Scuola Dottorale in Scienze Matematiche e Fisiche

Dottorato di Ricerca in Matematica
XXVII Ciclo

HIGHER RANK ARTIN'S CONJECTURE WITH WEIGHT AND AVERAGE RESULTS

Candidato:
Lorenzo Menici

Relatore:
Prof. Francesco Pappalardi

Coordinatore:
Prof. Luigi Chierchia

Anno Accademico 2015/2016

Introduction

Artin's conjecture (AC) on primitive roots is one of the most important open problems in number theory. The conjecture states that for any given integer $a \neq 0, -1$ which is not a square there exist infinitely many prime numbers p such that a is a primitive root modulo p. More precisely, if $N_a(x) := \#\{p \leqslant x : \mathbb{F}_p^* = \langle a \pmod p \rangle\}$, then as $x \to \infty$

$$N_a(x) \sim A(a)\,\mathrm{Li}(x)\ ,$$

where the constant $A(a)$ is a rational multiple of the so-called Artin's constant

$$A = \prod_p \left(1 - \frac{1}{p(p-1)}\right)\ .$$

Many attempts have been made to prove this conjecture and, so far, the only proofs of the "classical" AC and of many of its "variations" (like the higher rank AC, the weighted AC and the AC on average, studied in this thesis) rely on the Generalized Riemann Hypothesis (GRH). In particular, the classical AC has been proved under GRH by Hooley [9], so that we have the following:

Theorem (Hooley)**.** *Consider an integer $a \neq 0, -1$ which is not a perfect square and let h be the largest integer such that $a = a_0^h$; denote with d the discriminant of the quadratic extension $\mathbb{Q}(\sqrt{a})$. Assuming GRH for the number field $\mathbb{Q}(\zeta_n, a^{1/n})$ for every squarefree n, then*

$$N_a(x) = \delta_a\,\mathrm{Li}(x) + O_a\left(\frac{x \log\log x}{\log^2 x}\right)\ ,$$

where

$$\delta_a = \sum_{n \geqslant 1} \frac{\mu(n)}{[\mathbb{Q}(\zeta_n, a^{1/n}) : \mathbb{Q}]} = \begin{cases} A(h) & \text{if } d \not\equiv 1 \ (\mathrm{mod} 4)\,, \\ \left(1 - \mu(|d|) \prod_{\substack{q \mid d \\ q \mid h}} \frac{1}{q-2} \prod_{\substack{q \mid d \\ q \nmid h}} \frac{1}{q^2-q-1}\right) A(h) & \text{if } d \equiv 1 \ (\mathrm{mod} 4)\,, \end{cases}$$

with

$$A(h) = \prod_{p \nmid h} \left(1 - \frac{1}{p(p-1)}\right) \prod_{p \mid h} \left(1 - \frac{1}{p-1}\right)\ .$$

A possible generalization of the classical AC[1] is the so-called "higher rank AC" or "r-rank AC", meaning that we now deal with a finitely generated subgroup of the rationals $\Gamma \subset \mathbb{Q}$ of rank $r < \infty$ (instead of the classical 1-rank conjecture): this subgroup will have the form $\Gamma = \langle g_1, \ldots, g_r \rangle$ where $(g_1 \ldots g_r)$ is an r-tuple of multiplicatively independent rational numbers and its reduction $\Gamma_p = \langle g_1 \pmod p, \ldots, g_r \pmod p \rangle$ is well-defined for almost all prime numbers.

In Chapter 1 we will see some results concerning the r-rank AC, where one is interested in those primes p for which the index $i_p := [\mathbb{F}_p^* : \Gamma_p] = 1$, together with the "quasi" r-rank AC, where one looks after those primes for which $i_p = m$ for a certain natural number m dividing $p-1$: these results will be used to prove the original results of Chapters 2 and 3.

Chapter 2 deals with what can be called "weighted r-rank AC", meaning that we consider the sum

$$\sum_{p \leqslant x} f(i_p) \tag{1}$$

where $f(n)$ is a generic arithmetic function that "weights" the indices i_p. This is the r-rank generalization of the work of Pappalardi [23], where the specific case $\Gamma = \langle 2 \rangle$ was considered. Various theorems on the asymptotic behavior for $x \to \infty$ of the sum (1) are presented, both unconditionally and under GRH, together with different applications. The original results of this Chapter appear in the submitted paper [16].

In Chapter 3 is presented a joint work with Cihan Pehlivan [17] on the r-rank AC on average. This work is the higher rank generalization of the original work of Stephens [31], where it was proved that, if $T > \exp(4(\log x \log\log x)^{1/2})$, then

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

where D is an arbitrary constant greater than 1; in the same paper it was also proved that, assuming $T > \exp(6(\log x \log\log x)^{1/2})$, then

$$\frac{1}{T}\sum_{a \leqslant T} \{N_a(x) - A\,\mathrm{Li}(x)\}^2 \ll \frac{x^2}{(\log x)^{D'}},$$

for any constant $D' > 2$. In Chapter 3 the analogous averages are studied, for the case $\Gamma = \langle a_1, \cdots, a_r \rangle$, with $a_i \in \mathbb{Z}$ for all $i = 1, \ldots, r$; the following unconditional theorems are proved:

Theorem. *Let $T^* := \min\{T_i : i = 1, \ldots, r\} > \exp(4(\log x \log\log x)^{\frac{1}{2}})$ and $m \leqslant (\log x)^D$ for an arbitrary positive constant D. Then*

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

[1] For an exhaustive survey that discuss different generalizations of AC, see [20].

where $C_{r,m} := \sum_{n\geqslant 1}\frac{\mu(n)}{(nm)^r\varphi(nm)}$ *and* $M > 1$ *is arbitrarily large.*

Theorem. *Let* $T^* > \exp(6(\log x \log\log x)^{\frac{1}{2}})$ *and* $m \leqslant (\log x)^D$ *for an arbitrary positive constant* D*. Then*

$$\frac{1}{T_1\cdots T_r}\sum_{\substack{a_i\in\mathbb{Z}\\ 0<a_1\leqslant T_1\\ \vdots\\ 0<a_r\leqslant T_r}}\left\{N_{\langle a_1,\cdots,a_r\rangle,m}(x) - C_{r,m}\,\mathrm{Li}(x)\right\}^2 \ll \frac{x^2}{(\log x)^{M'}}$$

where $M' > 2$ *is arbitrarily large.*

Finally, in Chapter 4 we expose the ongoing work that will be subject of a future joint paper with Francesco Pappalardi [18].

Notations

We give a list of notations we will use in the thesis. We denote with $\mathbb{Z}$ the ring of integers and with $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ respectively the field of rational, real and complex numbers. If not differently specifies, p, q and ℓ will always denote prime numbers. $\mathbb{F}_p$ is the finite field with p elements. Given an integer $n \neq 0$, its p-adic valuation is $v_p(n) = \max\{k \in \mathbb{N} : p^k \mid n\}$; hence, the p-adic valuation of a rational number $g = a/b$ is defined as $v_p(g) = v_p(a) - v_p(b)$.

In the whole thesis, $\Gamma \subset \mathbb{Q}^*$ is a finitely generated subgroup of the rationals with rank r: we can think about it as $\Gamma = \langle g_1, \ldots, g_r \rangle$ with generators g_i multiplicatively independent, that is $g_1^{e_1} g_2^{e_2} \cdots g_r^{e_r} = 1$ only if $e_1 = e_2 = \ldots = e_r = 0$. We define $\mathrm{Supp}(\Gamma) = \{p : v_p(g) \neq 0, g \in \Gamma\}$ and $\sigma_\Gamma = \prod_{p \in \mathrm{Supp}(\Gamma)} p$ The reduction of Γ modulo a prime p is well defined for every prime $p \nmid \sigma_\Gamma$ and it's denoted as $\Gamma_p = \langle g_1 \pmod p, \ldots, g_r \pmod p \rangle$. The order of Γ_p is indicated as $|\Gamma_p|$ and the relative index is $i_p = [\mathbb{F}_p^* : \Gamma_p]$.

For every positive integer n, we set $K_n(\Gamma) := \mathbb{Q}(\zeta_n, \Gamma^{1/n})$, the (Kummer) field generated by the n-th roots of the elements of Γ and by the n-th root of unity $\zeta_n = e^{2\pi i/n}$; we also indicate with $k_n(\Gamma) := [K_n(\Gamma) : \mathbb{Q}]$ the relative degree.

For two real functions $f(x), g(x)$, we write $f(x) = O(g(x))$ (or equivalently $f(x) \ll g(x)$) as $x \to \infty$ if and only if there exists a constant $C > 0$ and a real number x_0 such that $|f(x)| \leqslant Cg(x)$ for all $x \geqslant x_0$. As a consequence, $O(1)$ stands for an arbitrary constant. We write $f(x) = o(g(x))$ if $\lim_{x \to \infty} f(x)/g(x) = 0$.

The logarithmic integral $\mathrm{Li}(x)$ is defined as

$$\mathrm{Li}(x) := \int_2^x \frac{dt}{\log t}$$

and from the Prime Number Theorem we know that, asymptotically as $x \to \infty$, $\mathrm{Li}(x) \sim x/\log x \sim \pi(x)$, where $\pi(x) := \#\{p \leqslant x\}$ is the prime counting function.

Given a number field K (i.e. a finite-dimensional field extension of $\mathbb{Q}$), we consider the set $\mathcal{I}$ of the non-zero ideals I of its ring of integers $\mathcal{O}_K$. The Dedekind zeta function of K is then defined as

$$\zeta_K(s) := \sum_{I \in \mathcal{I}} \frac{1}{(N(I))^s}$$

where $N(I) = [\mathcal{O}_K : I]$ is the norm of the ideal I and $s = \sigma + it$ is a complex number: it can be shown that $\zeta_K(s)$ has an analytic continuation to a meromorphic function on $\mathbb{C}\backslash\{1\}$, having a single pole at $s = 1$. The Generalized Riemann Hypothesis (GRH) is an unproven conjecture which says that if $\zeta_K(s) = 0$ and $0 < \sigma < 1$, then $\sigma = 1/2$.

Acknowledgements

First of all, I want to thank my advisor, Francesco Pappalardi, for all the help, answers and patience he has generously offered to me during all the period of preparation of this thesis. Moreover, I would like to thank him for his moral support and understanding in my difficult times.

I also would like to thank Cihan Pehlivan for his efforts in our joint work on the average of r-rank Artin's conjecture.

Finally, I want to thank my partner Angelita and my parents for their constant support during these years.

Contents

Introduction **i**

Notations **v**

Acknowledgements **vii**

1 Higher rank Artin's conjecture on primitive roots: an overview **1**
- 1.1 Artin's conjecture on primitive roots: an overview . . . 1
  - 1.1.1 The Chebotarev Density Theorem . . . 2
- 1.2 r-rank Artin's conjecture . . . 3
- 1.3 r-rank quasi-Artin's conjecture . . . 5

2 r-rank Artin's conjecture with weights **7**
- 2.1 Introduction . . . 7
- 2.2 Main results for $\sum_{p\leqslant x,\, p\nmid\sigma_\Gamma} f(i_p)$ . . . 9
  - 2.2.1 Conditional case . . . 9
  - 2.2.2 Unconditional case . . . 11
- 2.3 Examples and applications . . . 14
  - 2.3.1 $f(n)$ multiplicative function . . . 15
  - 2.3.2 $f(n) = \chi_B(n)$ characteristic function of a subset $B \subset \mathbb{N}$ . . . 20
  - 2.3.3 Indices i_p in arithmetic progression . . . 23
  - 2.3.4 Average order of Γ_p over primes . . . 25

3 Average r-rank Artin's conjecture **27**
- 3.1 Introduction . . . 27
- 3.2 Notations and conventions . . . 30
- 3.3 Lemmata . . . 30
- 3.4 Proof of Theorem 1 . . . 38
- 3.5 Proof of Theorem 2 . . . 44

4 Work in progress **51**

Bibliography **55**

Chapter 1

Higher rank Artin's conjecture on primitive roots: an overview

In this Chapter we present some results that will be used in Chapters 2 and 3.

1.1 Artin's conjecture on primitive roots: an overview

We describe in this Section the basic ideas behind the study of Artin's conjecture on primitive roots; we first focus on the classical 1-rank case, then we generalize the problem for a generic (finite) rank r.

In 1927 Artin conjectured that, given any number $a \in \mathbb{Q}\backslash\{0,-1\}$ which is not a perfect square, then there exist infinitely many prime numbers p for which a is a primitive root modulo p. Moreover, Artin estimated that if we denote $N_a(x) := \#\{p \leqslant x : [\mathbb{F}_p^* : \langle a \pmod p\rangle] = 1\}$, then

$$N_a(x) \sim \delta_a \operatorname{Li}(x) ,$$

as $x \to \infty$, where δ_a is a non-vanishing constant depending only on a.

For a fixed prime number p, a rational number a such that $v_p(a) = 0$ is a primitive root modulo p if and only if $a^{\frac{p-1}{q}} \not\equiv 1 \pmod p$ for every prime $q \mid (p-1)$. In order to study the asymptotic behavior of $N_a(x)$ as $x \to \infty$ we can think of fixing q in order to look after those primes $p \equiv 1 \pmod q$ such that $a^{\frac{p-1}{q}} \not\equiv 1 \pmod p$ and we do that for every fixed prime number q. Consequently, a not be a primitive root modulo p if the conditions $p \equiv 1 \pmod q$ and $a^{\frac{p-1}{q}} \equiv 1 \pmod p$ are simultaneously satisfied. But $p \equiv 1 \pmod q$ if and only if the equation $x^q \equiv 1 \pmod p$ has q distinct solutions and $a^{\frac{p-1}{q}} \not\equiv 1 \pmod p$ if and only if the equation $x^q \equiv a \pmod p$ is solvable. Then, the primes $p \equiv 1 \pmod q$ satisfying $a^{\frac{p-1}{q}} \not\equiv 1 \pmod p$ split completely in the field $K_q(a) = \mathbb{Q}(\zeta_q, a^{1/q})$; since the converse is also true, we have

$$p \equiv 1 \pmod q \wedge a^{\frac{p-1}{q}} \equiv 1 \pmod p \Longleftrightarrow p \text{ splits completely in } K_q(a)\ .$$

So if we indicate with $P_p[K_q(a)]$ the probability that a prime p splits completely in $K_q(a)$, a naive probabilistic approach to Artin's conjecture should lead to the probability

$$\prod_q (1 - P_p[K_q(a)])$$

for a to be a primitive root modulo p. Unfortunately, for generic primes p, p', q, q' the events $P_p[K_q(a)]$ and $P_{p'}[K_{q'}(a)]$ are not in general independent and the previous reasoning must be modified, as was already known to Artin himself by the numerical results of the Lehmers [14].

