Bull. Aust. Math. Soc. **109** (2024), 476–485
doi:10.1017/S0004972723000606

ON QUADRATIC FIELDS GENERATED BY POLYNOMIALS

IGOR E. SHPARLINSKI

(Received 22 April 2023; accepted 22 May 2023; first published online 29 June 2023)

Abstract

Let $f(X) \in \mathbb{Z}[X]$ be a polynomial of degree $d \ge 2$ without multiple roots and let $\mathcal{F}(N)$ be the set of Farey fractions of order N. We use bounds for some new character sums and the square-sieve to obtain upper bounds, pointwise and on average, on the number of fields $\mathbb{Q}(\sqrt{f(r)})$ for $r \in \mathcal{F}(N)$, with a given discriminant.

2020 *Mathematics subject classification*: primary 11L40; secondary 11N36, 11R11.

Keywords and phrases: quadratic fields, square sieve, character sums.

1. Introduction

1.1. Motivation. Since the work of Shanks [14], there have been many investigations of properties of quadratic fields $\mathbb{Q}(\sqrt{a})$, for $a \in \mathcal{A}$, where $\mathcal{A}$ is some sequence of arithmetic interest, including values of exponential polynomials [1, 12, 13, 16, 17], coordinates of integer points on algebraic curves [2–4, 6] and polynomial values [5, 11]. Kulkarni and Levin [10] considered statistical properties of quadratic fields $\mathbb{Q}(\sqrt{f(r)})$ generated by polynomials $f(X) \in \mathbb{Z}[X]$ evaluated at rational points.

To define the quantities of interest, for an integer N, we denote by $\mathcal{F}(N)$ the set of all *Farey fractions* of order N and their reciprocals, that is,

$$\mathcal{F}(N) = \{a/b : \ a, b \in \{0, \dots, N\}, \ b \ne 0, \ \gcd(a, b) = 1\}.$$

Given a nonconstant polynomial $f(X) \in \mathbb{Z}[X]$ of degree d without multiple roots, we denote by $\mathcal{R}_f(N)$ the set of discriminants of the quadratic fields $\mathbb{Q}(\sqrt{f(r)})$ for $r \in \mathcal{F}(N)$.

Similarly, define the set $\mathcal{Q}_f(N)$ of discriminants of the quadratic fields $\mathbb{Q}\sqrt{f(n)})$ for $n \in \{1, \dots, N\}$. For linear and quadratic polynomials f, Cutter *et al.* [5, Theorems 1A and 1B] gave an asymptotic formula for $\#\mathcal{Q}_f(N)$. In the case of quadratic polynomials, Luca and Shparlinski [11, Theorem 2] improved the saving in the error term of [5, Theorem 1B] from $\log N$ to $N^{-1/3}$. For polynomials f of higher degree $d \ge 3$, an

During the preparation of this work, the author was supported by the Australian Research Council Grant DP200100355.

asymptotic formula for $\#\mathcal{Q}_f(N)$ is only known conditionally under the ABC-conjecture (see [5, Theorem 1C]). Several additional results on the distribution of the fields $\mathbb{Q}(\sqrt{f(n)})$ for $n \in \{1, \dots, N\}$ have been given in [12].

Kulkarni and Levin [10] initiated the study of the distribution of the fields $\mathbb{Q}(\sqrt{f(r)})$ for $r \in \mathcal{F}(N)$. In particular, by a special case of [10, Theorem 1.2],

$$\#\mathcal{R}_f(N) \geq c(f)\frac{N^2}{(\log N)^2}, \tag{1.1}$$

with some constant $c(f) > 0$ depending only on f. To show (1.1), Kulkarni and Levin [10] used a slightly modified result of Stewart and Top [15, Theorem 2] on squarefree parts of binary forms.

Here we use a different approach similar to that of [12] to obtain some results about the statistics of individual values of discriminants of the fields $\mathbb{Q}(\sqrt{f(r)})$ for $r \in \mathcal{F}(N)$. More precisely, our approach is based on the square-sieve of Heath-Brown [7] combined with various bounds on double character sums.

1.2. General conventions. We use the Landau symbols 'O' and 'o' as well as the Vinogradov symbols '$\gg$' and '$\ll$' with their usual meanings. We recall that $A = O(B)$, $A \ll B$ and $B \gg A$ are all equivalent to the inequality $|A| \leq cB$ with some constant $c > 0$, while $A = o(B)$ means that A/B tends to zero. The implied constants in 'O', '$\ll$' and '$\gg$' may depend on the polynomial $f(X)$.

