

Average r -rank Artin conjecture

by

LORENZO MENICI (Roma) and CIHAN PEHLIVAN (Istanbul)

1. Introduction. Artin's conjecture for primitive roots (1927) states that for any integer $a \neq 0, \pm 1$ which is not a perfect square there exist infinitely many prime numbers p for which a is a primitive root modulo p . In particular, Artin conjectured that the number of primes not exceeding x for which a is a primitive root, $N_a(x)$, asymptotically satisfies

$$N_a(x) \sim A(a) \operatorname{Li}(x) \quad \text{as } x \rightarrow \infty,$$

where $\operatorname{Li}(x)$ is the logarithmic integral and the positive constant $A(a)$ depends on the integer a . A breakthrough in this area was achieved by Hooley's [8] who proved Artin's conjecture under the assumption of the Generalized Riemann Hypothesis (GRH) for the Dedekind zeta function over the Kummer extension $\mathbb{Q}(a^{1/k}, \zeta_k)$ for any positive square-free integer k . Several generalizations of Artin's original conjecture were studied by many authors during the following years (for an exhaustive survey see [10]). A first unconditional result on Artin's conjecture in the 3-rank case was found by Gupta and Ram Murty [5], improved a few years later by Heath-Brown [7].

In the case of rank $r = 1$, a first study of the average behavior of $N_a(x)$ was proposed by Stephens [14] in 1969: Stephens proved that if $T > \exp(4(\log x \log \log x)^{1/2})$, then

$$(1) \quad \frac{1}{T} \sum_{a \leq T} N_a(x) = \sum_{p \leq x} \frac{\varphi(p-1)}{p-1} + O\left(\frac{x}{(\log x)^D}\right) \\ = A \operatorname{Li}(x) + O\left(\frac{x}{(\log x)^D}\right),$$

where φ is the Euler totient function, $A := \prod_p \left(1 - \frac{1}{p(p-1)}\right)$ is Artin's constant

2010 *Mathematics Subject Classification*: Primary 11R45; Secondary 11N69, 11A07, 11L40.

Key words and phrases: Artin's conjecture, primitive roots, multiple Ramanujan sum.

Received 11 August 2015; revised 13 January 2016.

Published online 22 June 2016.

and D is an arbitrary constant greater than 1. Stephens also proved that if $T > \exp(6(\log x \log \log x)^{1/2})$, then

$$(2) \quad \frac{1}{T} \sum_{a \leq T} \{N_a(x) - A \operatorname{Li}(x)\}^2 \ll \frac{x^2}{(\log x)^{D'}}$$

for any constant $D' > 2$. In 1976, Stephens refined his results with different methods [15], getting both the asymptotic bounds (1) and (2) under the weaker assumption $T > \exp(C(\log x)^{1/2})$ with C a positive constant.

For any $a \in \mathbb{N} \setminus \{0, \pm 1\}$ and $m \in \mathbb{N}$, let $N_{a,m}(x)$ be the number of primes $p \equiv 1 \pmod{m}$ not exceeding x such that $[\mathbb{F}_p^* : \langle a \pmod{p} \rangle] = m$. For $T > \exp(4(\log x \log \log x)^{1/2})$ Moree [11] showed that

$$(3) \quad \frac{1}{T} \sum_{a \leq T} N_{a,m}(x) = \sum_{\substack{p \leq x \\ p \equiv 1 \pmod{m}}} \frac{\varphi((p-1)/m)}{p-1} + O\left(\frac{x}{(\log x)^E}\right)$$

for any constant $E > 1$.

In the present work, we will discuss the average version of the r -rank Artin quasi primitive root conjecture, adapting the methods used in [14] by Stephens to the case of rank r . Let $\Gamma \subset \mathbb{Q}^*$ be a multiplicative subgroup of finite rank r . For almost all primes, namely those primes p such that for all $g \in \Gamma$ the p -adic valuation $v_p(g)$ is 0, one can consider the reduction group

$$\Gamma_p = \{g \pmod{p} : g \in \Gamma\},$$

which is a well defined subgroup of the multiplicative group \mathbb{F}_p^* . We denote by $N_{\Gamma,m}(x)$ the number of primes $p \equiv 1 \pmod{m}$ not exceeding x for which $[\mathbb{F}_p^* : \Gamma_p] = m$. It was proven by Cangelmi, Pappalardi and Susa [12, 2, 13], assuming the GRH for $\mathbb{Q}(\zeta_k, \Gamma^{1/k})$ for any natural number k , that for any $\varepsilon > 0$, if $m \leq x^{\frac{r-1}{(r+1)(4r+2)} - \varepsilon}$, then

$$N_{\Gamma,m}(x) = \left(\delta_\Gamma^m + O\left(\frac{1}{\varphi(m^{r+1})(\log x)^r}\right) \right) \operatorname{Li}(x) \quad \text{as } x \rightarrow \infty,$$

where δ_Γ^m is a rational multiple of

$$C_r = \sum_{n \geq 1} \frac{\mu(n)}{n^r \varphi(n)} = \prod_p \left(1 - \frac{1}{p^r(p-1)} \right).$$

Here we restrict ourselves to studying subgroups $\Gamma = \langle a_1, \dots, a_r \rangle$, with $a_i \in \mathbb{Z}$ for all $i = 1, \dots, r$, and we prove the following theorems:

THEOREM 1. *Suppose*

$$T^* := \min\{T_i : i = 1, \dots, r\} > \exp(4(\log x \log \log x)^{1/2})$$

and $m \leq (\log x)^D$ for an arbitrary positive constant D . Then

$$\frac{1}{T_1 \cdots T_r} \sum_{\substack{a_i \in \mathbb{Z} \\ 0 < a_i \leq T_i \\ 1 \leq i \leq r}} N_{\langle a_1, \dots, a_r \rangle, m}(x) = C_{r,m} \text{Li}(x) + O\left(\frac{x}{(\log x)^M}\right),$$

where

$$C_{r,m} := \sum_{n \geq 1} \frac{\mu(n)}{(nm)^r \varphi(nm)}$$

and $M > 1$ is arbitrarily large.

THEOREM 2. *Suppose $T^* > \exp(6(\log x \log \log x)^{1/2})$ and $m \leq (\log x)^D$ for an arbitrary positive constant D . Then*

$$\frac{1}{T_1 \cdots T_r} \sum_{\substack{a_i \in \mathbb{Z} \\ 0 < a_i \leq T_i \\ 1 \leq i < r}} \{N_{\langle a_1, \dots, a_r \rangle, m}(x) - C_{r,m} \text{Li}(x)\}^2 \ll \frac{x^2}{(\log x)^{M'}}$$

where $M' > 2$ is arbitrarily large.

Now since $\varphi(mn) = \varphi(m)\varphi(n) \text{gcd}(m, n) / \varphi(\text{gcd}(m, n))$ and $\text{gcd}(m, n)$ is a multiplicative function of n for any fixed integer m , we also have the following Euler product expansion:

$$\begin{aligned} C_{r,m} &= \frac{1}{m^r \varphi(m)} \sum_{n \geq 1} \frac{\mu(n)}{n^r \varphi(n)} \prod_{p | \text{gcd}(m, n)} \left(1 - \frac{1}{p}\right) \\ &= \frac{1}{m^r \varphi(m)} \prod_{p | m} \left[1 - \frac{1}{p^r(p-1)} \left(1 - \frac{1}{p}\right)\right] \prod_{p \nmid m} \left(1 - \frac{1}{p^r(p-1)}\right) \\ &= \frac{1}{m^{r+1}} \prod_{p | m} \left(1 - \frac{p^r}{p^{r+1} - 1}\right)^{-1} C_r. \end{aligned}$$

The results found in the present paper (see in particular (8) and Lemma 2) will lead as a side product to the asymptotic identity

$$\frac{1}{T_1 \cdots T_r} \sum_{\substack{a_i \in \mathbb{Z} \\ 0 < a_i \leq T_i \\ 1 \leq i \leq r}} N_{\langle a_1, \dots, a_r \rangle, m}(x) = \sum_{\substack{p \leq x \\ p \equiv 1 \pmod{m}}} \frac{J_r((p-1)/m)}{(p-1)^r} + O\left(\frac{x}{(\log x)^M}\right)$$

if $T_i > \exp(4(\log x \log \log x)^{1/2})$ for all $i = 1, \dots, r$, $m \leq (\log x)^D$ and $M > 1$ is an arbitrary constant, where

$$J_r(n) = n^r \prod_{\substack{\ell | n \\ \ell \text{ prime}}} \left(1 - \frac{1}{\ell^r}\right)$$

is *Jordan's totient function*. This provides a natural generalization of Moree's result in [11].

Theorem 2 leads to the following corollary:

COROLLARY 1. *For any $\epsilon > 0$, let*

$$\mathcal{H} := \{(a_1, \dots, a_r) \in \mathbb{Z}^r : 0 < a_i \leq T_i, i \in \{1, \dots, r\}, \\ |N_{\langle a_1, \dots, a_r \rangle, m}(x) - C_{r,m} \text{Li}(x)| > \epsilon \text{Li}(x)\}.$$

Then, supposing $T^ > \exp(6(\log x \log \log x)^{1/2})$, we have*

$$\#\mathcal{H} \leq KT_1 \dots T_r / \epsilon^2 (\log x)^F$$

for every positive constant F , where K is an absolute positive constant.