1.1.1 The Chebotarev Density Theorem

One of the main tools used in the study to Artin's conjecture on primitive roots is the *Chebotarev Density Theorem* [3]. This powerful theorem can be stated as follows:

Theorem 1.1.1 (Chebotarev)**.** *Let F be a number field and K/F a finite Galois extension with Galois group $G = \mathrm{Gal}(K/F)$; given any conjugacy class $C \subset G$, then the set of unramified primes $\mathfrak{p} \subset \mathcal{O}_F$ for which the Frobenius substitution $\sigma_{\mathfrak{p}}$ has conjugacy class C has density $|C|/|G|$.*

In our case, we are interested in those primes $p \in \mathbb{Z}$ that split completely in $K_q(a)$, so that the conjugacy class we are dealing with is the trivial one $C = \{\mathrm{id}\}$. From Chebotarev Density Theorem then

$$\#\{p \leqslant x : \text{ splits completely in } K_q(a)\} \sim \frac{1}{[K_q(a) : \mathbb{Q}]} \mathrm{Li}(x)\ ,$$

as $x \to \infty$.

For any squarefree n, we can consider the compositum $K_m(a)$ of the fields $K_q(a)$ with $q \mid m$ and we have $K_m(a) = \mathbb{Q}(\zeta_m, a^{1/m})$; since we are looking for those primes p that do not split in any $K_q(a)$, by the inclusion-exclusion principle we are led to formulate Artin's conjecture as follows:

Conjecture 1.1.2 (Artin)**.** *Let $a \in \mathbb{Q}\backslash\{0, \pm 1\}$ and $h = \max\{n \in \mathbb{N} : a \in \mathbb{Q}^{*n}\}$, then*

$$N_a(x) = \#\{p \leqslant x : [\mathbb{F}_p^* : \langle a \ (mod\ p)\rangle] = 1\} \sim \delta_a \,\mathrm{Li}(x)\ , \qquad x \to \infty\ ,$$

with

$$\delta_a = \sum_{m \geqslant 1} \frac{\mu(m)}{[K_m(a) : \mathbb{Q}]} = \begin{cases} A(h) & \text{if } d \not\equiv 1 \ (\mathrm{mod} 4)\,, \\ \left(1 - \mu(|d|) \prod_{\substack{q \mid d \\ q \mid h}} \frac{1}{q-2} \prod_{\substack{q \mid d \\ q \nmid h}} \frac{1}{q^2-q-1}\right) A(h) & \text{if } d \equiv 1 \ (\mathrm{mod} 4)\,, \end{cases}$$

and

$$A(h) = \prod_p \left(1 - \frac{(p,h)}{p(p-1)}\right) .$$

Now let $i_p := [\mathbb{F}_p^* : \langle a \pmod p\rangle]$, $\mathrm{Supp}(a) := \{p : v_p(a) \neq 0\}$ and, for any squarefree m, $\pi_a(x,m) := \{p \leqslant x : p \notin \mathrm{supp}(a), m \mid i_p\}$; we notice that, for any prime $p \notin \mathrm{Supp}(a)$,

$$p \equiv 1 \pmod m \wedge a^{\frac{p-1}{m}} \equiv 1 \pmod p \iff m \mid i_p .$$

The following theorem is effective version of Chebotarev Density Theorem due to Lagarias and Odlyzko [12]:

Theorem 1.1.3. *Assuming GRH for the Dedekind zeta function of $K_m(a)$, then*

$$\pi_a(x,m) = \frac{1}{[K_m(a) : \mathbb{Q}]} \mathrm{Li}(x) + O(\sqrt{x}\log(mx)) . \tag{1.1}$$

Unconditionally, there exists an absolute constant A such that, if $m \leqslant (\log x)^{1/7}$, then

$$\pi_a(x,m) = \frac{1}{[K_m(a) : \mathbb{Q}]} \mathrm{Li}(x) + O(x\exp(-A\sqrt{\log x}/m)) . \tag{1.2}$$

Conjecture 1.1.2 was first proven by Hooley [9] assuming GRH for the Dedekind zeta function associated to the field $K_m(a)$ for any m. The necessity of assuming GRH can be explained as follows: one can prove unconditionally that, if $\xi(x)$ is a real-valued function that goes to infinity slowly enough, then the proportion of prime numbers p that do not split completely in $K_q(a)$ for any prime $q \leqslant \xi(x)$ is exactly δ_a as $x \to \infty$, but one cannot prove the same for those primes $q > \xi(x)$. The reason for that lies in the tail of the inclusion-exclusion: without GRH, the errors for all the prime numbers $q > \xi(x)$ due to unconditional version of Chebotarev Density Theorem (1.2) give a contribution that overwhelms the main term $\delta_a x/\log x$ in Artin's conjecture. But, assuming GRH, the errors from (1.1) in the tail give an overall error which is $o(x/\log x)$.

1.2 r-rank Artin's conjecture

One of the most impressive results on Artin's conjecture is the unconditional theorem by Gupta and Ram Murty [7] and its successive refinement by Heath-Brown [10]: it is a 3-rank case whose main result can be stated as follows:

Theorem (Gupta, Ram Murty, Heath-Brown)**.** *Let a_1, a_2 and a_3 be non-zero multiplicatively independent integers. Suppose that none of a_1, a_2, a_3, $-3a_1a_2$, $-3a_1a_3$, $-3a_2a_3$ and $a_1a_2a_3$ is a square. Then for at least one $i \in \{1,2,3\}$ we have*

$$N_{a_i}(x) \gg \frac{x}{\log^2 x} .$$

If we consider Γ_p, the reduction modulo p of a finitely generated subgroup of rationals $\Gamma \subset \mathbb{Q}^*$ of rank $r \geqslant 1$, the problem is now to study the asymptotic behavior of the quantity $N_\Gamma(x) := \#\{p \leqslant x : [\mathbb{F}_p^* : \Gamma_p] = 1\}$. The strategy is similar to the one used in the 1-rank case but, instead of the field $K_m(a)$ previously discussed, we now need to take into account the field $K_m(\Gamma) = \mathbb{Q}(\zeta_m, \Gamma^{1/m})$. This problem has been studied by Pappalardi in [24] and few years later together with Cangelmi in [2]:

Theorem 1.2.1 (Pappalardi)**.** *Let $\Gamma \subset \mathbb{Q}^*$ be a finitely generated subgroup of rank r. Assuming GRH for the Dedekind zeta function of $\mathbb{Q}(\zeta_m, \Gamma^{1/m})$, we have*

$$N_\Gamma(x) = \delta_\Gamma \frac{x}{\log x} + O\left(\frac{x}{(\log x)^{r+1}(\log\log x)^r}\right) ,$$

where the implied O-constant depends only on Γ and

$$\delta_\Gamma = \sum_{m \geqslant 1} \frac{\mu(n)}{[\mathbb{Q}(\zeta_m, \Gamma^{1/m}) : \mathbb{Q}]} .$$

The density δ_Γ was first computed in [24] for the case $\Gamma = \langle p_1, \ldots, p_r\rangle$ with p_i odd prime for every $i = 1, \ldots, r$ and successively in the general case $\Gamma \subset \mathbb{Q}^*$ in [2]. In order to perform density computations in the r-rank case, we need expressions for the degree $k_n(\Gamma) := [K_n(\Gamma) : \mathbb{Q}]$. We know (see Lang [13, Theorem 8.1]) that the degree of the extension

$$k_n(\Gamma) = \varphi(n)\#\left\{\Gamma\mathbb{Q}(\zeta_n)^{*n}/\mathbb{Q}(\zeta_n)^{*n}\right\} . \tag{1.3}$$

In particular, to express δ_Γ as an Euler product, we should exploit a useful formula for $k_n(\Gamma)$; we can investigate the properties of this extension degree using the results in [25, Lemma 1, Corollary 1]:

Lemma 1.2.2. *(Pappalardi) Let $\Gamma \subset \mathbb{Q}^*$, if $\alpha = v_2(n)$ is the 2–adic valuation, then*

$$k_n(\Gamma) = \frac{\varphi(n)\,|\Gamma(n)|}{|\widetilde{\Gamma}(n)|} , \tag{1.4}$$

where

$$\Gamma(n) = \Gamma \cdot \mathbb{Q}^{*n}/\mathbb{Q}^{*n}$$

and

$$\widetilde{\Gamma}(n) = (\Gamma \cap \mathbb{Q}(\zeta_n)^{*^{2^\alpha}})\,\mathbb{Q}^{*^{2^\alpha}}/\mathbb{Q}^{*^{2^\alpha}} .$$

Moreover, if $\Gamma \subset \mathbb{Q}^+$, then

$$\widetilde{\Gamma}(n) = \left\{m \in \mathbb{N} :\ m \mid \sigma_\Gamma,\ m^{2^{\alpha-1}}\mathbb{Q}^{*^{2^\alpha}} \in \Gamma(2^\alpha),\ \Delta(m) \mid n\right\} , \tag{1.5}$$

where $\Delta(m)$ is the field discriminant of the real quadratic extension $\mathbb{Q}(\sqrt{m})$.

Different results in this thesis depend on equation (1.5), which holds only for r-rank positive subgroups of the rationals. To widen the validity of these results, the author, in collaboration with Francesco Pappalardi, is currently working on a generalization of equation (1.5) to the case of arbitrary finitely generated subgroups $\Gamma \subset \mathbb{Q}^*$, as will be briefly discussed in Chapter 4.

Similarly to the 1-rank case, the key ingredient for the proof of Theorem 1.2.1 is the Chebotarev Density Theorem, which provides us with an asymptotic formula with error for $\pi_\Gamma(x,n) := \#\{p \leqslant x : p \nmid \sigma_\Gamma , n | i_p\}$. The following statement is obtained using the effective versions[30, Théorème 4] and [26, Lemma 4.1] in the conditional case, [12, Theorem 1.3–1.4] and [25, Lemma 4] in the unconditional case.

Theorem 1.2.3 (Chebotarev Density Theorem)**.** *Let $\Gamma \subset \mathbb{Q}^*$ be a finitely generated subgroup of rank r and $n \in \mathbb{N}^+$. suppose that the Generalized Riemann Hypothesis (GRH) holds for the Dedekind zeta function of $K_n(\Gamma)$. Then, as $x \to \infty$,*

$$\pi_\Gamma(x,n) = \frac{1}{k_n(\Gamma)} \operatorname{li}(x) + O_\Gamma\left(\sqrt{x}\log(xn^{r+1})\right) . \tag{1.6}$$

Unconditionally, there exist constants c_1 and c_2 depending only on Γ such that, uniformly for

$$n \leqslant c_1 \left(\frac{\log x}{(\log\log x)^2}\right)^{1/(3r+3)} ,$$

as $x \to \infty$,

$$\pi_\Gamma(x,n) = \frac{1}{k_n(\Gamma)} \operatorname{li}(x) + O_\Gamma\left(\frac{x}{e^{c_2 \sqrt[6]{\log x}\cdot \sqrt[3]{\log\log x}}}\right) . \tag{1.7}$$

1.3 r-rank quasi-Artin's conjecture

For every m dividing $p-1$, let

$$N_\Gamma(x,m) := \#\{p \leqslant x : p \nmid \sigma_\Gamma , i_p = m\} ; \tag{1.8}$$

the asymptotic behavior of $N_\Gamma(x,m)$ is the subject of study of the so-called r-rank quasi-Artin's conjecture.

Concerning the case $r=1$, the first result of this kind, due to Murata, appears in [22]:

Theorem 1.3.1. *(Murata) Let $\Gamma = \langle g \rangle$ with $g \in \mathbb{Q}^* \backslash \{\pm 1\}$ not a perfect square. Assuming GRH, for every $\epsilon > 0$ we have*

$$N_{\langle g \rangle}(x,m) = \rho_{\langle g \rangle, m} \operatorname{li}(x) + O\left(\frac{m^\epsilon x \log\log x}{\log^2 x}\right) , \tag{1.9}$$

where the implied constant depends only on ϵ.

Recently in [26] Pappalardi and Susa proved the following:

Theorem 1.3.2. *(Pappalardi, Susa) Let $\Gamma \subset \mathbb{Q}^*$ be finitely generated subgroup of rank $r \geqslant 2$ and let $m \in \mathbb{N}$. Assume that the GRH holds for the fields of the form $\mathbb{Q}(\zeta_k, \Gamma^{1/k})$ with $k \in \mathbb{N}$. Then, for any $\epsilon > 0$ and for $m \leqslant x^{\frac{r-1}{(r+1)(4r+2)}-\epsilon}$,*

$$N_\Gamma(x,m) = \left(\rho_{\Gamma,m} + O\left(\frac{1}{\varphi(m^{r+1})\log^r x}\right)\right) \mathrm{li}(x),$$

where

$$\rho_{\Gamma,m} := \sum_{n\geqslant 1} \frac{\mu(n)}{k_{mn}(\Gamma)} \ . \tag{1.10}$$

In particular, if $\Gamma \subset \mathbb{Q}^+ = \{q \in \mathbb{Q} : q > 0\}$ and with the notation $\Gamma(k) = \Gamma \cdot \mathbb{Q}^{*k}/\mathbb{Q}^{*k}$,

$$\rho_{\Gamma,m} \ll \frac{1}{\varphi(m)|\Gamma(m)|} \prod_{\substack{p>2 \\ p\nmid m}} \left(1 - \frac{1}{(p-1)|\Gamma(p)|}\right) \ . \tag{1.11}$$

Notice that $\rho_{\Gamma,m}$ is a rational multiple of

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

the so-called r-Artin's constant.

Chapter 2

r-rank Artin's conjecture with weights

The results discussed in this Chapter appears in the work [16].

2.1 Introduction

Given an arithmetic function $f : \mathbb{N} \to \mathbb{C}$, we study the asymptotic behavior of the sum

$$\sum_{\substack{p \leqslant x \\ p \nmid \sigma_\Gamma}} f(i_p) , \qquad x \to \infty . \tag{2.1}$$

In the case

$$f(n) = \chi_{\{1\}}(n) = \begin{cases} 1 & \text{if } n = 1 , \\ 0 & \text{if } n > 1 , \end{cases}$$

we obtain the generalization of the original Artin's conjecture on primitive roots to the case of subgroups of rationals with finite rank r for which the main result is Theorem 1.2.1. The sum (2.1) is the r-rank generalization of the analogous sum considered in [23], where the author focused on the case $\Gamma = \langle 2 \rangle$. Notice that, from (1.8), the sum (2.1) can be rewritten as

$$\sum_{\substack{p \leqslant x \\ p \nmid \sigma_\Gamma}} f(i_p) = \sum_{m \geqslant 1} f(m) \, N_\Gamma(x, m) . \tag{2.2}$$

Setting

$$\pi_\Gamma(x, n) := \# \left\{ p \leqslant x : \; p \nmid \sigma_\Gamma \, , \; n | i_p \right\} \; ,$$

we have shown in Chapter 1 that, when $\Gamma = \langle a \rangle$, with $a \in \mathbb{Z} \backslash \{0, \pm 1\}$ being not a perfect square, the intuition behind Hooley's proof of Artin's conjecture (under GRH) is based on the identity

$$\# \{p \leqslant x : \ p \nmid \sigma_\Gamma \, , \ i_p = 1\} = \sum_{n \geqslant 1} \mu(n) \pi_\Gamma(x, n), \tag{2.3}$$

which is nothing but the inclusion-exclusion principle. The natural generalization of (2.3) is the identity

$$\sum_{\substack{p \leqslant x \\ p \nmid \sigma_\Gamma}} f(i_p) = \sum_{n \geqslant 1} \widetilde{f}(n) \pi_\Gamma(x, n) \ , \tag{2.4}$$

where, by Möbius inversion, $\widetilde{f}(n) = \sum_{d|n} \mu(n/d) f(d)$ and $f(m) = \sum_{n|m} \widetilde{f}(n)$.

