Canad. Math. Bull. 2026, pp. 1–20
http://dx.doi.org/10.4153/S000843952610191X
© The Author(s), 2026. Published by Cambridge University Press on behalf of Canadian Mathematical Society. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (https://creativecommons.org/licenses/by/4.0), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

Character sums of division polynomials twisted by multiplicative functions

Subham Bhakta

Abstract. Let E be an elliptic curve over the finite field $\mathbb{F}_p$, and $P \in E(\mathbb{F}_p)$ be an $\mathbb{F}_p$-rational point. We obtain nontrivial estimates for multiplicative character sums associated with the division polynomials $\psi_n(P)$ twisted by several multiplicative functions, where $\psi_n(P)$ denotes the nth division polynomial evaluated at P.

1 Introduction

1.1 Setup

Let E be an elliptic curve over $\mathbb{F}_p$ of characteristic $p > 3$ given by the Weierstrass equation as follows, with coefficients in $\mathbb{F}_p$:

$$y^2 = x^3 + ax + b.$$

For any integer $n \geq 0$, define the nth division polynomial $\psi_n \in \mathbb{F}_p[x, y]$ as follows:

$$\begin{aligned}
&\psi_0 = 0, \quad \psi_1 = 1, \quad \psi_2 = 2y,\\
&\psi_3 = 3x^4 + 6ax^2 + 12bx - a^2,\\
&\psi_4 = 4y(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3),
\end{aligned}$$

with subsequent polynomials given by

$$\begin{aligned}
\psi_{2n+1} &= \psi_{n+2}\psi_n^3 - \psi_{n+1}^3\psi_{n-1}, \quad n \geq 2,\\
\psi_{2n}\psi_2 &= \psi_n(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2), \quad n \geq 3,
\end{aligned}$$

for more details, see [15, Exercise 3.7], combined with the discussion in [15, Chapter III.1].

Denote by $E(\mathbb{F}_p)$ the group of points on E defined over $\mathbb{F}_p$. We can interpret each ψ_n as a rational function on $E(\mathbb{F}_p)$. The multiplication of $P \in E$ by n is given as a

Received by the editors August 15, 2025; revised March 11, 2026; accepted March 16, 2026.
Published online on Cambridge Core March 25, 2026.
This research was partially supported by the Australian Research Council Grant DP230100530.
AMS subject classification: **11G07**, **11L40**, **11N25**, **11N60**.
Keywords: Twisted character sum, division polynomial, arithmetic functions.

https://doi.org/10.4153/S000843952610191X Published online by Cambridge University Press

rational map by

$$[n](P) = \left(\frac{x(P)\psi_n^2(P) - \psi_{n-1}(P)\psi_{n+1}(P)}{\psi_n(P)^2}, \right.$$
$$\left. \frac{\psi_{n-1}(P)^2\psi_{n+2}(P) - \psi_{n-2}(P)\psi_{n+1}(P)^2}{4y(P)\psi_n(P)^3} \right).$$

It is well known that

$$\psi_{m+n}(P)\psi_{m-n}(P)\psi_r^2(P)$$
$$= \psi_{m+r}(P)\psi_{m-r}(P)\psi_n^2(P) - \psi_{n+r}(P)\psi_{n-r}(P)\psi_m(P)^2$$

for any integers $m > n > r$, see, for example, [15, Exercise 3.7(g)]. It turns out that $\psi_n(P)$ is periodic, and the period could be as large as $(p-1)\operatorname{ord} P$, where $\operatorname{ord} P \geq 3$ is the order of P in the group $E(\mathbb{F}_q)$, see [14, Corollary 9] (which also addresses the case $\operatorname{ord} P = 2$).

Let χ be a multiplicative character of $\mathbb{F}_p^*$ of a small order. We consider the sequence $\chi(\psi_n(P))$, where of course we set $\chi(0) = 0$. Then $\chi(\psi_n(P))$ is periodic, whose period can be much smaller (see Section 2) compared to the period of $\psi_n(P)$. For points $P \in E(\mathbb{F}_p)$ of large orders, Shparlinski and Stange [13] have obtained nontrivial estimates for the character sums of the form

$$\sum_{1 \leq n \leq N} \chi(\psi_n(P)),$$

for quadratic characters χ of $\mathbb{F}_p$, and obtained a nontrivial bound provided $p^{1/2+\varepsilon} \leq N \leq \operatorname{ord} P$, for some fixed $\varepsilon > 0$.

Studying the character values $\chi(\psi_n(P))$ has implications for understanding the distribution of rational points on elliptic curves over $\mathbb{Q}$. More specifically, let $E/\mathbb{Q}$ be an elliptic curve given by an integral Weierstrass equation, and let $P \in E(\mathbb{Q})$ be a non-torsion integral point with everywhere good reduction (see [2, Section 5.1] for an example). We can write the points $nP \in E(\mathbb{Q})$ in lowest terms as

$$nP = \left(\frac{a_{nP}}{d_{nP}^2}, \frac{b_{nP}}{d_{nP}^3} \right),$$

where $d_{nP} \in \mathbb{N}$ and $\gcd(a_{nP}b_{nP}, d_{nP}) = 1$. Then [1, Theorem A] or [18, Proposition 3.4] implies that $d_{nP} = |\psi_n(P)|$, where ψ_n is the nth division polynomial associated with $E/\mathbb{Q}$. Consequently, at least for even Dirichlet characters χ of prime modulus p, we study $\chi(d_{nP})$, that is, the distribution of $d_{nP} \bmod p$. See also some related discussions in [2, Section 6].

In this article, we study the correlation between the character values $\chi(\psi_n(P))$ and various multiplicative functions. More precisely, for a given point $P \in E(\mathbb{F}_p)$, we study the twisted sums of the form

$$S_{f,\chi,P}(N) = \sum_{1 \leq n \leq N} f(n)\chi(\psi_n(P)),$$

where f is a suitable multiplicative function.

https://doi.org/10.4153/S000843952610191X Published online by Cambridge University Press

1.2 Main results

1.2.1 Preliminaries

Twists of trace functions with suitable multiplicative functions have been studied by Korolev and Shparlinski [10]. A key ingredient of their study involves a certain correlation property (see [10, Corollary 4.2]) of trace functions. Building upon the work of Shparlinski and Stange [13], we first show in Lemma 2.4 that our function $\chi(\psi_n(P))$ also enjoys similar properties.

Throughout the whole article, we set χ to always denote a multiplicative character on $\mathbb{F}_p^*$ of order d, and

$$R = d \operatorname{ord} P. \tag{1.1}$$

For $n \geq 1$ and $v \geq 1$, let $\tau_v(n)$ denote the v-fold divisor function, defined as

$$\tau_v(n) = \sum_{n_1 n_2 \dots n_v = n} 1,$$

where the sum runs over ordered v-tuples $(n_1, n_2, \dots, n_v)$ of positive integers such that $n_1 n_2 \dots n_v = n$. In other words, $\tau_v(n)$ is the coefficient of n^{-s} in the Dirichlet series

$$\zeta(s)^v = \sum_{n=1}^{\infty} \tau_v(n) n^{-s}.$$

1.2.2 A general bound

For any fixed $C \geq 1$, let us recall the well-known estimate from [9, Equation (1.80)]

$$\sum_{1 \leq n \leq N} \tau_v(n)^C \ll N (\log N)^{v^C - 1}, \tag{1.2}$$

where the implied constants depend on v and C.

The function $\tau_v(n)$ is multiplicative and also satisfies

$$\tau_v(mn) \leq \tau_v(m)\tau_v(n) \qquad \text{for all } m, n \in \mathbb{N}. \tag{1.3}$$

These properties follow, for example, from the description of τ_v at products of prime powers given in [9, Equation (1.25)].

