

**RESEARCH ARTICLE**

# On Artin's conjecture on average and short character sums

Oleksiy Klurman<sup>1</sup> | Igor E. Shparlinski<sup>2</sup>  | Joni Teräväinen<sup>3</sup><sup>1</sup>School of Mathematics, University of Bristol, Bristol, UK<sup>2</sup>School of Mathematics and Statistics, University of New South Wales, Sydney, Australia<sup>3</sup>Department of Mathematics and Statistics, University of Turku, Turku, Finland**Correspondence**

Igor E. Shparlinski, School of Mathematics and Statistics, University of New South Wales, Sydney, NSW 2052, Australia.

Email: [igor.shparlinski@unsw.edu.au](mailto:igor.shparlinski@unsw.edu.au)**Funding information**

Australian Research Council, Grant/Award Numbers: DP230100530, DP230100534; Knut and Alice Wallenberg Fellowship; European Union's Horizon Europe Research and Innovation Programme under Marie Skłodowska-Curie, Grant/Award Number: 101058904; Academy of Finland, Grant/Award Number: 362303

**Abstract**

Let  $N_a(x)$  denote the number of primes up to  $x$  for which the integer  $a$  is a primitive root. We show that  $N_a(x)$  satisfies the asymptotic predicted by Artin's conjecture for almost all  $1 \leq a \leq \exp((\log \log x)^2)$ . This improves on a result of Stephens (1969). A key ingredient in the proof is a new short character sum estimate over the integers, improving on the range of a result of Garaev (2006).

**MSC 2020**

11A07, 11L40, 11N25 (primary)

## 1 | INTRODUCTION

### 1.1 | Background and set-up

Artin's famous conjecture on primitive roots asserts that any integer  $a \neq -1$ , which is not a perfect square, is a primitive root for a set of primes of positive relative density, with the density depending

on the arithmetic structure of  $a$ . This has been established conditionally under the generalised Riemann hypothesis (GRH) for Dedekind zeta functions of certain number fields, in a celebrated work of Hooley [5].

More precisely, if  $a$  is an integer that is not  $-1$  or a perfect square, let  $b \in \mathbb{N}$  be the squarefree part of  $a$  and let  $h \geq 1$  be the largest integer such that  $a$  is a perfect  $h$ th power. We also define

$$A(h) = \prod_{\ell|h} \left(1 - \frac{1}{\ell-1}\right) \prod_{\ell \nmid h} \left(1 - \frac{1}{\ell(\ell-1)}\right),$$

where  $\ell$  runs over primes. Denoting

$$N_a(x) = \#\{p \leq x : a \text{ is a primitive root modulo } p\},$$

by a result of Hooley [5, Section 7] under GRH we have

- if  $b \not\equiv 1 \pmod{4}$ , then

$$N_a(x) = A(h)\pi(x) + O_a\left(\frac{x \log \log x}{(\log x)^2}\right);$$

- if  $b \equiv 1 \pmod{4}$ , then

$$N_a(x) = A(h) \left(1 - \mu(b) \prod_{\substack{\ell|h \\ \ell|b}} \frac{1}{\ell-2} \prod_{\substack{\ell \nmid h \\ \ell|b}} \frac{1}{\ell^2 - \ell - 1}\right) \pi(x) + O_a\left(\frac{x \log \log x}{(\log x)^2}\right),$$

where, as usual,  $\mu(b)$  denotes the Möbius function,  $\pi(x)$  is the prime counting function, and  $O_\rho$  and  $\ll_\rho$  indicates that the implied constants may depend on the parameter  $\rho$ ; see Section 1.3 for an exact definition. We also refer to the exhaustive survey of Moree [10] for a wide variety of other results and references; see also [7, 8, 13] for more recent developments and further references.

In another direction, we mention the celebrated result of Heath-Brown [4], improving on a beautiful work of Gupta and Murty [3], which shows that Artin's conjecture holds for all but possibly two primes. Heath-Brown also shows that

$$\#\{a \leq y : \limsup_{x \rightarrow \infty} N_a(x) < \infty\} \ll (\log y)^2.$$

However, the methods of [3, 4] do not yield an asymptotic for  $N_a(x)$  for almost all  $a$  (and in fact the lower bounds are off from the conjectured magnitude by a factor of  $(\log x)^{-1}$ , since all the primes  $p$  detected are such that  $(p-1)/K$  has at most two prime factors for some small positive integer  $K$ ).

Since an unconditional proof of Artin's conjecture still seems to be out of reach, it is interesting to study  $N_a(x)$  for almost all  $a$  (with an ultimate goal of reducing the amount of averaging). We observe that for a 'typical' integer  $a$ , we have  $h = 1$ , while  $b$  is quite large, making the main terms

in the above asymptotic formulas for  $N_a(x)$  to be  $A\pi(x)$  in both cases, with

$$A = A(1) = \prod_{\ell} \left( 1 - \frac{1}{\ell(\ell-1)} \right) = 0.373955 \dots, \quad (1.1)$$

which is called *Artin's constant*.