To prove the unconditional results of Section 2.2.2, we will provide in Lemma 2.2.3 the unconditional analogue of Theorems 1.3.1 and 1.3.2.

Remarks/assumptions.

- The sum appearing in the right-hand side of equation (2.2) is finite: in fact, $N_\Gamma(x, m) = 0$ if $m \geqslant x$;
- from the estimate (1.11), obviously $\rho_{\Gamma,m} \ll 1/\varphi(m)$;
- if not conversely specified, p and q indicate prime numbers;
- we will indicate $(a, b) := \gcd(a, b)$;
- in the whole paper we will suppose that

$$\sum_{m \geqslant 1} |f(m)| \, \rho_{\Gamma,m} < \infty \tag{2.5}$$

together with

$$\sum_{m \geqslant 1} \frac{|\widetilde{f}(m)|}{k_m(\Gamma)} < \infty \ . \tag{2.6}$$

For the theorems we are going to prove, the results of Matthews [15] are vital and, in our particular case, they can be summarized through the following:

Lemma 2.1.1. *(Matthews) Let $\Gamma \subset \mathbb{Q}^*$ be a finitely generated subgroup of rank $r \geqslant 2$; then for every $t \in \mathbb{R}$, $t > 1$, we have*

$$\#\{p \notin \mathrm{supp}(\Gamma) : |\Gamma_p| \leqslant t\} = O_\Gamma \left(\frac{t^{1+1/r}}{\log t} \right) \ .$$

2.2 Main results for $\sum_{p\leqslant x,\, p\nmid\sigma_\Gamma} f(i_p)$

2.2.1 Conditional case

The following theorems are r-rank generalizations of the conditional statements in [23, Theorem 2]:

Theorem 2.2.1. *Let $\Gamma \subset \mathbb{Q}^*$ be a finitely generated subgroup of rank r and let $f : \mathbb{N} \to \mathbb{C}$ be an arithmetic function such that $\max_{m\leqslant z}\{|f(m)|\} \ll (\log z)^C$, for some positive real constant C; assuming that the GRH holds for the Dedekind zeta function of the field $\mathbb{Q}(\zeta_k, \Gamma^{1/k})$ for each $k \in \mathbb{N}$, then*

$$\sum_{\substack{p\leqslant x\\ p\nmid\sigma_\Gamma}} f(i_p) \sim \sum_{m\geqslant 1} f(m)\rho_{\Gamma,m}\,\mathrm{Li}(x) = \sum_{n\geqslant 1} \frac{\widetilde{f}(n)}{k_n(\Gamma)}\,\mathrm{Li}(x)\ , \qquad \text{as } x\to\infty\ , \tag{2.7}$$

where $\widetilde{f}(n) = \sum_{d|n} \mu(n/d)f(d)$.

Proof. We first consider the case $r \geqslant 2$. Using the identity (2.2), we split our sum as

$$\sum_{m\leqslant y} f(m)\,N_\Gamma(x,m) + \sum_{y<m<z} f(m)\,N_\Gamma(x,m) + \sum_{m\geqslant z} f(m)\,N_\Gamma(x,m)\ . \tag{2.8}$$

We first deal with the last sum in (2.8) and, in order to do that, we use the results of Lemma 2.1.1, under the choice $z = x^{\frac{1}{r+1}}(\log x)^B$, with $B \geqslant C$:

$$\begin{aligned}\left|\sum_{m\geqslant z} f(m)\,N_\Gamma(x,m)\right| &\leqslant \max_{m\leqslant x}\{|f(m)|\}\,\#\left\{p\notin \mathrm{supp}(\Gamma) : |\Gamma_p| \leqslant \frac{x}{z}\right\}\\ &\ll (\log x)^C\,O_\Gamma\left(\frac{(x/z)^{1+1/r}}{\log(x/z)}\right) = o(\mathrm{Li}(x))\ .\end{aligned}$$

Concerning the first sum in (2.8), we choose $y = x^{\frac{r-1}{(r+1)(4r+2)+1}}$ so that we can make use of Theorem 1.3.2 and get

$$\begin{aligned}\sum_{m\leqslant y} f(m)\,N_\Gamma(x,m) &= \sum_{m\geqslant 1} f(m)\rho_{\Gamma,m}\,\mathrm{Li}(x) + O\left(\sum_{m>y} f(m)\rho_{\Gamma,m}\,\mathrm{Li}(x)\right) + O\left(\frac{\mathrm{Li}(x)}{\varphi(m^{r+1})\log^r x}\right)\\ &= \sum_{m\geqslant 1} f(m)\rho_{\Gamma,m}\,\mathrm{Li}(x) + o(\mathrm{Li}(x))\ ,\end{aligned}$$

where the last equality comes from the hypothesis that $\sum_{m\geqslant 1}|f(m)|\rho_{\Gamma,m}$ converges. Finally, the middle term in (2.8) is estimated using the conditional version of Chebotarev Density Theorem, equation (1.6), as

$$\left|\sum_{y<m<z} f(m)\, N_\Gamma(x,m)\right| \leqslant (\log z)^C \sum_{y<m<z} \pi_\Gamma(x,m) = (\log z)^C \sum_{y<m<z} \left[\frac{\mathrm{Li}(x)}{k_m(\Gamma)} + O_\Gamma\big(\sqrt{x}\log(xm^{r+1})\big)\right]$$

$$= O\left(x(\log x)^{C-1} \sum_{m<z} \frac{1}{k_m(\Gamma)}\right) + O\left(z(\log x)^{C+1}\sqrt{x}\right) .$$

From Hooley's work [9], we know that if $k_n(a) = [\mathbb{Q}(\zeta_n, a^{1/n}) : \mathbb{Q}]$ is the degree of a Kummer extension for a fixed integer a, $a \neq 0, \pm 1$, then writing $a = b^h$ for some integer $b = b_0 b_1^2$, with b_0 squarefree integer and $h = \max\{n \in \mathbb{N} : a = b^n\}$, we have

$$k_n(a) = \frac{n\varphi(n)}{\delta(n)(n,h)} ,$$

where $\delta(n) = 1, 2$ depends on the congruence class of $a \pmod 4$; now, if $g_1 = a/b$ with $(a,b) = 1$, since $\mathbb{Q}((a/b)^{1/n}) = \mathbb{Q}((ab^{n-1})^{1/n})$, the previous argument still works to give the lower bound

$$k_m(\Gamma) = [\mathbb{Q}(\zeta_m, {g_1}^{1/m}, \ldots, {g_r}^{1/m}) : \mathbb{Q}] \geqslant [\mathbb{Q}(\zeta_m, {g_1}^{1/m}) : \mathbb{Q}] \geqslant \frac{m\varphi(m)}{C} \tag{2.9}$$

for a fixed $C \in \mathbb{N}$. In the end, using Abel's summation,

$$\left|\sum_{y<m<z} f(m)\, N_\Gamma(x,m)\right| = O\left(\frac{x}{z}(\log x)^C\right) + O\left(z(\log x)^{C+1}\sqrt{x}\right) = o(\mathrm{Li}(x)) .$$

The proof still works when $r = 1$ if, instead of Theorem 1.3.2, we exploit Theorem 1.3.1. □

Theorem 2.2.2. *Let $\Gamma \subset \mathbb{Q}^*$ be a finitely generated subgroup of rank r and let $f : \mathbb{N} \to \mathbb{C}$ be an arithmetic function such that $f(m) \geqslant 0$ for every m; assuming that the GRH holds for the Dedekind zeta function of the field $\mathbb{Q}(\zeta_k, \Gamma^{1/k})$ for each $k \in \mathbb{N}$, then*

$$\sum_{\substack{p\leqslant x\\ p\nmid\sigma_\Gamma}} f(i_p) \gtrsim \sum_{m\geqslant 1} f(m)\rho_{\Gamma,m}\,\mathrm{Li}(x) , \tag{2.10}$$

where $g(x) \gtrsim h(x)$ if for every $\epsilon > 0$ exists x_ϵ such that $|g(x)| \geqslant (1+\epsilon)|h(x)|$ whenever $x > x_\epsilon$.

Proof. Suppose initially that $r \geqslant 2$. The proof is easily adapted from the one of [23, Theorem 2.b] and proceeds as follows: take $y = x^\alpha$ with $0 < \alpha < \frac{r-1}{(r+1)(4r+2)}$, then by Theorem 1.3.2

$$\begin{aligned}
\sum_{\substack{p\leqslant x\\ p\nmid\sigma_\Gamma}} f(i_p) &= \sum_{m\geqslant 1} f(m)\, N_\Gamma(x,m) \geqslant \sum_{m\leqslant y} f(m)\, N_\Gamma(x,m)\\
&= \sum_{m\leqslant y} f(m) \left(\rho_{\Gamma,m} + O\left(\frac{1}{\varphi(m^{r+1})\log^r x}\right)\right) \mathrm{Li}(x)\\
&= \sum_{m\geqslant 1} f(m)\,\rho_{\Gamma,m}\,\mathrm{Li}(x) - \sum_{m>y} f(m)\,\rho_{\Gamma,m}\,\mathrm{Li}(x) - O\left(\frac{1}{\log^r x}\sum_{m\leqslant y}\frac{f(m)}{\varphi(m^{r+1})}\right)\mathrm{Li}(x)\\
&= \left(\sum_{m\geqslant 1} f(m)\,\rho_{\Gamma,m} - o(1)\right)\mathrm{Li}(x)\ ,
\end{aligned}$$

where we have used the convergence of the series $\sum_{m\geqslant 1} f(m)/\varphi(m^{r+1})$, which is a consequence of the assumption (2.5) together with the bound $|\Gamma(m)| \geqslant m^r/\Delta_r(\Gamma)|$, where $\Delta_r(\Gamma)$ is a computable constant which depends only on Γ (see [25], equation (7)). Also in this proof, we deal with the case $r = 1$ using the results in Theorem 1.3.1 analogously to what we have done before with Theorem 1.3.2 when $r \geqslant 2$. □

2.2.2 Unconditional case

Here follows an upper bound for $N_\Gamma(x,m)$ without assuming GRH and, to to this, we need the unconditional statement in Theorem 1.2.3:

Lemma 2.2.3. *Let $\Gamma \subset \mathbb{Q}^*$ be a finitely generated subgroup of rank $r \geqslant 2$; there exists a computable constant c_1 depending only on Γ such that, if $m \leqslant c_1\left(\frac{\log x}{(\log\log x)^2}\right)^\alpha$ with $\alpha < \frac{1}{3r+3}$, then*

$$N_\Gamma(x,m) \leqslant \rho_{\Gamma,m}\,\mathrm{Li}(x) + o\left(\frac{1}{\varphi(m^{r+1})}\right)\mathrm{Li}(x)\ . \tag{2.11}$$

Proof. As a consequence of the inclusion-exclusion principle we can write

$$N_\Gamma(x,m) = \sum_{k\geqslant 1} \mu(k)\,\pi_\Gamma(x,mk)\ .$$

For every $y \in [1,x]$, if $P(y)$ denotes the product of the prime numbers less or equal than y then

$$N_\Gamma(x,m) \leqslant \sum_{d|P(y)} \mu(d)\,\pi_\Gamma(x,md)\ .$$

Given the computable constant c_1 of Theorem 1.2.3, we choose y such that

$$mP(y) \leqslant c_1\left(\frac{\log x}{(\log\log x)^2}\right)^{\frac{1}{3r+3}}\ , \tag{2.12}$$

so that we can apply the unconditional version of the Chebotarev Density Theorem:

$$\begin{aligned} N_\Gamma(x,m) &\leqslant \sum_{d|P(y)} \mu(d)\left[\frac{\mathrm{Li}(x)}{k_{md}(\Gamma)} + O_\Gamma\left(x\exp\left(-c_2(\log x)^{1/6}(\log\log x)^{1/3}\right)\right)\right] \\ &= \rho_{\Gamma,m}\,\mathrm{Li}(x) + O\left(\sum_{d\geqslant y}\frac{\mathrm{Li}(x)}{k_{md}(\Gamma)}\right) + O_\Gamma\left(2^{\pi(y)}x\exp\left(-c_2(\log x)^{1/6}(\log\log x)^{1/3}\right)\right) \end{aligned} \tag{2.13}$$

for a certain computable constant c_2. From [26, Corollary 4.3] we know that

$$\frac{1}{k_{md}(\Gamma)} \leqslant \frac{2^r\Delta_r(\Gamma)}{(md)^r\varphi(md)}$$

for a certain constant $\Delta_r(\Gamma)$ depending only on Γ. Through partial summation we obtain the following bound:

$$\sum_{d\geqslant y}\frac{1}{k_{md}} \ll \frac{1}{\varphi(m^{r+1})}\sum_{d\geqslant y}\frac{1}{d^r\varphi(d)} \ll \frac{1}{y^r\varphi(m^{r+1})}\ .$$

Choosing $y = \log\log\log x$, which satisfies the condition (2.12) as can be seen from [28, formula (3.15)], the two error terms in (2.13) become

$$O\left(\frac{\mathrm{Li}(x)}{y^r\,\varphi(m^{r+1})}\right) + O_\Gamma\left(2^{\pi(y)}x\exp\left(-c_2(\log x)^{1/6}(\log\log x)^{1/3}\right)\right) = o\left(\frac{\mathrm{Li}(x)}{\varphi(m^{r+1})}\right)\ .$$

□

Theorem 2.2.4. *Let $\Gamma \subset \mathbb{Q}^*$ be a finitely generated subgroup of rank $r \geqslant 2$ and let $f : \mathbb{N} \to \mathbb{C}$ be an arithmetic function such that $\max_{m\leqslant x}\{|f(m)|\} \ll x^{1-\delta}$, for some real constant $0 < \delta < 1$; if the series $\sum_{n\geqslant 1}|f(n)|/\varphi(n)$ converges, then*

$$\sum_{\substack{p\leqslant x\\ p\nmid\sigma_\Gamma}} f(i_p) \lesssim \sum_{m\geqslant 1} f(m)\rho_{\Gamma,m}\,\mathrm{Li}(x)\ , \qquad \text{as } x\to\infty\ , \tag{2.14}$$

where $g(x) \lesssim h(x)$ if $\forall\epsilon > 0$ exists x_ϵ such that $|g(x)| \leqslant (1+\epsilon)|h(x)|$ whenever $x > x_\epsilon$.