We say that a multiplicative function $f : \mathbb{N} \to \mathbb{C}$ is a τ_v-bounded multiplicative function if $|f(n)| \leq \tau_v(n)$ for all $n \in \mathbb{N}$. We refer the reader to [11, Sections 1.2 and 1.3] for examples of various τ_v-bounded multiplicative functions. Analogous to [10, Theorem 2.2], we have the following result.

Theorem 1.1 *Fix $0 < \varepsilon \leq 1/2$ and an integer $v \geq 1$. Assume that*

$$R \geq p^{1/2+\varepsilon}. \tag{1.4}$$

For any integer N satisfying

$$p^{1/12} R^{5/6+\varepsilon} \leq N \leq R, \tag{1.5}$$

https://doi.org/10.4153/S000843952610191X Published online by Cambridge University Press

and any τ_ν-bounded multiplicative function $f(n)$, we have

$$|S_{f,\chi,P}(N)| \ll N\frac{(\log\log R)^\nu}{\log R},$$

where the implied constant may depend on ε, ν, and d.

Note that (1.5) enforces (1.4). Moreover, Remark 2.5 and the proof of Theorem 1.1 together show that, for any quadratic character χ, the same bound for $S_{f,\chi,P}(N)$ holds, but rather over the extended range $p^{1/2+\varepsilon} \le N \le R$.

1.2.3 A power saving for certain 1-bounded *f*

Throughout the whole article, we say that a multiplicative function $f : \mathbb{N} \to \mathbb{C}$ is a 1-bounded multiplicative function if $|f(n)| \le 1$ for all $n \in \mathbb{N}$. In particular, a 1-bounded multiplicative function is the same as a τ_1-bounded multiplicative function.

When f is a Dirichlet character, we get a power saving compared to the trivial bound in certain ranges of R. More precisely, we prove the following estimate.

Theorem 1.2 *Let R be as in (1.1), and assume that*

$$R \ge p^{1/2}\exp(2.1\log p/\log\log p). \tag{1.6}$$

Then, for any fixed Dirichlet character ψ and any integer $1 \le N \le R$, we have

$$|S_{\psi,\chi,P}(N)| \ll p^{1/12}R^{5/6}(\log R)(\log\log R)^{1/3},$$

where the implied constant may depend on d and ψ.

One can easily note from the argument in Section 3.3 that the weaker condition (1.6) does not work in Theorem 1.1.

Furthermore, we study the sums twisted by $f = \mu^2$, where as usual, μ denotes the Möbius functions, and obtain a power saving in certain ranges. For this, we study certain Type-I sums associated with $\chi(\psi_n(P))$, as done for the proof of [12, Theorem 1.1], and prove the following estimate.

Theorem 1.3 *Let R and ε be as in (1.4). Then for any integer $1 \le N \le R$, we have*

$$\begin{aligned}\left|S_{\mu^2,\chi,P}(N)\right| \ll{}& N^{1/2}p^{1/24}R^{5/12}(\log R)^{3/2}(\log\log R)^{1/6}\\ &+ Np^{-\varepsilon/2}\exp((\log 2 + o(1))\log R/\log\log R),\end{aligned}$$

where the implied constant may depend on d and ε.

It is evident from the proof of Theorem 1.3 that a slightly weaker condition on R can also be imposed. However, this comes at the expense of a weaker bound in the second term of the estimate. Furthermore, the same argument applies for estimating $S_{\mu^{(k)},\chi,P}$, where $\mu^{(k)}$ denotes the characteristic function of k-free numbers.

To understand the strengths of Theorems 1.2 and 1.3 compared to Theorem 1.1, at least for 1-bounded multiplicative functions, consider the range of N in (1.5).

https://doi.org/10.4153/S000843952610191X Published online by Cambridge University Press

Certainly, within this range, both theorems save a power compared to the trivial bounds. In fact, over this range of N, we have a simplified estimate

$$|S_{\mu^2,\chi,P}(N)| \ll Np^{-\varepsilon/4},$$

where again, the implied constant may depend on d and ε.

1.2.4 An estimation over smooth numbers

We begin by recalling that a positive integer n is called y-smooth if $P(n) \le y$, where $P(n)$ denotes the largest prime divisor of n. For $2 \le y \le N$, we denote by $\mathcal{S}(N, y)$ the set of y-smooth integers up to N. As usual, denote $\Psi(N, y) = \sharp\, \mathcal{S}(N, y)$.

Let Ψ_y denote the characteristic function of y-smooth numbers. Clearly, Ψ_y is multiplicative, and we are interested in the sum

$$S_{\Psi_y,\chi,P}(N) = \sum_{n\in\mathcal{S}(N,y)} \chi(\psi_n(P)),$$

which admits the trivial upper bound $|S_{\Psi_y,\chi,P}(N)| \le \Psi(N, y)$.

For various estimates of $\Psi(N, y)$ in various ranges of y, the reader may refer to [4, 6–8]. In this article, we use the following estimate, stated in a form that is adequate for our purposes. For some $\alpha(N, y)$, it is well known that

$$\Psi(N, y) = N^{\alpha(N,y)+o(1)}, \tag{1.7}$$

provided that $y \le N$ and $y \to \infty$; which, for example, follows from [7, Theorem 1], also mentioned in [12, Section 1.3]. Here, $\alpha(N, y)$ satisfies

$$\alpha(N, y) = (1 + o(1))\frac{\log(1 + y/\log N)}{\log y}. \tag{1.8}$$

See [7, Theorem 2] for a more precise asymptotic formula for $\alpha(N, y)$.

In particular, it is certainly useful to note the following facts:

- If $\log y/\log\log N \to \infty$, then $\alpha(N, y) = 1 + o(1)$.
- If $y = (\log N)^K$ for some fixed $K \ge 1$ (i.e., the case of *very smooth* numbers), then $\alpha(N, y) = 1 - \frac{1}{K} + o(1)$, which also reflects the sparsity of *very smooth* numbers.

Theorem 1.4 *Let R be as in (1.6), and $1 \le N \le R$ be any integer. Then for any $N \ge y \ge (\log N)^{\frac{3+\sqrt{5}}{2}}$, we have*

$$|S_{\Psi_y,\chi,P}(N)| \ll y^{1/2}p^{\frac{1}{24(\alpha+2)}}R^{\frac{5}{12(\alpha+2)}}N^{-\gamma}\Psi(N, y)N^{o(1)}, \tag{1.9}$$

where

$$\alpha = \alpha(N, y), \quad \text{and} \quad \gamma = \frac{\alpha^2 + \alpha - 1}{2(\alpha + 2)},$$

and the implied constant in (1.9) may depend on d.

The condition on y in Theorem 1.4 is needed, because the estimate is meaningful when $\gamma > 0$, that is, when $\alpha(N, y) > \frac{\sqrt{5}-1}{2}$. Furthermore, we obtain a power saving in

https://doi.org/10.4153/S000843952610191X Published online by Cambridge University Press

(1.9), provided that N is in the range

$$N^{\alpha^2+\alpha-1} > p^{1/12}R^{5/6+\varepsilon}, \quad \text{for some } \varepsilon > 0.$$

In fact, since $N \le R$ and $R \ll p$, we must then need that $\alpha^2 + \alpha > 23/12$, that is, we need $\alpha > 0.972$, in other words, $y \ge (\log N)^{35.72}$.

In particular, when $\log y/\log\log N \to \infty$, we have $\alpha = 1 + o(1)$, and in that case, we have a cleaner estimate of the form

$$|S_{\Psi_y,\chi,P}(N)| \ll y^{1/2}p^{1/72}R^{5/36}N^{-1/6+o(1)}\Psi(N,y),$$

which is certainly nontrivial in the range $N \gg y^3 p^{1/12}R^{5/6+3\varepsilon}$, for some $\varepsilon > 0$, and also saves a power compared to the trivial bound. However, again since $N \le R$, we need $y \ll R^{1/18-\varepsilon}p^{-1/36}$.