For a real $A \geq 1$, we write $a \sim A$ to indicate that $A \leq a \leq 2A$.

1.3. Our results. Given a squarefree integer $s \geq 1$ and an arbitrary integer $N \geq 1$, we let

$$R_f(s, N) = \#\{r \in \mathcal{F}(N) : \ \mathbb{Q}(\sqrt{f(r)}) = \mathbb{Q}(\sqrt{s})\}.$$

For a similar quantity

$$Q_f(s, N) = \#\{n \in \{1, \dots, N\} : \ \mathbb{Q}(\sqrt{f(n)}) = \mathbb{Q}(\sqrt{s})\},$$

the upper bound

$$Q_f(s, N) \ll N^{1/2} \log N$$

is given in [12, Theorem 1.1] and a similar argument can easily yield

$$R_f(s, N) \ll N^{3/2} \log N.$$

However, here we take advantage of having essentially a two-dimensional problem and thus we can get savings from each variable (the numerator and denominator of $r \in \mathcal{F}(N)$). Hence, we obtain a stronger bound.

THEOREM 1.1. *Let $f(X) \in \mathbb{Z}[X]$ be a fixed polynomial of degree $d \geq 2$ having only simple roots. Then uniformly over squarefree integers $s \geq 1$ and for any integer $N \geq 2$,*

$$R_f(s, N) \ll N^{4/3}(\log N)^{4/3}.$$

https://doi.org/10.1017/S0004972723000606 Published online by Cambridge University Press

We also show that on average over $s \in \{1, \ldots, S\}$, a better bound can be obtained provided that S is in a certain specific region with respect to N. More precisely, let us define

$$T_f(S, N) = \sum_{\substack{s=1 \\ s \text{ squarefree}}}^{S} R_f(s, N).$$

Clearly, from Theorem 1.1 and also from the trivial bound,

$$T_f(S, N) \ll \min\{N^{4/3} S (\log N)^{4/3}, N^2\}. \tag{1.2}$$

Similarly, we note that the argument of the proof of [12, Theorem 1.3] immediately implies

$$T_f(S, N) \ll N^{3/2+o(1)} S^{3/4}. \tag{1.3}$$

We now obtain a bound which improves (1.2) and (1.3) for $S \le N^{4/5}$.

THEOREM 1.2. *Let $f(X) \in \mathbb{Z}[X]$ be a fixed polynomial of degree $d \ge 2$ having only simple roots. Then uniformly for $S \ge 1$,*

$$T_f(S, N) \le N^{4/3+o(1)} S^{5/6}, \quad \text{as } N \to \infty.$$

In particular, we see from Theorem 1.2 that for all but $o(N^2)$ elements $r \in \mathcal{F}(N)$, the field $\mathbb{Q}(\sqrt{f(r)})$ is of discriminant at least $N^{4/5+o(1)}$.

2. Preparations

2.1. Preliminary discussion. In [10], as in [5, 11, 12], we observe that studying the fields $\mathbb{Q}(\sqrt{f(r)})$ for $r \in \mathcal{F}(N)$ is equivalent to studying the squarefree parts of $f(r)$. To be more precise, for a rational number $\rho \ne 0$, we define the squarefree part $S(\rho)$ as the smallest positive integer $s = S(\rho)$ such that ρ can be written as

$$\rho = \pm s a^2 / b^2$$

with some integers a and b (it is also convenient to set $S(0) = 1$). In particular, $S(f(r))$ is the discriminant of $\mathbb{Q}(\sqrt{f(r)})$ and thus

$$R_f(s, N) = \#\{r \in \mathcal{F}(N) : \ S(f(r)) = s\}.$$

Next, since we are interested in upper bounds, it is convenient to discard the condition $\gcd(a, b) = 1$. In the definition of $R_f(s, N)$, we let r run through N^2 (not necessarily distinct) integer ratios a/b with $1 \le a, b \le N$. Hence, we work with

$$R_f^*(s, N) = \#\{(a, b) \in \{1, \ldots, N\}^2 : \ S(f(a/b)) = s\}$$

and thus with

$$T_f^*(s, N) = \sum_{\substack{s=1 \\ s \text{ squarefree}}}^{S} R_f^*(s, N).$$

https://doi.org/10.1017/S0004972723000606 Published online by Cambridge University Press

Finally, considering the discriminant of f, we note that if $f(X) \in \mathbb{Z}[X]$ has only simple roots, then for a sufficiently large p (depending on f), it also has only simple roots modulo p. Everywhere below, we assume that our primes are large enough to have this property.

