$$\begin{aligned}\sum_{f \in \mathcal{M}_{n,p}} \Big(\frac{\mathrm{Disc}(f)}{p}\Big)\mathbf{e}_p(\langle \boldsymbol{\lambda} \circ f\rangle) \\ = \sum_{f \in \mathcal{L}_{n,p}} \Big(\frac{\mathrm{Disc}(f)}{p}\Big)\mathbf{e}_p(\langle \boldsymbol{\lambda} \circ f\rangle) + O(p^{n-1}) \\ = \sum_{f \in \mathcal{L}_{n,p}} \Big(\frac{\mathrm{Disc}(f_{u,v})}{p}\Big)\mathbf{e}_p(\langle \boldsymbol{\lambda} \circ f_{u,v}\rangle) + O(p^{n-1}).\end{aligned} \tag{2.10}$$

Since $n(n-1)$ is even, by Lemma 2.4 we have

$$\Big(\frac{\mathrm{Disc}(f_{u,v})}{p}\Big) = \Big(\frac{\mathrm{Disc}(f)}{p}\Big).$$

Thus, summing (2.10) over all pairs $(u,v) \in \mathbb{F}_p^* \times \mathbb{F}_p$ and changing the order of summation, we obtain

$$\begin{aligned}\sum_{f \in \mathcal{M}_{n,p}} \Big(\frac{\mathrm{Disc}(f)}{p}\Big)\mathbf{e}_p(\langle \boldsymbol{\lambda} \circ f\rangle) \\ = \frac{1}{p(p-1)} \sum_{f \in \mathcal{L}_{n,p}} \Big(\frac{\mathrm{Disc}(f)}{p}\Big) \sum_{(u,v) \in \mathbb{F}_p^* \times \mathbb{F}_p} \mathbf{e}_p(\langle \boldsymbol{\lambda} \circ f_{u,v}\rangle) + O(p^{n-1}).\end{aligned}$$

Extending the summation to all pairs $(u,v) \in \mathbb{F}_p \times \mathbb{F}_p$ introduces an error $O(p^{n-1})$ which is admissible, so we obtain

$$\begin{aligned}\sum_{f \in \mathcal{M}_{n,p}} \Big(\frac{\mathrm{Disc}(f)}{p}\Big)\mathbf{e}_p(\langle \boldsymbol{\lambda} \circ f\rangle) \\ = \frac{1}{p(p-1)} \sum_{f \in \mathcal{L}_{n,p}} \Big(\frac{\mathrm{Disc}(f)}{p}\Big) \sum_{(u,v) \in \mathbb{F}_p^2} \mathbf{e}_p(\langle \boldsymbol{\lambda} \circ f_{u,v}\rangle) + O(p^{n-1}).\end{aligned} \tag{2.11}$$

Recalling the notation (2.2) we write

$$\sum_{(u,v) \in \mathbb{F}_p^2} \mathbf{e}_p(\langle \boldsymbol{\lambda} \circ f_{u,v}\rangle) = \sum_{(u,v) \in \mathbb{F}_p^2} \mathbf{e}_p\Big(\sum_{j=1}^n \lambda_j A_{f,j}(u,v)\Big).$$

We now see from (2.11) that it is enough to show that for any $f \in \mathcal{L}_{n,p}$ the Deligne bound (see [21, Section 11.11]) applies to the last sum and thus implies the bound

$$\sum_{(u,v) \in \mathbb{F}_p^2} \mathbf{e}_p\Big(\sum_{j=1}^n \lambda_j A_{f,j}(u,v)\Big) = O(p). \tag{2.12}$$

For this we have to show that the highest form of the polynomial

$$F_f(U,V) = \sum_{j=1}^{n} \lambda_j A_{f,j}(U,V) \in \mathbb{F}_p[U,V]$$

is nonsingular. Since $\boldsymbol{\lambda}$ is not identical to zero there is m such that $\lambda_m \neq 0$ and $\lambda_j = 0$ for $j > m$ (this condition is void if $m = n$).

We see from (2.3) that $A_{f,j}(U,V)$ is a homogeneous polynomial of degree $\deg A_{f,j}(U,V) = j$, $j = 1,\dots,n$. Hence the highest form of $F_f(U,V)$ is $\lambda_m A_{f,m}(U,V)$. Therefore, to establish the bound (2.12), it is sufficient to show that the polynomial $\lambda_m A_{f,m}(U,V)$ is nonsingular, that is, that the equations

$$\frac{\partial A_{f,m}(U,V)}{\partial U} = 0 \tag{2.13}$$

and

$$\frac{\partial A_{f,m}(U,V)}{\partial V} = 0 \tag{2.14}$$

have no common zero $(u_0, v_0) \neq (0,0)$ in the algebraic closure of $\mathbb{F}_p$.

Now, if $u_0 = 0$, then from (2.14) we conclude that $v_0 = 0$, which is impossible. Indeed, from (2.3) we see that

$$A_{f,m}(U,V) \equiv \binom{n}{m} V^m \pmod{U}$$

in the ring $\mathbb{F}_p[U,V]$. Hence

$$\frac{\partial A_{f,m}(U,V)}{\partial V} \equiv \binom{n}{m} m V^{m-1} \pmod{U},$$

which implies the above claim.

If $u_0 \neq 0$, then by the Euler formula for partial derivatives we have

$$U\frac{\partial A_{f,m}(U,V)}{\partial U} + V\frac{\partial A_{f,m}(U,V)}{\partial V} = mU^m \frac{f^{(n-m)}(U^{-1}V)}{(n-m)!}.$$

Therefore, we conclude from the equations (2.13) and (2.14) that v_0/u_0 is a zero of $f^{(n-m)}(X)$, and also by (2.3) and (2.14), v_0/u_0 is also a zero of $f^{(n-m+1)}(X)$. Hence $\operatorname{Res}(f^{(n-m)}, f^{(n-m+1)}) = 0$, which contradicts the condition that $f \notin \mathcal{F}_{n,p}$. Thus, we have the bound (2.12) and the desired result follows. ∎

We now recall the definition of the Jacobi symbol (u/m) modulo an odd square-free integer m:

$$\Big(\frac{u}{m}\Big) = \prod_{\substack{p \mid m \\ p \text{ prime}}} \Big(\frac{u}{p}\Big),$$

where, as before, $(\frac{u}{p})$ is the Legendre symbol (that is, the quadratic character) modulo a prime p, see [21, Section 3.5]).

We now extend the definition of $\mathcal{M}_{n,p}$ to residue rings, and use $\mathcal{M}_{n,m}$ to denote the set of monic polynomials of degree n over $\mathbb{Z}_m$.

Now, using the Chinese Remainder Theorem for character sums, see [21, Equation (12.21)], we see that Lemma 2.6 implies the following identity.