Proof. We start splitting the (finite) sum $\sum_{m\geqslant 1} f(m)N_\Gamma(x,m)$ as

$$\sum_{m\leqslant y} f(m)N_\Gamma(x,m) + \sum_{y<m<z} f(m)N_\Gamma(x,m) + \sum_{m\geqslant z} f(m)N_\Gamma(x,m)\ .$$

From Lemma 2.2.3, there exists a computable constant c_1 such that, choosing $y = c_1\left(\frac{\log x}{(\log\log x)^2}\right)^{1/(3r+3)}$, then

$$\begin{aligned}\sum_{m\leqslant y} f(m)N_\Gamma(x,m) \leqslant \sum_{m\leqslant y} f(m)\left[\rho_{\Gamma,m} + o\left(\frac{1}{\varphi(m^{r+1})}\right)\right]\operatorname{Li}(x) = \\ = \sum_{m\geqslant 1} f(m)\rho_{\Gamma,m}\operatorname{Li}(x) + O\left(\sum_{m>y} f(m)\rho_{\Gamma,m}\operatorname{Li}(x)\right) + \sum_{m\leqslant y} f(m)\, o\left(\frac{\operatorname{Li}(x)}{\varphi(m^{r+1})}\right) = \\ = \sum_{m\geqslant 1} f(m)\rho_{\Gamma,m}\operatorname{Li}(x) + o(\operatorname{Li}(x))\ . \qquad (2.15)\end{aligned}$$

Thanks to Lemma 2.1.1 we estimate

$$\sum_{m\geqslant z} f(m)N_\Gamma(x,m) \leqslant \max_{m\leqslant x}\{|f(m)|\}\, O_\Gamma\left(\frac{(x/z)^{1+1/r}}{\log(x/z)}\right) \ll \frac{x^{1-\delta}(x/z)^{1+1/r}}{\log(x/z)}\ ,$$

which becomes $o(\operatorname{Li}(x))$ taking $z = x^{\frac{r+2-\delta r}{r+1}}$. Finally, the last estimate we need is

$$\sum_{y<m<z} f(m)N_\Gamma(x,m) \leqslant \sum_{y<m<z} |f(m)|\,\pi(x;1,m) \ll \sum_{m>y}\frac{|f(m)|}{\varphi(m)}\operatorname{Li}(x) = o(\operatorname{Li}(x))\ ,$$

where we have used the Brun-Titchmarsh Theorem together with the convergence of the series $\sum_{m\geqslant 1}|f(m)|/\varphi(m)$. □

The following Theorem gives an unconditional estimate for the sum $\sum_{\substack{p\leqslant x\\ p\nmid\sigma_\Gamma}} f(i_p)$.

Theorem 2.2.5. *Let $\Gamma\subset\mathbb{Q}^*$ be a finitely generated subgroup of rank $r\geqslant 2$ and let $f:\mathbb{N}\to\mathbb{C}$ be an arithmetic function with $\widetilde{f}(n)=\sum_{d|n}\mu(n/d)f(d)$. Suppose that $\sum_{n\geqslant 1}|\widetilde{f}(n)|/\varphi(n)$ converges and that $\sum_{n>x}|\widetilde{f}(n)|/n = o(\log^{-1}x)$, then*

$$\sum_{n\geqslant 1}\widetilde{f}(n)\pi_\Gamma(x,n) \sim \sum_{n\geqslant 1}\frac{\widetilde{f}(n)}{k_n(\Gamma)}\operatorname{Li}(x)\ , \qquad (2.16)$$

as $x\to\infty$.

Proof. We first perform the following splitting,

$$\sum_{n\geqslant 1}\widetilde{f}(n)\pi_\Gamma(x,n) = \sum_{n\leqslant y}\widetilde{f}(n)\pi_\Gamma(x,n) + \sum_{n>y}\widetilde{f}(n)\pi_\Gamma(x,n)\ ,$$

where, as in the previous proof, $y = c_1 \left(\frac{\log x}{(\log\log x)^2}\right)^{1/(3r+3)}$ and c_1 is the constant appearing in unconditional statement of Theorem 1.2.3. Hence, the first sum is

$$\begin{aligned}\sum_{n\leqslant y} \widetilde{f}(n)\pi_\Gamma(x,n) &= \sum_{n\leqslant y} \widetilde{f}(n) \left(\frac{\mathrm{Li}(x)}{k_n(\Gamma)} + O_\Gamma\left(x\exp\left(-c_2(\log x)^{1/6}(\log\log x)^{1/3}\right)\right)\right) \\ &= \sum_{n\geqslant 1} \frac{\widetilde{f}(n)}{k_n(\Gamma)}\,\mathrm{Li}(x) + O\left(\sum_{n>y} \frac{|\widetilde{f}(n)|}{k_n(\Gamma)}\,\mathrm{Li}(x)\right) \\ &\quad + O_\Gamma\left(\frac{x\log x}{(\log\log x)^2}\exp\left(-c_2(\log x)^{1/6}(\log\log x)^{1/3}\right)\right) \\ &= \sum_{n\geqslant 1} \frac{\widetilde{f}(n)}{k_n(\Gamma)}\,\mathrm{Li}(x) + o(\mathrm{Li}(x))\ ,\end{aligned}$$

where the assumption (2.6) has been used. To conclude the proof, we split the second sum as

$$\sum_{n>y} \widetilde{f}(n)\pi_\Gamma(x,n) = \sum_{y<n\leqslant\sqrt{x}} \widetilde{f}(n)\pi_\Gamma(x,n) + \sum_{n>\sqrt{x}} \widetilde{f}(n)\pi_\Gamma(x,n)\ ;$$

since $\pi_\Gamma(x,n) \leqslant \pi(x;1,n) = \#\{p \leqslant x : n \mid p-1\}$, by the Brun-Titchmarsh Theorem we have

$$\sum_{y<n\leqslant\sqrt{x}} \widetilde{f}(n)\pi_\Gamma(x,n) \ll \sum_{y<n\leqslant\sqrt{x}} |\widetilde{f}(n)| \frac{x}{\varphi(n)\log(x/n)} = o(\mathrm{Li}(x))\ ,$$

while

$$\sum_{n>\sqrt{x}} \widetilde{f}(n)\pi_\Gamma(x,n) \leqslant \sum_{n>\sqrt{x}} |g(n)|\#\{m \leqslant x : n \mid m-1\} \ll \sum_{n>\sqrt{x}} |\widetilde{f}(n)|\frac{x}{n} = o(\mathrm{Li}(x))\ .$$

□

2.3 Examples and applications

In this section we want to generalize some applications in [23] to the higher rank case: we will do it in the case $\Gamma \subset \mathbb{Q}^+$, where $\mathbb{Q}^+$ denotes the set of positive rational numbers. We first compute the densities corresponding to the cases $f(n)$ multiplicative and totally multiplicative function respectively, where $f : \mathbb{N} \to \mathbb{C}$ is the arithmetic function appearing in the sum (2.1). Lastly we will apply those results to the case of $f(n) = \chi_B(n)$, the characteristic function of certain subsets $B \subset \mathbb{N}$, and $f(n) = \chi(n) \bmod b$, a Dirichlet character modulo b.

2.3.1 $f(n)$ multiplicative function

Suppose that the arithmetic function $f(n)$ in (2.1) is multiplicative; consequently, also $\widetilde{f}(n)$ is multiplicative. We want to compute the density

$$\delta_{\Gamma,f} := \sum_{n\geqslant 1} \frac{\widetilde{f}(n)}{k_n(\Gamma)} \ . \tag{2.17}$$

From now on, we will restrict to the case $\Gamma \subset \mathbb{Q}^+$, so that we can make use of Lemma kngamma. In order to compute the density (2.17) we begin splitting it as a sum over odd integers, S_o, plus a sum over even integers, S_e:

$$\delta_\Gamma = S_o + S_e = \sum_{\substack{n\geqslant 1\\ 2\nmid n}} \frac{\widetilde{f}(n)}{\varphi(n)|\Gamma(n)|}|\widetilde{\Gamma}(n)| + \sum_{\substack{n\geqslant 1\\ 2|n}} \frac{\widetilde{f}(n)}{\varphi(n)|\Gamma(n)|}|\widetilde{\Gamma}(n)| \ .$$

To lighten the next formulas, we denote

$$h(n) := \frac{\widetilde{f}(n)}{\varphi(n)|\Gamma(n)|} \ ,$$

which is a multiplicative function since $\widetilde{f}(n)$, $\varphi(n)$ and $|\Gamma(n)|$ are. Noticing that $\widetilde{\Gamma}(n) = 1$ whenever n is odd, the sum over odd integers has the following Euler product:

$$S_o = \sum_{\substack{n\geqslant 1\\ 2\nmid n}} h(n) = \prod_{p\geqslant 3}\left(\sum_{k\geqslant 0} h(p^k)\right) \ .$$

For every $m \mid \sigma_\Gamma$ we write $\Delta(m) = 2^{v_2(\Delta(m))}m'$; hence the sum over even integers can be written as

$$\begin{aligned} S_e = \sum_{\substack{n\geqslant 1\\ 2\nmid n}} h(n) \sum_{m\in\widetilde{\Gamma}(n)} 1 &= \sum_{m|\sigma_\Gamma} \sum_{\substack{\alpha\geqslant 1\\ m^{2^{\alpha-1}}\mathbb{Q}^{*2^\alpha}\in\Gamma(2^\alpha)}} \sum_{\substack{n\geqslant 1\\ v_2(n)=\alpha\\ \Delta(m)|n}} h(n) = \sum_{m|\sigma_\Gamma} \sum_{\substack{\alpha\geqslant 1\\ m^{2^{\alpha-1}}\mathbb{Q}^{*2^\alpha}\in\Gamma(2^\alpha)\\ \alpha\geqslant v_2(\Delta(m))}} h(2^\alpha) \sum_{\substack{n\geqslant 1\\ 2\nmid n\\ m'|n}} h(n) \\ &= \sum_{m|\sigma_\Gamma} \sum_{\substack{\alpha\geqslant 1\\ m^{2^{\alpha-1}}\mathbb{Q}^{*2^\alpha}\in\Gamma(2^\alpha)\\ \alpha\geqslant v_2(\Delta(m))}} h(2^\alpha) \prod_{\substack{p\geqslant 3\\ p\nmid m'}}\left(\sum_{k\geqslant 0} h(p^k)\right) \prod_{\substack{p\geqslant 3\\ p|m'}}\left(\sum_{j\geqslant 1} h(p^j)\right) \\ &= \sum_{m|\sigma_\Gamma} \sum_{\substack{\alpha\geqslant 1\\ m^{2^{\alpha-1}}\mathbb{Q}^{*2^\alpha}\in\Gamma(2^\alpha)\\ \alpha\geqslant v_2(\Delta(m))}} h(2^\alpha) \prod_{\substack{p\geqslant 3\\ p|m'}}\left[1 + \left(\sum_{j\geqslant 1} h(p^j)\right)^{-1}\right]^{-1} \ . \end{aligned}$$

We define

$$t_m := \begin{cases} \min\{z \in \mathbb{N} \cup \{0\} : \ m^{2^z} \mathbb{Q}^{*2^{z+1}} \in \Gamma(2^{z+1})\} & \text{if } \exists z \in \mathbb{N} \text{ such that } m^{2^z} \in \Gamma(2^{z+1}), \\ \infty & \text{otherwhise}, \end{cases}$$

and $\gamma_m := \max\{1 + t_m, v_2(\Delta(m))\}$, so that

$$\begin{aligned} \delta_{\Gamma,f} =& S_o \left\{ 1 + \sum_{m|\sigma_\Gamma} \sum_{\alpha \geqslant \gamma_m} h(2^\alpha) \prod_{\substack{p \geqslant 3 \\ p|m'}} \left[1 + \left(\sum_{j \geqslant 1} h(p^j) \right)^{-1} \right]^{-1} \right\} \\ =& \prod_p \left(\sum_{k \geqslant 0} h(p^k) \right) \left(\sum_{\beta \geqslant 0} h(2^\beta) \right)^{-1} \left\{ 1 + \sum_{m|\sigma_\Gamma} \sum_{\alpha \geqslant \gamma_m} h(2^\alpha) \prod_{\substack{p \geqslant 3 \\ p|m}} \left[1 + \left(\sum_{j \geqslant 1} h(p^j) \right)^{-1} \right]^{-1} \right\}. \end{aligned}$$

Rearranging the terms in the previous expression we arrive at

$$\delta_{\Gamma,f} = \prod_p \left(\sum_{k \geqslant 0} h(p^k) \right) \left\{ 1 + \sum_{\substack{m|\sigma_\Gamma \\ m \neq 1}} \frac{\sum_{\alpha \geqslant \gamma_m} h(2^\alpha)}{\sum_{\beta \geqslant 1} h(2^\beta)} \prod_{p|2m} \left[1 + \left(\sum_{j \geqslant 1} h(p^j) \right)^{-1} \right]^{-1} \right\}.$$

In order to express $\delta_{\Gamma,f}$ in terms of the function $f(n)$, we note that $\widetilde{f}(p^k) = f(p^k) - f(p^{k-1})$; moreover, the sum $\sum_{\alpha \geqslant \gamma_m} h(2^\alpha)$ becomes zero if $\gamma_m = \infty$. Hence we obtain

$$\begin{aligned} \delta_{\Gamma,f} =& \prod_p \left[1 - \frac{1}{(p-1)|\Gamma(p)|} + \frac{p}{p-1} \sum_{k \geqslant 1} \frac{f(p^k)}{p^k} \left(\frac{1}{|\Gamma(p^k)|} - \frac{1}{p|\Gamma(p^{k+1})|} \right) \right] \times \\ & \left\{ 1 + \sum_{\substack{m|\sigma_\Gamma \\ m \neq 1 \\ \gamma_m < \infty}} \frac{-\frac{f(2^{\gamma_m - 1})}{2^{\gamma_m - 1}|\Gamma(2^{\gamma_m})|} + 2 \sum_{\alpha \geqslant \gamma_m} \frac{f(2^\alpha)}{2^\alpha} \left(\frac{1}{|\Gamma(2^\alpha)|} - \frac{1}{2|\Gamma(2^{\alpha+1})|} \right)}{-\frac{1}{|\Gamma(2)|} + 2 \sum_{\beta \geqslant 1} \frac{f(2^\beta)}{2^\beta} \left(\frac{1}{|\Gamma(2^\beta)|} - \frac{1}{2|\Gamma(2^{\beta+1})|} \right)} \times \right. \\ & \left. \prod_{q|2m} \left[1 + \left(-\frac{1}{(q-1)|\Gamma(q)|} + \frac{q}{q-1} \sum_{j \geqslant 1} \frac{f(q^j)}{q^j} \left(\frac{1}{|\Gamma(q^j)|} - \frac{1}{q|\Gamma(q^{j+1})|} \right) \right)^{-1} \right]^{-1} \right\}. \end{aligned}$$