2.2. Character sums modulo primes. Our proofs rest on some bounds for character sums. For an odd integer m, we use

$$\left(\frac{k}{m}\right), \quad k, m \in \mathbb{Z};\ m \geq 1, \text{odd},$$

to denote, as usual, the Jacobi symbol of k modulo m. Furthermore, when we write

$$\left(\frac{f(a/b)}{m}\right), \quad a, b \in \mathbb{Z};\ m \geq 1, \text{odd},$$

the value $f(a/b)$ is computed modulo m and, in particular, $\gcd(b/\gcd(a,b), m) = 1$.

We also denote

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

LEMMA 2.1. *Let $f(X) \in \mathbb{Z}[X]$ be a fixed polynomial of degree $d \geq 2$ having only simple roots. For all primes p and all integers λ and μ with*

$$\gcd(\lambda, \mu, p) = 1, \tag{2.1}$$

we have

$$\sum_{a=1}^{p} \sum_{b=1}^{p-1} \left(\frac{f(a/b)}{p}\right) \mathbf{e}_p(\lambda a + \mu b) \ll p.$$

PROOF. Let W be the desired sum. Making the change of variable $a \mapsto ab$ (which for every fixed b runs through the full residue system modulo p together with a) and then adding the value $b = 0$ to the sum, we obtain

$$\begin{aligned} W &= \sum_{a=1}^{p} \sum_{b=1}^{p-1} \left(\frac{f(a)}{p}\right) \mathbf{e}_p(\lambda ab + \mu b) \\ &= \sum_{a=1}^{p} \left(\frac{f(a)}{p}\right) \sum_{b=1}^{p} \mathbf{e}_p((\lambda a + \mu)b) + O(p). \end{aligned}$$

The sum over b vanishes unless $\lambda a + \mu \equiv 0 \pmod{p}$, which by (2.1) is possible for only one value of a modulo p. Hence, $W = O(p)$. □

We also recall the classical Weil bound for pure character sums (see [9, Theorem 11.23]).

https://doi.org/10.1017/S0004972723000606 Published online by Cambridge University Press

LEMMA 2.2. *Let $f(X) \in \mathbb{Z}[X]$ be a fixed polynomial of degree $d \ge 2$, having only simple roots. For all primes p,*

$$\sum_{a=1}^{p} \left(\frac{f(a)}{p}\right) \ll p^{1/2}.$$

Lemma 2.2 immediately implies the following corollary.

COROLLARY 2.3. *Let $f(X) \in \mathbb{Z}[X]$ be a fixed polynomial of degree $d \ge 2$ having only simple roots. For all primes p,*

$$\sum_{a=1}^{p} \sum_{b=1}^{p-1} \left(\frac{f(a/b)}{p}\right) \ll p^{3/2}.$$

2.3. Character sums modulo products of two primes. The following result is a direct implication of the Chinese remainder theorem for character sums (see [9, (12.20) and (12.21)]) combined with Lemma 2.1 and Corollary 2.3.

LEMMA 2.4. *Let $f(X) \in \mathbb{Z}[X]$ be a fixed polynomial of degree $d \ge 2$ having only simple roots. Let $m = \ell p$ for two distinct primes $\ell, p \sim z$ for some real $z \ge 1$. We have*

$$\sum_{a=1}^{m} \sum_{\substack{b=1 \\ \gcd(b,m)=1}}^{m} \left(\frac{f(a/b)}{m}\right) \mathbf{e}_m(\lambda a + \mu b) \ll \begin{cases} z^3 & \text{if } \gcd(\lambda,\mu,m) = m, \\ z^{5/2} & \text{if } 1 < \gcd(\lambda,\mu,m) < m, \\ z^2 & \text{if } \gcd(\lambda,\mu,m) = 1. \end{cases}$$

Using the standard reduction between complete and incomplete sums (see [9, Section 12.2]), we obtain the following result.