Proof. The proof is a trivial generalization of that in [14, Corollary, p. 187]. ■

2. Notation and conventions. In order to simplify the formulas, we introduce the following notation. Underlined letters stand for general r -tuples defined within some set, e.g. $\underline{a} = (a_1, \dots, a_r) \in (\mathbb{F}_p^*)^r$ or $\underline{T} = (T_1, \dots, T_r) \in (\mathbb{R}^{>0})^r$; moreover, given two r -tuples, \underline{a} and \underline{n} , their scalar product is $\underline{a} \cdot \underline{n} = a_1 n_1 + \dots + a_r n_r$, and we write e.g. $\underline{a} \leq \underline{n}$ if $a_i \leq n_i$ for all i . The null vector is $\underline{0} = \{0, \dots, 0\}$. Similarly, if $\underline{\chi} = (\chi_1, \dots, \chi_r)$ is an r -tuple of Dirichlet characters and $\underline{a} \in \mathbb{Z}^r$, then we denote $\underline{\chi}(\underline{a}) = \chi_1(a_1) \dots \chi_r(a_r) \in \mathbb{C}$.

In addition, $(q, \underline{a}) := (q, a_1, \dots, a_r) = \text{gcd}(q, a_1, \dots, a_r)$; otherwise, to avoid possible misinterpretations, we will write explicitly $\text{gcd}(n_1, \dots, n_r)$ instead of (\underline{n}) . Given any r -tuple $\underline{a} \in \mathbb{Z}^r$, we indicate with

$$\langle \underline{a} \rangle_p := \langle a_1 \pmod{p}, \dots, a_r \pmod{p} \rangle$$

the reduction modulo p of the subgroup $\langle \underline{a} \rangle = \langle a_1, \dots, a_r \rangle \subset \mathbb{Q}$; if $\Gamma = \langle a_1, \dots, a_r \rangle$, then $\Gamma_p = \langle \underline{a} \rangle_p$.

In the whole paper, ℓ and p will always indicate prime numbers. For a finite field \mathbb{F}_p , we set $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$ and $\widehat{\mathbb{F}_p^*}$ will denote its relative dual group (or character group). Finally, given an integer a , $v_p(a)$ is its p -adic valuation.

3. Lemmata. Let $q > 1$ be an integer and let $\underline{n} \in \mathbb{Z}^r$. We define the *multiple Ramanujan sum* as

$$c_q(\underline{n}) := \sum_{\substack{\underline{a} \in (\mathbb{Z}/q\mathbb{Z})^r \\ (q, \underline{a})=1}} e^{2\pi i \underline{a} \cdot \underline{n} / q}.$$

It is well known (see [6, Theorem 272]) that, for any integer n ,

$$(4) \quad c_q(n) = \mu\left(\frac{q}{(q, n)}\right) \frac{\varphi(q)}{\varphi(q/(q, n))}.$$

In the following lemma, we generalize this result to r -rank.

LEMMA 1. *Let*

$$J_r(m) := m^r \prod_{\ell|m} \left(1 - \frac{1}{\ell^r}\right)$$

be Jordan's totient function. Then

$$c_q(\underline{n}) = \mu\left(\frac{q}{(q, \underline{n})}\right) \frac{J_r(q)}{J_r(q/(q, \underline{n}))}.$$

Proof. Let us start by considering the case when $q = \ell$ is prime. Then

$$\begin{aligned} c_\ell(\underline{n}) &= \sum_{\underline{a} \in (\mathbb{Z}/\ell\mathbb{Z})^r \setminus \{0\}} e^{2\pi i \underline{a} \cdot \underline{n} / \ell} \\ &= -1 + \prod_{j=1}^r \sum_{a_j=1}^{\ell} e^{2\pi i a_j n_j / \ell} = \begin{cases} -1 & \text{if } \ell \nmid \gcd(n_1, \dots, n_r), \\ \ell^r - 1 & \text{otherwise.} \end{cases} \end{aligned}$$

Next we consider the case when $q = \ell^k$ with $k \geq 2$ and ℓ prime. We need to show that

$$c_{\ell^k}(\underline{n}) = \begin{cases} 0 & \text{if } \ell^{k-1} \nmid \gcd(n_1, \dots, n_r), \\ -\ell^{r(k-1)} & \text{if } \ell^{k-1} \parallel \gcd(n_1, \dots, n_r), \\ \ell^{rk} (1 - 1/\ell^r) & \text{if } \ell^k \mid \gcd(n_1, \dots, n_r). \end{cases}$$

To do so, we write

$$\begin{aligned} c_{\ell^k}(\underline{n}) &= \sum_{\substack{\underline{a} \in (\mathbb{Z}/\ell^k\mathbb{Z})^r \\ (\ell, \underline{a})=1}} e^{2\pi i \underline{a} \cdot \underline{n} / \ell^k} \\ &= c_{\ell^k}(n_1) \prod_{j=2}^r \sum_{a_j=1}^{\ell^k} e^{2\pi i a_j n_j / \ell^k} + c_{\ell^k}(n_2, \dots, n_r) \sum_{j=1}^k \sum_{\substack{a_1 \in \mathbb{Z}/\ell^k\mathbb{Z} \\ (a_1, \ell^k) = \ell^j}} e^{2\pi i a_1 n_1 / \ell^k} \\ &= c_{\ell^k}(n_1) \prod_{j=2}^r \sum_{a_j=1}^{\ell^k} e^{2\pi i a_j n_j / \ell^k} + c_{\ell^k}(n_2, \dots, n_r) \sum_{j=1}^k c_{\ell^{k-j}}(n_1). \end{aligned}$$

If we apply (4), we obtain

$$\begin{aligned} c_{\ell^k}(n_1, \dots, n_r) &= \mu\left(\frac{\ell^k}{(\ell^k, n_1)}\right) \frac{\varphi(\ell^k)}{\varphi(\ell^k/(\ell^k, n_1))} \prod_{j=2}^r \sum_{a_j=1}^{\ell^k} e^{2\pi i a_j n_j / \ell^k} \\ &\quad + c_{\ell^k}(n_2, \dots, n_r) \sum_{j=1}^k \mu\left(\frac{\ell^{k-j}}{(\ell^{k-j}, n_1)}\right) \frac{\varphi(\ell^{k-j})}{\varphi(\ell^{k-j}/(\ell^{k-j}, n_1))}. \end{aligned}$$

Now, for $k \geq 2$, we distinguish two cases:

- (1) $\ell^{k-1} \nmid \gcd(n_1, \dots, n_r)$,
- (2) $\ell^{k-1} \mid \gcd(n_1, \dots, n_r)$.

In the first case we can assume, without loss of generality, that $\ell^{k-1} \nmid n_1$. Hence $\mu(\ell^k/(\ell^k, n_1)) = 0$ and if $k_1 = v_\ell(n_1) < k - 1$, then

$$\mu\left(\frac{\ell^{k-j}}{(\ell^{k-j}, n_1)}\right) = \mu(\ell^{\max\{0, k-k_1-j\}}) = \begin{cases} 0 & \text{if } 1 \leq j \leq k - k_1 - 2, \\ -1 & \text{if } j = k - k_1 - 1, \\ 1 & \text{if } j \geq k - k_1. \end{cases}$$

Hence

$$\sum_{j=1}^k \mu\left(\frac{\ell^{k-j}}{(\ell^{k-j}, n_1)}\right) \frac{\varphi(\ell^{k-j})}{\varphi(\ell^{k-j}/(\ell^{k-j}, n_1))} = -\ell^{k_1} + \sum_{j=k-k_1}^k \varphi(\ell^{k-j}) = 0.$$

In the second case, from the definition of $c_q(\underline{n})$ we find

$$\begin{aligned} c_{\ell^k}(\underline{n}) &= \ell^{r(k-1)} c_\ell\left(\frac{n_1}{\ell^{k-1}}, \dots, \frac{n_r}{\ell^{k-1}}\right) \\ &= \begin{cases} \ell^{rk}(1 - 1/\ell^r) & \text{if } \ell^k \mid \gcd(n_1, \dots, n_r), \\ -\ell^{r(k-1)} & \text{if } \ell^{k-1} \parallel \gcd(n_1, \dots, n_r). \end{cases} \end{aligned}$$

So, the formula holds for $q = \ell^k$.