In particular, Stephens [14], improving on a previous result of Goldfeld [2], established in 1969 the following almost all result.

**Theorem A.** *Let  $D \geq 1$ , and let  $x, y \geq 3$  satisfy*

$$y \geq \exp \left( 6(\log x \log \log x)^{1/2} \right). \quad (1.2)$$

*Then we have*

$$|N_a(x) - A\pi(x)| \leq \frac{\pi(x)}{(\log x)^D} \quad (1.3)$$

*for all but  $O_D(y/(\log x)^D)$  integers  $a \in [-y, y]$ .*

In this paper, we augment the ideas of Stephens [14] with arguments involving short character sums and the anatomy of integers and reduce quite significantly the range (1.2) of  $y$  for which (1.3) holds.

**Theorem 1.1.** *Let  $D \geq 10$ , and let  $x, y \geq 100$  satisfy*

$$y \geq \exp \left( \frac{60(D+1)}{\log 2} \cdot \frac{(\log \log x)^2}{\log \log \log x} \right). \quad (1.4)$$

*Then we have*

$$|N_a(x) - A\pi(x)| \leq \frac{\pi(x)}{(\log x)^D}$$

*for all but  $O_D(y/(\log x)^D)$  integers  $a \in [-y, y]$ .*

## 1.2 | Short character sums

As in [14], our approach is based on bounds for short character sums for almost all integer moduli. However, we can obtain cancellation in significantly shorter character sums, leading to an improved range in the application to Artin's conjecture. We refer to [6, Chapter 3] for the relevant background on character sums.

**Theorem 1.2.** *Let  $x, y \geq 3$  and*

$$3 \leq \lambda \leq (\log y)/(\log \log y)^2, \quad (1.5)$$

and suppose that

$$\exp(20\lambda(\log(\lambda \log \log x))(\log \log x)) \leq y \leq x. \quad (1.6)$$

Then, for all but at most  $O(x^{0.49})$  natural numbers  $q \leq x$ , we have

$$\max_{\chi \in \mathcal{X}_q^*} \left| \sum_{1 \leq a \leq y} \chi(a) \right| \ll y/(\log y)^{\lambda \log 2 - 1}, \quad (1.7)$$

where  $\mathcal{X}_q^*$  denotes the set of all primitive Dirichlet characters modulo  $q$ .

*Remark 1.3.* It is important to note that the implied constants in Theorem 1.2 do not depend on  $\lambda$ , which we choose to grow with  $x$  in the proof of Theorem 1.1; see (3.1).

*Remark 1.4.* From the proof of Theorem 1.2 in Section 2, one can see that one could enlarge the range of  $y$  in (1.6) by replacing  $20\lambda$  with  $7.721\lambda$  there, at the cost of increasing the size of the exceptional set of natural numbers from  $O(x^{0.49})$  to  $O(x^{1-\delta})$  for some small  $\delta > 0$ . On the other hand, one can decrease the size of the exceptional set of natural numbers to  $O(x^{c/K})$  (with an absolute constant  $c > 0$ ) by replacing  $20\lambda$  with  $K\lambda$  in (1.6) for  $K$  a large constant. For our application, it is helpful to have an exponent smaller than  $1/2$ .

We remark that a result of Garaev [1, Theorem 9] gives a power-saving bound for the character sums in (1.7) for almost all moduli  $q \leq x$ , provided that

$$y = \exp\left(c\sqrt{\log x}\right)$$

for a suitable constant  $c > 0$ . In fact, [1, Theorem 10] gives more flexibility for larger values of  $y$ . Here we are mostly interested in small values of  $y$ , which are not covered by the results of [1].

### 1.3 | Notation

We recall that the notations  $U = O(V)$ ,  $U \ll V$  and  $V \gg U$  are equivalent to  $|U| \leq cV$  for some positive constant  $c$ , which we take to be absolute unless indicated with subindices. For example,  $O_D$  and  $\ll_D$  both mean the implied constant may depend on the parameter  $D$ . We use  $U \asymp V$  as a shorthand for  $U \ll V \ll U$ .

The letter  $p$ , with or without subscripts, always denotes a prime number.

We use  $\sum_{r \pmod{q}}^*$  to denote summation over the primitive residue classes modulo  $q$ .

We denote by  $\mathcal{X}_q$  the set of Dirichlet characters modulo  $q$  and by  $\mathcal{X}_q^*$  the set of primitive Dirichlet characters modulo  $q$ .

We use the standard notation  $\mu(n)$ ,  $\varphi(n)$  and  $\Omega(n)$  for the Möbius function, the Euler function, and the number of prime divisors function (counted with multiplicities), respectively. Furthermore,  $\pi(x)$  denotes the number of primes  $p \leq x$ .

Finally, we use  $\#S$  to denote the cardinality of a finite set  $S$ .