LEMMA 2.9: *Let p and q be two sufficiently large distinct primes and let $m = pq$. Then, for $n \geqslant 3$ we have*

$$\sum_{f \in \mathcal{M}_{n,m}} \Big(\frac{\mathrm{Disc}(f)}{m}\Big) = 0.$$

Similarly, we see that Lemmas 2.7 and 2.8, together with the Chinese Remainder Theorem for mixed sums of additive and multiplicative characters, see [21, Equation (12.21)], yield the following bound.

LEMMA 2.10: *Let p and q be two sufficiently large distinct primes and let $m=pq$. Then, for $n \geqslant 3$ and any $\boldsymbol{\lambda} \in \mathbb{Z}_m^n$, in the notation* (2.7)*, we have*

$$\sum_{f \in \mathcal{M}_{n,m}} \Big(\frac{\mathrm{Disc}(f)}{m}\Big)\mathbf{e}_m(\langle \boldsymbol{\lambda} \circ f \rangle) \ll \min\{m^{(3n+1)/4}, m^{n-1}\}.$$

We now derive our main tool.

LEMMA 2.11: *Let p and q be two sufficiently large distinct primes and let $m=pq$. Then we have*

$$\sum_{f \in \mathcal{P}_n(H)} \Big(\frac{\mathrm{Disc}(f)}{m}\Big) \ll ((H/m)^{n-1} \log m + (\log m)^n) \begin{cases} m^{(3n+1)/4} & \text{if } n \geqslant 5, \\ m^{n-1} & \text{if } n = 3, 4. \end{cases}$$

Proof. Clearly the above sum can be split into $O(H^n/m^n)$ complete sums, which all vanish by Lemma 2.9, and also, for $k = 0, \dots, n-1$ into $O(H^k/m^k+1)$ hybrid sums, that are complete with respect to exactly k variables and incomplete with respect to the remaining $n-k$ variables. Using the standard reduction between complete and incomplete sums (see [21, Section 12.2]) and applying Lemma 2.10 (for incomplete sums), we derive

$$\sum_{f \in \mathcal{P}_n(H)} \Big(\frac{\mathrm{Disc}(f)}{m}\Big) \ll \sum_{k=0}^{n-1} (H^k/m^k + 1) \min\{m^{(3n+1)/4}, m^{n-1}\} (\log m)^{n-k},$$

which implies the result. ∎

3. Proof of Theorem 1.1

3.1. The bound (1.2): the determinant method. We need some results about equations involving discriminants, which could be of independent interest.

Lemma 3.1: *Let $n \geqslant 3$, let $a_2, \dots, a_{n-1} \in \mathbb{Z}$ and let $d_0, d_1, d_2 \in \mathbb{Q}$ such that $(d_0, d_1) \neq (0, 0)$. Moreover, let $u \in \mathbb{Z}$ be square-free such that neither $|u|(n-1)^{n-1}$ nor $|u|n^n$ is a square. Then, for any $c \geqslant 1$, the system of equations*

$$\begin{aligned} z^2 &= u \,\mathrm{Disc}(X^n + a_{n-1}X^n + \cdots + a_1 X + a_0) \\ 0 &= d_0 a_0 + d_1 a_1 + d_2 \end{aligned}$$

has at most $H^{1/2+o(1)}$ solutions $z, a_0, a_1 \in \mathbb{Z}$ such that

$$|a_0|, |a_1| \leqslant H \quad \text{and} \quad |z| \leqslant H^c.$$

Proof. This is a straightforward generalization of [12, Lemma 8], which dealt with the special case $u = 1$. Lemmas 2.2 and 2.3 now play the role of [12, Lemma 5] and [12, Lemma 6], respectively. The proof can then be followed in a completely analogous way to the proof of [12, Lemma 8]. ∎

We also need the following technical result, which generalises [12, Lemma 11].

LEMMA 3.2: *Let $u \in \mathbb{Z}\backslash\{0\}$, and let $N(H)$ be the number of coefficients $a_2, \ldots, a_{n-1} \in \mathbb{Z}$ such that $|a_i| \leqslant H \quad (2 \leqslant i \leqslant n-1)$ and the polynomial*

$$Z^2 - u \operatorname{Disc}(X^n + a_{n-1}X^{n-1} + \cdots + a_2X^2 + A_1X + A_0) \in \mathbb{Z}[A_0, A_1, Z] \tag{3.1}$$

as a polynomial in A_0, A_1, Z is not absolutely irreducible. Then

$$N(H) \ll H^{n-3}.$$

Proof. The special case $u = 1$ is just [12, Lemma 11]. However, if the polynomial (3.1) factorises over $\mathbb{C}[A_0, A_1, Z]$, then

$$u \operatorname{Disc}(X^n + a_{n-1}X^{n-1} + \cdots + a_2X^2 + A_1X + A_0) \in \mathbb{C}[A_0, A_1] \tag{3.2}$$

is a perfect square in $\mathbb{C}[A_0, A_1]$ whence, as $u \neq 0$, also the polynomial (3.2) with $u = 1$ is a square in $\mathbb{C}[A_0, A_1]$. Hence also the polynomial (3.1) with $u = 1$ factorises over $\mathbb{C}[A_0, A_1, Z]$. The result therefore follows immediately from the special case $u = 1$. ∎

Given a square-free integer u, we denote by $\mathcal{T}_n(H, u)$ the set of $f \in \mathcal{I}_n(H)$ for which the square-free part of $\Delta(f)$ is u, that is, $\Delta(f) = r^2u$ for some integer $r \geqslant 1$, and by $T_n(H, u)$ the cardinality of this set.

LEMMA 3.3: *Uniformly over square-free integers u with the condition that neither $|u|(n-1)^{n-1}$ nor $|u|n^n$ is a square, we have the following estimate*

$$T_n(H, u) \leqslant H^{n-2+\sqrt{2}+o(1)}.$$

Proof. Let us fix some $\varepsilon > 0$. By Lemma 2.1, $\operatorname{Disc}(f)$ and $\Delta(f)$ have the same square-free part. So, for square-free $u \in \mathbb{Z}$, we see that $T_n(H, u)$ is the number of solutions $a_0, \ldots, a_{n-1} \in \mathbb{Z}, r \in \mathbb{N}$ of the Diophantine equation

$$r^2u = \operatorname{Disc}(X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0) \tag{3.3}$$

such that $|a_i| \leqslant H \quad (0 \leqslant i \leqslant n-1)$. On writing $z = |ru|$ one observes that $T_n(H, u)$ is at most the number of solutions $a_0, \ldots, a_{n-1} \in \mathbb{Z}$, $z \in \mathbb{N}$, of

$$z^2 = u \operatorname{Disc}(X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0) \tag{3.4}$$

such that $|a_i| \leqslant H$ $(0 \leqslant i \leqslant n-1)$, and that (3.3) and the conditions $|a_i| \leqslant H$ $(0 \leqslant i \leqslant n-1)$ force $r \leqslant H^{c_1}$, $|u| \leqslant H^{c_2}$ for some constants $c_1, c_2 > 0$ only depending on n, so $z \leqslant H^c$ for some $c \geqslant 1$ depending only on n. To bound the number of these solutions, we can now, in a completely analogous way, follow