This formula can be made more compact introducing appropriate quantities, as we do in the following:

Theorem 2.3.1. *Given a subset $\Gamma \subset \mathbb{Q}^+$ of finite rank r and a multiplicative function $f(n)$, then*

$$\delta_{\Gamma,f} = \prod_p (1 + A_p) \left\{ 1 + \sum_{\substack{m|\sigma_\Gamma \\ m\neq 1 \\ \gamma_m<\infty}} \left(1 + \frac{B_m}{A_2}\right) \prod_{q|2m} \left(1 + A_q^{-1}\right)^{-1} \right\} , \tag{2.18}$$

where

$$A_p = A_p^{\Gamma,f} = -\frac{1}{(p-1)|\Gamma(p)|} + \frac{p}{p-1} \sum_{k\geqslant 1} \frac{f(p^k)}{p^k} \left(\frac{1}{|\Gamma(p^k)|} - \frac{1}{p|\Gamma(p^{k+1})|} \right) \tag{2.19}$$

and

$$B_m = B_m^{\Gamma,f} = 2 \sum_{\alpha=1}^{\gamma_m-1} \frac{f(2^{\alpha-1}) - f(2^\alpha)}{2^\alpha |\Gamma(2^\alpha)|} , \tag{2.20}$$

Let us focus on the case $r = 1$, i.e. suppose $\Gamma = \langle a \rangle$ with $a \in \mathbb{Q}^* \backslash \{\pm 1\}$. We first state the following:

Lemma 2.3.2. *Let $\Gamma = \langle a \rangle$ with $a \in \mathbb{Q}^* \backslash \{\pm 1\}$ and let h be the largest integer such that $a = b^h$ for some rational number $b = b_1 b_2^2$, with $b_1 \in \mathbb{Z}$ unique squarefree integer with such a property. For any $m \neq 1$ squarefree positive integer we have $t_{b_1} = v_2(h)$ and $t_m = \infty$ if $m \neq b_1$.*

Proof. First note that in this case

$$|\langle a \rangle(n)| = \left| \frac{\langle b^h \rangle \mathbb{Q}^{*n}}{\mathbb{Q}^{*n}} \right| = \frac{n}{(n,h)} .$$

Since $|\langle a \rangle(2^{z+1})| = 2^{z+1}/(2^{z+1}, h) = 2^{\max\{0, z+1-v_2(h)\}}$, we have that $t_m \geqslant v_2(h)$ for all integers $m \neq 1$. Also note that, if we write

$$h = h' 2^{v_2(h)} = 2^{v_2(h)} + h'' 2^{v_2(h)+1},$$

then

$$a = b_1^{2^{v_2(h)}} \cdot \left(b_1^{h''} b_2^{h'} \right)^{2^{v_2(h)+1}}$$

so that

$$a \cdot (\mathbb{Q}^*)^{2^{v_2(h)+1}} = b_1^{2^{v_2(h)}} \cdot (\mathbb{Q}^*)^{2^{v_2(h)+1}} .$$

We deduce that

$$\langle a \rangle (2^{v_2(h)+1}) = \{ (\mathbb{Q}^*)^{2^{v_2(h)+1}}, b_1^{2^{v_2(h)}} \cdot (\mathbb{Q}^*)^{2^{v_2(h)+1}} \} .$$

which implies that $t_{b_1} = v_2(h)$. More in general, for $z = v_2(h) + k$ and $k \geqslant 0$,

$$\langle a\rangle(2^{z+1}) \quad = \quad \left\{a^j \cdot (\mathbb{Q}^*)^{2^{z+1}} \;:\; j \in \mathbb{Z}/2^{k+1}\mathbb{Z}\right\} \; .$$

For $m \neq 1$ square free, the identity

$$m^{2^z} \cdot (\mathbb{Q}^*)^{2^{z+1}} = a^j \cdot (\mathbb{Q}^*)^{2^{z+1}} = b_1^{j2^{v_2(h)}} \cdot \left(b_1^{h''} b_2^{h'}\right)^{j2^{v_2(h)+1}} (\mathbb{Q}^*)^{2^{z+1}}$$

is satisfied if and only if $j = 2^k$ and $m = b_1$. □

Lemma 2.3.2 leads to the following:

Theorem 2.3.3. *Let $\Gamma = \langle a\rangle$ with $a \in \mathbb{Q}^+\backslash\{1\}$, where h is the largest integer such that $a = b^h$ and $b = b_1 b_2^2$, with $b_1 \in \mathbb{Z}$ unique squarefree integer with such a property. Then*

$$\delta_{\langle a\rangle, f} = \prod_p (1 + A_p) \left\{ 1 + \left(1 + \frac{B_{b_1}}{A_2}\right) \prod_{q|2b_1} \left(1 + (A_q')^{-1}\right)^{-1} \right\} , \tag{2.21}$$

with

$$A_p = A_p^{\langle a\rangle, f} = -\frac{(p,h)}{p(p-1)} + \frac{p}{p-1} \sum_{k\geqslant 1} \frac{f(p^k)}{p^{2k}} \left((p^k, h) - \frac{(p^{k+1}, h)}{p^2} \right) \tag{2.22}$$

and

$$B_{b_1} = B_{b_1}^{\langle a\rangle, f} = 2 \sum_{\alpha=1}^{\gamma_{b_1}-1} [f(2^{\alpha-1}) - f(2^\alpha)] \frac{(2^\alpha, h)}{2^{2\alpha}} \, , \tag{2.23}$$

with $\gamma_{b_1} - 1 = \max\{v_2(h), v_2(\Delta(a)) - 1\}$.

We can now easily retrieve the classical result of Hooley [9, Theorem] from Theorem 2.3.3 in the case of positive rationals, choosing $f(n) = \chi_{\{1\}}(n)$:

Theorem 2.3.4 (Hooley)**.** *Consider a positive rational $a \neq 0$ which is not a perfect square and let h be the largest integer such that $a = b^h$; denote with d the discriminant of the quadratic extension $\mathbb{Q}(\sqrt{a})$. Assuming GRH for the number field $\mathbb{Q}(\zeta_n, a^{1/n})$ for every squarefree n, then*

$$N_a(x) \sim \delta_a \,\mathrm{Li}(x)$$

as $x \to \infty$, where

$$\delta_a = \sum_{n\geqslant 1} \frac{\mu(n)}{[\mathbb{Q}(\zeta_n, a^{1/n}) : \mathbb{Q}]} = \begin{cases} A(h) & \text{if } d \equiv 2,3 \,(\mathrm{mod} 4)\,, \\ \left(1 - \mu(|d|) \prod_{\substack{q|d \\ q|h}} \frac{1}{q-2} \prod_{\substack{q|d \\ q\nmid h}} \frac{1}{q^2-q-1}\right) A(h) & \text{if } d \equiv 1 \,(\mathrm{mod} 4)\,, \end{cases}$$

with

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

In general, the expressions (2.19) and (2.20) cannot be further simplified, unless we make additional suppositions on Γ and consequently on $|\Gamma(p^k)|$. An interesting case is the following:

Corollary 2.3.5. *Suppose $\Gamma = \langle p_1, \ldots, p_r\rangle$, with p_i generic prime number, then for any multiplicative function $f(n)$ we have*

$$\delta_{\langle p_1,\ldots,p_r\rangle, f} = \prod_p (1 + A_p)\left\{1 + \sum_{\substack{m|\sigma_\Gamma \\ m\neq 1}}\left(1 + \frac{B_m}{A_2}\right)\prod_{q|2m}\left(1 + A_q^{-1}\right)^{-1}\right\} , \tag{2.24}$$

where

$$A_p = A_p^{\langle p_1,\ldots,p_r\rangle, f} = -\frac{1}{(p-1)p^r} + \frac{p^{r+1}-1}{(p-1)p^r}\sum_{k\geqslant 1}\frac{f(p^k)}{p^{k(r+1)}} \tag{2.25}$$

and

$$B_m = B_m^{\langle p_1,\ldots,p_r\rangle, f} = \begin{cases} 0 & \text{if } m \equiv 1 \,(\mathrm{mod} 4)\,, \\ \frac{1-f(2)}{2^r} & \text{if } m \equiv 3 \,(\mathrm{mod} 4)\,, \\ \frac{1}{2^r}\left[1 - f(2)\left(\frac{2^{r+1}-1}{2^{r+1}}\right) - \frac{f(4)}{2^{r+1}}\right] & \text{if } m \equiv 2 \,(\mathrm{mod} 4)\,. \end{cases} \tag{2.26}$$

Moreover, if $f(n)$ is totally multiplicative and the series $\sum_{k\geqslant 1}(f(p)/p^{r+1})^k$ converges for every p, then

$$A_p = A_p^{\langle p_1,\ldots,p_r\rangle, f} = \frac{p(f(p)-1)}{(p-1)(p^{r+1}-f(p))} \tag{2.27}$$

and

$$B_m = B_m^{\langle p_1,\ldots,p_r\rangle, f} = \begin{cases} 0 & \text{if } m \equiv 1 \,(\mathrm{mod} 4)\,, \\ \frac{1-f(2)}{2^r} & \text{if } m \equiv 3 \,(\mathrm{mod} 4)\,, \\ \frac{1-f(2)}{2^r}\left(1 - \frac{f(2)}{2^{r+1}}\right) & \text{if } m \equiv 2 \,(\mathrm{mod} 4)\,. \end{cases} \tag{2.28}$$

Proof. It is sufficient to apply Theorem 2.3.1 with $|\Gamma(p^k)| = p^{kr}$ because of [2, Proposition 2]. Moreover, since $t_m = 0$ for every $m \mid \sigma_\Gamma$, notice also that

$$\gamma_m = \begin{cases} 1 & \text{if } m \equiv 1 \,(\mathrm{mod} 4)\,, \\ 3 & \text{if } m \equiv 2 \,(\mathrm{mod} 4)\,, \\ 2 & \text{if } m \equiv 3 \,(\mathrm{mod} 4)\,. \end{cases}$$

□

Notice that the previous Corollary holds, in general, for all the subgroups $\Gamma \subset \mathbb{Q}^*$ such that $|\Gamma(n)| = n^r$ for every natural number n.

2.3.2 $f(n) = \chi_B(n)$ characteristic function of a subset $B \subset \mathbb{N}$

Let χ_B be the characteristic function of a subset $B \subset \mathbb{N}$, then defining

$$\pi_{\Gamma,B}(x) := \#\{p \leqslant x : \; p \nmid \sigma_\Gamma \,, \; i_p \in B\} = \sum_{m \geqslant 1} \chi_B(m)\, N_\Gamma(x,m)$$

by Möbius inversion formula we obtain

$$\pi_{\Gamma,B}(x) = \sum_{m \geqslant 1} \widetilde{\chi}_B(m)\, \pi_\Gamma(x,m) \;,$$

where

$$\widetilde{\chi}_B(m) = \sum_{d \mid m} \mu(m/d)\, \chi_B(d) = \sum_{\substack{d \mid m \\ d \in B}} \mu(m/d) \;.$$

Define

$$\delta_{\Gamma,B} := \sum_{n \geqslant 1} \frac{\widetilde{\chi}_B(n)}{k_n(\Gamma)} \;;$$

then, assuming GRH, we have from Theorem 2.2.1 that

$$\pi_{\Gamma,B}(x) \sim \delta_{\Gamma,B}\, \mathrm{Li}(x)$$

as $x \to \infty$. We will also see explicitly some examples where the unconditional results from Theorems 2.2.4 and 2.2.5 can be applied.

$\chi_{\mathcal{P}}(n)$ **characteristic function of the primes**

Let $B = \mathcal{P}$ be the set of prime numbers. Applying Theorem 2.2.1 we obtain the asymptotic density result appeared in [24, Theorem 1.1] in the case $\Gamma = \langle a_1, \ldots, a_r \rangle$, with $a_1, \ldots, a_r$ multiplicatively independent integers different from $0, \pm 1$ and not all perfect squares.