LEMMA 2.5. *Let $f(X) \in \mathbb{Z}[X]$ be a fixed polynomial of degree $d \ge 2$ having only simple roots. Let $m = \ell p$ for two distinct primes $\ell, p \sim z$ for some real $z \ge 1$. For any integers $m \ge N \ge 1$,*

$$\sum_{a=1}^{N} \sum_{\substack{b=1 \\ \gcd(b,m)=1}}^{N} \left(\frac{f(a/b)}{m}\right) \ll N^2 z^{-1} + z^2 (\log z)^2.$$

PROOF. We use the well-known bound (see, for example, [9, Bound (8.6)])

$$\sum_{a=1}^{N} \mathbf{e}_m(\lambda z) \ll \frac{m}{|\lambda| + 1},$$

which holds for any integers λ with $|\lambda| \le m/2$ and $N \le m$. As in [9, Lemma 12.1],

$$\sum_{a=1}^{N} \sum_{\substack{b=1 \\ \gcd(b,m)=1}}^{N} \left(\frac{f(a/b)}{m}\right) - \frac{N^2}{m^2} \sum_{a=1}^{m} \sum_{\substack{b=1 \\ \gcd(b,m)=1}}^{m} \left(\frac{f(a/b)}{m}\right) \ll E, \tag{2.2}$$

https://doi.org/10.1017/S0004972723000606 Published online by Cambridge University Press

where

$$E = \sum_{\substack{\lambda,\mu=0\\(\lambda,\mu)\neq(0,0)}}^{m-1} \frac{1}{(|\lambda|+1)(|\mu|+1)} \Bigg| \sum_{a=1}^{m} \sum_{\substack{b=1\\ \gcd(b,m)=1}}^{m} \Big(\frac{f(a/b)}{m}\Big) \mathbf{e}_m(\lambda a + \mu b) \Bigg|.$$

Recalling Lemma 2.4, we see that the contribution E_1 to E from the pairs (λ,μ) with $\gcd(\lambda,\mu,m) = 1$ can be estimated as

$$E_1 \ll z^2 \sum_{\substack{\lambda,\mu=0\\(\lambda,\mu)\neq(0,0)}}^{m-1} \frac{1}{(|\lambda|+1)(|\mu|+1)} \ll z^2 (\log m)^2 \ll z^2 (\log z)^2.$$

Next, by Lemma 2.4, we estimate the contribution E_2 to E from the pairs (λ,μ) with $1 < \gcd(\lambda,\mu,m) < m$ as

$$E_2 \ll z^{5/2} \sum_{\substack{\lambda,\mu=0\\1<\gcd(\lambda,\mu,m)<m}}^{m-1} \frac{1}{(|\lambda|+1)(|\mu|+1)}.$$

Since ℓ and p are of the same size and due to the symmetry between λ and μ, it is enough to estimate

$$\widetilde{E}_2 = z^{5/2} \sum_{\substack{\lambda=0\\ p\mid\lambda}}^{m-1} \sum_{\substack{\mu=1\\ p\mid\mu}}^{m-1} \frac{1}{(|\lambda|+1)(|\mu|+1)} = z^{5/2} \sum_{\substack{\lambda=0\\ p\mid\lambda}}^{m-1} \frac{1}{|\lambda|+1} \sum_{\substack{\mu=1\\ p\mid\mu}}^{m-1} \frac{1}{|\mu|+1}.$$

Handling the sum over λ in a very crude way and discarding the condition $p \mid \lambda$,

$$\widetilde{E}_2 \le z^{5/2} \sum_{\lambda=0}^{m-1} \frac{1}{|\lambda|+1} \sum_{\substack{\mu=1\\ p\mid\mu}}^{m-1} \frac{1}{|\mu|+1} \ll z^{5/2} (\log m) \sum_{\substack{\mu=1\\ p\mid\mu}}^{m} \frac{1}{|\mu|+1}$$

$$= z^{5/2} (\log m) \sum_{\eta=1}^{\ell} \frac{1}{|\eta p|+1} \ll z^{3/2} (\log z)^2.$$

Hence,

$$E_2 \ll z^{3/2} (\log z)^2,$$

which is dominated by the contribution from E_1 and we obtain

$$E \ll z^2 (\log z)^2.$$

Substituting this bound in (2.2) and using Lemma 2.4 again (this time in the case $\gcd(\lambda,\mu,m) = m$), we conclude the proof. □