## 2 | PROOF OF THE CHARACTER SUM BOUND

### 2.1 | Preliminaries

In this section, we prove Theorem 1.2. We begin with a useful estimate for the number of integers with a given number of prime factors.

**Lemma 2.1.** *Let  $x \geq 3$  and let  $m$  be a positive integer. Then we have*

(i) *for  $3 \log \log x \leq m \leq (\log x) / \log 2$ ,*

$$\frac{x}{2^m \log x} \ll \#\{n \leq x : \Omega(n) = m\} \ll \frac{x}{2^m} \log \frac{x}{2^m} + 1;$$

(ii) *for any  $m \leq (\log x) / \log 2$ ,*

$$\#\{n \leq x : \Omega(n) = m\} \gg \frac{x}{2^m \log x}.$$

*Proof.* If  $(\log x) / \log 2 - 1/10 < m \leq (\log x) / \log 2$ , then clearly

$$\{n \leq x : \Omega(n) = m\} = \{2^m\}.$$

Hence the cardinality to be estimated is equal to 1, so both bounds (i) and (ii) are trivial.

For  $3 \log \log x \leq m \leq (\log x) / \log 2 - 1/10$ , the bound (i), and thus also (ii) in this range, follows from a result of Nicolas [12] (see also [15, Part II, Equation (6.30) and Exercise 217], which in fact gives an asymptotic formula

$$\#\{n \leq x : \Omega(n) = m\} = (C + O((\log y)^{-\eta}))y \log y, \tag{2.1}$$

where  $y = x/2^m$ ,  $\eta > 0$  is some absolute constant, and the constant  $C = 0.3786 \dots$  is given by an explicit Euler product (note that  $y \geq 2^{1/10} > 1$ ). Indeed, we note that (2.1) always gives the desired upper bound (even in the regime when  $y \ll 1$ ). To extract a lower bound from (2.1) we need to assume that  $y \rightarrow \infty$ . However since  $2^m \in \{n \leq x : \Omega(n) = m\}$  in the above range of  $m$ , for  $y < \log \log x$  the lower bound is trivial, so we indeed get (i).

Finally, to establish the lower bound (ii) for  $m < 3 \log \log x$ , we note that in this range

$$\begin{aligned} \#\{n \leq x : \Omega(n) = m\} &\geq \#\{2^{m-1}p : p \leq x/2^{m-1}\} \\ &= \pi(x/2^{m-1}) \gg \frac{x}{2^m \log(x/2^m)} \gg \frac{x}{2^m \log x}, \end{aligned}$$

which concludes the proof. □

*Remark 2.2.* We remark that the coefficient 3 in Lemma 2.1(i) can be replaced with  $2 + \delta$  with any fixed  $\delta > 0$ .

## 2.2 | Proof of Theorem 1.2

We may assume that  $x$  is larger than any given absolute constant. We may also assume that  $y \leq x^{0.34}$ , say, since otherwise the result follows from the Burgess bound [6, Theorem 12.4]. By applying Garaev's result [1, Theorem 10] with  $\delta = 1/10$ , we may further assume that

$$y \leq \exp((\log x)^{0.51}), \quad (2.2)$$

say.

For  $w \in \mathbb{N}$ , let

$$\mathcal{A}_w(y) = \{a \leq y : \Omega(a) = w\}.$$

For  $k \in \mathbb{N}$ , we also denote

$$S_k(w, x, y) = \sum_{q \leq x} \max_{\chi \in \mathcal{X}_q^*} \left| \sum_{a \in \mathcal{A}_w(y)} \chi(a) \right|^{2k}.$$

We first give a bound for  $S_k(w, x, y)$ . By replacing the maximum with summation over all primitive characters and applying the multiplicative large sieve [6, Theorem 7.13], we have

$$S_k(w, x, y) \leq \sum_{q \leq x} \sum_{\chi \in \mathcal{X}_q^*} \left| \sum_{a \in \mathcal{A}_w(y)} \chi(a) \right|^{2k} \ll (x^2 + y^k) T_k(w, y), \quad (2.3)$$

where

$$T_k(w, y) = \sum_{m \leq y^k} r_k(m, w, y)^2$$

is the number of solutions to the equation

$$a_1 \cdots a_k = b_1 \cdots b_k, \quad a_1, b_1, \dots, a_k, b_k \in \mathcal{A}_w(y).$$

By considering the number of choices for  $(a_1, \dots, a_k)$  for a given  $k$ -tuple  $(b_1, \dots, b_k) \in \mathcal{A}_w(y)^k$ , we have

$$T_k(w, y) \leq \binom{kw}{\underbrace{w, \dots, w}_{k \text{ times}}} (\#\mathcal{A}_w(y))^k,$$

since each choice of  $a_1, \dots, a_k$  corresponds to partitioning the multi-set of the  $kw$  (not necessary distinct) primes dividing  $b_1 \cdots b_k$  into  $k$  groups of  $w$  primes. Using the elementary inequalities

$$(n/e)^n \leq n! \leq e^2(n/e)^{n+1},$$

we see that

$$\binom{kw}{\underbrace{w, \dots, w}_{k \text{ times}}} = \frac{(kw)!}{(w!)^k} \leq e^2 \frac{(kw/e)^{kw+1}}{(w/e)^{kw}} = e w k^{kw+1}.$$