1.3 Notations

Throughout this article, as usual, the notations $U = O(V)$ and $U \ll V$ are equivalent to $|U| \le cV$ for some positive constant c, which may depend on d (order of χ), integer ν, parameter $\varepsilon > 0$, and q (modulus of the Dirichlet character ψ).

Furthermore, we write $U^{o(1)}$ for any quantity V, which for any $\delta > 0$ satisfies $|V| \le C(d,\nu,q,\delta)U^{\delta}$, with some constant $C(d,\nu,q,\delta)$ that may depend on d, ν, q, and δ. In particular, the property $U^{o(1)} \cdot U^{o(1)} = U^{o(1)}$ makes some of the estimates more compact.

We use $\tau(n)$ to denote the number of positive integer factors of an integer $n \ne 0$ and use $\varphi(n)$ to denote the Euler function.

We denote $\mathbf{e}_R(n) = \exp(2\pi i n/R)$. Finally, we use $\sharp\, \mathcal{S}$ to denote the cardinality of a finite set $\mathcal{S}$, and throughout the rest of the article, we write $\sum_{n\le N}$ to denote the summation over integers $1 \le n \le N$.

2 Character sums with division polynomials

2.1 Preliminary

In this section, we establish the key results involving the division polynomials, which are needed for proving the results stated in Section 1.2.

As usual, for any $\Psi \in \mathbb{F}_p(E)$, we define

$$\deg \Psi = \sum_{\substack{P\in E(\overline{\mathbb{F}_p})\\ v_P(\Psi)>0}} v_P(\Psi),$$

where $v_P(\Psi)$ is the multiplicity of P as a zero of Ψ (and thus this is a finite sum over all zeros of Ψ).

Let us again recall R from (1.1). Note that [13, Lemma 3.1] for $s = d$ implies that the sequence $\chi(\psi_n(P))$ is periodic with a period dividing R, as long as $\operatorname{ord} P \ge 3$. Recall the following estimate from [3, Lemma 2.3].

https://doi.org/10.4153/S000843952610191X Published online by Cambridge University Press

Lemma 2.1 *Let χ be any non-principal multiplicative character of $\mathbb{F}_p^*$, and R be as in (1.1). Assume that Ψ is not a nontrivial power of a function in $\overline{\mathbb{F}_p(E)}$. Then, we have the following estimate uniformly over $a \in \mathbb{Z}$:*

$$\left| \sum_{n \le R} \chi(\Psi(nP))\, \mathbf{e}_R(an) \right| \ll \deg \Psi \cdot \sqrt{p},$$

where the implied constant may depend on d.

We also need the following lemma to show that the functions of our requirements satisfy the condition of Lemma 2.1.

Lemma 2.2 *Let m_1, m_2, n_1, n_2 be positive integers satisfying*

$$\gcd(m_1 n_1, m_2 n_2) = \gcd(m_1 n_2, m_2 n_1). \tag{2.1}$$

Suppose further that

$$m_1 \neq m_2 \quad \text{and} \quad n_1 \neq n_2. \tag{2.2}$$

Then, the function

$$\Psi(Q) = \psi_{m_1 n_1} \cdot \psi_{m_2 n_2} \cdot \psi_{m_1 n_2}^{-1} \cdot \psi_{m_2 n_1}^{-1}(Q)$$

is not a nontrivial power of any function in $\overline{\mathbb{F}_p(E)}$.

Proof For any integer h, note that ψ_h has $h^2 - 1$ simple zeros (see [15, Exercise III.3.7]).

Clearly, then the product $\psi_{m_1 n_1} \cdot \psi_{m_2 n_2}$ has

$$(m_1 n_1)^2 + (m_2 n_2)^2 - 2\gcd(m_1 n_1, m_2 n_2)$$

many simple zeros, and $\gcd(m_1 n_1, m_2 n_2) - 1$ many zeros of multiplicity 2. Similarly, $\psi_{m_1 n_2} \cdot \psi_{m_2 n_1}$ has

$$(m_1 n_2)^2 + (m_2 n_1)^2 - 2\gcd(m_1 n_2, m_2 n_1)$$

many simple zeros, and $\gcd(m_1 n_2, m_2 n_1) - 1$ many of zeros of multiplicity 2.

In particular, if $\Psi = G^v$ for some $v \ge 2$ and $G \in \overline{\mathbb{F}_p(E)}$, then

$$\widetilde{\Psi} = \Psi \cdot \psi_{m_1 n_2}^2 \cdot \psi_{m_2 n_1}^2$$

has the property that each zero of $\widetilde{\Psi}$ has multiplicity at least two. Therefore, each simple zero of $\psi_{m_1 n_1} \cdot \psi_{m_2 n_2}$ must also be a simple zero of $\psi_{m_1 n_2} \cdot \psi_{m_2 n_1}$, and vice versa. Therefore, the total number of simple zeros for both $\psi_{m_1 n_1} \cdot \psi_{m_2 n_2}$ and $\psi_{m_1 n_2} \cdot \psi_{m_2 n_1}$ coincides. We get a contradiction due to the imposed conditions at (2.1) and (2.2). ∎

To establish the main result of this section, we need one more ingredient from [13, Lemma 3.2], which demonstrates an *almost multiplicative* nature of $\chi(\psi_n(P))$.

Lemma 2.3 *Let χ be a multiplicative character. Then for any integers m, n, we have*

$$\chi(\psi_{mn}(P)) = \chi(\psi_m(nP))\chi(\psi_n(P))^{m^2}.$$

https://doi.org/10.4153/S000843952610191X Published online by Cambridge University Press

2.2 Correlations of character values

Lemma 2.4 *Let R be as in (1.6), and $1 \le N \le R$ be any integer. Then, for any distinct primes $\ell_1, \ell_2 \le R$, we have*

$$\left| \sum_{n \le N} \chi(\psi_{\ell_1 n}(P)) \overline{\chi(\psi_{\ell_2 n}(P))} \right| \ll \max\{\ell_1, \ell_2\} p^{\frac{1}{12}} R^{5/6} (\log R)(\log\log R)^{1/3},$$

where the implied constant may depend on d.

Proof Let a be an integer. Denote

$$S_{\ell_1,\ell_2}(a) = \sum_{n \le R} \chi(\psi_{\ell_1 n}(P)) \overline{\chi(\psi_{\ell_2 n}(P))}\, \mathbf{e}_R(an).$$

For a parameter L to be determined later, we consider the set of integers

$$\mathcal{R}_d = \{1 \le r \le L : \ r \equiv 1 (\mathrm{mod}\ d),\ \gcd(r, \ell_1\ell_2 R) = 1\}.$$

Clearly by the same argument as in the proof of [3, Lemma 2.4], we have

$$\sharp\, \mathcal{R}_d \ge \frac{\varphi(\ell_1\ell_2 R)(L-1)}{d\ell_1\ell_2 R} - \tau(\ell_1\ell_2 R).$$

Since $\tau(\ell_1\ell_2 R) \ll \tau(R)$ and $\ell_1, \ell_2 \le R$, by the standard estimates of the functions $\tau(n)$ and $\varphi(n)$ (see [5, Theorems 317 and 328], for instance), we have

$$\sharp\, \mathcal{R}_d \gg \frac{L}{\log\log R}, \tag{2.3}$$

provided that

$$L \ge \exp(0.7 \log p / \log\log p). \tag{2.4}$$

Let us now set

$$W = \sum_{r \in \mathcal{R}_d} \sum_{n \le R} \chi(\psi_{\ell_1 rn}(P)) \overline{\chi(\psi_{\ell_2 rn}(P))}\, \mathbf{e}_R(arn).$$