the proof from [12, Section 5], which deals with the special case $u = 1$: First, fix $a_2, \dots, a_{n-1}$; there are $O(H^{n-2})$ choices. By Lemma 3.2, we may assume that

$$z^2 - u \operatorname{Disc}(X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0) \tag{3.5}$$

as a polynomial in z, a_1, a_0 is absolutely irreducible. We can therefore apply [12, Lemma 12], and the same calculation as in [12] shows that there exist $J \ll H^{\sqrt{2}/2+\varepsilon}$ polynomials $g_1, \dots, g_J \in \mathbb{Z}[Z, A_1, A_0]$, such that each g_j is coprime with the polynomial (3.5) and has degree bounded only in terms of n and ε, and every solution (z, a_1, a_0) to (3.4) with

$$|a_1|, |a_0| \leqslant H \quad \text{and} \quad z \leqslant H^c \tag{3.6}$$

in addition satisfies $g_j(z, a_1, a_0) = 0$ for some $j \in \{1, \dots, J\}$, apart possibly from some exceptional set of solutions of cardinality at most $H^{\sqrt{2}+o(1)}$. So we have to consider J systems of two Diophantine equations, each consisting of (3.4) and the equation $g_j(z, a_1, a_0) = 0$ for some $j \in \{1, \dots, J\}$.

Fix any of those systems. Then it is enough to show that there are at most $H^{\sqrt{2}/2+o(1)}$ integer solutions satisfying (3.6) to this system. To this end, as in [12], we can eliminate z from the system, resulting in one Diophantine equation $f_j(a_1, a_0) = 0$, where $f_j \in \mathbb{Z}[A_1, A_0]$, which is a non-zero rational polynomial by the coprimality of g_j and (3.5). This can be factored over $\mathbb{Q}$, and as in [12], for each factor that is at least quadratic, the bound of Bombieri and Pila [7] yields at most $H^{1/2+o(1)}$ integer solutions with $|a_1|, |a_0| \leqslant H$, which is more than satisfactory, as from (3.4), for each pair (a_1, a_0), we get at most two solutions z. The case of linear factors is covered by Lemma 3.1, again yielding at most $H^{1/2+o(1)}$ solutions satisfying (3.6).

All together, over all $J \ll H^{\sqrt{2}/2+\varepsilon}$ systems, and considering the exceptional set, we obtain at most

$$H^{\sqrt{2}+o(1)} + H^{\sqrt{2}/2+\varepsilon}H^{1/2+o(1)} = H^{\sqrt{2}+o(1)}$$

integer solutions with (3.6), provided that $\varepsilon < \sqrt{2} - 1$. Taking into account the $O(H^{n-2})$ choices for $a_2, \dots, a_n$ from the beginning, we obtain

$$T_n(H, u) \leqslant H^{n-2+\sqrt{2}+o(1)},$$

as required. ∎

By Lemma 2.1 we have

$$N_n(H, \Delta) \leqslant T_n(H, u),$$

where u is the square-free part of Δ, and using Lemma 3.3, we now obtain the bound (1.2).

3.2. The bound (1.3): the square-sieve method. We recall the definitions of $\mathcal{T}_n(H, u)$ and $T_n(H, u) = \#\mathcal{T}_n(H, u)$ from Section 3.1.

Lemma 3.4: *Uniformly over square-free integers u we have the following estimate:*

$$T_n(H, u) \ll \begin{cases} H^{n-2n/(3n+3)}(\log H)^{(5n+1)/(3n+3)} & \text{if } n \geqslant 5, \\ H^{n-n/(2n-1)}(\log H)^{(3n-2)/(2n-1)} & \text{if } n = 3, 4. \end{cases}$$

Proof. As before, by Lemma 2.1, $\mathrm{Disc}(f)$ and $\Delta(f)$ have the same square-free part, and thus $T_n(H, u)$ is the number of polynomials $f \in \mathcal{I}_n(H)$ for which the square-free part of $\mathrm{Disc}(f)$ is u.

We now apply the square sieve of Heath-Brown [15] to the discriminants $\mathrm{Disc}(f)$ of polynomials $f \in \mathcal{I}_n(H)$.

Take now a real $z \geqslant 2$ and denote by $\mathcal{Q}_z$ the set of all primes p in the interval $(z, 2z]$ and by $\pi(z, 2z)$ the cardinality of this set, that is $\pi(z, 2z) = \pi(2z) - \pi(z)$ where, as usual, $\pi(x)$ is the number of primes $p \leqslant x$.

Clearly, for any $f \in \mathcal{T}_n(H, u)$ the product $u\,\mathrm{Disc}(f)$ is a perfect square, and thus, for a prime $p \geqslant 3$ we have

$$\Big(\frac{u\,\mathrm{Disc}(f)}{p}\Big) = 1,$$

unless $p \mid u\,\mathrm{Disc}(f)$, or equivalently $p \mid \mathrm{Disc}(f)$ (as $u \mid \mathrm{Disc}(f)$), in which case we have

$$\Big(\frac{u\,\mathrm{Disc}(f)}{p}\Big) = 0.$$

Note that the condition $f \in \mathcal{T}_n(H, u) \subseteq \mathcal{I}_n(H)$ automatically implies that $\mathrm{Disc}(f) \neq 0$.

Hence, for any $f \in \mathcal{T}_n(H, u)$ we have

$$\sum_{p \in \mathcal{Q}_z} \Big(\frac{u\,\mathrm{Disc}(f)}{p}\Big) = \pi(z, 2z) + O(\omega(\mathrm{Disc}(f))), \tag{3.7}$$

where $\omega(d)$ is the number of prime divisors of the integer $d \neq 0$.

Since $f \in \mathcal{I}_n(H)$, we trivially have $\mathrm{Disc}(f) = H^{O(1)}$. Now, using the trivial bound $\omega(d) = O(\log d)$ and imposing the restriction

$$z \geqslant (\log H)^2, \tag{3.8}$$

we see from the prime number theorem that

$$\pi(z, 2z) + O(\omega(\mathrm{Disc}(f))) \geqslant \frac{1}{2}\pi(z, 2z) \tag{3.9}$$

provided that H is large enough (certainly (3.8) can be substantially relaxed, but this does not affect our result).