Lemma 2.3.6. *Under GRH, if $\Gamma \subset \mathbb{Q}^*$ is a finitely generated subgroup of rank r, then*

$$N_\Gamma(x) = \#\{p \leqslant x : \ p \nmid \sigma_\Gamma \, , \ i_p = 1\} \sim \delta_{\Gamma,\mathcal{P}} \operatorname{Li}(x) \, , \qquad \text{as } x \to \infty \, ,$$

where

$$\delta_{\Gamma,\mathcal{P}} = \sum_{m \geqslant 1} \frac{\mu(m)}{k_m(\Gamma)} \, .$$

$\chi_B(n)$ **multiplicative function**

Suppose $B \subset \mathbb{N}$ is such that $\chi_B(n)$ is multiplicative, then we can apply Theorem 2.3.1 with $f(n) = \chi_B(n)$ to get the following:

Theorem 2.3.7. *Consider the r-rank subgroup $\Gamma \subset \mathbb{Q}^+$ and a subset $B \subset \mathbb{N}$ such that its characteristic function $\chi_B(n)$ is multiplicative; assuming GRH we have*

$$\pi_{\Gamma,B}(x) \sim \delta_{\Gamma,B} \operatorname{Li}(x) \, , \qquad x \to \infty \, ,$$

where

$$\delta_{\Gamma,B} = \prod_p (1 + A_p) \left\{ 1 + \sum_{\substack{m \mid \sigma_\Gamma \\ m \neq 1 \\ \gamma_m < \infty}} \left(1 + \frac{B_m}{A_2}\right) \prod_{q \mid 2m} \left(1 + A_q^{-1}\right)^{-1} \right\} , \tag{2.29}$$

where

$$A_p = A_p^{\Gamma,B} = -\frac{1}{(p-1)|\Gamma(p)|} + \frac{p}{p-1} \sum_{k \geqslant 1} \frac{\chi_B(p^k)}{p^k} \left(\frac{1}{|\Gamma(p^k)|} - \frac{1}{p|\Gamma(p^{k+1})|} \right) \tag{2.30}$$

and

$$B_m = B_m^{\Gamma,B} = 2 \sum_{\alpha=1}^{\gamma_m - 1} \frac{\chi_B(2^{\alpha-1}) - \chi_B(2^\alpha)}{2^\alpha |\Gamma(2^\alpha)|} \, . \tag{2.31}$$

We can apply the previous results in the simpler case $\Gamma = \langle p_1, \ldots, p_r \rangle$ to get the following:

Corollary 2.3.8. *Let $\Gamma = \langle p_1, \dots, p_r \rangle$, with p_i generic prime number. For every subset $B \subset \mathbb{N}$ such that its characteristic function $\chi_B(n)$ is multiplicative, assuming GRH we have*

$$\pi_{\Gamma,B}(x) \sim \delta_{\langle p_1,\dots,p_r \rangle, B} \operatorname{Li}(x) , \qquad x \to \infty ,$$

with

$$\delta_{\langle p_1,\dots,p_r \rangle, B} = \prod_p (1 + A_p) \left\{ 1 + \sum_{\substack{m | \sigma_\Gamma \\ m \neq 1}} \left(1 + \frac{B_m}{A_2} \right) \prod_{q | 2m} \left(1 + A_q^{-1} \right)^{-1} \right\} , \tag{2.32}$$

where

$$A_p = A_p^{\langle p_1,\dots,p_r \rangle, B} = -\frac{1}{(p-1)p^r} + \frac{p^{r+1}-1}{(p-1)p^r} \sum_{\substack{k \geqslant 1 \\ p^k \in B}} \frac{1}{p^{k(r+1)}}$$

and

$$B_m = B_m^{\langle p_1,\dots,p_r \rangle, B} = \begin{cases} 0 & \text{if } m \equiv 1 \,(\text{mod} 4) , \\ \frac{1-\chi_B(2)}{2^r} & \text{if } m \equiv 3 \,(\text{mod} 4) , \\ \frac{1}{2^r} \left[1 - \chi_B(2) \left(\frac{2^{r+1}-1}{2^{r+1}} \right) - \frac{\chi_B(4)}{2^{r+1}} \right] & \text{if } m \equiv 2 \,(\text{mod} 4) . \end{cases}$$

$$A_p = \begin{cases} 0 & \text{if } p \in B , \\ -\frac{1}{p^r(p-1)} & \text{if } p \notin B . \end{cases}$$

and

$$B_m = \begin{cases} 0 & \text{if } m \equiv 1 \,(\text{mod} 4) \text{ or } 2 \in B , \\ \frac{1}{2^r} & \text{if } m \equiv 2, 3 \,(\text{mod} 4) \text{ and } 2 \notin B . \end{cases}$$

Let us consider some examples in a more detailed way.

Example 1. Let $H_k = \{n \in \mathbb{N} : n = m^k,\ m \in \mathbb{N}\}$ be the set of *k-powers*. For $k \geqslant 2$, the sum

$$\sum_{n \in H_k} \frac{1}{\varphi(n)} = \sum_{m \geqslant 1} \frac{1}{\varphi(m^k)}$$

converges, so that from Theorems 2.2.4 and 2.2.2 we derive the following:

Corollary 2.3.9. *Let $\Gamma \subset \mathbb{Q}^*$ be a finitely generated subgroup and let $H_k = \{n \in \mathbb{N} : n = m^k,\ m \in \mathbb{N}\}$ be the set of k-powers, with $k \geqslant 2$. Then, as $x \to \infty$, $\pi_{\Gamma,H_k}(x) \lesssim \delta_{\Gamma,H_k} \operatorname{Li}(x)$ unconditionally and $\pi_{\Gamma,H_k}(x) \gtrsim \delta_{\Gamma,H_k} \operatorname{Li}(x)$ under GRH.*

In the case $\Gamma = \langle p_1, \ldots, p_r\rangle$, formula (2.32) can be applied with

$$A_p = A_p^{\langle p_1,\ldots,p_r\rangle, H_k} = -\frac{p^{k(r+1)-r} - p}{(p-1)(p^{k(r+1)}-1)}$$

and

$$B_m = B_m^{\langle p_1,\ldots,p_r\rangle, H_k} = \begin{cases} 0 & \text{if } m \equiv 1 \,(\text{mod} 4)\,, \\ \frac{1}{2^r} & \text{if } m \equiv 3 \,(\text{mod} 4)\,, \\ \frac{1}{2^r}\left(1 - \frac{\chi_{H_k}(4)}{2^{r+1}}\right) & \text{if } m \equiv 2 \,(\text{mod} 4)\,. \end{cases}$$

In Table 2.1 we compute the density values δ_{Γ,H_k} for the cases $k = 2, 3, 4$ and $\Gamma = \langle p_i, p_j\rangle$, with distinct $p_i, p_j \in \{2, 3, 5, 7, 11, 13\}$, and compare them with the numerical results $\delta_{\Gamma,H_k}^{p<2^{37}}$, computed up to $p < 2^{37}$, using the software GP/PARI CALCULATOR Version 2.7.5[1].

Example 2. Let $k \geqslant 2$, let $F_k = \{n \in \mathbb{N} : v_p(n) < k, \forall p \text{ prime}\}$ be the set of *k-free numbers.* Since

$$\widetilde{\chi}_{F_k}(n) = \begin{cases} \mu(m) & \text{if } n = m^k\,, \\ 0 & \text{otherwise}\,, \end{cases}$$

the conditions of Theorem 2.2.5 are satisfied, so that we can state the following:

Corollary 2.3.10. *Let $\Gamma \subset \mathbb{Q}^*$ be a finitely generated subgroup and let $F_k = \{n \in \mathbb{N} : v_p(n) < k, \forall p \text{ prime}\}$ be the set of k-free numbers, with $k \geqslant 2$. Then, as $x \to \infty$, $\pi_{\Gamma,F_k}(x) \sim \delta_{\Gamma,H_k}\operatorname{Li}(x)$ unconditionally.*

If $\Gamma = \langle p_1, \ldots, p_r\rangle$, formula (2.32) holds with

$$A_p = A_p^{\langle p_1,\ldots,p_r\rangle, F_k} = -\frac{1}{p^{k(r+1)-1}(p-1)}$$

and

$$B_m = B_m^{\langle p_1,\ldots,p_r\rangle, F_k} = \begin{cases} 0 & \text{if } m \equiv 1, 3 \,(\text{mod} 4)\,, \\ \frac{1-\chi_{F_k}(4)}{2^{2r+1}} & \text{if } m \equiv 2 \,(\text{mod} 4)\,. \end{cases}$$

2.3.3 Indices i_p in arithmetic progression

Given two coprime positive integers a and b, consider the set

$$S_\Gamma(x; a, b) := \{p \leqslant x : \ p \nmid \sigma_\Gamma\,, \ i_p \equiv a \,(\text{mod}\, b)\}$$

[1]Together with Henri Cohen's script (see http://pari.math.u-bordeaux.fr/Scripts/), which includes the function `prodeuleratt` for calculating Euler products.

Table 2.1: Comparison between the theoretical (GRH) δ_{Γ,H_k} and numerical (up to $p < 2^{37}$) density $\delta^{p<2^{37}}_{\Gamma,H_k}$, where $\Gamma = \langle p_i, p_j \rangle$, $p_i, p_j \in \{2, 3, 5, 7, 11, 13\}$.

Γ	δ_{Γ,H_2} $\delta^{p<2^{37}}_{\Gamma,H_2}$	δ_{Γ,H_3} $\delta^{p<2^{37}}_{\Gamma,H_3}$	δ_{Γ,H_4} $\delta^{p<2^{37}}_{\Gamma,H_4}$
$\langle 2,3 \rangle$	0.7204017835 0.7204008108	0.7035521973 0.7035514839	0.6982514901 0.6982504751
$\langle 2,5 \rangle$	0.7237918508 0.7237946933	0.7062105809 0.7062128444	0.7006387110 0.7006414714
$\langle 2,7 \rangle$	0.7216069808 0.7216104694	0.7039046595 0.7039091705	0.6982955321 0.6983004502
$\langle 2,11 \rangle$	0.7216653483 0.7216666678	0.7039211320 0.7039209604	0.6982975876 0.6982978180
$\langle 2,13 \rangle$	0.7217878018 0.7217875330	0.7040379691 0.7040386343	0.6984125550 0.6984125509
$\langle 3,5 \rangle$	0.7255448866 0.7255450297	0.7028723530 0.7028728547	0.7002221463 0.7002227099
$\langle 3,7 \rangle$	0.7233268507 0.7233301700	0.7004972642 0.7004996641	0.6978294779 0.6978328171
$\langle 3,11 \rangle$	0.7234237628 0.7234241660	0.7005403348 0.7005412999	0.6978658086 0.6978673966
$\langle 3,13 \rangle$	0.7235577077 0.7235598185	0.7006673436 0.7006681588	0.6979919473 0.6979936959
$\langle 5,7 \rangle$	0.7269084536 0.7269133076	0.7030468041 0.7030492041	0.7002439449 0.7002473531
$\langle 5,11 \rangle$	0.7269744910 0.7269774849	0.7030549572 0.7030499313	0.7002449623 0.7002449623
$\langle 5,13 \rangle$	0.7270967856 0.7270997051	0.7031695617 0.7031721896	0.7003586371 0.7003617319
$\langle 7,11 \rangle$	0.7248102383 0.7248161001	0.7007270610 0.7007316472	0.6978984668 0.6979033861
$\langle 7,13 \rangle$	0.7249343967 0.7249362846	0.7008434877 0.7008475860	0.6980139575 0.6980175153
$\langle 11,13 \rangle$	0.7250010696 0.7250008316	0.7008517199 0.7008527808	0.6980149847 0.6980159664

with cardinality $N_\Gamma(x; a, b) = \#S_\Gamma(x; a, b)$. Let $\chi : \mathbb{N} \to \mathbb{C}$ be a Dirichlet character modulo b, then the ortogonality relations can be used to define the following characteristic function:

$$\chi_{a,b}(n) := \frac{1}{\varphi(b)} \sum_{\chi \bmod b} \overline{\chi}(a)\chi(n) = \begin{cases} 1 & \text{if } n \equiv a \pmod b \\ 0 & \text{otherwhise} \end{cases} .$$

Consider the density

$$\delta_{\Gamma,(a,b)} := \delta_{\Gamma,S_\Gamma(a,b)} = \sum_{n\geqslant 1} \frac{\widetilde{\chi}_{a,b}(n)}{k_n(\Gamma)} = \frac{1}{\varphi(b)} \sum_{\chi \bmod b} \overline{\chi}(a)\delta_\chi \ ,$$

where

$$\delta_\chi = \sum_{n\geqslant 1} \frac{\widetilde{\chi}(n)}{k_n(\Gamma)} \ . \tag{2.33}$$

From Theorem 2.2.1 follows the following:

Corollary 2.3.11. *Let $\Gamma \subset \mathbb{Q}^*$ be a finitely generated subgroup. On GRH we have, as $x \to \infty$,*

$$N_\Gamma(x; a, b) \sim \delta_{\Gamma,(a,b)} \operatorname{Li}(x) \ .$$

A Dirichlet character $\chi(n)$ is a totally multiplicative function, so in the case $\Gamma \subset \mathbb{Q}^+$ we can compute the density (2.33) making use of formula (2.18). In the specific case $\Gamma = \langle p_1, \ldots, p_r\rangle$ we can apply formulas (2.24), (2.27) and (2.28) to get

$$\begin{aligned} \delta_{\langle p_1,\ldots,p_r\rangle,(a,b)} =& \frac{1}{\varphi(b)} \sum_{\chi \bmod b} \overline{\chi}(a) \prod_p (1 + A_p) \times \\ & \left\{ 1 + \sum_{\substack{m \mid p_1\cdots p_r \\ m\neq 1}} \left(1 + \frac{B_m}{A_2}\right) \prod_{q\mid 2m} \left[1 + A_q^{-1}\right]^{-1} \right\} , \end{aligned} \tag{2.34}$$

with

$$A_p = A_p^{\langle p_1,\ldots,p_r\rangle,\chi} = \frac{p(\chi(p) - 1)}{(p-1)(p^{r+1} - \chi(p))} \tag{2.35}$$

and

$$B_m = B_m^{\langle p_1,\ldots,p_r\rangle,\chi} = \begin{cases} 0 & \text{if } m \equiv 1 \,(\operatorname{mod} 4)\,, \\ \frac{1-\chi(2)}{2^r} & \text{if } m \equiv 3 \,(\operatorname{mod} 4)\,, \\ \frac{1-\chi(2)}{2^r}\left(1 - \frac{\chi(2)}{2^{r+1}}\right) & \text{if } m \equiv 2 \,(\operatorname{mod} 4)\,. \end{cases} \tag{2.36}$$

2.3.4 Average order of Γ_p over primes

In the special case when $\Gamma = \langle g\rangle$, where $g \in \mathbb{Q}^*\backslash\{\pm 1\}$, Kurlberg and Pomerance [11, Theorem 2] proved under GRH an asymptotic formula for the average over primes up to x of the order $o_p(g) = |\langle g \pmod p\rangle|$:

$$\frac{1}{\operatorname{Li}(x)} \sum_{p\leqslant x} o_p(g) = \frac{c_g}{2} x + O\left(\frac{x}{(\log x)^{2-4/\log\log\log x}}\right) ,$$

as $x \to \infty$, where

$$c_g := \sum_{n \geqslant 1} \frac{\varphi(n)\,\mathrm{Rad}(n)(-1)^{\omega(n)}}{n^2 k_n(\langle g \rangle)} \ .$$

For a finitely generated subgroup $\Gamma \subset \mathbb{Q}^*$ of rank r, the previous result has been generalized by Pehlivan in [27]:

$$\frac{1}{\mathrm{Li}(x^{t+1})} \sum_{p \leqslant x} |\Gamma_p|^t = c_{\Gamma,t} + O_{\Gamma,t}\left(\frac{\log\log x}{(\log x)^r}\right) \ , \tag{2.37}$$

as $x \to \infty$, where

$$c_{\Gamma,t} := \sum_{n \geqslant 1} \frac{J_t(n)(\mathrm{Rad}(n))^t(-1)^{\omega(n)}}{n^{2t} k_n(\langle g \rangle)}$$

with the Jordan's totient function defined by $J_t(n) := n^t \prod_{q|n}(1 - 1/q^t)$. We can retrieve the main term in (2.37), as $x \to \infty$, choosing the function $f(n) = 1/n^t$ and, starting with the sum

$$\frac{1}{\mathrm{Li}(x^{t+1})} \sum_{p \leqslant x} \frac{1}{i_p^t} \ ,$$

all we need to do is to perform a summation by parts after writing

$$\frac{1}{i_p^t} = \sum_{ab|i_p} \frac{\mu(a)}{b^t} \ .$$

Chapter 3

Average r-rank Artin's conjecture

The results discussed in this Chapter appears in the joint work of the author with Cihan Pehlivan [17].