Therefore

$$T_k(w, y) \ll w k^{kw+1} (\#\mathcal{A}_w(y))^k,$$

which after the substitution in (2.3) implies

$$S_k(w, x, y) \ll w k^{kw+1} (x^2 + y^k) (\#\mathcal{A}_w(y))^k. \tag{2.4}$$

We now define the integer  $k \geq 1$  by the inequalities

$$y^k < x^2 \leq y^{k+1}. \tag{2.5}$$

For a given  $\delta > 0$ , we consider the set

$$\mathcal{E}(w, x, y; \delta) = \left\{ q \leq x : \max_{\chi \in \mathcal{X}_q^*} \left| \sum_{a \in \mathcal{A}_w(y)} \chi(a) \right| \geq \delta \cdot \#\mathcal{A}_w(y) \right\}.$$

From (2.4) and our choice of  $k$ , we derive

$$\begin{aligned} \#\mathcal{E}(w, x, y; \delta) &\ll (\#\mathcal{A}_w(y)\delta)^{-2k} y^{k+1} (\#\mathcal{A}_w(y))^k w k^{kw+1} \\ &\ll k w y \left( \frac{k^w y}{\delta^2 \#\mathcal{A}_w(y)} \right)^k. \end{aligned} \tag{2.6}$$

We impose the restriction

$$w \leq \lambda \log \log y. \tag{2.7}$$

Note that by the assumption (1.5) on  $\lambda$  we have  $w \leq (\log y)/(\log \log y)$ . By Lemma 2.1(ii), under the condition (2.7) we have

$$\#\mathcal{A}_w(y) \gg \frac{y}{2^w \log y}.$$

Hence, taking  $\delta = (\log y)^{-\lambda \log 2}$  in the bound (2.6), we obtain

$$\#\mathcal{E}(w, x, y; (\log y)^{-\lambda \log 2}) \ll k w y (k^w (\log y)^{4\lambda \log 2})^k, \tag{2.8}$$

Next, recalling the choice of  $k$  from (2.5), we see that

$$2 \frac{\log x}{\log y} - 1 \leq k < 2 \frac{\log x}{\log y}. \tag{2.9}$$

Hence, we derive from (2.8) that

$$\#\mathcal{E}(w, x, y; (\log y)^{-\lambda \log 2}) \ll x^\xi,$$

where, using the upper bound on  $k$  from (2.9), we conclude

$$\xi = 2 \frac{w \log \log x + 4\lambda(\log 2)(\log \log y)}{\log y} + O\left(\frac{\log(kwy)}{\log x}\right).$$

Recalling our assumptions (1.5), (2.2), (2.7) and the estimate (2.9) again, we see that

$$\frac{\log(kwy)}{\log x} \ll (\log x)^{-0.48}.$$

Now, from (1.5), (2.7), and then also from (1.6), we derive

$$\begin{aligned} \xi &\leq 2 \frac{w \log \log x + 4\lambda(\log 2)(\log \log y)}{\log y} + O((\log x)^{-0.48}) \\ &\leq 2\lambda \frac{(\log \log x)(\log \log y)}{\log y} + O((\log x)^{-0.48} + (\log \log y)^{-1}) \\ &\leq 2\lambda \frac{\log(20\lambda \log(\lambda \log \log x)) + \log \log \log x}{20\lambda \log(\lambda \log \log x)} \\ &\quad + O((\log x)^{-0.48} + (\log \log y)^{-1}) \\ &\leq \frac{2 \log(20\lambda)}{20 \log \lambda} + \frac{2 \log \log(\lambda \log \log x)}{20 \log(\lambda \log \log x)} + \frac{2}{20} + \frac{1}{1000} \\ &\leq \frac{2 \log 60}{20 \log 3} + \frac{1}{1000} + \frac{2}{20} + \frac{1}{1000} \\ &\leq 0.485, \end{aligned}$$

provided that  $x$  (and hence  $y$ ) is large enough in absolute terms. This implies that

$$\#\mathcal{E}(w, x, y; (\log y)^{-\lambda \log 2}) \leq x^{0.485} \tag{2.10}$$

for each  $w$  satisfying (2.7) and any  $x$  that is large enough in absolute terms.

It now remains to estimate the quantity

$$F_\lambda(y) = \#\{a \leq y : \Omega(a) > \lambda \log \log y\}.$$

Using Lemma 2.1(i), which applies since by (1.5), we have  $\lambda \geq 3$ , we derive

$$\begin{aligned} F_\lambda(y) &\leq \sum_{\lambda \log \log y < m \leq (\log y)/\log 2} \#\{a \leq y : \Omega(a) = m\} \\ &\ll y \log y \sum_{m > \lambda \log \log y} 2^{-m} + \log y \\ &\ll y(\log y)^{1-\lambda \log 2} + \log y \ll y(\log y)^{1-\lambda \log 2}, \end{aligned} \tag{2.11}$$

since under (1.5) we clearly have the bound  $(\log y)^{\lambda \log 2} = y^{o(1)}$ .