Hence, from (3.7) and (3.9) we conclude that

$$\frac{2}{\pi(z, 2z)} \sum_{p \in \mathcal{Q}_z} \Big(\frac{u\,\mathrm{Disc}(f)}{p}\Big) \geqslant 1.$$

Squaring, summing over all $f \in \mathcal{T}_n(H, u)$ and then expanding the summation to all $f \in \mathcal{P}_n(H)$, we obtain

$$\begin{aligned} T_n(H, u) &\leqslant \frac{4}{\pi(z, 2z)^2} \sum_{f \in \mathcal{T}_n(H,u)} \Big| \sum_{p \in \mathcal{Q}_z} \Big(\frac{u\,\mathrm{Disc}(f)}{p}\Big)\Big|^2 \\ &\leqslant \frac{4}{\pi(z, 2z)^2} \sum_{f \in \mathcal{P}_n(H)} \Big| \sum_{p \in \mathcal{Q}_z} \Big(\frac{u\,\mathrm{Disc}(f)}{p}\Big)\Big|^2. \end{aligned}$$

Now, expanding the square and then changing the order of summation and using the multiplicativity of the Jacobi symbol, we derive

$$\begin{aligned} T_n(H, u) &\leqslant \frac{4}{\pi(z, 2z)^2} \sum_{f \in \mathcal{P}_n(H)} \sum_{p,q \in \mathcal{Q}_z} \Big(\frac{u\,\mathrm{Disc}(f)}{pq}\Big) \\ &= \frac{4}{\pi(z, 2z)^2} \sum_{p,q \in \mathcal{Q}_z} \Big(\frac{u}{pq}\Big) \sum_{f \in \mathcal{P}_n(H)} \Big(\frac{\mathrm{Disc}(f)}{pq}\Big). \end{aligned} \tag{3.10}$$

Hence

$$T_n(H, u) \ll \frac{1}{\pi(z, 2z)^2} \sum_{p,q \in \mathcal{Q}_z} \Big| \sum_{f \in \mathcal{P}_n(H)} \Big(\frac{\mathrm{Disc}(f)}{pq}\Big)\Big|.$$

If $n \geqslant 5$ we apply now the first bound of Lemma 2.11 for the inner sum for $O(\pi(z, 2z)^2)$ primes $p \neq q$ and the trivial bound H^n for $\pi(z, 2z)$ choices of primes $p = q$. Taking also into consideration that

$$\pi(z, 2z) \gg \frac{z}{\log z}$$

and $pq \leqslant 4z^2$, we derive

$$\begin{aligned} T_n(H,u) &\ll z^{-1}H^n \log z + (H/z^2)^{n-1} z^{(3n+1)/2} \log z + z^{(3n+1)/2} (\log z)^n \\ &\ll z^{-1}H^n \log z + H^{n-1} z^{-n/2+5/2} \log z + z^{(3n+1)/2} (\log z)^n. \end{aligned}$$

Choosing $z = H^{2n/(3n+3)} (\log H)^{-2(n-1)/(3n+3)}$, thus the condition (3.8) is satisfied, we obtain the desired bound.

For $n = 3, 4$, we apply now the second bound of Lemma 2.11 for the inner sum for $O(\pi(z, 2z)^2)$ primes $p \neq q$ and the trivial bound H^n for $\pi(z, 2z)$ choices of primes $p = q$. Taking also into consideration that

$$\pi(z, 2z) \gg \frac{z}{\log z}$$

and $pq \leqslant 4z^2$, we derive

$$T_n(H,u) \ll z^{-1}H^n \log z + H^{n-1} \log z + z^{2n-2} (\log z)^n.$$

Choosing $z = H^{n/(2n-1)} (\log H)^{-(n-1)/(2n-1)}$, thus the condition (3.8) is satisfied, we conclude the proof. ∎

As before, by Lemma 2.1 we have

$$N_n(H, \Delta) \leqslant T_n(H, u), \tag{3.11}$$

where u is the square-free part of Δ, and using Lemma 3.4, we now obtain the bound (1.3) and conclude the proof of Theorem 1.1.

4. Proof of Theorem 1.2

4.1. Bounds of mean of sums of Jacobi symbols. We also make use of the following bounds of character sums "on average" over square-free moduli which are due to Heath-Brown [16, Corollary 3]. In fact we only need a very special case of this result (combined with the Cauchy inequality), which we present in the following form.

Lemma 4.1: *For all real positive numbers $D \geqslant 1$ and $Z \geqslant 1$, such that $DZ \to \infty$,*

$$\frac{1}{Z} \sum_{\substack{m \leqslant Z \\ m \text{ odd square-free}}} \left| \sum_{|\Delta| \leqslant D} \left(\frac{\Delta}{m}\right) \right| \leqslant (DZ)^{o(1)} \sqrt{D(D/Z+1)}.$$

4.2. Optimization of power sums. We need the following technical result, see [14, Lemma 2.4].

Lemma 4.2: *For $I, J \in \mathbb{N}$ let*

$$F(Z) = \sum_{i=1}^{I} A_i Z^{a_i} + \sum_{j=1}^{J} B_j Z^{-b_j},$$

where A_i, B_j, a_i and b_j are positive for $1 \leqslant i \leqslant I$ and $1 \leqslant j \leqslant J$. Let $0 \le Z_1 \le Z_2$. Then there is some $z \in [Z_1, Z_2]$ with

$$F(z) \ll \sum_{i=1}^{I} \sum_{j=1}^{J} (A_i^{b_j} B_j^{a_i})^{1/(a_i+b_j)} + \sum_{i=1}^{I} A_i Z_1^{a_i} + \sum_{j=1}^{J} B_j Z_2^{-b_j},$$

where the implied constant depends only on I and J.

4.3. Concluding the proof. Using (3.11) and also that

$$\Big(\frac{u}{pq}\Big) = \Big(\frac{\Delta}{pq}\Big),$$

where u is the square-free part of Δ, we can see that the bound (3.10) implies

$$M_n(H, D) \leqslant \frac{4}{\pi(z, 2z)^2} \sum_{p,q \in \mathcal{Q}_z} \sum_{|\Delta| \leqslant D} \Big(\frac{\Delta}{pq}\Big) \sum_{f \in \mathcal{P}_n(H)} \Big(\frac{\mathrm{Disc}(f)}{pq}\Big).$$

Hence

$$M_n(H, D) \ll \frac{1}{\pi(z, 2z)^2} \sum_{p,q \in \mathcal{Q}_z} \Big| \sum_{|\Delta| \leqslant D} \Big(\frac{\Delta}{pq}\Big) \Big| \Big| \sum_{f \in \mathcal{P}_n(H)} \Big(\frac{\mathrm{Disc}(f)}{pq}\Big) \Big|.$$

Continuing as in Section 3.2, and separating the contribution from the terms with $p = q$, we obtain

$$M_n(H, D) \ll z^{-1} D H^n \log z + \frac{1}{\pi(z, 2z)^2} \sum_{\substack{p,q \in \mathcal{Q}_z \\ p \neq q}} \Big| \sum_{|\Delta| \leqslant D} \Big(\frac{\Delta}{pq}\Big) \Big| \Big| \sum_{f \in \mathcal{P}_n(H)} \Big(\frac{\mathrm{Disc}(f)}{pq}\Big) \Big|.$$

If $n \geqslant 5$ we apply now the first bound of Lemma 2.11 for the inner sum and then the bound of Lemma 4.1, and thus derive (after replacing all power logarithms with $H^{o(1)}$)

$$M_n(H, D) \ll z^{-1} D H^{n+o(1)} + H^{o(1)}((H/z^2)^{n-1} + 1) z^{(3n+1)/2} \sqrt{D(D/z^2 + 1)}.$$