2.4. Large sieve inequality for Jacobi symbols. We also make use of the following bound of character sums 'on average' over odd squarefree moduli, which is due to Heath-Brown [8, Theorem 1].

https://doi.org/10.1017/S0004972723000606 Published online by Cambridge University Press

LEMMA 2.6. *For all real positive numbers U and Z such that $UZ \to \infty$ and complex-valued functions $\psi(s)$,*

$$\sum_{\substack{m \le Z \\ m \text{ odd squarefree}}} \left| \sum_{\substack{s \le U \\ s \text{ squarefree}}} \psi(s) \left(\frac{s}{m}\right) \right|^2 \le (UZ)^{o(1)} (U+Z) \sum_{1 \le s \le U} |\psi(s)|^2.$$

3. Proofs of the main results

3.1. Proof of Theorem 1.1. Let us fix some sufficiently large real $z > 1$ and let $\mathcal{L}_z$ be the set of primes $\ell \sim z$. By the prime number theorem,

$$\frac{z}{\log z} \ll \#\mathcal{L}_z \ll \frac{z}{\log z}.$$

For a rational number r, we consider the sum

$$U(r,z) = \sum_{\ell \in \mathcal{L}_z}^{*} \left(\frac{r}{\ell}\right),$$

where, as before, r is computed modulo ℓ and Σ^* means that the primes ℓ dividing the denominator of r are excluded.

If $r = a/b$ is a perfect square in $\mathbb{Q}$, that is, $\sqrt{r} \in \mathbb{Q}$, then

$$U(r,z) = \#\mathcal{L}_z + O(\log h),$$

where $h = \max\{|a|, |b|\} + 1$ and the term $O(\log h)$ accounts for $\ell \mid ab$. For each $r \in Q$ with $S(f(r)) = s$, we see that $sf(r)$ is a perfect square. Thus, for such $r \in \mathcal{F}(N)$,

$$U(sf(r), z) = \#\mathcal{L}_z + O(\log N) \ge \tfrac{1}{2}\#\mathcal{L}_z,$$

provided that

$$z \ge N^{1/2} \ge (\log N)^3 \tag{3.1}$$

and N is large enough. In particular,

$$(\#\mathcal{L}_z)^2 R_f^*(s,N) \le 4 \sum_{a,b=1}^{N} (U(sf(a/b), z))^2. \tag{3.2}$$

Squaring out, changing the order of summation, and separating the 'diagonal term' $N\#\mathcal{L}_z$ corresponding to $\ell = p$, we see that

$$\sum_{a,b=1}^{N} (U(sf(a/b), z))^2 \le N^2 \#\mathcal{L}_z + \sum_{\substack{\ell, p \in \mathcal{L}_z \\ \ell \ne p}} \sum_{a=1}^{N} \sum_{\substack{b=1 \\ \gcd(b, \ell p) = 1}}^{N} \left(\frac{sf(n)}{\ell p}\right). \tag{3.3}$$

https://doi.org/10.1017/S0004972723000606 Published online by Cambridge University Press

Substituting (3.3) in (3.2) yields

$$R_f^*(s,N) \ll \frac{(\log z)^2}{z^2}\Big(N^2\frac{z}{\log z} + \sum_{\substack{\ell,p\in\mathcal{L}_z\\ \ell\neq p}}\sum_{a=1}^{N}\sum_{\substack{b=1\\ \gcd(b,\ell p)=1}}^{N}\Big(\frac{sf(n)}{\ell p}\Big)\Big)$$
$$\ll \frac{N^2\log z}{z} + \frac{(\log z)^2}{z^2}\sum_{\substack{\ell,p\in\mathcal{L}_z\\ \ell\neq p}}\sum_{a=1}^{N}\sum_{\substack{b=1\\ \gcd(b,\ell p)=1}}^{N}\Big(\frac{sf(n)}{\ell p}\Big). \tag{3.4}$$

Since $\ell p \geq z^2 > N$, we can apply Lemma 2.5 to the inner sum in (3.4), which yields

$$\sum_{\substack{\ell,p\in\mathcal{L}_z\\ \ell\neq p}}\sum_{a=1}^{N}\sum_{\substack{b=1\\ \gcd(b,\ell p)=1}}^{N}\Big(\frac{sf(n)}{\ell p}\Big) \ll (\#\mathcal{L}_z)^2(N^2z^{-1} + z^2(\log z)^2),$$

which, after substitution in (3.4), implies

$$R_f^*(s,N) \ll N^2z^{-1}\log z + N^2z^{-1} + z^2(\log z)^2$$
$$\ll N^2z^{-1}\log z + z^2(\log z)^2.$$

Choosing $z = N^{2/3}(\log N)^{-1/3}$ (which obviously satisfies (3.1)), yields $R_f^*(s,N) \ll N^{4/3}(\log N)^{4/3}$, which, in turn, implies the desired result.