Since each $r \in \mathcal{R}_d$ is co-prime to R, it is clear that

$$S_{\ell_1,\ell_2}(a) = \frac{1}{\sharp\, \mathcal{R}_d} W. \tag{2.5}$$

https://doi.org/10.4153/S000843952610191X Published online by Cambridge University Press

Applying Cauchy–Schwarz combined with Lemma 2.3, we get

$$\begin{aligned}|W|^2 &\le R\sum_{n\le R}\left|\sum_{r\in\mathcal{R}_d}\chi(\psi_{\ell_1 rn}(P))\overline{\chi(\psi_{\ell_2 rn}(P))}\,\mathbf{e}_R(arn)\right|^2\\ &= R\sum_{n\le R}\left|\sum_{r\in\mathcal{R}_d}\chi(\psi_{\ell_1 r}(nP))\overline{\chi(\psi_{\ell_2 r}(nP))}\chi(\psi_n(P))^{\ell_1^2-\ell_2^2}\,\mathbf{e}_R(arn)\right|^2\\ &= R\sum_{n\le R}\left|\sum_{r\in\mathcal{R}_d}\chi(\psi_{\ell_1 r}(nP))\overline{\chi(\psi_{\ell_2 r}(nP))}\,\mathbf{e}_R(arn)\right|^2\\ &\le R\sum_{r_1,r_2\in\mathcal{R}_d}\left|\sum_{n\le R}\chi(\Psi_{r_1,r_2}(nP))\,\mathbf{e}_R(a(r_1-r_2)n)\right|,\end{aligned}\tag{2.6}$$

where $\Psi_{r_1,r_2}\in\mathbb{F}_p(E)$ is given by the following:

$$\Psi_{r_1,r_2}(Q)=\psi_{\ell_1 r_1}(Q)\cdot\psi_{\ell_2 r_2}(Q)\cdot\psi_{\ell_2 r_1}^{-1}(Q)\cdot\psi_{\ell_1 r_2}^{-1}(Q).$$

Clearly, we have

$$\deg\Psi_{r_1,r_2}\ll(L\cdot\max\{\ell_1,\ell_2\})^2.$$

Now, for any $r_1\ne r_2\in\mathcal{R}_d$, we have

$$\gcd(\ell_1 r_1,\ell_2 r_2)=\gcd(r_1,r_2)=\gcd(\ell_1 r_2,\ell_2 r_1).\tag{2.7}$$

Therefore, Lemma 2.2 shows that Ψ_{r_1,r_2} is not a nontrivial power of any $G\in\overline{\mathbb{F}_p(E)}$. Applying Lemma 2.1 to the inner sum in (2.6) for each non-diagonal terms $r_1\ne r_2$, and trivially estimating the contributions from the diagonal terms $r_1=r_2$, we obtain

$$\begin{aligned}|W|^2 &\le R^2\sharp\,\mathcal{R}_d+R\sum_{r_1\ne r_2\in\mathcal{R}_d}\left|\sum_{n\le R}\chi(\Psi_{r_1,r_2}(nP))\,\mathbf{e}_R(a(r_1-r_2)n)\right|\\ &\ll R^2\sharp\,\mathcal{R}_d+R(\sharp\,\mathcal{R}_d)^2\cdot\deg\Psi_{r_1,r_2}\cdot\sqrt{p}\\ &\ll R^2\sharp\,\mathcal{R}_d+R(\sharp\,\mathcal{R}_d)^2(L\cdot\max\{\ell_1,\ell_2\})^2\cdot\sqrt{p}.\end{aligned}$$

In particular, (2.3) and (2.5) imply that

$$|S_{\ell_1,\ell_2}(a)|\ll RL^{-1/2}(\log\log R)^{1/2}+R^{1/2}L\max\{\ell_1,\ell_2\}p^{1/4}.$$

The proof concludes, choosing $L=R^{1/3}p^{-1/6}(\log\log R)^{1/3}$ (clearly L satisfies (2.4) because of the condition (1.6)), and by the completing technique as in [9, Section 12.2]. ∎

Remark 2.5 Following the proof of Lemma 2.4, one observes that the assumption $\ell_1,\ell_2\le R$ is in fact unnecessary. It was imposed only to justify the estimate

$$\frac{\phi(\ell_1\ell_2 R)}{d\ell_1\ell_2 R}\gg\frac{1}{\log\log(\ell_1\ell_2 R)}\gg\frac{1}{\log\log R}.$$

If, however, one of ℓ_1 or ℓ_2 exceeds R, the same conclusion continues to hold; simply because we have $1-\frac{1}{\ell}\ge 1/2$ for any prime ℓ. For simplicity of exposition, we have

https://doi.org/10.4153/S000843952610191X Published online by Cambridge University Press

stated Lemma 2.4 under the condition $\ell_1, \ell_2 \le R$, as this is the only case required in the proof of Theorem 1.1.

Moreover, if both ℓ_1, ℓ_2 are odd, and χ is quadratic, then just by Lemmas 2.1 and 2.3, we immediately have

$$\left|\sum_{n\le N} \chi(\psi_{\ell_1 n}(P))\overline{\chi(\psi_{\ell_2 n}(P))}\right| \ll (\max\{\ell_1,\ell_2\})^2 p^{1/2}(\log R).$$

Due to (1.4), of course, the bound above is better than Lemma 2.4, as long as ℓ_1, ℓ_2 are fixed.

Remark 2.6 If we take $m_1, m_2 \le R$ to be two distinct positive integers. Then, by the same argument in the proof of Lemma 2.1, we have the following weaker estimate:

$$\left|\sum_{n\le N} \chi(\psi_{m_1 n}(P))\overline{\chi(\psi_{m_2 n}(P))}\right| \ll \max\{m_1,m_2\} p^{\frac{1}{12}} R^{5/6}(\log R)^{4/3}.$$

In particular, we have

$$\left|\sum_{N\le n\le 2N} \chi(\psi_{m_1 n}(P))\overline{\chi(\psi_{m_2 n}(P))}\right| \ll \max\{m_1,m_2\} p^{\frac{1}{12}} R^{5/6}(\log R)^{4/3}. \tag{2.8}$$

The reason for the weaker bound is that the identity (2.7) does not necessarily hold, unless r_1, r_2 are primes. In that case, $\mathcal{R}_d$ is essentially a set of primes, and we then have to argue as in the proof of [13, Theorem 5.1], where the argument does not allow us to replace the factor $(\log R)^{1/3}$ by $(\log\log R)^{1/3}$.

Following the argument in the remark above, we also have the following estimate for any m:

$$\left|\sum_{n\le N} \chi(\psi_{mn}(P))\right| \ll m p^{\frac{1}{12}} R^{5/6}(\log R)^{4/3}. \tag{2.9}$$

In fact, one can get here $(\log R)(\log\log R)^{1/3}$ instead of $(\log R)^{4/3}$. This is because $\psi_{mr_1}\cdot\psi_{mr_2}^{-1}$ is not a power of any function in $\overline{\mathbb{F}_p}(E)$ for any integers $r_1 \ne r_2$.

However, the dependence of m in (2.9) would be too restrictive for us to prove Theorem 1.3. To overcome that obstacle, we use Lemma 2.3 to get a sum associated with the point $mP \in E(\mathbb{F}_p)$ (see Lemma 2.8 below). To handle the extra twisting factors $\chi(\psi_m(P))^{n^2}$ arising from Lemma 2.3, we first need the following estimate, which essentially generalizes both [3, Lemma 2.4] and [13, Theorem 5.1].