After some trivial manipulations, we obtain

$$M_n(H, D) \ll H^{o(1)} \mathcal{M}, \tag{4.1}$$

where

$$\mathcal{M} = z^{-1}DH^n + z^{-(n-3)/2}DH^{n-1} + z^{-(n-5)/2}D^{1/2}H^{n-1} + z^{(3n-1)/2}D + z^{(3n+1)/2}D^{1/2}.$$

Since we obviously have $z^{-1}DH^n \geqslant z^{-(n-3)/2}DH^{n-1}$ we can simplify the above bound as

$$\begin{aligned}\mathcal{M} &\ll z^{-1}DH^n + z^{-(n-5)/2}D^{1/2}H^{n-1} + z^{(3n-1)/2}D + z^{(3n+1)/2}D^{1/2}\\ &= (z^{-1}D^{1/2}H^n + z^{-(n-5)/2}H^{n-1} + z^{(3n-1)/2}D^{1/2} + z^{(3n+1)/2})D^{1/2}.\end{aligned}$$

We now apply Lemma 4.2 with $I=J=2$, $Z_1=(\log H)^2$ (see (3.8)), $Z_2=(DH)^{100}$ and parameters

$$\begin{aligned}&(A_1,a_1) = (D^{1/2},(3n-1)/2), && (A_2,a_2) = (1,(3n+1)/2),\\ &(B_1,b_1) = (D^{1/2}H^n,1), && (B_2,b_2) = (H^{n-1},(n-5)/2).\end{aligned}$$

We now compute

$$\begin{aligned}(A_1^{b_1}B_1^{a_1})^{1/(a_1+b_1)} &= (D^{1/2}(D^{1/2}H^n)^{(3n-1)/2})^{2/(3n+1)}\\ &= D^{1/2}H^{n(3n-1)/(3n+1)},\\ (A_1^{b_2}B_2^{a_1})^{1/(a_1+b_2)} &= (D^{(n-5)/4}(H^{n-1})^{(3n-1)/2})^{1/(2n-3)}\\ &= D^{(n-5)/(8n-12)}H^{(n-1)(3n-1)/(4n-6)},\\ (A_2^{b_1}B_1^{a_2})^{1/(a_2+b_1)} &= ((D^{1/2}H^n)^{(3n+1)/2})^{2/(3n+3)}\\ &= D^{(3n+1)/(6n+6)}H^{n(3n+1)/(3n+3)},\\ (A_2^{b_2}B_2^{a_2})^{1/(a_2+b_2)} &= ((H^{n-1})^{(3n+1)/2})^{1/(2n-2)}\\ &= H^{(3n+1)/4}.\end{aligned}$$

Certainly the contribution from the terms involving Z_1 and Z_2 is negligible. We also note that for $n \geqslant 5$ we have

$$D^{1/2}H^{n(3n-1)/(3n+1)} \geqslant H^{n(3n-1)/(3n+1)} \geqslant H^{(3n+1)/4}.$$

Hence the last term $H^{(3n+1)/4}$ can be omitted. Furthermore, for $n \geqslant 5$ we also have

$$\frac{n-5}{8n-12} \leqslant \frac{3n+1}{6n+6} \quad \text{and} \quad \frac{(n-1)(3n-1)}{4n-6} \leqslant \frac{n(3n+1)}{3n+3}.$$

Hence the second term $D^{(n-5)/(8n-12)}H^{(n-1)(3n-1)/(4n-6)}$ can be omitted too. Thus we obtain

$$\mathcal{M} \ll DH^{n(3n-1)/(3n+1)} + D^{(3n+1)/(6n+6)+1/2}H^{n(3n+1)/(3n+3)}.$$

Recalling (4.1) we obtain

$$M_n(H,D) \leqslant DH^{n(3n-1)/(3n+1)+o(1)} + D^{(3n+2)/(3n+3)}H^{n(3n+1)/(3n+3)+o(1)}.$$

We now observe that the second term improved the trivial bound $M_n(H,D) \ll H^n$ only for $D \leqslant H^{2n/(3n+2)}$, in which case the second term also dominates the first term as

$$DH^{n(3n-1)/(3n+1)} \leqslant D^{(3n+2)/(3n+3)}H^{n(3n+1)/(3n+3)}$$

is equivalent to $D \leqslant H^{4n/(3n+1)}$. The desired result now follows.

5. Proof of Theorem 1.4

Write $H = A + B + C + D$. There are $O(A)$ choices for a, so it suffices to show that for fixed $a \in [C, C + A]$ there are at most $H^{o(1)}$ solutions $(b, r) \in \mathbb{Z}^2$, $b \in [D, D + B]$ to the equation

$$ur^2 - n^n b^{n-1} = (n-1)^{n-1}a^n.$$

As $n \equiv 1 \pmod 4$, substituting $t = b^{(n-1)/2}$, it is enough to uniformly in a bound the number of $r, t \in \mathbb{Z}$, $|r|, |t| \ll H^{n/2}$, such that

$$ur^2 - n^n t^2 = (n-1)^{n-1}a^n. \tag{5.1}$$

Note that $(n-1)^{n-1}a^n \neq 0$ as $n > 1$ and $a \in [C, C + A]$ where $C \geqslant 1$. If $-un^n$ is a square in $\mathbb{Z}$, then we can factor the left-hand side of (5.1) and use the divisor function estimate $\tau(m) = m^{o(1)}$ for all $m \in \mathbb{Z}\backslash\{0\}$ to see that (5.1) has at most $H^{o(1)}$ solutions $r, t \in \mathbb{Z}$. If $-un^n$ is no square, then the left-hand side of (5.1) is a Pellian type equation and though (5.1) has possibly infinitely many solutions $r, t \in \mathbb{Z}$, the number of solutions such that $|r|, |t| \ll H^{n/2}$ by a familiar result can be bounded by $H^{o(1)}$; see, for example, [27, Lemma 3] for arbitrary quadratic polynomials.

6. Concluding Comments

6.1. Discriminants of splitting fields of polynomials. As mentioned in Remark 1.3, it is certainly interesting to count the discriminants of splitting fields of polynomials $f \in \mathcal{I}_n(H)$. Unfortunately our basic tool, Lemma 2.1, does not generalise to the discriminants of these fields. Motivated by this and also by an apparently terminological oversight at the beginning of [2, Section 1] (where $\Delta(f)$ is called the discriminant of the splitting field of f), we give two examples showing that such a direct analogue of Lemma 2.1 is false.