Finally, we claim that if $q', q'' \in \mathbb{N}$ are such that $\gcd(q', q'') = 1$, then

$$c_{q'q''}(\underline{n}) = c_{q'}(\underline{n}) c_{q''}(\underline{n});$$

this amounts to saying that the multiple Ramanujan sum is multiplicative in q . Indeed,

$$\begin{aligned} \sum_{\substack{\underline{a} \in (\mathbb{Z}/q'\mathbb{Z})^r \\ (q', \underline{a})=1}} e^{2\pi i \underline{a} \cdot \underline{n}/q'} & \sum_{\substack{\underline{b} \in (\mathbb{Z}/q''\mathbb{Z})^r \\ (q'', \underline{b})=1}} e^{2\pi i \underline{b} \cdot \underline{n}/q''} \\ &= \sum_{\substack{\underline{a} \in (\mathbb{Z}/q'\mathbb{Z})^r \\ \underline{b} \in (\mathbb{Z}/q''\mathbb{Z})^r \\ \gcd(q', \underline{a})=1 \\ \gcd(q'', \underline{b})=1}} e^{2\pi i [n_1(q''a_1 + q'b_1) + \dots + n_r(q''a_r + q'b_r)]/(q'q'')}, \end{aligned}$$

and the result follows from the remark that since $\gcd(q', q'') = 1$,

- for all $j = 1, \dots, r$, if a_j runs through a complete set of residues modulo q' , and b_j runs through a complete set of residues modulo q'' , then $q''a_j + q'b_j$ runs through a complete set of residues modulo $q'q''$;
- for all $\underline{a} \in (\mathbb{Z}/q'\mathbb{Z})^r$ and $\underline{b} \in (\mathbb{Z}/q''\mathbb{Z})^r$,

$$\begin{aligned} \gcd(q', \underline{a}) = 1 \text{ and } \gcd(q'', \underline{b}) = 1 \\ \Leftrightarrow \gcd(q'q'', q'b_1 + q''a_1, \dots, q'b_r + q''a_r) = 1. \end{aligned}$$

The lemma now follows from the multiplicativity of μ and of J_r . ■

From the previous lemma we deduce the following corollary:

COROLLARY 2. *Let p be an odd prime, and let $m \in \mathbb{N}$ be a divisor of $p - 1$. Given an r -tuple $\underline{\chi} = (\chi_1, \dots, \chi_r)$ of Dirichlet characters modulo p , set*

$$c_m(\underline{\chi}) := \frac{1}{(p-1)^r} \sum_{\substack{\alpha \in (\mathbb{F}_p^*)^r \\ [\mathbb{F}_p^* : \langle \alpha \rangle_p] = m}} \underline{\chi}(\alpha).$$

Then

$$(5) \quad c_m(\underline{\chi}) = \frac{1}{(p-1)^r} \mu \left(\frac{p-1}{m \operatorname{gcd} \left(\frac{p-1}{m}, \frac{p-1}{\operatorname{ord}(\chi_1)}, \dots, \frac{p-1}{\operatorname{ord}(\chi_r)} \right)} \right) \times \frac{J_r((p-1)/m)}{J_r \left(\frac{p-1}{m \operatorname{gcd} \left(\frac{p-1}{m}, \frac{p-1}{\operatorname{ord}(\chi_1)}, \dots, \frac{p-1}{\operatorname{ord}(\chi_r)} \right)} \right)}.$$

Proof. Fix a primitive root $g \in \mathbb{F}_p^*$. For each $j = 1, \dots, r$, let $n_j \in \mathbb{Z}/(p-1)\mathbb{Z}$ be such that

$$\chi_j = \chi_j(g) = e^{2\pi i n_j / (p-1)}.$$

Write $\alpha_j = g^{a_j}$ for $j = 1, \dots, r$. Then

$$[\mathbb{F}_p^* : \langle \alpha \rangle_p] = m \Leftrightarrow (p-1, \underline{a}) = m.$$

Therefore, naming $t = (p-1)/m$, we have

$$(6) \quad c_m(\underline{\chi}) = \frac{1}{(p-1)^r} \sum_{\substack{\alpha \in (\mathbb{F}_p^*)^r \\ (p-1, \underline{a}) = m}} \chi_1(g)^{a_1} \cdots \chi_r(g)^{a_r} \\ = \frac{1}{(p-1)^r} \sum_{\substack{\underline{a}' \in (\mathbb{Z}/t\mathbb{Z})^r \\ (t, \underline{a}') = 1}} e^{2\pi i \underline{a}' \cdot \underline{n} / t} = \frac{1}{(p-1)^r} c_{(p-1)/m}(\underline{n}).$$

By definition we have $\operatorname{ord}(\chi_j) = (p-1)/\operatorname{gcd}(n_j, p-1)$, so

$$\frac{p-1}{m \operatorname{gcd} \left(\frac{p-1}{m}, \underline{n} \right)} = \frac{p-1}{m \operatorname{gcd} \left(\frac{p-1}{m}, \frac{p-1}{\operatorname{ord}(\chi_1)}, \dots, \frac{p-1}{\operatorname{ord}(\chi_r)} \right)},$$

and this together with Lemma 1 concludes the proof. ■

For a fixed rank r , define

$$R_p(m) := \#\{ \underline{a} \in (\mathbb{Z}/(p-1)\mathbb{Z})^r : (\underline{a}, p-1) = m \}.$$

Then using the well-known properties of the Möbius function, we can write

$$R_p(m) = \sum_{\underline{a} \in (\mathbb{Z}/(p-1)\mathbb{Z})^r} \sum_{n | \left(\frac{a}{m}, \frac{p-1}{m} \right)} \mu(n) = \sum_{n | \frac{p-1}{m}} \mu(n) [h_m(n)]^r,$$

where

$$h_m(n) = \#\left\{a \in \mathbb{Z}/(p-1)\mathbb{Z} : n \mid \frac{a}{m}\right\} = \frac{p-1}{nm},$$

so that

$$(7) \quad R_p(m) = \left(\frac{p-1}{m}\right)^r \sum_{n \mid \frac{p-1}{m}} \frac{\mu(n)}{n^r} = J_r\left(\frac{p-1}{m}\right).$$

Defining

$$(8) \quad \begin{aligned} S_m(x) &:= \frac{1}{m^r} \sum_{\substack{p \leq x \\ p \equiv 1 \pmod{m}}} \sum_{n \mid \frac{p-1}{m}} \frac{\mu(n)}{n^r} \\ &= \sum_{\substack{p \leq x \\ p \equiv 1 \pmod{m}}} \frac{1}{(p-1)^r} J_r\left(\frac{p-1}{m}\right), \end{aligned}$$

we have the following lemma.

LEMMA 2. *If $m \leq (\log x)^D$ with D an arbitrary positive constant, then for every constant $M > 1$,*

$$S_m(x) = C_{r,m} \operatorname{Li}(x) + O\left(\frac{x}{m^r(\log x)^M}\right),$$

where $C_{r,m} = \sum_{n \geq 1} \frac{\mu(n)}{(nm)^r \varphi(nm)}$.

Proof. We choose an arbitrary positive constant B , and for every coprime integers a and b , we denote $\pi(x; a, b) = \#\{p \leq x : p \equiv a \pmod{b}\}$, then

$$\begin{aligned} S_m(x) &= \sum_{n \leq x} \frac{\mu(n)}{(nm)^r} \pi(x; 1, nm) \\ &= \sum_{n \leq (\log x)^B} \frac{\mu(n)}{(nm)^r} \pi(x; 1, nm) + O\left(\sum_{(\log x)^B < n \leq x} \frac{1}{(nm)^r} \pi(x; 1, nm)\right). \end{aligned}$$

The sum in the error term is

$$\begin{aligned} \sum_{(\log x)^B < n \leq x} \frac{1}{(nm)^r} \pi(x; 1, nm) &\leq \frac{1}{m^r} \sum_{n > (\log x)^B} \frac{1}{n^r} \sum_{\substack{2 \leq a \leq x \\ a \equiv 1 \pmod{mn}}} 1 \\ &\leq \frac{1}{m^{r+1}} \sum_{n > (\log x)^B} \frac{x}{n^{r+1}} \\ &\ll \frac{x}{m^{r+1}(\log x)^{rB}}. \end{aligned}$$

For the main term we apply the Siegel–Walfisz Theorem [17], which states that for any positive constants B and C , if $a \leq (\log x)^B$, then

$$\pi(x; 1, a) = \frac{\text{Li}(x)}{\varphi(a)} + O\left(\frac{x}{(\log x)^C}\right).$$

So, if we restrict $m \leq (\log x)^D$ for any positive constant D , then

$$\begin{aligned} S_m(x) &= \sum_{n \leq (\log x)^B} \frac{\mu(n)}{(nm)^r \varphi(mn)} \text{Li}(x) + O\left(\frac{x}{(\log x)^C} \sum_{n \leq (\log x)^B} \frac{1}{(nm)^r}\right) \\ &\quad + O\left(\frac{x}{m^{r+1}(\log x)^{rB}}\right) \\ &= C_{r,m} \text{Li}(x) + O\left(\sum_{n > (\log x)^B} \frac{\text{Li}(x)}{(nm)^r \varphi(nm)}\right) + O\left(\frac{x \log \log x}{m^r (\log x)^C}\right) \\ &\quad + O\left(\frac{x}{m^{r+1}(\log x)^{rB}}\right) \\ &= C_{r,m} \text{Li}(x) + O\left(\frac{1}{m^r \varphi(m)} \sum_{n > (\log x)^B} \frac{\text{Li}(x)}{n^r \varphi(n)}\right) \\ &\quad + O\left(\frac{x \log \log x}{m^r (\log x)^C}\right) + O\left(\frac{x}{m^{r+1}(\log x)^{rB}}\right), \end{aligned}$$

where we have used the elementary inequality $\varphi(mn) \geq \varphi(m)\varphi(n)$. Since, for every $n \geq 3$, we have (see [1, Theorem 8.8.7])

$$(9) \quad \frac{n}{\varphi(n)} < e^\gamma \log \log n + \frac{3}{\log \log n} \ll \log \log n,$$

it follows that

$$\sum_{n > (\log x)^B} \frac{1}{n^r \varphi(n)} \ll \sum_{n > (\log x)^B} \frac{\log \log n}{n^{r+1}} \ll \frac{\log \log \log x}{(\log x)^{rB}}.$$

Thus

$$\frac{1}{m^r \varphi(m)} \sum_{n > (\log x)^B} \frac{1}{n^r \varphi(n)} \text{Li}(x) \ll \frac{x}{m^r \varphi(m) (\log x)^{rB}},$$

proving the lemma. ■

The following lemma concerns the Titchmarsh Divisor Problem [16] in the case of primes $p \equiv 1 \pmod{m}$. Asymptotic results on this topic can be found in [3] and [4].