Lemma 2.7 *Let q and $1 \le k \le q$ be any two fixed integers, and R be as in (1.6). Then for any integer $1 \le N \le R$, we have*

$$\left|\sum_{\substack{n\le N\\ n\equiv k \pmod q}} \chi(\psi_n(P))\right| \ll p^{1/12} R^{5/6}(\log R)(\log\log R)^{1/3},$$

where the implied constant may depend on d.

https://doi.org/10.4153/S000843952610191X Published online by Cambridge University Press

Proof For a suitable parameter L, consider the set of integers

$$\mathcal{R}_{d,q} = \{r < L : r \equiv 1 (\mathrm{mod}\ dq),\ \gcd(r, R) = 1\},$$

where again, d is the order of χ.

Since q, d are both fixed, by the same argument as in the proof of [3, Lemma 2.4], we have

$$\sharp\, \mathcal{R}_{d,q} \gg \frac{L}{\log\log R}, \quad \text{provided that} \quad L \geq \exp(0.7 \log p / \log\log p).$$

Then, for any $r \in \mathcal{R}_{d,q}$,

$$\sum_{\substack{n \leq R \\ n \equiv k (\mathrm{mod}\ q)}} \chi(\psi_n(P)) e_R(an) = \sum_{\substack{n \leq R \\ n \equiv k (\mathrm{mod}\ q)}} \chi(\psi_{nr}(P)) e_R(anr).$$

In particular, the desired sum is bounded by $\frac{1}{\sharp\, \mathcal{R}_{d,q}} \cdot |W_k|$, where

$$W_k = \sum_{r \in \mathcal{R}_{d,q}} \sum_{\substack{n \leq R \\ n \equiv k (\mathrm{mod}\ q)}} \chi(\psi_{nr}(P)) e_R(anr).$$

By Cauchy–Schwarz and Lemma 2.3, we have

$$\begin{aligned} |W_k|^2 &\leq R \sum_{n \leq R} \left| \sum_{r \in \mathcal{R}_{d,q}} \chi(\psi_{rn}(P)) e_R(arn) \right|^2 \\ &= R \sum_{n \leq R} \left| \sum_{r \in \mathcal{R}_{d,q}} \chi(\psi_r(nP)) \chi(\psi_n(P)) e_R(arn) \right|^2 \\ &= R \sum_{n \leq R} \left| \sum_{r \in \mathcal{R}_{d,q}} \chi(\psi_r(nP)) e_R(arn) \right|^2 \\ &\leq R \sum_{r_1, r_2 \in \mathcal{R}_{d,q}} \left| \sum_{n \leq R} \chi(\psi_{r_1} \cdot \psi_{r_2}^{-1}(nP)) e_R(a(r_1 - r_2)n) \right|. \end{aligned}$$

From this point, we proceed exactly as in the proof of [3, Lemma 2.4], applying the completing technique from [9, Section 12.2] to conclude. ∎

Now, we are ready to weaken the dependence of m in (2.9).

Lemma 2.8 *Let R and ε be as in Theorem 1.1, and $m \leq R$ be any positive integer satisfying $(m, R) \leq p^{\varepsilon/2}$. Then for any integer $1 \leq N \leq R$, we have*

$$\left| \sum_{n \leq N} \chi(\psi_{mn}(P)) \right| \ll p^{1/12} R^{5/6} (\log R)(\log\log R)^{1/3},$$

where the implied constant may depend on d and ε.

https://doi.org/10.4153/S000843952610191X Published online by Cambridge University Press

Proof By Lemma 2.3, we can rewrite the sum as

$$\left|\sum_{n\le N}\chi(\psi_n(mP))\chi(\psi_m(P))^{n^2}\right| \ll \sum_{k\le d}\left|\sum_{\substack{n\le N\\ n\equiv k \pmod d}}\chi(\psi_n(mP))\right|.$$

Now, applying Lemma 2.7 to each of the inner sums with $q = d$, and noting that

$$\operatorname{ord}(mP) = \frac{\operatorname{ord}(P)}{(m, \operatorname{ord}(P))} \ge p^{1/2+\varepsilon/2},$$

the proof follows, because mP satisfies (1.6) for any $p > C(\varepsilon)$, where $C(\varepsilon) > 0$ is some constant depending only on ε. ∎

3 Proof of Theorem 1.1

Let us recall the sum of our interest

$$S_{f,\chi,P}(N) = \sum_{n\le N} f(n)\chi(\psi_n(P)),$$

where N, χ, and f be as in Theorem 1.1.

To estimate the sum, we closely follow the approach outlined in [10]. Let $2 \le x < y \le N$ be parameters to be chosen appropriately, and consider the interval $I = (x, y]$. We then split the sum according to whether the indices have no prime factors in I, or have at least one prime factor in I, and estimate each contribution separately.

To make the splitting more systematic, denote $\mathcal{A}_r(N, I)$ the set of integers $1 \le n \le N$ with exactly r prime factors (counted with multiplicities) in I. Note that $\mathcal{A}_r(N, I) = \varnothing$ for any $r \gg \log N$. Therefore, we can write

$$S_{f,\chi,P}(N) = \sum_{r\ll \log N} U_{f,r}(N, I), \tag{3.1}$$

where we denote

$$U_{f,r}(N, I) = \sum_{n\in\mathcal{A}_r(N,I)} f(n)\chi(\psi_n(P)).$$

For the rest of this section, we abuse the notation by writing U_r in place of $U_{f,r}(N, I)$.

3.1 Treatment for U_0

The fundamental lemma of combinatorial sieve [17, Theorem 4.4] shows that the set $\mathcal{A}_0(N, I)$ is small when x and y are widely separated parameters. However, we need an estimate for the sum of τ_ν-bounded functions over this small set. We simply use the following estimate, readily available from [10, Equations (8-2) and (8-3)]:

$$|U_0| \ll N\exp\left(-\frac{\log N}{4\log x}\right)(\log N)^{\frac{\nu^2-1}{2}} + \frac{N(\log N)^{\nu-1}}{(\log y)^\nu}(\log x)^\nu. \tag{3.2}$$

A similar analysis could also be found in [16, Lemma 2.2].

https://doi.org/10.4153/S000843952610191X Published online by Cambridge University Press

3.2 Treatment for U_r for $r > 0$

We can split the sum U_r as

$$U_r = U_{r,1} + U_{r,2},$$

where $U_{r,1}$ denotes the contribution from the integers $n \in \mathcal{A}_r(N, I)$ whose prime divisors from the interval I all appear with multiplicity one. The remaining contribution, coming from integers where at least one prime divisor from I appears with multiplicity at least two, is denoted by $U_{r,2}$.

Note that the sums $U_{r,2}$ are much easier to handle, as crudely using the *submultiplicative* property of $\tau_v(n)$ from (1.2) and (1.3) for $C = 1$, we have

$$\begin{aligned}\left|\sum_{r \ll \log N} U_{r,2}\right| &\le \sum_{\substack{x < \ell \le y \\ \ell \text{ prime}}} \sum_{1 \le s \le \frac{N}{\ell^2}} \left|f(\ell^2 s)\right| \le \sum_{\substack{x < \ell \le y \\ \ell \text{ prime}}} \tau_v(\ell^2) \sum_{1 \le s \le \frac{N}{\ell^2}} \tau_v(s) \\ &\ll N(\log N)^{v-1} \sum_{\substack{x < \ell \\ \ell \text{ prime}}} \frac{\tau_v(\ell^2)}{\ell^2} \ll \frac{N(\log N)^{v-1}}{x \log x}.\end{aligned} \tag{3.3}$$