3.1 Introduction

In the case of rank $r = 1$, a first unconditional result on the average behavior of $N_a(x)$ was presented by Goldfeld [6] in 1967, who proved that for any constant $D > 1$, if $A = \prod_p \left(1 - \frac{1}{p(p-1)}\right)$ indicates the Artin's constant, the asymptotic formula

$$N_a(x) = A\,\mathrm{Li}(x) + O\left(\frac{x}{(\log x)^D}\right)$$

holds for all integers $a \leqslant N$ with at most

$$c_1 N^{9/10}(5\log x + 1)^{g+D+2}\ , \qquad g = \frac{\log x}{\log N}\ ,$$

exceptions, where c_1 and the constant implied by the O-notation are positive and depend at most on D.

Stephens [31] in 1969 proved that, if $T > \exp(4(\log x \log\log x)^{1/2})$, then

$$\frac{1}{T}\sum_{a\leqslant T} N_a(x) = \sum_{p\leqslant x}\frac{\varphi(p-1)}{p-1} + O\left(\frac{x}{(\log x)^D}\right) = A\,\mathrm{Li}(x) + O\left(\frac{x}{(\log x)^D}\right)\ , \tag{3.1}$$

where φ is the Euler totient function 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

$$\frac{1}{T}\sum_{a\leqslant T}\{N_a(x) - A\,\mathrm{Li}(x)\}^2 \ll \frac{x^2}{(\log x)^{D'}}\ , \tag{3.2}$$

for any constant $D' > 2$. In 1976, Stephens refined his results with different methods [32], getting both the asymptotic bounds (3.1) and (3.2) under the weaker assumption $T > \exp(C(\log x)^{1/2})$, with C positive constant.

If we set, for any $a \in \mathbb{N}\backslash\{0, \pm 1\}$ and $m \in \mathbb{N}$, $N_{a,m}(x)$ to be the number of primes $p \equiv 1 \pmod m$ not exceeding x such that the index $[\mathbb{F}_p^* : \langle a \pmod p\rangle] = m$, then for $T > \exp(4(\log x \log\log x)^{1/2})$ Moree [21] showed that

$$\frac{1}{T}\sum_{a\leqslant T} N_{a,m}(x) = \sum_{\substack{p\leqslant x \\ p\equiv 1 \pmod m}} \frac{\varphi((p-1)/m)}{p-1} + O\left(\frac{x}{(\log x)^E}\right), \tag{3.3}$$

for any constant $E > 1$.

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

Theorem 3.1.1. *Let* $T^* := \min\{T_i : i = 1, \ldots, r\} > \exp(4(\log x \log\log x)^{\frac{1}{2}})$ *and* $m \leqslant (\log x)^D$ *for an arbitrary positive constant* D. *Then*

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

where

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

and $M > 1$ *is arbitrarily large.*

Theorem 3.1.2. *Let* $T^* > \exp(6(\log x \log\log x)^{\frac{1}{2}})$ *and* $m \leqslant (\log x)^D$ *for an arbitrary positive constant* D. *Then*

$$\frac{1}{T_1 \cdots T_r} \sum_{\substack{a_i\in\mathbb{Z} \\ 0<a_1\leqslant T_1 \\ \vdots \\ 0<a_r\leqslant T_r}} \left\{N_{\langle a_1,\cdots,a_r\rangle,m}(x) - C_{r,m}\,\mathrm{Li}(x)\right\}^2 \ll \frac{x^2}{(\log x)^{M'}}$$

where $M' > 2$ *is arbitrarily large.*

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

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

The results found in the present paper (see in particular equation (3.8) and Lemma 3.3.3) will lead as a side product to the asymptotic identity

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

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

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

is the so called *Jordan's totient function*. This provides a natural generalization of Moree's result in [21].

Theorem 3.1.2 leads to the following Corollary:

Corollary 3.1.3. *For any $\epsilon > 0$, let*

$$\mathcal{H} := \{\underline{a} \in \mathbb{Z}^r : 0 < a_i \leqslant T_i, i \in \{1,\dots,r\}, |N_{\underline{a},m}(x) - C_{r,m}\,\mathrm{Li}(x)| > \epsilon\,\mathrm{Li}(x)\} \ ;$$

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

$$\#\mathcal{H} \leqslant K|\underline{T}|/\epsilon^2(\log x)^F$$

for every positive constant F.

Proof of Corollary 3.1.3. The proof of this Corollary is a trivial generalization of that in [31] (Corollary, page 187). □

3.2 Notations and conventions

In order to simplify the formulas, we introduce the following notations. 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 $\underline{a} \cdot \underline{n} = a_1 n_1 + \cdots + a_r n_r$. The null vector is $\underline{0} = \{0, \dots, 0\}$. Similarly, $\underline{\chi} = (\chi_1, \dots, \chi_r)$ is a r-tuple of Dirichlet characters and, given $\underline{a} \in \mathbb{Z}^r$, we denote the product $\underline{\chi}(\underline{a}) = \chi_1(a_1) \cdots \chi_r(a_r) \in \mathbb{C}$.

In addition, $(q, \underline{a}) := (q, a_1, \dots, a_r) = \gcd(q, a_1, \dots, a_r)$; otherwise, to avoid possible misinterpretations, we will write explicitly $\gcd(n_1, \dots, n_r)$ 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. Given a finite field $\mathbb{F}_p$, then $\mathbb{F}_p^* = \mathbb{F}_p \backslash \{0\}$ 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.

3.3 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 [8, Theorem 272]) that, given any integer n,

$$c_q(n) = \mu\left(\frac{q}{(q,n)}\right) \frac{\varphi(q)}{\varphi\left(\frac{q}{(q,n)}\right)}. \tag{3.4}$$

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

Lemma 3.3.1. *Let*

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

be the Jordan's totient function, then

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

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

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

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

$$c_{\ell^k}(\underline{n}) = \begin{cases} 0 & \text{if } \ell^{k-1} \nmid \gcd(n_1,\cdots,n_r)\,, \\ -\ell^{r(k-1)} & \text{if } \ell^{k-1} \| \gcd(n_1,\cdots,n_r)\,, \\ \ell^{rk}\left(1-\frac{1}{\ell^r}\right) & \text{if } \ell^k \mid \gcd(n_1,\cdots,n_r)\,. \end{cases}$$

To prove that, we start writing

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

If we apply (3.4), we obtain

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

Now, for $k \geqslant 2$, let us distinguish the two cases:

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

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

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

Hence

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

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

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

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

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

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

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

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

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

The proof of the Lemma now follows from the multiplicativity of μ and of J_r. $\square$

From the previous Lemma we deduce the following Corollary:

Corollary 3.3.2. *Let p be an odd prime, let $m \in \mathbb{N}$ be a divisor of $p-1$. Given a r-tuple $\underline{\chi} = (\chi_1, \dots, \chi_r)$ of Dirichlet characters modulo p, we set*

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

Then

$$c_m(\underline{\chi}) = \frac{1}{(p-1)^r} \, \mu \left(\frac{p-1}{m \gcd\left(\frac{p-1}{m}, \frac{p-1}{\operatorname{ord}(\chi_1)}, \dots, \frac{p-1}{\operatorname{ord}(\chi_r)}\right)} \right) \frac{J_r\left(\frac{p-1}{m}\right)}{J_r\left(\frac{p-1}{m \gcd\left(\frac{p-1}{m}, \frac{p-1}{\operatorname{ord}(\chi_1)}, \dots, \frac{p-1}{\operatorname{ord}(\chi_r)}\right)} \right)} \ . \tag{3.5}$$

Proof. Let us 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

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

if we write $\alpha_j = g^{a_j}$ for $j = 1, \dots, r$, then

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

Therefore, naming $t = \frac{p-1}{m}$, we have

$$\begin{aligned} c_m(\underline{\chi}) &= \frac{1}{(p-1)^r} \sum_{\substack{\underline{a} \in (\mathbb{F}_p^*)^r \\ (p-1, \underline{a}) = m}} \chi_1(g)^{a_1} \cdots \chi_r(g)^{a_r} \\ &= \frac{1}{(p-1)^r} \sum_{\substack{\underline{a}' \in (\mathbb{Z}/t\mathbb{Z})^r \\ (t, \underline{a}') = 1}} e^{2\pi i \underline{a}' \cdot \underline{n}/t} = \frac{1}{(p-1)^r} c_{\frac{p-1}{m}}(\underline{n}). \end{aligned} \tag{3.6}$$

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

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

and this, together with Lemma 1, concludes the proof. $\square$

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

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

where

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

so that

$$R_p(m) = \left(\frac{p-1}{m}\right)^r \sum_{n\mid\frac{p-1}{m}} \frac{\mu(n)}{n^r} = J_r\left(\frac{p-1}{m}\right) . \tag{3.7}$$

Defining

$$S_m(x) := \frac{1}{m^r} \sum_{\substack{p\leqslant x\\ p\equiv 1 \pmod m}} \sum_{n\mid\frac{p-1}{m}} \frac{\mu(n)}{n^r} = \sum_{\substack{p\leqslant x\\ p\equiv 1 \pmod m}} \frac{1}{(p-1)^r} J_r\left(\frac{p-1}{m}\right) , \tag{3.8}$$

we have the following Lemma:

Lemma 3.3.3. *If $m \leqslant (\log x)^D$, with D arbitrary positive constant, then for every arbitrary constant $M > 1$*

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

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

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

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

The sum in the error term is

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

For the main term we apply the Siegel–Walfisz Theorem [34], which states that for every arbitrary positive constants B and C, if $a \leqslant (\log x)^B$, then

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

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

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

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

$$\frac{n}{\varphi(n)} < e^\gamma \log\log n + \frac{3}{\log\log n} \ll \log\log n , \tag{3.9}$$

then

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

Thus

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

proving the lemma for a suitable choice of D, B and C. □

The following Lemma concerns the Titchmarsh Divisor Problem [33] in the case of primes $p \equiv 1 \pmod m$. Asymptotic results on this topic can be found in [4] and [5].

Lemma 3.3.4. *Let τ be the divisor function and $m \in \mathbb{N}$. If $m \leqslant (\log x)^D$ for an arbitrary positive constant D, we have the following inequality:*

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

Proof. Let us write $p-1 = mjk$ so that $jk \leqslant (x-1)/m$ and let us set $Q = \sqrt{\frac{x-1}{m}}$ and distinguish the three cases

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

So we have the identity

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

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

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

for $m \leqslant (\log x)^D$ with D arbitrary positive constant, then we obtain

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

Now, substitute the elementary inequality $\varphi(km) \geqslant m\varphi(k)$ and use a result of Montgomery [19]

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

where

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

which in particular implies that, for Q large enough,

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

Finally

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

□

Lemma 3.3.5. *Let p be an odd prime number and let $\chi \neq \chi_0$ be a non-principal Dirichlet character modulo p. Define*

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

then

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

Proof. From equation (3.6) and Lemma 3.3.1, we have

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

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

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

where

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

Then

$$d_{m,i}(\chi) = \frac{1}{(p-1)} \sum_{d|t} \mu^2\left(\frac{t}{d}\right) \frac{J_r(t)}{d^{r-1} J_r\left(\frac{t}{d}\right)} \sum_{k|\frac{u}{d}} \frac{\mu(k)}{k^{r-1}}$$
$$\leqslant \frac{1}{p-1} \sum_{d|t} \mu^2\left(\frac{t}{d}\right) d = \frac{t}{p-1} \sum_{k|t} \frac{\mu^2(k)}{k} = \frac{1}{m} \prod_{\ell | \frac{p-1}{m}} \left(1 + \frac{1}{\ell}\right)$$

□

3.4 Proof of Theorem 1

We follow the method of Stephens [31]. By exchanging the order of summation we obtain that

$$\sum_{\substack{\underline{a} \in \mathbb{Z}^r \\ 0 < a_1 \leqslant T_1 \\ \vdots \\ 0 < a_r \leqslant T_r}} N_{\langle \underline{a} \rangle, m}(x) = \sum_{\substack{p \leqslant x \\ p \equiv 1 \pmod m}} M_p^m(\underline{T}) \ ,$$

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

$$M_p^m(\underline{T}) = \sum_{\substack{\underline{a} \in \mathbb{Z}^r \\ 0 < a_1 \leqslant T_1 \\ \vdots \\ 0 < a_r \leqslant T_r}} t_{p,m}(\underline{a}) \ ,$$

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

$$t_{p,m}(\underline{a}) = \sum_{\underline{\chi} \in (\widehat{\mathbb{F}_p^*})^r} c_m(\underline{\chi}) \underline{\chi}(\underline{a}) \ ; \tag{3.10}$$

so we have

$$\sum_{\substack{\underline{a} \in \mathbb{Z}^r \\ 0 < a_1 \leqslant T_1 \\ \vdots \\ 0 < a_r \leqslant T_r}} N_{\langle \underline{a} \rangle, m}(x) = \sum_{\substack{p \leqslant x \\ p \equiv 1 \pmod m}} \sum_{\substack{\underline{a} \in \mathbb{Z}^r \\ 0 < a_1 \leqslant T_1 \\ \vdots \\ 0 < a_r \leqslant T_r}} \sum_{\underline{\chi} \in (\widehat{\mathbb{F}_p^*})^r} c_m(\underline{\chi}) \underline{\chi}(\underline{a}) \ . \tag{3.11}$$

Let $\underline{\chi}_0 := (\chi_0, \ldots, \chi_0)$ be the r-tuple consisting of all principal characters, then

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

Denoting $|\underline{T}| := \prod_{i=1}^r T_i$ and $T^* := \min\{T_i : i = 1, \ldots, r\}$, through (3.8) and (3.7), we can write the main term in (3.11) as

$$\begin{aligned} & \frac{1}{|\underline{T}|} \sum_{\substack{p \leqslant x \\ p \equiv 1 \pmod m}} \sum_{\substack{\underline{a} \in \mathbb{Z}^r \\ 0 < a_1 \leqslant T_1 \\ \vdots \\ 0 < a_r \leqslant T_r}} c_m(\underline{\chi}_0) \underline{\chi}_0(\underline{a}) \\ = & \frac{1}{|\underline{T}|} \sum_{\substack{p \leqslant x \\ p \equiv 1 \pmod m}} c_m(\underline{\chi}_0) \prod_{i=1}^r \{\lfloor T_i \rfloor - \lfloor T_i/p \rfloor\} \\ = & \sum_{\substack{p \leqslant x \\ p \equiv 1 \pmod m}} c_m(\underline{\chi}_0) \left(1 - \frac{r}{p} + \cdots + \frac{1}{p^r} + \sum_{i=1}^r O\left(\frac{1}{T_i}\right)\right) \\ = & \sum_{\substack{p \leqslant x \\ p \equiv 1 \pmod m}} c_m(\underline{\chi}_0) + O\left(\sum_{\substack{p \leqslant x \\ p \equiv 1 \pmod m}} \frac{1}{p} \right) + O\left(\frac{x}{T^* \log x}\right) \\ = & S_m(x) + O(\log\log x) + O\left(\frac{x}{T^* \log x}\right) \ . \end{aligned}$$