LEMMA 3. Let τ be the divisor function and $m \in \mathbb{N}$. If $m \leq (\log x)^D$ for an arbitrary positive constant D , then

$$\sum_{\substack{p \leq x \\ p \equiv 1 \pmod{m}}} \tau\left(\frac{p-1}{m}\right) \leq \frac{8x}{m}.$$

Proof. Write $p - 1 = mj k$ so that $j k \leq (x - 1)/m$ and set $Q = \sqrt{(x - 1)/m}$. We distinguish three cases:

- $j \leq Q, k > Q,$
- $j > Q, k \leq Q,$
- $j \leq Q, k \leq Q.$

So we have the identity

$$\begin{aligned} \sum_{\substack{p \leq x \\ p \equiv 1 \pmod{m}}} \tau\left(\frac{p-1}{m}\right) &= \sum_{j \leq Q} \sum_{\substack{Q < k \leq Q^2/j \\ mjk+1 \text{ prime}}} 1 + \sum_{k \leq Q} \sum_{\substack{Q < j \leq Q^2/k \\ mjk+1 \text{ prime}}} 1 \\ &\quad + \sum_{j \leq Q} \sum_{\substack{k \leq Q \\ mjk+1 \text{ prime}}} 1 \\ &= 2 \sum_{k \leq Q} \sum_{\substack{mkQ+1 < p \leq x \\ p \equiv 1 \pmod{km}}} 1 + \sum_{k \leq Q} \sum_{\substack{p \leq mkQ+1 \\ p \equiv 1 \pmod{km}}} 1 \\ &= 2 \sum_{k \leq Q} (\pi(x; 1, km) - \pi(mkQ + 1; 1, km)) \\ &\quad + \sum_{k \leq Q} \pi(mkQ + 1; 1, km) \\ &= 2 \sum_{k \leq Q} \pi(x; 1, km) - \sum_{k \leq Q} \pi(mkQ + 1; 1, km). \end{aligned}$$

Using the Montgomery–Vaughan version of the Brun–Titchmarsh Theorem,

$$\pi(x; a, q) \leq \frac{2x}{\varphi(q) \log(x/q)},$$

for $m \leq (\log x)^D$ with D an arbitrary positive constant we obtain

$$\begin{aligned} \sum_{\substack{p \leq x \\ p \equiv 1 \pmod{m}}} \tau\left(\frac{p-1}{m}\right) &\leq 2 \sum_{k \leq Q} \frac{2x}{\varphi(km) \log(x/km)} \\ &\leq \frac{4x}{\log(x/mQ)} \sum_{k \leq Q} \frac{1}{\varphi(km)} \leq \frac{8x}{\log(x/m)} \sum_{k \leq Q} \frac{1}{\varphi(km)}. \end{aligned}$$

Now, substitute the elementary inequality $\varphi(km) \geq m\varphi(k)$ and use a result

of Montgomery [9],

$$\sum_{k \leq Q} \frac{1}{\varphi(k)} = A \log Q + B + O\left(\frac{\log Q}{Q}\right),$$

where

$$A = \frac{\zeta(2)\zeta(3)}{\zeta(6)} = 1.9436\dots \quad \text{and} \quad B = A\gamma - \sum_{n=1}^{\infty} \frac{\mu^2(n) \log n}{n\varphi(n)} = -0.0606\dots,$$

which in particular implies that, for Q large enough,

$$A \log Q - 1 \leq \sum_{k \leq Q} \frac{1}{\varphi(k)} \leq A \log Q \leq \log(x/m).$$

This yields the desired conclusion. ■

LEMMA 4. *Let p be an odd prime number and let $\chi \neq \chi_0$ be a non-principal Dirichlet character modulo p . Define*

$$d_{m,i}(\chi) := \sum_{\substack{\underline{\chi} \in (\widehat{\mathbb{F}_p^*})^r \\ \chi_i = \chi}} |c_m(\underline{\chi})|.$$

Then

$$d_{m,i}(\chi) \leq \frac{1}{m} \prod_{\ell | \frac{p-1}{m}} \left(1 + \frac{1}{\ell}\right).$$

Proof. From (6) and Lemma 1, we have

$$\begin{aligned} & d_{m,i}(\chi) \\ &= \frac{1}{(p-1)^r} \sum_{\substack{\underline{n} \in (\mathbb{Z}/(p-1)\mathbb{Z})^r \\ n_i = n}} \mu^2\left(\frac{(p-1)/m}{((p-1)/m, \underline{n})}\right) \frac{J_r((p-1)/m)}{J_r((p-1)/m/((p-1)/m, \underline{n}))}, \end{aligned}$$

where $\chi = e^{2\pi i n/(p-1)}$ with $n \in \mathbb{Z}/(p-1)\mathbb{Z} \setminus \{0\}$; naming $t = (p-1)/m$ and $u = \gcd(t, n_i)$ we get

$$d_{m,i}(\chi) = \frac{1}{(p-1)^r} \sum_{d|t} \mu^2\left(\frac{t}{d}\right) \frac{J_r(t)}{J_r(t/d)} H(d),$$

where

$$H(d) := \#\{\underline{x} \in (\mathbb{Z}/(p-1)\mathbb{Z})^{r-1} : (u, \underline{x}) = d\} = \left(\frac{p-1}{d}\right)^{r-1} \sum_{k | \frac{u}{d}} \frac{\mu(k)}{k^{r-1}}.$$

Then

$$\begin{aligned}
 d_{m,i}(\chi) &= \frac{1}{p-1} \sum_{d|t} \mu^2\left(\frac{t}{d}\right) \frac{J_r(t)}{d^{r-1} J_r(t/d)} \sum_{k|\frac{t}{d}} \frac{\mu(k)}{k^{r-1}} \\
 &\leq \frac{1}{p-1} \sum_{d|t} \mu^2\left(\frac{t}{d}\right) d = \frac{t}{p-1} \sum_{k|t} \frac{\mu^2(k)}{k} = \frac{1}{m} \prod_{\ell|\frac{p-1}{m}} \left(1 + \frac{1}{\ell}\right). \blacksquare
 \end{aligned}$$

4. Proof of Theorem 1. We follow the method of Stephens [14]. By exchanging the order of summation we obtain

$$\sum_{\substack{\underline{a} \in \mathbb{Z}^r \\ 0 < \underline{a} \leq \underline{T}}} N_{\underline{a},m}(x) = \sum_{\substack{p \leq x \\ p \equiv 1 \pmod{m}}} M_p^m(\underline{T}),$$

where $M_p^m(\underline{T})$ is the number of r -tuples $\underline{a} \in \mathbb{Z}^r$ with $0 < a_i \leq T_i$ and $v_p(a_i) = 0$ for $i = 1, \dots, r$ whose reduction modulo p satisfies $[\mathbb{F}_p^* : \langle \underline{a} \rangle_p] = m$. We can write

$$M_p^m(\underline{T}) = \sum_{\substack{\underline{a} \in \mathbb{Z}^r \\ 0 < \underline{a} \leq \underline{T}}} t_{p,m}(\underline{a})$$

with

$$t_{p,m}(\underline{a}) = \begin{cases} 1 & \text{if } [\mathbb{F}_p^* : \langle \underline{a} \rangle_p] = m, \\ 0 & \text{otherwise.} \end{cases}$$

Given an r -tuple $\underline{\chi}$ of Dirichlet characters mod p , by orthogonality relations it is easy to verify that

$$(10) \quad t_{p,m}(\underline{a}) = \sum_{\underline{\chi} \in (\widehat{\mathbb{F}_p^*})^r} c_m(\underline{\chi}) \underline{\chi}(\underline{a}),$$

so we have

$$(11) \quad \sum_{\substack{\underline{a} \in \mathbb{Z}^r \\ 0 < \underline{a} \leq \underline{T}}} N_{\underline{a},m}(x) = \sum_{\substack{p \leq x \\ p \equiv 1 \pmod{m}}} \sum_{\substack{\underline{a} \in \mathbb{Z}^r \\ 0 < \underline{a} \leq \underline{T}}} \sum_{\underline{\chi} \in (\widehat{\mathbb{F}_p^*})^r} c_m(\underline{\chi}) \underline{\chi}(\underline{a}).$$