In particular, for the polynomial $f(X) = X^4 - 2$ it is easy to check that the splitting field L of f over $\mathbb{Q}$ is given by $L = \mathbb{Q}(\sqrt[4]{2}, i)$ and that $|L : \mathbb{Q}| = 8$. Further, it is not hard to see that $\sqrt[4]{2}(1 + 2i)$ satisfies the equation

$$F(\sqrt[4]{2}(1 + 2i)) = 0,$$

where $F(X)$ is the degree 8 polynomial $F(X) = X^8 + 28X^4 + 2500$ which is irreducible in $\mathbb{Q}[X]$. Hence

$$L = \mathbb{Q}(\sqrt[4]{2}(1 + 2i)).$$

Using the discriminant formula for trinomials, one finds that

$$\mathrm{Disc}(f) = -2^{11} \quad \text{and} \quad \mathrm{Disc}(F) = 2^{62} \cdot 3^8 \cdot 5^{12}.$$

As $\mathrm{Disc}(f) < 0$ and $\mathrm{Disc}(F) > 0$, by Lemma 2.1 the ratio of $\mathrm{Disc}(f)$ and the discriminant Δ of L is not a rational square (in fact, using for example *Sage*, one can check that $\Delta = 2^{24}$, so $\Delta/\mathrm{Disc}(f) = -2^{13}$; see also Global Number Field 8.0.16777216.2 in [30]).

A slightly more complicated non-binomial example is given by the polynomial $f(X) = X^4 - X - 1$. *Magma* computes the defining polynomial of the splitting field of f as

$$\begin{aligned} F(X) = {} & X^{24} + 90X^{21} - 70X^{20} + 5695X^{18} - 18690X^{17} + 34895X^{16} \\ & + 225900X^{15} - 1544060X^{14} + 3867780X^{13} + 18840027X^{12} \\ & - 62876100X^{11} + 228621050X^{10} - 222888810X^9 \\ & + 999415025X^8 + 9907474500X^7 - 24575577355X^6 \\ & + 34467394920X^5 + 232838692457X^4 - 705674357100X^3 \\ & + 2030693398335X^2 - 2155371295770X + 1779496656001. \end{aligned}$$

Since $\mathrm{Disc}(f) = 283$ and

$$\begin{aligned}\mathrm{Disc}(F) = {} & 2^{144} \cdot 3^{24} \cdot 17^8 \cdot 37^4 \cdot 73^2 \cdot 83^2 \cdot 101^2 \cdot 181^2 \cdot 227^2 \cdot 283^{12} \\ & \cdot 359^4 \cdot 8867^8 \cdot 9473^2 \cdot 47777^4 \cdot 1271971^2 \cdot 1660069^4 \\ & \cdot 970293859^2 \cdot 4552394491^2 \cdot 857054278934851321^2 \\ & \cdot 15214846801156875 61^2,\end{aligned}$$

the presence of the even power of 283 in the prime number factorisation of $\mathrm{Disc}(F)$ and Lemma 2.1 show that the ratio of $\mathrm{Disc}(f)$ and the discriminant of the splitting field is not a rational square.

We note that both approaches, via the determinant method and via the square sieve, are flexible enough to admit several variations in the way we count polynomials. For example, one can fix some of the coefficients, or make them run in a non-cubic box, $[-H_0, H_0] \times \cdots \times [-H_{n-1}, H_{n-1}]$, or move the boxes away from the origin, as in Section 1.4.

6.2. Discriminants of polynomials. It is also natural to ask about the number $D_n(H)$ of distinct discriminants that are generated by all polynomials from $\mathcal{I}_n(H)$. It is reasonable to expect $D_n(H) = H^{n+o(1)}$, however this question seems to be open. We briefly note that trinomials immediately imply $D_n(H) \gg H^2$. Indeed, we consider the discriminants

$$\mathrm{Disc}(X^n + aX - b) = (-1)^{(n-1)(n+2)/2}((n-1)^{n-1}a^n + n^n b^{n-1})$$

of trinomials $X^n + aX - b$ (see for example, [43, Theorem 2]) with

$$H/2 \leqslant a \leqslant H \quad \text{and} \quad 1 \leqslant b \leqslant \frac{H}{3n}$$

with the additional condition

$$a \equiv 0 \pmod 2 \quad \text{and} \quad b \equiv 2 \pmod 4$$

to guarantee the irreducibility by the Eisenstein criterion. We claim all such pairs (a, b) generate distinct discriminants. Indeed, if

$$(n-1)^{n-1}a_1^n + n^n b_1^{n-1} = (n-1)^{n-1}a_2^n + n^n b_2^{n-1}$$

then for $a_1 = a_2$ we also have $b_1 = b_2$. So we can now assume that $a_1 > a_2$. In this case we obtain

$$\begin{aligned}(n-1)^{n-1}a_1^n - (n-1)^{n-1}a_2^n &\geqslant (n-1)^{n-1}a_1^n - (n-1)^{n-1}(a_1-1)^n\\ &\geqslant n(n-1)^{n-1}(H/2)^{n-1} + O(H^{n-2})\\ &= 2^{-n+1}n(n-1)^{n-1}H^{n-1} + O(H^{n-2})\end{aligned}$$

while

$$n^n b_2^{n-1} - n^n b_1^{n-1} \leqslant n^n b_2^{n-1} \leqslant 3^{-n+1}nH^{n-1}$$

which is impossible for a sufficiently large H.

Unfortunately, this argument does not give the lower bound $H^{2+o(1)}$ for the number of distinct discriminants of fields generated by roots of polynomials in $\mathcal{I}_n(f)$, improving Corollary 1.6, since having distinct discriminants of polynomials does not imply necessarily distinct discriminants of fields.

Finally, we note that our methods can also be used to investigate the discriminants of the fields generated by some other special families of polynomials. For example, one of such families is given by quadrinomials $X^n + aX^2 + bX + c$ for the discriminant of which an explicit formula has been given by Otake and Shaska [32].

7. Appendix

7.1. Preliminary discussion. We use this opportunity to fix an error in [12]. Namely [12, Lemmas 5 and 6] (and consequently [12, Lemma 8]) are not correct as stated if the degree n is of the form $n = m^2$ or $n = m^2 + 1$ for some odd m, and therefore [12, Lemma 8] cannot always be directly applied in these cases as well. This does not affect the main results [12, Theorems 1 and 2] in these cases, so let us quickly explain how to amend the proof:

7.2. The case of $n = m^2$. If $n = m^2$ for odd m, then we can directly handle the contribution of a_n such that $z^2 - \Delta(a_1, \ldots, a_n)$ is reducible: [12, Lemma 6] as well as [12, Lemma 5] in the case of $c_1 \neq 0$ are still correct. As a substitute for [12, Lemma 5] for $c_1 = 0$, we can use [18, Satz 1] (see also [19, Section 1]). The latter result shows that for fixed $a_1, \ldots, a_{n-2} \in \mathbb{Z}$, there are, uniformly in $a_1, \ldots, a_{n-2}$, only finitely many rational specialisations for a_{n-1}, for which the resulting polynomial $f(X) = X^n + a_1X^{n-1} + \cdots + a_n$, regarded as a polynomial in $\mathbb{Q}(a_n)[X]$, does not have Galois group S_n over the rational function

field $\mathbb{Q}(a_n)$. Only in these cases $z^2-\Delta(a_1,\dots,a_n)$, as a polynomial in z and a_n, can be reducible over $\mathbb{Q}$, since otherwise having Galois group S_n over $\mathbb{Q}(a_n)$ excludes the possibility that the discriminant $\Delta(a_1,\dots,a_n)$ is a square in $\mathbb{Q}(a_n)$. Therefore there can be only $O(1)$ many exceptional 'bad planes' given by [12, Equation (5)], for which the bound in [12, Lemma 8] does not hold true. Just using the trivial bound $O(H)$ for the number of solutions in these cases instead of the bound provided by [12, Lemma 8] is acceptable, as the resulting bound of $O(H^{n-2})$ (for fixing $a_1,\dots,a_{n-2}$) times $O(1)$ (for the number of exceptional 'bad planes') times $O(H)$ (trivially bounding the solutions instead of using the bound from [12, Lemma 8]) is certainly $H^{n-2+\sqrt{2}+o(1)}$. This fixes the error for $n=m^2$ and odd m.