3.2. Proof of Theorem 1.2. We follow the proof of Theorem 1.1. Using (3.2) for each squarefree $s \in \{1,\dots,S\}$, we write

$$T_f^*(S,N) \ll z^{-2}(\log z)^2 \sum_{\substack{s=1\\ s \text{ squarefree}}}^{S}\sum_{a,b=1}^{N}(U(sf(a/b),z))^2. \tag{3.5}$$

Instead of (3.3), we have

$$\sum_{\substack{s=1\\ s \text{ squarefree}}}^{S}\sum_{a,b=1}^{N}(U(sf(a/b),z))^2$$
$$\leq N^2S\#\mathcal{L}_z + \sum_{\substack{\ell,p\in\mathcal{L}_z\\ \ell\neq p}}\sum_{\substack{s=1\\ s \text{ squarefree}}}^{S}\sum_{a=1}^{N}\sum_{\substack{b=1\\ \gcd(b,\ell p)=1}}^{N}\Big(\frac{sf(n)}{\ell p}\Big)$$
$$\leq N^2S\#\mathcal{L}_z + \sum_{\substack{\ell,p\in\mathcal{L}_z\\ \ell\neq p}}\sum_{\substack{s=1\\ s \text{ squarefree}}}^{S}\Big(\frac{s}{\ell p}\Big)\sum_{a=1}^{N}\sum_{\substack{b=1\\ \gcd(b,\ell p)=1}}^{N}\Big(\frac{f(n)}{\ell p}\Big).$$

https://doi.org/10.1017/S0004972723000606 Published online by Cambridge University Press

Applying Lemma 2.5, we obtain

$$\sum_{\substack{s=1\\ s \text{ squarefree}}}^{S} \sum_{a,b=1}^{N} (U(sf(a/b), z))^2$$

$$\ll N^2 S \#\mathcal{L}_z + (N^2 z^{-1} + z^2 (\log z)^2) \sum_{\substack{\ell,p \in \mathcal{L}_z \\ \ell \neq p}} \left| \sum_{\substack{s=1\\ s \text{ squarefree}}}^{S} \left(\frac{s}{\ell p}\right) \right|. \tag{3.6}$$

We use the Cauchy inequality to derive from Lemma 2.6 that

$$\begin{aligned} \sum_{\substack{\ell,p \in \mathcal{L}_z \\ \ell \neq p}} \left| \sum_{\substack{s=1\\ s \text{ squarefree}}}^{S} \left(\frac{s}{\ell p}\right) \right| &\ll \left((\#\mathcal{L}_z)^2 \sum_{\substack{\ell,p \in \mathcal{L}_z \\ \ell \neq p}} \left| \sum_{\substack{s=1\\ s \text{ squarefree}}}^{S} \left(\frac{s}{\ell p}\right) \right|^2 \right)^{1/2} \\ &\ll ((S + z^2) S^{1+o(1)} z^{2+o(1)})^{1/2} \\ &\ll S^{1+o(1)} z^{1+o(1)} + S^{1/2+o(1)} z^{2+o(1)}, \end{aligned}$$

as $z, S \to \infty$. After substitution in (3.6), the last inequality yields

$$\begin{aligned} &\sum_{\substack{s=1\\ s \text{ squarefree}}}^{S} \sum_{a,b=1}^{N} (U(sf(a/b), z))^2 \\ &\quad \ll N^2 S \#\mathcal{L}_z + (N^2 z^{-1} + z^2 (\log z)^2)(S^{1+o(1)} z^{1+o(1)} + S^{1/2+o(1)} z^{2+o(1)}) \\ &\quad \ll N^2 S^{1+o(1)} z^{1+o(1)} + S^{1+o(1)} z^{3+o(1)} + S^{1/2+o(1)} z^{4+o(1)}, \end{aligned}$$