Let $\underline{\chi}_0 := (\chi_0, \dots, \chi_0)$ be the r -tuple of principal characters. Then

$$\begin{aligned}
 c_m(\underline{\chi}_0) &= \frac{1}{(p-1)^r} \sum_{\substack{\underline{a} \in (\mathbb{F}_p^*)^r \\ [\mathbb{F}_p^* : \langle \underline{a} \rangle_p] = m}} \underline{\chi}_0(\underline{a}) \\
 &= \frac{1}{(p-1)^r} \#\{\underline{a} \in (\mathbb{Z}/(p-1)\mathbb{Z})^r : (a, p-1) = m\} = \frac{1}{(p-1)^r} R_p(m).
 \end{aligned}$$

Denoting $|T| := \prod_{i=1}^r T_i$ and $T^* := \min\{T_i : i = 1, \dots, r\}$, through (8) and (7), we can write the main term in (11) as

$$\begin{aligned} \frac{1}{|T|} & \sum_{\substack{p \leq x \\ p \equiv 1 \pmod{m}}} \sum_{\substack{a \in \mathbb{Z}^r \\ 0 < a \leq T}} c_m(\chi_0) \chi_0(\underline{a}) \\ &= \frac{1}{|T|} \sum_{\substack{p \leq x \\ p \equiv 1 \pmod{m}}} c_m(\chi_0) \prod_{i=1}^r \{[T_i] - [T_i/p]\} \\ &= \sum_{\substack{p \leq x \\ p \equiv 1 \pmod{m}}} c_m(\chi_0) \left(\left(1 - \frac{1}{p}\right)^r + \sum_{i=1}^r O\left(\frac{1}{T_i}\right) \right) \\ &= \sum_{\substack{p \leq x \\ p \equiv 1 \pmod{m}}} c_m(\chi_0) + O\left(\sum_{\substack{p \leq x \\ p \equiv 1 \pmod{m}}} \frac{1}{p} \right) + O\left(\frac{x}{T^* \log x} \right) \\ &= S_m(x) + O(\log \log x) + O\left(\frac{x}{T^* \log x} \right). \end{aligned}$$

By hypothesis $m \leq (\log x)^D$, $D > 0$, and $T^* > \exp(4(\log x \log \log x)^{1/2})$, so we can apply Lemma 2 to obtain

$$\frac{1}{|T|} \sum_{\substack{p \leq x \\ p \equiv 1 \pmod{m}}} \sum_{\substack{a \in \mathbb{Z}^r \\ 0 < a \leq T}} c_m(\chi_0) \chi_0(\underline{a}) = C_{r,m} \text{Li}(x) + O\left(\frac{x}{m^r (\log x)^M} \right)$$

for any $M > 1$. For the error term we need to estimate the sum

$$\begin{aligned} (12) \quad E_{r,m}(x) &:= \frac{1}{|T|} \sum_{\substack{p \leq x \\ p \equiv 1 \pmod{m}}} \sum_{\chi \in \widehat{(\mathbb{F}_p^*)^r} \setminus \{\chi_0\}} \left| c_m(\chi) \sum_{\substack{a \in \mathbb{Z}^r \\ 0 < a \leq T}} \chi(\underline{a}) \right| \\ &\ll \sum_{i=1}^r \frac{1}{T_i} \sum_{\substack{p \leq x \\ p \equiv 1 \pmod{m}}} \sum_{\chi \in \widehat{\mathbb{F}_p^*} \setminus \{\chi_0\}} \left| d_{m,i}(\chi) \sum_{\substack{a \in \mathbb{Z} \\ 0 < a \leq T_i}} \chi(a) \right|, \end{aligned}$$

since the r main contributions to (12) come from the cases in which just one Dirichlet character in χ is non-principal, say $\chi_i = \chi \neq \chi_0$, while for every $j \neq i$ we choose $\chi_j = \chi_0$, giving

$$\left| \sum_{\substack{a \in \mathbb{Z}^r \\ 0 < a \leq T}} \chi(\underline{a}) \right| = \left| \sum_{\substack{a \in \mathbb{Z} \\ 0 < a \leq T_i}} \chi(a) \sum_{\substack{0 \leq j \leq r \\ j \neq i}} \sum_{\substack{a_j \in \mathbb{Z} \\ 0 < a_j \leq T_j \\ p \nmid a_j}} 1 \right| \leq \frac{|T|}{T_i} \left| \sum_{\substack{a \in \mathbb{Z} \\ 0 < a \leq T_i}} \chi(a) \right|.$$

Define

$$(13) \quad E_{r,m}^i(x) := \sum_{\substack{p \leq x \\ p \equiv 1 \pmod{m}}} \sum_{\chi \in \widehat{\mathbb{F}_p^*} \setminus \{\chi_0\}} d_{m,i}(\chi) \left| \sum_{\substack{a \in \mathbb{Z} \\ 0 < a \leq T_i}} \chi(a) \right|.$$

Then by Hölder’s inequality

$$(14) \quad \{E_{r,m}^i(x)\}^{2s_i} \leq \left\{ \sum_{\substack{p \leq x \\ p \equiv 1 \pmod{m}}} \sum_{\chi \in \widehat{\mathbb{F}_p^*} \setminus \{\chi_0\}} \{d_{m,i}(\chi)\}^{\frac{2s_i}{2s_i-1}} \right\}^{2s_i-1} \\ \times \sum_{\substack{p \leq x \\ p \equiv 1 \pmod{m}}} \sum_{\chi \in \widehat{\mathbb{F}_p^*} \setminus \{\chi_0\}} \left| \sum_{\substack{a \in \mathbb{Z} \\ 0 < a \leq T_i}} \chi(a) \right|^{2s_i}.$$

As before, given a primitive root g modulo p , write $\chi_j(g) = e^{2\pi i n_j / (p-1)}$ for every $j = 1, \dots, r$ with $n_j \in \mathbb{Z}/(p-1)\mathbb{Z}$, so that by (6),

$$\sum_{\chi \in \widehat{\mathbb{F}_p^*}^r \setminus \{\chi_0\}} c_m(\underline{\chi}) = \frac{1}{(p-1)^r} \sum_{\underline{n} \in (\mathbb{Z}/(p-1)\mathbb{Z})^r \setminus \{\mathbf{0}\}} c_{(p-1)/m}(\underline{n}).$$

Denoting again $t = (p-1)/m$, from Lemma 1 we derive

$$\sum_{\chi \in \widehat{\mathbb{F}_p^*} \setminus \{\chi_0\}} d_{m,i}(\chi) \leq \sum_{\underline{\chi} \in \widehat{\mathbb{F}_p^*}^r \setminus \{\chi_0\}} |c_m(\underline{\chi})| \\ \leq \sum_{d|t} \mu^2\left(\frac{t}{d}\right) \left[\frac{J_r(t)}{(p-1)^r J_r(t/d)} \right] \\ \times \#\{\underline{n} \in (\mathbb{Z}/(p-1)\mathbb{Z})^r : (t, \underline{n}) = d\} \\ = \sum_{d|t} \mu^2\left(\frac{t}{d}\right) \frac{J_r(t)}{d^r J_r(t/d)} \sum_{\substack{k|t \\ k|\frac{t}{d}}} \frac{\mu(k)}{k^r} = \frac{J_r(t)}{t^r} \sum_{d|t} \mu^2\left(\frac{t}{d}\right) \\ = \prod_{\ell|t} (1 - 1/\ell^r) 2^{\omega(t)} \leq 2^{\omega(t)}.$$

Set $D_{m,i}(p) := \max\{d_{m,i}(\chi) : \chi \in \widehat{\mathbb{F}_p^*} \setminus \{\chi_0\}\}$. Then for every $s_i \geq 1$,

$$\begin{aligned}
 & \sum_{\substack{p \leq x \\ p \equiv 1 \pmod{m}}} \sum_{\chi \in \widehat{\mathbb{F}_p^*} \setminus \{\chi_0\}} \{d_{m,i}(\chi)\}^{\frac{2s_i}{2s_i-1}} \\
 & \leq \sum_{\substack{p \leq x \\ p \equiv 1 \pmod{m}}} \sum_{\chi \in \widehat{\mathbb{F}_p^*} \setminus \{\chi_0\}} d_{m,i}(\chi) \{d_{m,i}(\chi)\}^{\frac{1}{2s_i-1}} \\
 & \leq \sum_{\substack{p \leq x \\ p \equiv 1 \pmod{m}}} \{D_{m,i}(p)\}^{\frac{1}{2s_i-1}} \sum_{\chi \in \widehat{\mathbb{F}_p^*} \setminus \{\chi_0\}} d_{m,i}(\chi) \\
 & \leq \sum_{\substack{p \leq x \\ p \equiv 1 \pmod{m}}} \{D_{m,i}(p)\}^{\frac{1}{2s_i-1}} 2^{\omega(\frac{p-1}{m})} \\
 & \leq m^{-\frac{1}{2s_i-1}} \sum_{\substack{p \leq x \\ p \equiv 1 \pmod{m}}} \prod_{\ell | \frac{p-1}{m}} \left(1 + \frac{1}{\ell}\right) 2^{\omega(\frac{p-1}{m})} \\
 & \ll m^{-\frac{1}{2s_i-1}} \sum_{\substack{p \leq x \\ p \equiv 1 \pmod{m}}} \prod_{\ell | \frac{p-1}{m}} \left(1 - \frac{1}{\ell}\right)^{-1} 2^{\omega(\frac{p-1}{m})} \\
 & \ll m^{-\frac{1}{2s_i-1}} \log \log x \sum_{\substack{p \leq x \\ p \equiv 1 \pmod{m}}} \tau\left(\frac{p-1}{m}\right) \ll m^{-\frac{2s_i}{2s_i-1}} x \log \log x,
 \end{aligned}$$

where we have used Lemmata 3 and 4 together with the simple observation

$$\{mD_{m,i}(p)\}^{\frac{1}{2s_i-1}} \leq \prod_{\ell | \frac{p-1}{m}} \left(1 + \frac{1}{\ell}\right)^{\frac{1}{2s_i-1}} \leq \prod_{\ell | \frac{p-1}{m}} \left(1 + \frac{1}{\ell}\right).$$