7.3. The case of $n=m^2+1$. If $n=m^2+1$ for odd $m\geqslant 3$, then n cannot be divisible by 3. In this case, at the outset instead of fixing $n-2$ coefficients $a_1,\dots,a_{n-2}$ we fix $n-2$ coefficients $a_1,\dots,a_{n-4},a_{n-2},a_{n-1}$ instead. As a substitute for [12, Lemma 5] in the case of $c_1\neq 0$ we prove the following result.

Lemma 7.1: *Let $m\geqslant 3$ be an odd integer, and let $n=m^2+1$. Further, let $a_1,\dots,a_{n-4},a_{n-2},a_{n-1}$ be fixed integers, and let $c_1,c_2\in\mathbb{Q}$ with $c_1\neq 0$. Then the polynomial*

$$z^2-\Delta(a_1,\dots,a_{n-4},c_1a_n+c_2,a_{n-2},a_{n-1},a_n)$$

is irreducible in $\mathbb{Q}[z,a_n]$.

Proof. We use the observation that for fixed $a_1,\dots,a_{n-4},a_{n-2},a_{n-1}$, the discriminant $\Delta(a_{n-3},a_n)=\Delta(a_1,\dots,a_n)$ as a polynomial in a_{n-3} and a_n is of the form

$$\Delta(a_{n-3},a_n)=(n-3)^{n-3}3^3a_{n-3}^n a_n^2+\Phi(a_{n-3},a_n), \tag{7.1}$$

where Φ has total degree strictly less than $n+2$. The proof is analogous to that of [12, Lemma 4], using the fact that $\Delta(a_1,\dots,a_n)$ is a weighted-homogeneous polynomial in the a_i, each a_i having weight i, and the total weight of $\Delta(a_1,\dots,a_n)$ is $n(n-1)$. Therefore, for fixed $a_1,\dots,a_{n-4},a_{n-2},a_{n-1}$ any monomial $a_{n-3}^{\alpha}a_n^{\beta}$ occurring in $\Delta(a_1,\dots,a_n)$ satisfies

$$(n-3)\alpha+n\beta\leqslant n(n-1). \tag{7.2}$$

For $\alpha=n$ and $\beta=2$ the left hand side of (7.2) just equals $n(n-1)$, whence the monomial $\delta_n a_{n-3}^n a_n^2$ occurs in $\Delta(a_{n-3},a_n)$, with a constant δ_n only depending

on n; note that we do not yet know whether $\delta_n \neq 0$. To establish (7.1) it is therefore enough to check that this is the only solution of (7.2) with $\alpha+\beta \geqslant n+2$, and then to evaluate δ_n. If $\alpha + \beta \geqslant n + 2$ and $\beta \geqslant 3$, then

$$\begin{aligned}(n-3)\alpha + n\beta &\geqslant (n-3)(n+2-\beta) + n\beta \\ &= (n-3)(n+2) + 3\beta \\ &= n(n-1) - 6 + 3\beta \geqslant n(n-1) + 3.\end{aligned}$$

If $\beta \leqslant 1$, then $\alpha + \beta \geqslant n + 2$ gives $\alpha > n$, which is impossible, because the maximum power of any a_i occurring in any monomial of $\Delta(a_1, \ldots, a_n)$ is at most n. The latter is easily checked by writing the discriminant $\Delta(a_1, \ldots, a_n)$ in the form

$$\Delta(a_1, \ldots, a_n) = (-1)^{n(n-1)/2} \operatorname{Res}(f, f')$$

(see the formula (2.1)), where $f = X^n + a_1X^{n-1} + \cdots + a_n$, expressing the resultant $\operatorname{Res}(f, f')$ of f and its derivative f' by the Sylvester formula as a certain determinant in $a_1, \ldots, a_n$, and checking that each a_i occurs in at most n columns. Hence

$$\Delta(a_{n-3}, a_n) = \delta_n a_{n-3}^n a_n^2 + \Phi(a_{n-3}, a_n),$$

where Φ has total degree less than $n + 2$. To determine the value of δ_n (which only depends on n as remarked above), we observe that, as n is coprime to 3, the trinomial $X^n + aX^3 + b$ has discriminant

$$(-1)^{n(n-1)/2} b^2 (n^n b^{n-3} + (-1)^{n+1}(n-3)^{n-3} 3^3 a^n)$$

(see, for example, [43, Theorem 2]), which immediately yields

$$\delta_n = (-1)^{n(n-1)/2+n+1}(n-3)^{n-3}3^3 = (n-3)^{n-3}3^3$$

as $n = m^2 + 1 \equiv 2 \pmod 4$. Having established (7.1), we see that for n coprime to 3 the number $(n-3)^{n-3}3^3$ cannot be a square, whence

$$\begin{aligned}z^2 - \Delta(a_1, \ldots, a_{n-4}, c_1a_n + c_2, a_{n-2}, a_{n-1}, a_n) \\ = z^2 - (n-3)^{n-3}3^3 c_1^n a_n^{n+2} + O(a_n^{n+1})\end{aligned}$$

is irreducible in $\mathbb{Q}[z, a_n]$. ∎

The special cases that a_{n-3} or a_n are being fixed (substitutes for the analogues of [12, Lemma 5] where $c_1 = 0$, and [12, Lemma 6], respectively) can be handled as above by the result of Hering [18], again using that n is coprime to 3. The argument can then be finished as above, using the main result of [41] instead

of [12, Lemma 10] to see that for n coprime to 3 the polynomial $X^n + aX^3 + b$ has Galois group S_n over any function field $K(a, b)$ where K is any field of characteristic zero.

Acknowledgement. The authors are grateful to Nicholas Katz for valuable discussions regarding several issues about discriminants of number fields and also for providing the second example of Section 6. The authors also would like to thank the referee for the careful reading of the paper and several valuable suggestions improving the exposition of the paper.

During the preparation of this work, A. O. was supported by the ARC Grant DP180100201 and I. S. was supported by the ARC Grant DP170100786.