3.2.1 Estimating $U_{r,1}$

Denote $\mathcal{A}'_r(N, I)$ be the set of integers that appear as an index in the sum $U_{r,1}$. Note that any $n \in \mathcal{A}'_r(N, I)$ has exactly r representations of the form $n = \ell m$, where the prime $\ell \in I$, and integer $m \in \mathcal{A}'_{r-1}(N/\ell, I)$, with $\gcd(m, \ell) = 1$. Due to the multiplicativity of f, we can write

$$U_{r,1} = r^{-1} \sum_{\ell \in I} f(\ell) \sum_{\substack{m \in \mathcal{A}'_{r-1}(N/\ell, I) \\ \gcd(m,\ell)=1}} f(m)\chi(\psi_{\ell m}(P)).$$

Now, dividing $I = (x, y]$ into $K = O(\log y)$ many dyadic intervals $I_k = (x_k, y_k]$ for $k = 0, 1, \dots, K$, as in [10, Equation (7-7)], we can write

$$U_{r,1} = \sum_{k=0}^{K} V_{k,r}, \tag{3.4}$$

where

$$\begin{aligned}V_{k,r} &= r^{-1} \sum_{\ell \in I_k} f(\ell) \sum_{\substack{m \in \mathcal{A}'_{r-1}(N/\ell, I) \\ \gcd(m,\ell)=1}} f(m)\chi(\psi_{\ell m}(P)) \\ &= r^{-1} \sum_{m \in \mathcal{A}'_{r-1}(N/x_k, I)} f(m) \sum_{\substack{\ell \in I_k \cap (1, N/m] \\ \gcd(m,\ell)=1}} f(\ell)\chi(\psi_{\ell m}(P)).\end{aligned}$$

Note that $|f(m)| \le \tau_v(m)$, and for each $m \in \mathcal{A}'_{r-1}(N/x_k, I)$, there exists at most r many $\ell \in I_k$ for which $\gcd(m, \ell) \ne 1$. Therefore, applying (1.2) with $C = 1$, we can write

https://doi.org/10.4153/S000843952610191X Published online by Cambridge University Press

$$V_{k,r} \ll r^{-1} W_{k,r} + N(\log N)^{\nu-1} x_k^{-1}, \tag{3.5}$$

where

$$W_{k,r} = \sum_{m \in \mathcal{A}'_{r-1}(N/x_k, I)} \tau_\nu(m) \left| \sum_{\ell \in I_k \cap (1, N/m]} f(\ell) \chi(\psi_{\ell m}(P)) \right|.$$

Crudely, summing over $m \le N/x_k$ and applying Cauchy–Schwarz, we have

$$\begin{aligned} |W_{k,r}|^2 &\le N x_k^{-1} (\log N)^{\nu^2-1} \sum_{m \le N/x_k} \left| \sum_{\ell \in I_k \cap (1, N/m]} f(\ell)\, \chi(\psi_{\ell m}(P)) \right|^2 \\ &\le N x_k^{-1} (\log N)^{\nu^2-1} \sum_{\ell_1, \ell_2 \in I_k} \left| \sum_{m \le N/\max\{x_k, \ell_1, \ell_2\}} \chi(\psi_{\ell_1 m}(P))\, \overline{\chi(\psi_{\ell_2 m}(P))} \right|, \end{aligned}$$

where we are using above that $|f(\ell_1) f(\ell_2)| = O(1)$, and the estimate from (1.2) for $C = 2$.

At this point, our argument deviates from the proof of [10, Theorem 2.1]. Instead of using [10, Corollary 4.2], we appeal to Lemma 2.4 to estimate the inner sums above for $\ell_1 \ne \ell_2$. Note that (1.4) implies (1.6) for any $p > C(\varepsilon)$, where $C(\varepsilon) > 0$ is some constant depending only on ε. Moreover, we estimate the contributions from $\ell_1 = \ell_2$ trivially, and get

$$\begin{aligned} |W_{k,r}|^2 &\ll \left(N x_k^{-1} \left(y_k N x_k^{-1} + y_k^3 p^{\frac{1}{12}} R^{5/6+o(1)} \right) \right) (\log N)^{\nu^2-1} \\ &\ll \left(N^2 x_k^{-1} + N x_k^2 p^{\frac{1}{12}} R^{5/6+o(1)} \right) (\log N)^{\nu^2-1}. \end{aligned}$$

Consequently, we deduce the following estimate from (3.4) and (3.5):

$$\begin{aligned} U_{r,1} &\ll r^{-1} \sum_{k=0}^{K} (W_{k,r} + rN(\log N)^{\nu-1} x_k^{-1}) \\ &\ll r^{-1} \left(N x^{-1/2} + y N^{1/2} p^{\frac{1}{24}} R^{5/12+o(1)} \right) (\log N)^{\frac{\nu^2-1}{2}} + N(\log N)^{\nu-1} x^{-1}. \end{aligned} \tag{3.6}$$

3.3 Concluding the proof

From (3.1), we have

$$S_{f,\chi,P}(N) \ll \sum_{\substack{r \ll \log N \\ r \ne 0}} |U_{r,1}| + \left| \sum_{\substack{r \ll \log N \\ r \ne 0}} U_{r,2} \right| + |U_0|.$$

Let us choose the parameters

$$x = (\log R)^{\nu^2+3}, \quad \text{and} \quad y = R^{\varepsilon/4}.$$

https://doi.org/10.4153/S000843952610191X Published online by Cambridge University Press

From (3.6), we have

$$\sum_{\substack{r\ll \log N\\ r\neq 0}} |U_{r,1}| \ll \frac{N}{\log R} + yN^{1/2}p^{\frac{1}{24}}R^{5/12+o(1)} \ll \frac{N}{\log R},$$

where the last inequality is due to the condition (1.5).

From (3.3), we have

$$\left|\sum_{\substack{r\ll \log N\\ r\neq 0}} U_{r,2}\right| \ll \frac{N(\log N)^{\nu-1}}{x\log x} \ll \frac{N}{\log R}.$$

The proof is now complete, as (3.2) implies $|U_0| \ll \varepsilon^{-\nu}N\frac{(\log\log R)^{\nu}}{\log R}$.

4 A power saving with certain twists

4.1 Proof of Theorem 1.2

To prove this, we do not quite follow the techniques of the previous section; rather, we simply apply Lemma 2.7. Suppose that ψ is a Dirichlet character modulo q. Then, we can write

$$S_{\psi,\chi,P}(N) = \sum_{k\leq q}\psi(k)\sum_{\substack{n\leq N\\ n\equiv k \pmod q}}\chi(\psi_n(P)).$$

The proof follows, immediately applying Lemma 2.7 to each of the q many inner sums.

4.2 Proof of Theorem 1.3

Let us first write

$$S_{\mu^2,\chi,P}(N) = \sum_{d\leq N^{1/2}}\mu(d)\sum_{n\leq N/d^2}\chi(\psi_{d^2n}(P)).$$

Then, we can split the sum as

$$S_{\mu^2,\chi,P}(N) = T_1 + T_2, \tag{4.1}$$

where we denote

$$T_1 = \sum_{\substack{d\leq N^{1/2}\\ \gcd(d,R)\leq p^{\epsilon/4}}}\mu(d)\sum_{n\leq N/d^2}\chi(\psi_{d^2n}(P)), \quad T_2 = S_{\mu^2,\chi,P}(N) - T_1.$$

To estimate T_1, first we split T_1 into $\log N$ many type I sums of the form

$$S(D,N) = \sum_{\substack{D\leq d<2D\\ \gcd(d,R)\leq p^{\epsilon/4}}}\mu(d)\sum_{n\leq N/d^2}\chi(\psi_{d^2n}(P)).$$

As for any such d above, we have $\gcd(d^2,R)\leq p^{\epsilon/2}$, Lemma 2.8 implies that

$$|S(D,N)| \ll Dp^{1/12}R^{5/6}(\log R)(\log\log R)^{1/3}. \tag{4.2}$$

https://doi.org/10.4153/S000843952610191X Published online by Cambridge University Press