To estimate the other factor in (14) we use [14, Lemma 5]:

$$\sum_{\substack{p \leq x \\ p \equiv 1 \pmod{m}}} \sum_{\chi \in \widehat{\mathbb{F}_p^*} \setminus \{\chi_0\}} \left| \sum_{\substack{a \in \mathbb{Z} \\ 0 < a \leq T_i}} \chi(a) \right|^{2s_i} \ll (x^2 + T_i^{s_i}) T_i^{s_i} (\log(eT_i^{s_i-1}))^{s_i^2-1}.$$

So, for every constant $M > 1$, we find

$$\begin{aligned}
 \frac{1}{|T|} \sum_{\substack{\underline{a} \in \mathbb{Z}^r \\ 0 < \underline{a} \leq T}} N_{\langle \underline{a} \rangle, m}(x) &= C_{r,m} \text{Li}(x) + O\left(\frac{x}{m^r (\log x)^M}\right) \\
 &+ O\left(\sum_{i=1}^r \frac{x}{T_i \log x}\right) + E_{r,m}(x)
 \end{aligned}$$

with

$$E_{r,m}(x) \ll \sum_{i=1}^r \frac{1}{T_i} \left[\left(\frac{x \log \log x}{m^{2s_i-1}} \right)^{2s_i-1} (x^2 + T_i^{s_i}) T_i^{s_i} (\log(eT_i^{s_i-1}))^{s_i-1} \right]^{\frac{1}{2s_i}}.$$

If we choose $s_i = \lfloor \frac{2 \log x}{\log T_i} \rfloor + 1$ for $i = 1, \dots, r$, then $T_i^{s_i-1} \leq x^2 < T_i^{s_i}$ and

$$E_{r,m}(x) \ll \frac{1}{m} \sum_{i=1}^r (x \log \log x)^{1-\frac{1}{2s_i}} (\log(ex^2))^{\frac{s_i^2-1}{2s_i}}.$$

Now, if $T_i > x^2$ for all $i = 1, \dots, r$, then $s_1 = \dots = s_r = 1$ and

$$E_{r,m}(x) \ll \frac{1}{m} (x \log \log x)^{1/2},$$

in particular, $E_{r,m}(x) \ll x/(\log x)^M$ for every constant $M > 1$. Otherwise, if $T_j \leq x^2$ for some $j \in \{1, \dots, r\}$, then $s_j \geq 2$ and the corresponding contribution to $E_{r,m}(x)$ will be

$$E_{r,m}^j(x) \ll \frac{1}{m} (x \log \log x)^{1-\frac{1}{2s_j}} (\log(ex^2))^{\frac{3 \log x}{2 \log T_j}}.$$

By hypothesis

$$(15) \quad T^* > \exp(4(\log x \log \log x)^{1/2})$$

and, through computations similar to those in [14, p. 184], we can derive

$$E_{r,m}(x) \ll \frac{1}{m} x \log \log x \cdot (T^*)^{-1/16}.$$

Also in this case, using (15), we have $E_{r,m}(x) \ll x/(\log x)^M$ for every $M > 1$. This ends the proof of Theorem 1. ■

5. Proof of Theorem 2. We now consider

$$H := \frac{1}{|\underline{T}|} \sum_{\substack{\underline{a} \in \mathbb{Z}^r \\ 0 < \underline{a} \leq \underline{T}}} \{N_{\langle \underline{a} \rangle, m}(x) - C_{r,m} \text{Li}(x)\}^2.$$

We start bounding H as follows:

$$\begin{aligned} & \sum_{\substack{\underline{a} \in \mathbb{Z}^r \\ 0 < \underline{a} \leq \underline{T}}} \{N_{\langle \underline{a} \rangle, m}(x) - C_{r,m} \text{Li}(x)\}^2 \\ & \leq \sum_{\substack{p, q \leq x \\ p, q \equiv 1 \pmod{m}}} M_{p,q}^m(\underline{T}) - 2C_{r,m} \text{Li}(x) \sum_{\substack{p \leq x \\ p \equiv 1 \pmod{m}}} M_p^m(\underline{T}) + |\underline{T}| (C_{r,m})^2 \text{Li}^2(x), \end{aligned}$$

where $M_{p,q}^m(\underline{T})$ denotes the number of r -tuples $\underline{a} \in \mathbb{Z}^r$ with $a_i \leq T_i$ and $v_p(a_i) = v_q(a_i) = 0$ for each $i = 1, \dots, r$ whose reductions modulo prime numbers p and q satisfy $[\mathbb{F}_p^* : \langle \underline{a} \rangle_p] = [\mathbb{F}_q^* : \langle \underline{a} \rangle_q] = m$.

From Theorem 1 we obtain

$$H \leq \frac{1}{|\underline{T}|} \sum_{\substack{p,q \leq x \\ p,q \equiv 1 \pmod{m}}} M_{p,q}^m(\underline{T}) - C_{r,m}^2 \text{Li}^2(x) + O\left(\frac{x^2}{(\log x)^{M'}}\right)$$

for every constant $M' > 2$. If we write

$$\sum_{\substack{p,q \leq x \\ p,q \equiv 1 \pmod{m}}} M_{p,q}^m(\underline{T}) = \sum_{\substack{p \leq x \\ p \equiv 1 \pmod{m}}} M_p^m(\underline{T}) + \sum_{\substack{p,q \leq x \\ p,q \equiv 1 \pmod{m} \\ p \neq q}} M_{p,q}^m(\underline{T}),$$

Theorem 1 gives, for arbitrary $M > 1$,

$$\sum_{\substack{p \leq x \\ p \equiv 1 \pmod{m}}} M_p^m(\underline{T}) = C_{r,m} |\underline{T}| \text{Li}(x) + O\left(\frac{|\underline{T}|x}{(\log x)^M}\right).$$

In the same spirit as in the proof of Theorem 1, we use (10) to deal with the sum

$$\begin{aligned} (16) \quad \sum_{\substack{p,q \leq x \\ p,q \equiv 1 \pmod{m} \\ p \neq q}} M_{p,q}^m(\underline{T}) &= \sum_{\substack{p,q \leq x \\ p,q \equiv 1 \pmod{m} \\ p \neq q}} \sum_{\substack{\underline{a} \in \mathbb{Z}^r \\ 0 < \underline{a} \leq \underline{T}}} t_{p,m}(\underline{a}) t_{q,m}(\underline{a}) \\ &= \sum_{\substack{p,q \leq x \\ p,q \equiv 1 \pmod{m} \\ p \neq q}} \sum_{\chi_1 \in (\widehat{\mathbb{F}}_p)^r} \sum_{\chi_2 \in (\widehat{\mathbb{F}}_q)^r} c_m(\chi_1) c_m(\chi_2) \sum_{\substack{\underline{a} \in \mathbb{Z}^r \\ 0 < \underline{a} \leq \underline{T}}} \chi_1(\underline{a}) \chi_2(\underline{a}), \end{aligned}$$

where χ_1 and χ_2 denote r -tuples of Dirichlet characters modulo p, q respectively. Therefore

$$\sum_{\substack{p,q \leq x \\ p,q \equiv 1 \pmod{m}}} M_{p,q}^m(\underline{T}) = H_1 + 2H_2 + H_3 + O(|\underline{T}| \text{Li}(x)),$$

where H_1, H_2, H_3 are the contributions to the sum (16) when, respectively: $\chi_1 = \chi_2 = \chi_0$; only one of χ_1 and χ_2 is equal to χ_0 ; neither χ_1 nor χ_2 is χ_0 . First we deal with the inner sum in H_1 . To avoid confusion, we write $\chi_0^{(p)}$ and $\chi_0^{(q)}$ for the r -tuples all of whose entries are the principal characters modulo p and modulo q respectively, so that

$$\sum_{\substack{\underline{a} \in \mathbb{Z}^r \\ 0 < \underline{a} \leq \underline{T}}} \chi_0^{(p)}(\underline{a}) \chi_0^{(q)}(\underline{a}) = \prod_{i=1}^r \left\{ [T_i] - \left\lfloor \frac{T_i}{p} \right\rfloor - \left\lfloor \frac{T_i}{q} \right\rfloor + \left\lfloor \frac{T_i}{pq} \right\rfloor \right\}.$$