Let

$$\mathcal{E}(x, y) = \bigcup_{0 \leq w \leq \lambda \log \log y} \mathcal{E}(w, x, y; (\log y)^{-\lambda \log 2}),$$

which by (2.10) and (1.5) is of cardinality

$$\begin{aligned} \#\mathcal{E}(x, y) &\leq x^{0.485} \lambda \log \log y \\ &\leq x^{0.485} \frac{\log y}{\log \log y} \ll x^{0.49}. \end{aligned}$$

Then, for any natural numbers  $w \leq \lambda \log \log y$  and  $q \leq x$  with  $q \notin \mathcal{E}(x, y)$ , we have

$$\max_{\chi \in \mathcal{X}_q^*} \left| \sum_{a \in \mathcal{A}_w(y)} \chi(a) \right| \ll y / (\log y)^{\lambda \log 2}. \tag{2.12}$$

Writing

$$\left| \sum_{a \leq y} \chi(a) \right| \leq \sum_{0 \leq w \leq \lambda \log \log y} \left| \sum_{a \in \mathcal{A}_w(y)} \chi(a) \right| + F_\lambda(y)$$

and using the bounds (2.11) and (2.12), and the assumed upper bound in (1.5) for  $\lambda$ , we conclude the proof.

### 3 | PROOF OF THEOREM 1.1

#### 3.1 | Moments of $N_a(x)$

The main task in this section is to prove the following second moment estimate.

**Proposition 3.1.** *Let the assumptions be as in Theorem 1.1. Then we have*

$$\sum_{|a| \leq y} |N_a(x) - A\pi(x)|^2 \ll_D y \frac{\pi(x)^2}{(\log x)^{3D}}.$$

The deduction of Theorem 1.1 from this is immediate via Chebyshev's inequality. For the proof of Proposition 3.1, we establish the following mean value estimate.

**Proposition 3.2.** *Let the assumptions be as in Theorem 1.1. Then we have*

$$\sum_{|a| \leq y} N_a(x) = 2Ay\pi(x) + O_D \left( y \frac{\pi(x)}{(\log x)^{3D}} \right).$$

*Proof.* Let us fix some  $D > 10$ . We may assume that  $x, y$  are larger than any given absolute constant. We are going to use Theorem 1.2 with

$$\lambda = \frac{3D + 2}{\log 2} \cdot \frac{\log \log(x^2)}{\log \log y} + \frac{1}{\log 2}. \tag{3.1}$$

Note that by (1.4) the condition (1.5) holds. Also note that for this choice of  $\lambda$  we have

$$y > \exp(20\lambda \log(\lambda(\log \log(x^2))) \log \log(x^2)).$$

Now, by Theorem 1.2, we see that there is a set  $\mathcal{E}$  of size  $\#\mathcal{E} \ll x^{1/2}$  (say) such that for all primes  $p \in [1, x] \setminus \mathcal{E}$  we have

$$\max_{\chi \in \mathcal{X}_p^*} \left| \sum_{1 \leq a \leq y} \chi(a) \right| \leq y/(\log x)^{3D+2}. \tag{3.2}$$

Let

$$\mathcal{P} = \{p \leq x\} \setminus \mathcal{E}.$$

Let us denote by  $\mathcal{G}_p$  the set of primitive roots modulo  $p$ . We can write

$$\begin{aligned} \sum_{-y \leq a \leq y} N_a(x) &= \sum_{-y \leq a \leq y} \sum_{\substack{p \leq x \\ a \in \mathcal{G}_p}} 1 = \sum_{p \leq x} \sum_{\substack{-y \leq a \leq y \\ a \in \mathcal{G}_p}} 1. \\ &= \sum_{p \in \mathcal{P}} \sum_{\substack{-y \leq a \leq y \\ a \in \mathcal{G}_p}} 1 + O(x^{1/2}y). \end{aligned} \tag{3.3}$$

Using the standard inclusion-exclusion argument to detect primitive roots (see, for example, [9, Problem 5.14; 11, Proposition 2.2]), we see that for any integer  $a$  we have

$$\frac{\varphi(p-1)}{p-1} \sum_{t|p-1} \frac{\mu(t)}{\varphi(t)} \sum_{\substack{\chi \in \mathcal{X}_p \\ \text{ord}(\chi)=t}} \chi(a) = \begin{cases} 1 & \text{if } a \in \mathcal{G}_p, \\ 0, & \text{otherwise,} \end{cases} \tag{3.4}$$

where  $\text{ord}(\chi)$  denotes the order of  $\chi$  in the group of characters  $\mathcal{X}_p$ .