Estimating rather trivially, we also have

$$|S(D,N)| \ll N/D. \tag{4.3}$$

In particular, choosing D_0 such that

$$D_0^2 p^{1/12} R^{5/6} (\log R)(\log\log R)^{1/3} = N,$$

and applying (4.2) for $D \le D_0$, and (4.3) for $D \ge D_0$, we finally derive

$$|T_1| \ll N^{1/2} p^{1/24} R^{5/12} (\log R)^{3/2} (\log\log R)^{1/6}.$$

On the other hand, we have

$$|T_2| = \left| \sum_{\substack{d \le N^{1/2} \\ \gcd(d,R) > p^{\varepsilon/4}}} \mu(d) \sum_{n \le N/d^2} \chi(\psi_{d^2 n}(P)) \right| \le \sum_{\substack{d \le N^{1/2} \\ \gcd(d,R) > p^{\varepsilon/4}}} \sum_{n \le N/d^2} 1.$$

$$\le N \sum_{\substack{d \le N^{1/2} \\ \gcd(d,R) > p^{\varepsilon/4}}} \frac{1}{d^2} + \sharp\{d \le N^{1/2} : \gcd(d,R) > p^{\varepsilon/4}\}.$$

To bound the first term above, note that if $\gcd(d,R) > p^{\varepsilon/4}$, then there exists a divisor $g \mid R$ with $g > p^{\varepsilon/4}$ such that $g \mid d$. In particular, we have

$$\sum_{\substack{d \le N^{1/2} \\ \gcd(d,R) > p^{\varepsilon/4}}} \frac{1}{d^2} \le \sum_{\substack{g \mid R \\ g > p^{\varepsilon/4}}} \sum_{\substack{d \le N^{1/2} \\ g \mid d}} \frac{1}{d^2} \ll \sum_{\substack{g \mid R \\ g > p^{\varepsilon/4}}} \frac{1}{g^2} \ll \frac{\tau(R)}{p^{\varepsilon/2}},$$

where $\tau(R) = \tau_1(R)$ denotes the number of divisors of R.

On the other hand, we also have

$$\sharp\{d \le N^{1/2} : \gcd(d,R) > p^{\varepsilon/4}\} \le \sum_{\substack{g \mid R \\ g > p^{\varepsilon/4}}} \sharp\{d \le N^{1/2} : g \mid d\} \ll \frac{N^{1/2}\tau(R)}{p^{\varepsilon/4}}.$$

Therefore, we derive

$$|T_2| \ll \frac{N\tau(R)}{p^{\varepsilon/2}} + \frac{N^{1/2}\tau(R)}{p^{\varepsilon/4}}. \tag{4.4}$$

Note that if $N < p^{\varepsilon/2}$, then the desired estimate at Theorem 1.3 holds trivially, as $R \ge p^{1/2}$ by (1.4). Hence, we may assume that $N \ge p^{\varepsilon/2}$. Consequently, from (4.4), we obtain

$$|T_2| \ll N p^{-\varepsilon/2} \exp((\log 2 + o(1)) \log R / \log\log R),$$

where we use the well-known bound for $\tau(R)$ (see [5, Theorem 317]). The proof now follows from (4.1).

https://doi.org/10.4153/S000843952610191X Published online by Cambridge University Press

5 Proof of Theorem 1.4

5.1 Preliminaries

5.1.1 Smooth numbers in a smaller range

We first need the following estimates.

Lemma 5.1 *Let $\alpha = \alpha(N, y)$ be as in (1.8). For any $1 \le L \le N$, we have*

$$\Psi(N/L, y) \ll \frac{1}{L^\alpha}\Psi(N, y), \quad \text{and} \tag{5.1}$$

$$\Psi(L, y) \ll L^\alpha N^{o(1)}. \tag{5.2}$$

Proof For (5.1), see [6, Section 2]. To prove (5.2), simply note that

$$\Psi(L, y) \ll \left(\frac{L}{N}\right)^\alpha \Psi(N, y) = L^\alpha N^{o(1)}, \tag{5.3}$$

where, of course, we are using (1.7) for the last equality. ∎

5.1.2 A decomposition of large smooth numbers

Let $L_0 \le N$ be a parameter to be chosen later. Note that any $n \in \mathcal{S}(N, y)$ with $n > L_0$ can be uniquely written as

$$n = \ell m, \quad \text{with} \quad L_0 < \ell \le P(\ell)L_0 \quad \text{and} \quad p(m) \ge P(\ell),$$

where $P(\ell)$ denotes the largest prime factor of ℓ and $p(m)$ denotes the smallest prime factor of m. Indeed, one can obtain such a decomposition by arranging all the prime factors of n as $p_1 \le p_2 \le \cdots \le p_K$, and keep collecting the numbers $p_1, p_1p_2, \ldots$, until we reach a number ℓ that just crosses L_0. See also [12, p. 9].

To show the uniqueness of the decomposition, write $n = p_1 \ldots p_K$ with $p_1 \le p_2 \le \cdots \le p_K$. Then ℓ must be of the form $p_1 \ldots p_S$ and m of the form $p_{S+1} \ldots p_K$ for some $S \le K$. Now, the condition $L_0 \le \ell \le P(\ell)L_0$ implies

$$L_0 \le p_1 \ldots p_S \qquad \text{and} \qquad p_1 \ldots p_{S-1} < L_0.$$

Hence, S is uniquely determined by L_0, which proves the uniqueness of the decomposition.

Then, we can write

$$S_{\Psi_y,\chi,P}(P) = \sum_{\substack{L_0 < \ell \le P(\ell)L_0 \\ \ell \in \mathcal{S}(N,y)}} \sum_{\substack{m \in \mathcal{S}(N/\ell, y) \\ p(m) \ge P(\ell)}} \chi(\psi_{\ell m}(P)) + O(L_0).$$

5.2 Concluding the proof

Note that the range of ℓ is given by $(L_0, yL_0]$. After the dyadic partition of this range, we see that there is some $L \in (L_0, yL_0]$ such that

$$S_{\Psi_y,\chi,P}(P) \ll U \log N + L_0, \tag{5.4}$$

https://doi.org/10.4153/S000843952610191X Published online by Cambridge University Press

where

$$U = \sum_{\substack{L<\ell\le \min\{P(\ell)L_0,2L\}\\ \ell\in\mathcal{S}(N,y)}} \sum_{\substack{m\in S(N/\ell,y)\\ p(m)\ge P(\ell)}} \chi(\psi_{\ell m}(P)).$$

We now argue exactly as in the proof of [12, Theorem 1.3], and obtain

$$U^2 \ll (\log N)^2\Psi(L,y) \times \sum_{q\le y}\sum_{m_1,m_2\in\mathcal{S}(N/L,y)} \left|\sum_{L/q<\ell\le 2L/q} \chi(\psi_{q\ell m_1}(P))\overline{\chi(\psi_{q\ell m_2}(P)}\right|.$$

For the rest of the proof, we set $\alpha = \alpha(N,y)$. Following the same argument as in [12], the contribution Y_1 from the diagonal terms with $m_1 = m_2$ is

$$\begin{aligned} Y_1 &\ll (\log N)^2\Psi(L,y)\sum_{q\le y}\Psi(N/L,y)L/q \\ &\ll LN^{-\alpha}\Psi(N,y)^2N^{o(1)}, \end{aligned}$$

where the inequality above follows combining (5.1) and the first inequality in (5.3), and also recalling that $\log y \le \log N = N^{o(1)}$.

To estimate the contribution Y_2 from the non-diagonal terms $m_1 \ne m_2$, we apply (2.8) instead of [12, Lemma 2.2], and obtain

$$\begin{aligned} Y_2 &\ll (\log N)^2\Psi(L,y)\cdot y\Psi(N/L,y)^2\cdot N/L\cdot p^{\frac{1}{12}}R^{5/6+o(1)} \\ &\ll yp^{1/12}R^{5/6}L^{-(\alpha+1)}\Psi(N,y)^2N^{1+o(1)}, \end{aligned}$$

where the last inequality follows by combining both parts of Lemma 5.1.