Using Lemma 2, with $M' > 2$ arbitrary we have

$$\begin{aligned}
 H_1 &= \sum_{\substack{p,q \leq x \\ p,q \equiv 1 \pmod{m} \\ p \neq q}} c_m(\chi_0^{(p)})c_m(\chi_0^{(q)}) \sum_{\substack{a \in \mathbb{Z}^r \\ 0 < a \leq T}} \chi_0^{(p)}(a)\chi_0^{(q)}(a) \\
 &= |\underline{T}| \sum_{\substack{p,q \leq x \\ p,q \equiv 1 \pmod{m} \\ p \neq q}} c_m(\chi_0^{(p)})c_m(\chi_0^{(q)}) \left(\left(1 - \frac{1}{p} - \frac{1}{q} + \frac{1}{pq}\right)^r + \sum_{i=1}^r O\left(\frac{1}{T_i}\right) \right) \\
 &= |\underline{T}| \left(\left(\sum_{\substack{p \leq x \\ p \equiv 1 \pmod{m}}} c_m(\chi_0^{(p)}) \right)^2 - \sum_{\substack{p \leq x \\ p \equiv 1 \pmod{m}}} (c_m(\chi_0^{(p)}))^2 \right) \left(1 + O\left(\frac{1}{T^*}\right)\right) \\
 &\quad + |\underline{T}| O\left(\frac{x \log \log x}{\log x}\right) \\
 &= |\underline{T}| \left(S_m^2(x) + O\left(\frac{x^2}{T^*(\log x)^2}\right) + O\left(\frac{x \log \log x}{\log x}\right) \right) \\
 &= |\underline{T}| \left(C_{r,m}^2 \text{Li}^2(x) + O\left(\frac{x^2}{m^r(\log x)^{M'}}\right) \right).
 \end{aligned}$$

Focus now on H_2 and assume without loss of generality that $\chi_1 = \chi_0 \neq \chi_2$:

$$\begin{aligned}
 H_2 &= \sum_{\substack{p,q \leq x \\ p,q \equiv 1 \pmod{m} \\ p \neq q}} \sum_{\chi_2 \in (\widehat{\mathbb{F}_q^*})^r \setminus \{\chi_0^{(q)}\}} c_m(\chi_0^{(p)})c_m(\chi_2) \sum_{\substack{a \in \mathbb{Z}^r \\ 0 < a \leq T}} \chi_0^{(p)}(a)\chi_2(a) \\
 &= \sum_{\substack{p \leq x \\ p \equiv 1 \pmod{m}}} c_m(\chi_0^{(p)}) \sum_{\substack{q \leq x \\ q \equiv 1 \pmod{m} \\ q \neq p}} \sum_{\chi_2 \in (\widehat{\mathbb{F}_q^*})^r \setminus \{\chi_0^{(q)}\}} c_m(\chi_2) \sum_{\substack{a \in \mathbb{Z}^r \\ 0 < a \leq T \\ p \nmid \prod_{i=1}^r a_i}} \chi_2(a).
 \end{aligned}$$

Just as in the proof of Theorem 1, the quantity

$$U_2 := \sum_{q \equiv 1 \pmod{m}} \sum_{\substack{q \leq x \\ \chi_2 \in (\widehat{\mathbb{F}_q^*})^r \setminus \{\chi_0^{(q)}\}}} \left| c_m(\chi_2) \sum_{\substack{a \in \mathbb{Z}^r \\ 0 < a \leq T}} \chi_2(a) \right|$$

can be estimated through Hölder’s inequality combined with the large sieve inequality, to get $U_2 \ll x/(\log x)^M$ for any constant $M > 1$. Moreover,

Lemma 3 gives

$$\begin{aligned}
 V_2 &:= \sum_{\substack{q \leq x \\ q \equiv 1 \pmod{m}}} \sum_{\chi_2 \in (\widehat{\mathbb{F}_q^*})^r \setminus \{\chi_0^{(q)}\}} \left| c_m(\chi_2) \sum_{\substack{a \in \mathbb{Z}^r \\ 0 < a \leq T \\ p \mid \prod_{i=1}^r a_i}} \chi_2(\underline{a}) \right| \\
 &\ll \frac{|T|}{p^r} \sum_{\substack{q \leq x \\ q \equiv 1 \pmod{m}}} \sum_{\chi_2 \in (\widehat{\mathbb{F}_q^*})^r \setminus \{\chi_0^{(q)}\}} |c_m(\chi_2)| \\
 &\ll \frac{|T|}{p^r} \sum_{\substack{q \leq x \\ q \equiv 1 \pmod{m}}} \tau\left(\frac{q-1}{m}\right) \\
 &\ll \frac{|T|x}{p^r m}.
 \end{aligned}$$

Thus, for every constant $M' > 2$,

$$H_2 \ll \sum_{\substack{p \leq x \\ p \equiv 1 \pmod{m}}} (U_2 + V_2) \ll \frac{|T|x^2}{(\log x)^{M'}}.$$

Finally, assume $\chi_1 \in \widehat{\mathbb{F}_p^*} \setminus \{\chi_0^{(p)}\}$ and $\chi_2 \in \widehat{\mathbb{F}_q^*} \setminus \{\chi_0^{(q)}\}$ with $p \neq q$; then $\chi_1 \chi_2$ is a primitive character modulo pq . To obtain an upper bound on

$$\begin{aligned}
 H_3 = \sum_{\substack{p, q \leq x \\ p, q \equiv 1 \pmod{m} \\ p \neq q}} \sum_{\chi_1 \in (\widehat{\mathbb{F}_p^*})^r \setminus \{\chi_0^{(p)}\}} \sum_{\chi_2 \in (\widehat{\mathbb{F}_q^*})^r \setminus \{\chi_0^{(q)}\}} c_m(\chi_1) c_m(\chi_2) \\
 \times \sum_{\substack{a \in \mathbb{Z}^r \\ 0 < a \leq T}} \chi_1(\underline{a}) \chi_2(\underline{a}),
 \end{aligned}$$

we will apply again Hölder’s inequality and the large sieve [14, Lemma 5]). To do so, since the r -tuples $\underline{\chi}_1$ and $\underline{\chi}_2$ in H_3 are both non-principal, we denote by $\chi_{1,i}$ the i th component of the r -tuple $\underline{\chi}_1$ (and similarly for $\chi_{2,i}$). Then the contributions to H_3 have two possible sources: a “diagonal” term H_3^d (in which for a certain $i \in \{1, \dots, r\}$ both $\chi_{1,i}$ and $\chi_{2,i}$ are non-principal) and a “non-diagonal” term H_3^{nd} (in which for no $i \in \{1, \dots, r\}$ is it possible to have $\chi_{1,i}$ and $\chi_{2,i}$ both non-principal). Analogously to what was done for the error term (12) in the proof of Theorem 1, the main contributions to H_3^d and H_3^{nd} come from the cases in which, for a certain r -tuple of characters modulo p or q , just one character is non-principal and the other $r - 1$ are

all principal. Explicitly, $H_3^d = \sum_{i=1}^r H_{3,i}$, where

$$\begin{aligned}
 H_{3,i} &:= \sum_{\substack{p,q \leq x \\ p,q \equiv 1 \pmod{m} \\ p \neq q}} \sum_{\substack{\chi_1 \in (\widehat{\mathbb{F}}_p^*)^r \\ \chi_1 \in \widehat{\mathbb{F}}_p^* \setminus \{\chi_0^{(p)}\}}} \sum_{\substack{\chi_2 \in (\widehat{\mathbb{F}}_q^*)^r \\ \chi_2 \in \widehat{\mathbb{F}}_q^* \setminus \{\chi_0^{(q)}\}}} c_m(\underline{\chi}_1) c_m(\underline{\chi}_2) \sum_{\substack{a \in \mathbb{Z}^r \\ 0 < a \leq T}} \underline{\chi}_1(a) \underline{\chi}_2(a) \\
 &\ll \frac{|T|}{T_i} \sum_{\substack{p,q \leq x \\ p,q \equiv 1 \pmod{m} \\ p \neq q}} \sum_{\substack{\chi_1 \in \widehat{\mathbb{F}}_p^* \setminus \{\chi_0^{(p)}\}}} \sum_{\substack{\chi_2 \in \widehat{\mathbb{F}}_q^* \setminus \{\chi_0^{(q)}\}}} d_{m,i}(\chi_1) d_{m,i}(\chi_2) \\
 &\quad \times \left| \sum_{\substack{a_i \in \mathbb{Z} \\ 0 < a_i \leq T_i}} \chi_1(a_i) \chi_2(a_i) \right|
 \end{aligned}$$

and $H_3^{nd} = \sum_{\substack{i,j=1 \\ i \neq j}}^r H_{3,ij}$, with

$$\begin{aligned}
 H_{3,ij} &:= \sum_{\substack{p,q \leq x \\ p,q \equiv 1 \pmod{m} \\ p \neq q}} \sum_{\substack{\chi_1 \in (\widehat{\mathbb{F}}_p^*)^r \\ \chi_1 \in \widehat{\mathbb{F}}_p^* \setminus \{\chi_0^{(p)}\}}} \sum_{\substack{\chi_2 \in (\widehat{\mathbb{F}}_q^*)^r \\ \chi_2 \in \widehat{\mathbb{F}}_q^* \setminus \{\chi_0^{(q)}\}}} c_m(\underline{\chi}_1) c_m(\underline{\chi}_2) \sum_{\substack{a \in \mathbb{Z}^r \\ 0 < a \leq T}} \underline{\chi}_1(a) \underline{\chi}_2(a) \\
 &\ll \frac{|T|}{T_i T_j} \sum_{\substack{p,q \leq x \\ p,q \equiv 1 \pmod{m} \\ p \neq q}} \sum_{\substack{\chi_1 \in \widehat{\mathbb{F}}_p^* \setminus \{\chi_0^{(p)}\}}} \sum_{\substack{\chi_2 \in \widehat{\mathbb{F}}_q^* \setminus \{\chi_0^{(q)}\}}} d_{m,i}(\chi_1) d_{m,j}(\chi_2) \\
 &\quad \times \left| \sum_{\substack{a_i, a_j \in \mathbb{Z} \\ 0 < a_i \leq T_i \\ 0 < a_j \leq T_j}} \chi_1(a_i) \chi_2(a_j) \right|.
 \end{aligned}$$