as $z, S \to \infty$ (note that all terms containing N get absorbed in $N^2 S^{1+o(1)} z^{1+o(1)}$). Substituting the last inequality in (3.5) gives

$$T_f^*(S, N) \ll N^2 S^{1+o(1)} z^{-1+o(1)} + S^{1+o(1)} z^{1+o(1)} + S^{1/2+o(1)} z^{2+o(1)},$$

as $z, S \to \infty$. We now take $z = N^{2/3} S^{1/6}$ to balance the first and the third terms (for which (3.1) is obviously satisfied). This yields

$$T_f^*(S, N) \ll N^{4/3+o(1)} S^{5/6} + N^{2/3+o(1)} S^{7/6} \tag{3.7}$$

(since we can always assume that $S = N^{O(1)}$).

We remark that by (1.2), the bound is trivial unless $N^{4/3+o(1)} S^{5/6} \le N^2$ or $S \le N^{4/5}$. However, under this condition, the last term in (3.7) can be dropped, which concludes the proof.

References

[1] W. D. Banks and I. E. Shparlinski, 'On coincidences among quadratic fields generated by the Shanks sequence', *Q. J. Math.* **68** (2017), 465–484.

[2] Y. Bilu, 'Counting number fields in fibers (with an Appendix by Jean Gillibert)', *Math. Z.* **288** (2018), 541–563.

https://doi.org/10.1017/S0004972723000606 Published online by Cambridge University Press

[3] Y. Bilu and J. Gillibert, 'Chevalley–Weil theorem and subgroups of class groups', *Israel J. Math.* **226** (2018), 927–956.
[4] Y. Bilu and F. Luca, 'Diversity in parametric families of number fields', in: *Number Theory—Diophantine Problems, Uniform Distribution and Applications* (eds. C. Elsholtz and P. Grabner) (Springer, Cham, 2017), 169–191.
[5] P. Cutter, A. Granville and T. J. Tucker, 'The number of fields generated by the square root of values of a given polynomial', *Canad. Math. Bull.* **46** (2003), 71–79.
[6] R. Dvornicich and U. Zannier, 'Fields containing values of algebraic functions', *Ann. Sc. Norm. Super. Pisa Cl. Sci. (5)* **21** (1994), 421–443.
[7] D. R. Heath-Brown, 'The square sieve and consecutive square-free numbers', *Math. Ann.* **266** (1984), 251–259.
[8] D. R. Heath-Brown, 'A mean value estimate for real character sums', *Acta Arith.* **72** (1995), 235–275.
[9] H. Iwaniec and E. Kowalski, *Analytic Number Theory* (American Mathematical Society, Providence, RI, 2004).
[10] K. Kulkarni and A. Levin, 'Hilbert's irreducibility theorem and ideal class groups of quadratic fields', *Acta Arith.,* to appear.
[11] F. Luca and I. E. Shparlinski, 'Discriminants of complex multiplication fields of elliptic curves over finite fields', *Canad. Math. Bull.* **50** (2007), 409–417.
[12] F. Luca and I. E. Shparlinski, 'Quadratic fields generated by polynomials', *Archiv Math.* **91** (2008), 399–408.
[13] R. D. Patterson, A. J. van der Poorten and H. C. Williams, 'Characterization of a generalized Shanks sequence', *Pacific J. Math.* **230** (2007), 185–215.
[14] D. Shanks, 'On Gauss's class number problems', *Math. Comp.* **23** (1969), 151–163.
[15] C. L. Stewart and J. Top, 'On ranks of twists of elliptic curves and power-free values of binary forms', *J. Amer. Math. Soc.* **8** (1995), 943–973.
[16] A. J. van der Poorten and H. C. Williams, 'On certain continued fraction expansions of fixed period length', *Acta Arith.* **89** (1999), 23–35.
[17] H. C. Williams, 'Some generalizations of the S_n sequence of Shanks', *Acta Arith.* **69** (1995), 199–215.

IGOR E. SHPARLINSKI, School of Mathematics and Statistics,
University of New South Wales, Sydney, NSW 2052, Australia
e-mail: igor.shparlinski@unsw.edu.au

https://doi.org/10.1017/S0004972723000606 Published online by Cambridge University Press