In particular, recalling that $L_0 < L \le yL_0$, we have

$$\begin{aligned} U^2 \ll Y_1 + Y_2 &\le (LN^{-\alpha} + yp^{1/12}R^{5/6}L_0^{-(\alpha+1)}N)\Psi(N,y)^2N^{o(1)} \\ &\le y(L_0N^{-\alpha} + p^{1/12}R^{5/6}L_0^{-(\alpha+1)}N)\Psi(N,y)^2N^{o(1)}. \end{aligned}$$

Choosing $L_0 = p^{\frac{1}{12(\alpha+2)}}R^{\frac{5}{6(\alpha+2)}}N^{\frac{\alpha+1}{\alpha+2}}$, we derive

$$U \le y^{1/2}p^{\frac{1}{24(\alpha+2)}}R^{\frac{5}{12(\alpha+2)}}N^{\frac{1-(\alpha^2+\alpha)}{2(\alpha+2)}}\Psi(N,y)N^{o(1)}.$$

Hence, (5.4) gives

$$\begin{aligned} S_{f_y,\chi,P}(N) \ll{}& y^{1/2}p^{\frac{1}{24(\alpha+2)}}R^{\frac{5}{12(\alpha+2)}}N^{\frac{1-(\alpha^2+\alpha)}{2(\alpha+2)}}\Psi(N,y)N^{o(1)} \\ &+ p^{\frac{1}{12(\alpha+2)}}R^{\frac{5}{6(\alpha+2)}}N^{\frac{\alpha+1}{\alpha+2}}. \end{aligned}$$

Setting $\gamma = \frac{\alpha^2+\alpha-1}{2(\alpha+2)}$, we have $\alpha - 2\gamma = \frac{\alpha+1}{\alpha+2}$, and hence we finally deduce

$$\begin{aligned} |S_{f_y,\chi,P}(N)| \ll{}& y^{1/2}p^{\frac{1}{24(\alpha+2)}}R^{\frac{5}{12(\alpha+2)}}N^{-\gamma}\Psi(N,y)N^{o(1)} \\ &+ p^{\frac{1}{12(\alpha+2)}}R^{\frac{5}{6(\alpha+2)}}N^{\alpha-2\gamma}. \end{aligned}$$

https://doi.org/10.4153/S000843952610191X Published online by Cambridge University Press

If $p^{\frac{1}{24(\alpha+2)}} R^{\frac{5}{12(\alpha+2)}} > N^{\gamma}$, then the stated bound at (1.9) is trivial. So, let us assume that $p^{\frac{1}{24(\alpha+2)}} R^{\frac{5}{12(\alpha+2)}} \leq N^{\gamma}$. In this case, the second term above is dominated by the first term because $\Psi(N, y)N^{o(1)} = N^{\alpha}$, and the proof concludes.

Remark 5.2 Following the arguments in Section 3.3, the main bottleneck in improving Theorem 1.1 lies in the estimation of U_0 in (3.2). Note that the integers in the set $\mathcal{A}_0(N, I)$ can be written as products of the form

$$(x - \text{smooth}) \times (y - \text{rough}).$$

This structure suggests that one might attempt to adapt the approach used in the proof of Theorem 1.4. However, as one may anticipate, complications arise for the integers whose x-smooth parts are small.

Remark 5.3 Consider the classical function $r_0(n)$, the characteristic function of integers that are sums of two squares. It is well-known (see [17, p. 98, Equation (4.90)], for instance) that

$$\sum_{n \leq N} r_0(n) \ll \frac{N}{(\log N)^{1/2}}.$$

Following the argument used in the proof of Theorem 1.1, one can easily deduce that

$$|S_{r_0,\chi,P}| \ll \frac{N}{(\log N)^{1/2}} \cdot \frac{\log\log R}{\log R}, \tag{5.5}$$

where R and ε be as in (1.4), and the implied constant in (5.5) may depend on d and ε.

Moreover, the same saving compared to the trivial estimate likely holds for many other multiplicative functions, *supported sparsely* on the integers and taking values in the intervals $[0, 1]$.

Acknowledgments The author is grateful to Igor E. Shparlinski for suggesting this project, and to Alina Ostafe and Igor E. Shparlinski for their valuable support and suggestions at various stages of this work. The author also sincerely thanks the referee for a careful reading of the manuscript and for many helpful suggestions, and thanks Jitendra Bajpai and Simon L. Rydin Myerson for helpful comments.

References

[1] M. Ayad, *Points S-entiers des courbes elliptiques*. Manuscripta Math. **76**(1992), nos. 3–4, 305–324.
[2] S. Bhakta, D. Loughran, S. L. Rydin Myerson, and M. Nakahara, *The elliptic sieve and Brauer groups*. Proc. Lond. Math. Soc. (3) **126**(2023), 1884–1922.
[3] S. Bhakta and I. E. Shparlinski, *On the correlations between character sums of division polynomials under shifts*. Ramanujan J. **68**(2025), 114.
[4] A. Granville, *Smooth numbers: Computational number theory and beyond*. In: J. P. Buhler and P. Stevenhagen (eds.), *Algorithmic number theory: Lattices, number fields, curves, and cryptography*, *Mathematical Sciences Research Institute Publications*, 44, Cambridge UniversityPress, Cambridge, 2008.
[5] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Oxford University Press, Oxford, 1979.

https://doi.org/10.4153/S000843952610191X Published online by Cambridge University Press

[6] A. J. Harper, *Minor arcs, mean values, and restriction theory for exponential sums over smooth numbers*. Compos. Math. **152**(2016), 1121–1158.
[7] A. Hildebrand and G. Tenenbaum, *On integers free of large prime factors*. Trans. Amer. Math. Soc. **296**(1986), 265–290.
[8] A. Hildebrand and G. Tenenbaum, *Integers without large prime factors*. J. de Théorie des Nombres de Bordeaux **5**(1993), 411–484.
[9] H. Iwaniec and E. Kowalski, *Analytic number theory*, American Mathematical Society, Providence, RI, 2004.
[10] M. Korolev and I. E. Shparlinski, *Sums of algebraic trace functions twisted by arithmetic functions*. Pacif. J. Math. **304**(2020), 505–522.
[11] A. P. Mangerel, *Divisor-bounded multiplicative functions in short intervals*. Res. Math. Sci. **10**(2023), 12.
[12] X. Shao, I. E. Shparlinski, and L. P. Wijaya, *Sums of Kloosterman sums over square-free and smooth integers*. Bull. Aust. Math. Soc. (2025), 1–13.
[13] I. E. Shparlinski and K. E. Stange, *Character sums with division polynomials*. Can. Math. Bull. **55**(2012), 850–857.
[14] J. H. Silverman, *p-adic properties of division polynomials and elliptic divisibility sequences*. Math. Annalen **332**(2005), 443–471.
[15] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, 106, Springer, Dordrecht, 2009.
[16] Y.-C. Sun, *On divisor bounded multiplicative functions in short intervals*. Preprint, 2024. https://arxiv.org/abs/2401.08432
[17] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*. 3rd ed., Graduate Studies in Mathematics, 163, American Mathematical Society, Providence, RI, 2015.
[18] M. Verzobio, *A recurrence relation for elliptic divisibility sequences*. Riv. Math. Univ. Parma (N.S.) **13**(2022), no. 1, 223–242.

UNSW Sydney, Australia
e-mail: subham.bhakta@unsw.edu.au

https://doi.org/10.4153/S000843952610191X Published online by Cambridge University Press