Separating the contribution of the principal character, corresponding to  $t = 1$  in (3.4), we arrive at

$$\sum_{p \in \mathcal{P}} \sum_{\substack{-y \leq a \leq y \\ a \in \mathcal{G}_p}} 1 = \#([-y, y] \cap \mathbb{Z}) \cdot \sum_{p \in \mathcal{P}} \frac{\varphi(p-1)}{p-1} + O(E + y \log y) \tag{3.5}$$

with

$$E = \sum_{p \in \mathcal{P}} \sum_{\substack{t|p-1 \\ t > 1}} \frac{|\mu(t)|}{\varphi(t)} \sum_{\substack{\chi \in \mathcal{X}_p^* \\ \text{ord}(\chi)=t}} \left| \sum_{-y \leq a \leq y} \chi(a) \right|,$$

where the  $O(y \log y)$  term comes from the contribution

$$\sum_{p \leq y} (2y/p + O(1)) = 2y \sum_{p \leq y} 1/p + O(1) \ll y \log y$$

of the principal characters modulo  $p$  on values  $a \equiv 0 \pmod{p}$ .

First, we note that

$$\sum_{p \in \mathcal{P}} \frac{\varphi(p-1)}{p-1} = \sum_{p \leq x} \frac{\varphi(p-1)}{p} + O(x^{1/2}).$$

Since by [14, Lemma 1] we have

$$\sum_{p \leq x} \frac{\varphi(p-1)}{p} = A\pi(x) + O_D\left(\frac{\pi(x)}{(\log x)^{3D}}\right), \tag{3.6}$$

with  $A$  given by (1.1), we can rewrite (3.5) as

$$\sum_{p \in \mathcal{P}} \sum_{\substack{-y \leq a \leq y \\ a \in \mathcal{G}_p}} 1 = 2Ay\pi(x) + O_D\left(\frac{y\pi(x)}{(\log x)^{3D}} + E\right). \tag{3.7}$$

Thus it remains to estimate  $E$ .

Using (3.2), we bound

$$E \ll_D \frac{y}{(\log x)^{3D+2}} \sum_{p \in \mathcal{P}} \sum_{\substack{t|p-1 \\ t>1}} \frac{|\mu(t)|}{\varphi(t)} \sum_{\substack{\chi \in \mathcal{X}_p^* \\ \text{ord}(\chi)=t}} 1. \tag{3.8}$$

Since the group  $\mathcal{X}_p$  is cyclic of order  $p-1$ , for each divisor  $t | p-1$  there are  $\varphi(t)$  characters  $\chi \in \mathcal{X}_p^*$  with  $\text{ord}(\chi) = t$ . Therefore we have

$$\sum_{\substack{t|p-1 \\ t>1}} \frac{|\mu(t)|}{\varphi(t)} \sum_{\substack{\chi \in \mathcal{X}_p^* \\ \text{ord}(\chi)=t}} 1 = \sum_{\substack{t|p-1 \\ t>1}} |\mu(t)| = 2^{\omega(p-1)} - 1.$$

Recalling (3.8), we see that

$$E \ll_D \frac{y}{(\log x)^{3D+1}} \sum_{p \leq x} 2^{\omega(p-1)} \ll \frac{yx}{(\log x)^{3D+2}} \ll \frac{y\pi(x)}{(\log x)^{3D}}$$

by the Titchmarsh divisor estimate

$$\sum_{p \leq x} 2^{\omega(p-1)} \ll x \tag{3.9}$$

(see [16]) and the prime number theorem. This together with (3.3) and (3.7) concludes the proof. □

### 3.2 | Proof of Proposition 3.1

Let  $D \geq 10$  be fixed. Expanding out the square and applying Proposition 3.2, we have

$$\begin{aligned} & \sum_{-y \leq a \leq y} |N_a(x) - A\pi(x)|^2 \\ &= \sum_{-y \leq a \leq y} N_a(x)^2 - 2A\pi(x) \sum_{-y \leq a \leq y} N_a(x) + A^2\pi(x)^2 \sum_{-y \leq a \leq y} 1 \\ &= \sum_{-y \leq a \leq y} N_a(x)^2 - 2A^2y\pi(x)^2 + O_D\left(\frac{y\pi(x)^2}{(\log x)^{3D}}\right). \end{aligned}$$

Let

$$Q = \{(p_1, p_2) \in [1, x]^2 : (\log x)^{3D+2} \leq p_1, p_2 \leq x, p_1 \neq p_2, p_1, p_2, p_1p_2 \notin \mathcal{E}\},$$

where  $\mathcal{E}$  is the set of natural numbers  $q \leq x^2$  for which

$$\max_{\chi \in \mathcal{X}_q^*} \left| \sum_{1 \leq a \leq y} \chi(a) \right| > \frac{y}{(\log x)^{3D+2}}.$$