References

[1] T. C. Anderson, A. Gafni, R. J. Lemke Oliver, D. Lowry-Duda, G. Shakan and R. Zhang, *Quantitative Hilbert irreducibility and almost prime values of polynomial discriminants*, International Mathematics Research Notices **2023** (2023), 2188–2214.

[2] A. Ash, J. Brakenhoff and T. Zarrabi, *Equality of polynomial and field discriminants*, Experimental Mathematics **16** (2007), 367–374.

[3] K. Belabas, M. Bhargava and C. Pomerance, *Error estimates for the Davenport–Heilbronn theorems*, Duke Mathematical Journal **153** (2010), 173–210.

[4] M. Bhargava, *Galois groups of random integer polynomials and van der Waerden's Conjecture*, `http://arxiv.org/abs/2111.06507`.

[5] M. Bhargava, A. Shankar and X. Wang, *Squarefree values of polynomial discriminants I*, Inventiones Mathematicae **228** (2022), 1037–1073.

[6] P.-Y. Bienvenu and T. H. Lê, *Linear and quadratic uniformity of the Möbius function over* $\mathbb{F}_q[t]$, Mathematika **65** (2019), 505–529.

[7] E. Bombieri and J. Pila, *The number of integral points on arcs and ovals*, Duke Mathematical Journal **59** (1989), 337–357.

[8] D. Carmon and Z. Rudnick, *The autocorrelation of the Möbius function and Chowla's conjecture for the rational function field*, Quarterly Journal of Mathematics **65** (2014), 53–61.
[9] R. Chela, *Reducible polynomials*, Journal of the London Mathematical Society **38** (1963), 183–188.
[10] K. Dalen, *On a theorem of Stickelberger*, Mathematica Scandinavica **3** (1955), 124–126.
[11] R. Dietmann, *On the distribution of Galois groups*, Mathematika **58** (2012), 35–44.
[12] R. Dietmann, *Probabilistic Galois theory*, Bulletin of the London Mathematical Society **45** (2013), 453–462.
[13] J. S. Ellenberg and A. Venkatesh, *The number of extensions of a number field with fixed degree and bounded discriminant*, Annals of Mathematics **163** (2006), 723–741.
[14] S. W. Graham and G. Kolesnik, *Van der Corput's Method of Exponential Sums*, London Mathematical Society Lecture Note Series, Vol. 126, Cambridge University Press, Cambridge, 1991.
[15] D. R. Heath-Brown, *The square sieve and consecutive squarefree numbers*, Mathematische Annalen **266** (1984), 251–259.
[16] D. R. Heath-Brown, *A mean value estimate for real character sums*, Acta Arithmetica **72** (1995), 235–275.
[17] D. R. Heath-Brown, *The density of rational points on curves and surfaces*, Annals of Mathematics **155** (2002), 553–595.
[18] H. Hering, *Seltenheit der Gleichungen mit Affekt bei linearem Parameter*, Mathematische Annalen **186** (1970), 263–270.
[19] H. Hering, *Über Koeffizientenbeschränkungen affektloser Gleichungen*, Mathematische Annalen **195** (1972), 121–136.
[20] R. Ibarra, H. Lembeck, M. Ozaslan, H. Smith and K. Stange, *Monogenic fields arising from trinomials*, Involve **15** (2022), 299–317.
[21] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, American Mathematical Society Colloquium Publications, Vol. 53, American Mathematical Society, Providence, RI, 2004.
[22] L. Jones, *A brief note on some infinite families of monogenic polynomials*, Bulletin of the Australian Mathematical Society **100** (2019), 239–244.
[23] L. Jones, *Monogenic polynomials with non-squarefree discriminant*, Proceedings of the American Mathematical Society **148** (2020), 1527–1533.
[24] L. Jones and D. White, *Monogenic trinomials with non-squarefree discriminant*, International Journal of Mathematics **32** (2021), Article no. 2150089.
[25] N. Katz, *Estimates for nonsingular mixed character sums*, International Mathematics Research Notices **2007** (2007), Article no. rnm069.
[26] K. S. Kedlaya, *A construction of polynomials with squarefree discriminants*, Proceedings of the American Mathematical Society **140** (2012), 3025–3033.
[27] S. V. Konyagin and I. E. Shparlinski, *On convex hull of points on modular hyperbolas*, Moscow Journal of Combinatorics and Number Theory **1** (2011), 43–51.
[28] S. Lang, *Algebraic Number Theory*, Graduate Texts in Mathematics, Vol. 110, Springer, Berlin, 1994.
[29] E. Larson and L. Rolen, *Upper bounds for the number of number fields with alternating Galois group*, Proceedings of the American Mathematical Society **141** (2013), 499–503.

[30] The LMFDB Collaboration, *LMFDB: The L-functions and modular forms database*, `http://www.lmfdb.org/NumberField`.

[31] A. Mukhopadhyay, M. R. Murty and K. Srinivas, *Counting squarefree discriminants of trinomials under abc*, Proceedings of the American Mathematical Society **137** (2009), 3219–3226.

[32] S. Otake and T. Shaska, *On the discriminant of certain quadrinomials*, in *Algebraic Curves and Their Applications*, Contemporary Mathematics, vol. 724, American Mathematical Society, Providence, RI, 2019, pp. 55–72.

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

[34] S. Porritt, *A note on exponential-Möbius sums over* $\mathbb{F}_q[t]$, Finite Fields and their Applications **51** (2018), 298–305.

[35] A. Rojas-León, *Estimates for singular multiplicative character sums*, International Mathematics Research Notices **2005** (2005), 1221–1234.

[36] M. Rosen, *Number Theory in Function Fields*, Graduate Texts in Mathematics, Vol. 210, Springer, New York, 2002.

[37] P. Salberger, *Counting rational points on projective varieties*, Proceedings of the London Mathematical Society **126** (2023), 1092–1133.

[38] I. E. Shparlinski, *Distribution of primitive and irreducible polynomials modulo a prime*, Diskretnaya Matematika **1** (1989), 117–124; English translation in Discrete Mathematics and Applications **1** (1991), 59–67.

[39] I. E. Shparlinski, *On quadratic fields generated by discriminants of irreducible trinomials*, Proceedings of the American Mathematical Society **138** (2010), 125–132.

[40] I. E. Shparlinski, *Distribution of polynomial discriminants modulo a prime*, Archiv der Mathematik **105** (2015), 251–259.

[41] J. H. Smith, *General trinomials having symmetric Galois group*, Proceedings of the American Mathematical Society **63** (1977), 208–212.

[42] L. Stickelberger, *Über eine neue Eigenschaft der Diskriminanten algebraischer Zahlkörper*, in *Verhandlungen des ersten Internationalen Mathematiker-Kongresses in Zürich vom 9. bis 11. August 1897*, Teubner, Leipzig, 1898, pp. 182–193.

[43] R. G. Swan, *Factorization of polynomials over finite fields*, Pacific Journal of Mathematics **12** (1962), 1099–1106.

[44] D. Zywina, *Hilbert's irreducibility theorem and the larger sieve*, `http://arxiv.org/abs/1011.6465`.