Dealing first with $H_{3,i}$, we use again Hölder’s inequality together with the large sieve to get

$$\begin{aligned}
 \frac{H_{3,i}}{|T|} &\ll \frac{1}{T_i} \left\{ \sum_{\substack{p,q \leq x \\ p,q \equiv 1 \pmod{m} \\ p \neq q}} \sum_{\substack{\chi_1 \in \widehat{\mathbb{F}}_p^* \setminus \{\chi_0^{(p)}\} \\ \chi_2 \in \widehat{\mathbb{F}}_q^* \setminus \{\chi_0^{(q)}\}}} [d_{m,i}(\chi_1) d_{m,i}(\chi_2)]^{\frac{2s_i}{2s_i-1}} \right\}^{\frac{2s_i-1}{2s_i}} \\
 &\quad \times \left\{ \sum_{\substack{p,q \leq x \\ p,q \equiv 1 \pmod{m} \\ p \neq q}} \sum_{\eta \pmod{pq}} \left| \sum_{\substack{a_i \in \mathbb{Z} \\ 0 < a_i \leq T_i}} \eta(a_i) \right|^{2s_i} \right\}^{1/2s_i} \\
 &\ll \frac{1}{T_i} \left\{ \left(\frac{x \log \log x}{m^2} \right)^{4s_i-2} (x^4 + T_i^{s_i}) T_i^{s_i} (\log(eT_i^{s_i-1}))^{s_i^2-1} \right\}^{1/2s_i}.
 \end{aligned}$$

We now choose $s_i = \lfloor \frac{4 \log x}{\log T_i} \rfloor + 1$, so that $T_i^{s_i-1} \leq x^4 \leq T_i^{s_i}$ and

$$\frac{H_{3,i}}{|\underline{T}|} \ll \frac{1}{m^2} x^{2-1/s_i} (\log \log x)^2 (\log(e x^4))^{\frac{s_i^2-1}{2s_i}}.$$

If $T_i > x^4$ then $s_i = 1$ and $H_{3,i}/|\underline{T}| \ll x(\log \log x)^2$. Otherwise, if $T_i \leq x^4$ then $s_i \geq 2$ and assuming $T_i > \exp(6(\log x \log \log x)^{1/2})$, similarly to what was done to prove Theorem 1 we get

$$\frac{H_{3,i}}{|\underline{T}|} \ll x^{2-1/s_i} (\log \log x)^2 (\log(e x^4))^{\frac{3 \log x}{\log T_i}} \ll \frac{x^2}{(\log x)^D}$$

for any positive constant $D > 2$.

It remains to estimate $H_{3,ij}$ where $i \neq j$. In this case $H_{3,ij}$ can be factorized into two products, and by the same methods used for (13) we get

$$\begin{aligned} \frac{H_{3,ij}}{|\underline{T}|} &\ll \frac{1}{T_i T_j} \sum_{\substack{p \leq x \\ p \equiv 1 \pmod{m}}} \sum_{\chi_1 \in \widehat{\mathbb{F}_p^*} \setminus \{\chi_0^{(p)}\}} d_{m,i}(\chi_1) \left| \sum_{\substack{a_i \in \mathbb{Z} \\ 0 < a_i \leq T_i}} \chi_1(a_i) \right| \\ &\times \sum_{\substack{q \leq x \\ q \equiv 1 \pmod{m}}} \sum_{\chi_2 \in \widehat{\mathbb{F}_q^*} \setminus \{\chi_0^{(q)}\}} d_{m,j}(\chi_2) \left| \sum_{\substack{a_j \in \mathbb{Z} \\ 0 < a_j \leq T_j}} \chi_2(a_j) \right| \\ &\ll \frac{1}{T_i} \left\{ \left(\frac{x \log \log x}{m^2} \right)^{2s_i-1} (x^2 + T_i^{s_i}) T_i^{s_i} (\log(e T_i^{s_i-1}))^{s_i^2-1} \right\}^{1/2s_i} \\ &\times \frac{1}{T_j} \left\{ \left(\frac{x \log \log x}{m^2} \right)^{2s_j-1} (x^2 + T_j^{s_j}) T_j^{s_j} (\log(e T_j^{s_j-1}))^{s_j^2-1} \right\}^{1/2s_j}. \end{aligned}$$

We choose $s_i = \lfloor \frac{2 \log x}{\log T_i} \rfloor + 1$ and $s_j = \lfloor \frac{2 \log x}{\log T_j} \rfloor + 1$, so that

$$\frac{H_{3,ij}}{|\underline{T}|} \ll \frac{x^2}{(\log x)^E}$$

for every constant $E > 2$.

Eventually, since $H_3 \ll H_3^d + H_3^{nd}$, summing the upper bounds for H_1 , H_2 and H_3 we get the proof of Theorem 2. ■

Acknowledgements. The results in this manuscript are part of the doctoral dissertation of the two authors at Università Roma Tre. The authors would like to thank Prof. Francesco Pappalardi for inspiring this work and for his precious suggestions concerning technical difficulties in the proofs. C. P. acknowledges the financial support provided by Università Roma Tre during his Ph.D. studies. Furthermore, during the final steps of the revision process, C. P. has been partially supported by TUBITAK within the project 113F059 entitled “The conjecture of Mazur–Tate–Teitelbaum,

CM elliptic curves and applications” as a postdoctoral researcher at Koc University.

References

- [1] L. Bach and F. Shallit, *Algorithmic Number Theory (Vol. I: Efficient Algorithms)*, MIT Press, Cambridge, 1996.
- [2] L. Cangelmi and F. Pappalardi, *On the r -rank Artin conjecture II*, J. Number Theory 75 (1999), 120–132.
- [3] A. T. Felix, *Generalizing the Titchmarsh divisor problem*, Int. J. Number Theory 8 (2012), 613–629.
- [4] A. Fiorilli, *On a theorem of Bombieri, Friedlander and Iwaniec*, Canad. J. Math. 64 (2012), 1019–1035.
- [5] R. Gupta and M. Ram Murty, *A remark on Artin’s conjecture*, Invent. Math. 78 (1984), 127–130.
- [6] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 4th ed., Oxford Univ. Press, London, 1975.
- [7] D. R. Heath-Brown, *Artin’s conjecture for primitive roots*, Quart. J. Math. Oxford (2) 37 (1986), 27–38.
- [8] C. Hooley, *On Artin’s conjecture*, J. Reine Angew. Math. 225 (1967), 209–220.
- [9] H. Montgomery, *Primes in arithmetic progressions*, Michigan Math. J. 17 (1970), 33–39.
- [10] P. Moree, *Artin’s primitive root conjecture—a survey*, Integers 12A (2012), A13, 100 pp.
- [11] P. Moree, *Asymptotically exact heuristics for (near) primitive roots*, J. Number Theory 83 (2000), 155–181.
- [12] F. Pappalardi, *The r -rank Artin conjecture*, Math. Comp. 66 (1997), 853–868.
- [13] F. Pappalardi and A. Susa, *An analogue to Artin’s conjecture for multiplicative subgroups of the rationals*, Arch. Math. (Basel) 101 (2013), 319–330.
- [14] P. J. Stephens, *An average result for Artin’s conjecture*, Mathematika 16 (1969), 178–188.
- [15] P. J. Stephens, *Prime divisors of second order linear recurrences. II*, J. Number Theory 8 (1976), 333–345.
- [16] E. C. Titchmarsh, *A divisor problem*, Rend. Circ. Mat. Palermo 54 (1930), 414–429.
- [17] A. Walfisz, *Zur additiven Zahlentheorie II*, Math. Z. 40 (1936), 592–607.

Lorenzo Menici
 Dipartimento di Matematica
 Università Roma Tre
 Largo S. L. Murialdo, 1
 I-00146 Roma, Italy
 E-mail: menici@mat.uniroma3.it

Cihan Pehlivan
 Department of Mathematics
 Koc University
 Rumelifeneri Yolu
 34450 Sarıyer-İstanbul, Turkey
 E-mail: cpehlivan@ku.edu.tr