We apply Theorem 1.2 with  $\lambda$  as in (3.1). Note that this is an admissible choice, since we have  $y > \exp(20\lambda \log(\lambda(\log \log(x^2)))(\log \log(x^2)))$ . Now we conclude that

$$\#\mathcal{E} \ll x^{2 \cdot 0.49} = x^{0.98}.$$

Hence we have

$$\begin{aligned} \#Q &= \#\{(p_1, p_2) \in [1, x]^2 : (\log x)^{3D+2} \leq p_1, p_2 \leq x, p_1 \neq p_2\} \\ &\quad + O(x^{1.98}). \end{aligned}$$

Again denoting by  $\mathcal{G}_p$  the set of primitive roots modulo  $p$ , we have

$$\sum_{-y \leq a \leq y} N_a(x)^2 = \sum_{-y \leq a \leq y} \sum_{\substack{p_1, p_2 \leq x \\ a \in \mathcal{G}_{p_1} \\ a \in \mathcal{G}_{p_2}}} 1 = \sum_{\substack{p_1, p_2 \leq x \\ (p_1, p_2) \in Q}} \sum_{\substack{-y \leq a \leq y \\ a \in \mathcal{G}_{p_1} \\ a \in \mathcal{G}_{p_2}}} 1 + O(yx^{1.98}).$$

Using (3.4), the main term in the above equation becomes

$$\begin{aligned} S &= \sum_{\substack{p_1, p_2 \leq x \\ (p_1, p_2) \in Q}} \frac{\varphi(p_1 - 1)\varphi(p_2 - 1)}{(p_1 - 1)(p_2 - 1)} \sum_{\substack{t_1 | p_1 - 1 \\ t_2 | p_2 - 1}} \frac{\mu(t_1)\mu(t_2)}{\varphi(t_1)\varphi(t_2)} \\ &\quad \sum_{\substack{\chi_1 \in \mathcal{X}_{p_1} \\ \text{ord}(\chi_1) = t_1}} \sum_{\substack{\chi_2 \in \mathcal{X}_{p_2} \\ \text{ord}(\chi_2) = t_2}} \sum_{-y \leq a \leq y} \chi_1 \chi_2(a), \end{aligned}$$

where  $\chi_1\chi_2(a) = \chi_1(a)\chi_2(a)$  is a now a character modulo  $p_1p_2$  (since  $p_1 \neq p_2$ ). Let us split this as

$$S = \sum_{\substack{p_1, p_2 \leq x \\ (p_1, p_2) \in \mathcal{Q}}} \frac{\varphi(p_1 - 1)\varphi(p_2 - 1)}{(p_1 - 1)(p_2 - 1)} \sum_{\substack{-y \leq a \leq y \\ \gcd(a, p_1 p_2) = 1}} 1 + S_1 + S_2 + S_3,$$

where  $S_1$  corresponds to those terms with  $t_1 = 1, t_2 > 1$ ,  $S_2$  corresponds to those terms with  $t_1 > 1, t_2 = 1$ , and  $S_3$  corresponds to those terms with  $t_1, t_2 > 1$ . By completing the sum over  $(p_1, p_2) \in \mathcal{Q}$  to all pairs  $(p_1, p_2) \in [1, x]^2$  and applying (3.6), we see that

$$\begin{aligned} S &= 2y \left( \sum_{p \leq x} \frac{\varphi(p-1)}{p-1} \left( 1 - \frac{1}{p} \right) \right)^2 \\ &\quad + S_1 + S_2 + S_3 + O_D \left( \frac{yx^2}{(\log x)^{3D+2}} \right) \\ &= 2A^2 y \pi(x)^2 + S_1 + S_2 + S_3 + O_D \left( \frac{y\pi(x)^2}{(\log x)^{3D}} \right). \end{aligned} \tag{3.10}$$

The sums  $S_1$  and  $S_2$  are bounded symmetrically; let us bound  $S_1$ . Note that if  $\chi_1$  is a non-principal character (mod  $p_1$ ) and  $\chi_0$  is the principal character (mod  $p_2$ ), by the assumption  $(p_1, p_2) \in \mathcal{Q}$  (which implies  $p_1 \notin \mathcal{E}$  and  $p_2 \geq (\log x)^{3D+2}$ ), we have

$$\left| \sum_{-y \leq a \leq y} \chi_1 \chi_0(a) \right| = \left| \sum_{-y \leq a \leq y} \chi_1(a) \right| + O \left( \frac{y}{p_2} \right) \ll_D \frac{y}{(\log x)^{3D+2}}.$$

Hence, we have

$$\begin{aligned} S_1 &\ll_D \frac{y}{(\log x)^{3D+2}} \sum_{p_1, p_2 \leq x} \sum_{t_1 | p_1 - 1} \frac{|\mu(t_1)|}{\varphi(t_1)} \sum_{\substack{\chi_1 \in \mathcal{X}_{p_1} \\ \text{ord}(\chi_1) = t_1}} 1 \\ &\ll \frac{y\pi(x)}{(\log x)^{3D+2}} \sum_{p_1 \leq x} 2^{\omega(p_1-1)} \\ &\ll \frac{y\pi(x)^2}{(\log x)^{3D}} \end{aligned}$$

by the Titchmarsh divisor bound (3.9).

We are left with bounding  $S_3$ . Since in this sum  $\chi_1\chi_2$  is a primitive character modulo  $p_1p_2 \leq x^2$  with  $p_1p_2 \notin \mathcal{E}$ , we have

$$S_3 \ll_D \frac{y}{(\log x)^{3D+2}} \sum_{p_1, p_2 \leq x} \sum_{\substack{t_1 | p_1 - 1 \\ t_2 | p_2 - 1}} \frac{|\mu(t_1)| |\mu(t_2)|}{\varphi(t_1)\varphi(t_2)} \sum_{\substack{\chi_1 \in \mathcal{X}_{p_1} \\ \text{ord}(\chi_1) = t_1 \\ \chi_2 \in \mathcal{X}_{p_2} \\ \text{ord}(\chi_2) = t_2}} 1$$

$$\begin{aligned} &\ll \frac{y}{(\log x)^{3D+2}} \left( \sum_{p \leq x} 2^{\omega(p-1)} \right)^2 \\ &\ll \frac{y\pi(x)^2}{(\log x)^{3D}} \end{aligned}$$

by the Titchmarsh divisor bound (3.9). Now the claim follows by collecting the bounds for  $S_1, S_2, S_3$  and recalling (3.10).

This concludes the proof of Proposition 3.1, which as we have mentioned, is enough to conclude the proof of Theorem 1.1.

## ACKNOWLEDGEMENTS

The authors thank Kaisa Matomäki for a helpful discussion on character sums and the referee for the careful reading of the manuscript. During the preparation of this work I.S. was supported by the Australian Research Council Grants DP230100530 and DP230100534 and by a Knut and Alice Wallenberg Fellowship. J.T. was supported by European Union's Horizon Europe research and innovation programme under Marie Skłodowska-Curie grant agreement no. 101058904, and Academy of Finland grant no. 362303. This work started while the authors were visiting Institut Mittag-Leffler, Sweden, during the programme 'Analytic Number Theory' in January–April 2024, whose hospitality and support are gratefully acknowledged.

Open access publishing facilitated by University of New South Wales, as part of the Wiley - University of New South Wales agreement via the Council of Australian University Librarians.

## JOURNAL INFORMATION

The *Bulletin of the London Mathematical Society* is wholly owned and managed by the London Mathematical Society, a not-for-profit Charity registered with the UK Charity Commission. All surplus income from its publishing programme is used to support mathematicians and mathematics research in the form of research grants, conference grants, prizes, initiatives for early career researchers and the promotion of mathematics.

## ORCID

Igor E. Shparlinski  <https://orcid.org/0000-0002-5246-9391>

## REFERENCES

1. M. Z. Garaev, *Character sums in short intervals and the multiplication table modulo a large prime*, *Monatsh. Math.* **143** (2006), 127–138.
2. M. Goldfeld, *Artin's conjecture on the average*, *Mathematika* **15** (1968), no. 2, 223–226.
3. R. Gupta and M. R. Murty, *A remark on Artin's conjecture*, *Invent Math.* **78** (1984), 127–130.
4. D. R. Heath-Brown, *Artin's conjecture for primitive roots*, *Q. J. Math.* **37** (1986), 27–38.
5. C. Hooley, *Artin's conjecture for primitive roots*, *J. reine angew. Math.* **225** (1967), 209–220.
6. H. Iwaniec and E. Kowalski, *Analytic number theory*, American Mathematical Society, Providence, RI, 2004.
7. O. Järviniemi and A. Perucca, *Unified treatment of Artin-type problems*, *Res. Number Theory* **9** (2023), Article 9.
8. O. Järviniemi, A. Perucca, and P. Sgobba, *Unified treatment of Artin-type problems II*, *Res. Number Theory* **11** (2025), Article 42.
9. R. Lidl and H. Niederreiter, *Finite fields*, Cambridge University Press, Cambridge, 1997.
10. P. Moree, *Artin's primitive root conjecture — a survey*, *Integers* **12** (2012), 1305–1416.
11. W. Narkiewicz, *Classical problems in number theory*, Polish Sci. Publ., Warszawa, 1986.

12. J. Nicolas, *Sur la distribution des nombres entiers ayant une quantité fixée de facteurs premiers*, Acta Arith. **44** (1984), 191–200.
13. A. Perucca and I. E. Shparlinski, *Uniform bounds for the density in Artin's conjecture on primitive roots*, Bull. Lond. Math. Soc. **57** (2025), 978–991.
14. P. J. Stephens, *An average result for Artin's conjecture*, Mathematika **16** (1969), 178–188.
15. G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Graduate Studies in Mathematics, vol. 163, American Mathematical Society, Providence, RI, 2015.
16. E. C. Titchmarsh, *A divisor problem*, Rend. Circ. Mat. Palermo (2) **54** (1930), 414–429; Correction: *ibid.* **57** (1933), 478–479.