By hypothesis $m \leqslant (\log x)^D$, $D > 0$, and $T^* > \exp(4(\log x \log\log x)^{1/2})$, so we can apply Lemma 3.3.3 to obtain

$$\frac{1}{|\underline{T}|} \sum_{\substack{p \leqslant x \\ p \equiv 1 \pmod m}} \sum_{\substack{\underline{a} \in \mathbb{Z}^r \\ 0 < a_1 \leqslant T_1 \\ \vdots \\ 0 < a_r \leqslant T_r}} c_m(\underline{\chi}_0) \underline{\chi}_0(\underline{a}) = C_{r,m} \operatorname{Li}(x) + O\left(\frac{x}{m^r (\log x)^M}\right) \ ,$$

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

$$E_{r,m}(x) := \frac{1}{|\underline{T}|} \sum_{\substack{p \leqslant x \\ p \equiv 1 \pmod m}} \sum_{\underline{\chi} \in \left(\widehat{\mathbb{F}_p^*}\right)^r \setminus \{\underline{\chi}_0\}} \left| c_m(\underline{\chi}) \sum_{\substack{\underline{a} \in \mathbb{Z}^r \\ 0 < a_1 \leqslant T_1 \\ \vdots \\ 0 < a_r \leqslant T_r}} \underline{\chi}(\underline{a}) \right| \tag{3.12}$$

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

since the r main contributions to (3.12) comes from the cases in which just one Dirichlet character in $\underline{\chi}$ is non-principal, say $\chi_i = \chi \neq \chi_0$, while for every $j \neq i$ we choose $\chi_j = \chi_0$, giving

$$\left| \sum_{\substack{\underline{a} \in \mathbb{Z}^r \\ 0 < a_1 \leqslant T_1 \\ \vdots \\ 0 < a_r \leqslant T_r}} \underline{\chi}(\underline{a}) \right| = \left| \sum_{\substack{a \in \mathbb{Z} \\ 0 < a \leqslant T_i}} \chi(a) \sum_{\substack{0 \leqslant j \leqslant r \\ j \neq i}} \sum_{\substack{a_j \in \mathbb{Z} \\ 0 < a_j \leqslant T_j \\ p \nmid a_j}} 1 \right| \leqslant \frac{|\underline{T}|}{T_i} \left| \sum_{\substack{a \in \mathbb{Z} \\ 0 < a \leqslant T_i}} \chi(a) \right| .$$

Define

$$E^i_{r,m}(x) := \sum_{\substack{p \leqslant x \\ p \equiv 1 \pmod m}} \sum_{\chi \in \widehat{\mathbb{F}_p^*} \setminus \{\chi_0\}} d_{m,i}(\chi) \left| \sum_{\substack{a \in \mathbb{Z} \\ 0 < a \leqslant T_i}} \chi(a) \right| , \tag{3.13}$$

then by Holder's inequality

$$\begin{aligned} \left\{E^i_{r,m}(x)\right\}^{2s_i} \leqslant & \left\{ \sum_{\substack{p \leqslant x \\ p \equiv 1 \pmod m}} \sum_{\chi \in \widehat{\mathbb{F}_p^*} \setminus \{\chi_0\}} \{d_{m,i}(\chi)\}^{\frac{2s_i}{2s_i - 1}} \right\}^{2s_i - 1} \\ & \times \sum_{\substack{p \leqslant x \\ p \equiv 1 \pmod m}} \sum_{\chi \in \widehat{\mathbb{F}_p^*} \setminus \{\chi_0\}} \left| \sum_{\substack{a \in \mathbb{Z} \\ 0 < a \leqslant T_i}} \chi(a) \right|^{2s_i} . \end{aligned} \tag{3.14}$$

As before, given a primitive root g modulo p, write $\chi_j(g) = e^{2\pi i n_j/(p-1)}$ for every $j = 1, \ldots, r$, with $n_j \in \mathbb{Z}/(p-1)\mathbb{Z}$, so that by equation (3.6)

$$\sum_{\underline{\chi} \in \left(\widehat{\mathbb{F}_p^*}\right)^r \setminus \{\underline{\chi}_0\}} c_m(\underline{\chi}) = \frac{1}{(p-1)^r} \sum_{\underline{n} \in \left(\frac{\mathbb{Z}}{(p-1)\mathbb{Z}}\right)^r \setminus \{\underline{0}\}} c_{\frac{p-1}{m}}(\underline{n}) \, .$$

Denoting again $t = (p-1)/m$, from Lemma 3.3.1 we derive the following upper bound:

$$\begin{aligned}
\sum_{\chi \in \widehat{\mathbb{F}_p^*} \setminus \{\chi_0\}} d_{m,i}(\chi) &\leqslant \sum_{\underline{\chi} \in \left(\widehat{\mathbb{F}_p^*}\right)^r \setminus \{\underline{\chi}_0\}} |c_m(\underline{\chi})| \\
&\leqslant \sum_{d|t} \mu^2\left(\frac{t}{d}\right) \left[\frac{J_r(t)}{(p-1)^r J_r(t/d)}\right] \# \left\{\underline{n} \in (\mathbb{Z}/(p-1)\mathbb{Z})^r : (t, \underline{n}) = d\right\} \\
&= \sum_{d|t} \mu^2\left(\frac{t}{d}\right) \frac{J_r(t)}{d^r J_r(t/d)} \sum_{k|\frac{t}{d}} \frac{\mu(k)}{k^r} = \frac{J_r(t)}{t^r} \sum_{d|t} \mu^2\left(\frac{t}{d}\right) \\
&= \prod_{\ell|t} \left(1 - \frac{1}{\ell^r}\right) 2^{\omega(t)} \leqslant 2^{\omega(t)} \, .
\end{aligned}$$

Call $D_{m,i}(p) := \max\{d_{m,i}(\chi) : \chi \in \widehat{\mathbb{F}_p^*} \setminus \{\chi_0\}\}$, then the following asymptotic estimate holds for every $s_i \geqslant 1$:

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

where we have used Lemma 3.3.4 and Lemma 3.3.5 together with the simple observation

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

To estimate the other factor in (3.14) we use Lemma 5 in [31]:

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

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

$$\frac{1}{|\underline{T}|} \sum_{\substack{\underline{a} \in \mathbb{Z}^r \\ 0 < a_1 \leqslant T_1 \\ \vdots \\ 0 < a_r \leqslant T_r}} N_{\langle \underline{a} \rangle, m}(x) = C_{r,m} \operatorname{Li}(x) + O\left(\frac{x}{m^r (\log x)^M} \right) + O\left(\sum_{i=1}^{r} \frac{x}{T_i \log x} \right) + E_{r,m}(x) ,$$

with

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

If we choose $s_i = \left\lfloor \frac{2 \log x}{\log T_i} \right\rfloor + 1$ for $i = 1, \ldots, r$, then $T_i^{s_i - 1} \leqslant x^2 < T_i^{s_i}$ 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 $i = 1, \ldots, r$, then $s_1 = \cdots = s_r = 1$ and

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

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

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

By hypothesis

$$T^* > \exp(4(\log x \log\log x)^{1/2}) \tag{3.15}$$

and, through computations similar to those in [31] (page 184), we can derive the following estimate:

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

Also in this case, using (3.15), we have $E_{r,m}(x) \ll x/(\log x)^M$ for every $M > 1$. This ends the proof of Theorem 3.1.1. □

3.5 Proof of Theorem 2

We now consider

$$H: \ = \frac{1}{|\underline{T}|} \sum_{\substack{\underline{a}\in\mathbb{Z}^r \\ 0<a_1\leqslant T_1 \\ \vdots \\ 0<a_r\leqslant T_r}} \left\{N_{\langle\underline{a}\rangle,m}(x) - C_{r,m}\,\mathrm{Li}(x)\right\}^2 .$$

We start bounding H as follows:

$$\sum_{\substack{\underline{a}\in\mathbb{Z}^r \\ 0<a_1\leqslant T_1 \\ \vdots \\ 0<a_r\leqslant T_r}} \left\{N_{\langle\underline{a}\rangle,m}(x) - C_{r,m}\,\mathrm{Li}(x)\right\}^2$$
$$\leqslant \sum_{\substack{p,q\leqslant x \\ p,q\equiv 1 \pmod m}} M^m_{p,q}(\underline{T}) - 2C_{r,m}\,\mathrm{Li}(x) \sum_{\substack{p\leqslant x \\ p\equiv 1 \pmod m}} M^m_p(\underline{T}) + |\underline{T}|(C_{r,m})^2\,\mathrm{Li}^2(x) ,$$

where $M^m_{p,q}(\underline{T})$ denotes the number of r-tuples $\underline{a}\in\mathbb{Z}^r$, with $a_i\leqslant T_i$ and $v_p(a_i)=v_q(a_i)=0$ for each $i=1,\ldots,r$, 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 3.1.1 we obtain

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

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

$$\sum_{\substack{p,q\leqslant x \\ p,q\equiv 1 \pmod m}} M^m_{p,q}(\underline{T}) = \sum_{\substack{p\leqslant x \\ p\equiv 1 \pmod m}} M^m_p(\underline{T}) + \sum_{\substack{p,q\leqslant x \\ p,q\equiv 1 \pmod m \\ p\neq q}} M^m_{p,q}(\underline{T}) ,$$

Theorem 3.1.1 gives, for arbitrary $M>1$,

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

In the same spirit as in the proof Theorem 3.1.1, we use equation (3.10) to deal with the following sum

$$\sum_{\substack{p,q\leqslant x\\ p,q\equiv 1 \pmod m\\ p\neq q}} M^m_{p,q}(\underline{T}) = \sum_{\substack{p,q\leqslant x\\ p,q\equiv 1 \pmod m\\ p\neq q}} \sum_{\substack{\underline{a}\in\mathbb{Z}^r\\ 0<a_1\leqslant T_1\\ \vdots\\ 0<a_r\leqslant T_r}} t_{p,m}(\underline{a})t_{q,m}(\underline{a})$$

$$= \sum_{\substack{p,q\leqslant x\\ p,q\equiv 1 \pmod m\\ p\neq q}} \sum_{\underline{\chi}_1\in(\widehat{\mathbb{F}_p})^r} \sum_{\underline{\chi}_2\in(\widehat{\mathbb{F}_q})^r} c_m(\underline{\chi}_1)c_m(\underline{\chi}_2) \sum_{\substack{\underline{a}\in\mathbb{Z}^r\\ 0<a_1\leqslant T_1\\ \vdots\\ 0<a_r\leqslant T_r}} \underline{\chi}_1(\underline{a})\underline{\chi}_2(\underline{a}) \ , \tag{3.16}$$

where $\underline{\chi}_1$ and $\underline{\chi}_2$ denote r-tuple of Dirichlet characters modulo p, q respectively. Therefore

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

where H_1, H_2, H_3 are the contributions to the sum (3.16) when $\underline{\chi}_1 = \underline{\chi}_2 = \underline{\chi}_0$, only one between $\underline{\chi}_1$ and $\underline{\chi}_2$ is equal to $\underline{\chi}_0$, neither $\underline{\chi}_1$ nor $\underline{\chi}_2$ is $\underline{\chi}_0$, respectively. First we deal with the inner sum in H_1. To avoid confusion, we set $\underline{\chi}_0^{(p)}$ and $\underline{\chi}_0^{(q)}$ as the r-tuples whose all entries are principal characters modulo p and modulo q respectively, so that

$$\sum_{\substack{\underline{a}\in\mathbb{Z}^r\\ 0<a_1\leqslant T_1\\ \vdots\\ 0<a_r\leqslant T_r}} \underline{\chi}_0^{(p)}(\underline{a})\underline{\chi}_0^{(q)}(\underline{a}) = \prod_{i=1}^{r}\left\{\lfloor T_i\rfloor - \left\lfloor\frac{T_i}{p}\right\rfloor - \left\lfloor\frac{T_i}{q}\right\rfloor + \left\lfloor\frac{T_i}{pq}\right\rfloor\right\} .$$

Using Lemma 3.3.3, with $M' > 2$ arbitrary constant:

$$H_1 = \sum_{\substack{p,q\leqslant x\\ p,q\equiv 1 \pmod m\\ p\neq q}} c_m(\underline{\chi}_0^{(p)})c_m(\underline{\chi}_0^{(q)}) \sum_{\substack{\underline{a}\in\mathbb{Z}^r\\ 0<a_1\leqslant T_1\\ \vdots\\ 0<a_r\leqslant T_r}} \underline{\chi}_0^{(p)}(\underline{a})\underline{\chi}_0^{(q)}(\underline{a})$$

$$= |\underline{T}| \sum_{\substack{p,q\leqslant x \\ p,q\equiv 1 \pmod m \\ p\neq q}} c_m(\underline{\chi}_0^{(p)})c_m(\underline{\chi}_0^{(q)})\left(1-\frac{r}{p}-\frac{r}{q}+\cdots+\frac{1}{(pq)^r}+\sum_{i=1}^{r} O\left(\frac{1}{T_i}\right)\right)$$

$$= |\underline{T}| \left(\left(\sum_{\substack{p\leqslant x \\ p\equiv 1 \pmod m}} c_m(\underline{\chi}_0^{(p)})\right)^2 - \sum_{\substack{p\leqslant x \\ p\equiv 1 \pmod m}} (c_m(\underline{\chi}_0^{(p)}))^2\right)$$

$$\times \left(1+O\left(\frac{1}{T^*}\right)\right) + |\underline{T}| O\left(\frac{x\log\log x}{\log x}\right)$$

$$= |\underline{T}| \left(S_m^2(x) + O\left(\frac{x^2}{T^*(\log x)^2}\right) + O\left(\frac{x\log\log x}{\log x}\right)\right)$$

$$= |\underline{T}| \left(C_{r,m}^2 \operatorname{Li}^2(x) + O\left(\frac{x^2}{m^r(\log x)^{M'}}\right)\right) .$$

Focus now on H_2 and assume without loss of generality that $\underline{\chi}_1 = \underline{\chi}_0 \neq \underline{\chi}_2$:

$$H_2 = \sum_{\substack{p,q\leqslant x \\ p,q\equiv 1 \pmod m \\ p\neq q}} \sum_{\underline{\chi}_2 \in (\widehat{\mathbb{F}_q^*})^r \setminus \{\underline{\chi}_0^{(q)}\}} c_m(\underline{\chi}_0^{(p)})c_m(\underline{\chi}_2) \sum_{\substack{\underline{a}\in\mathbb{Z}^r \\ 0<a_1\leqslant T_1 \\ \vdots \\ 0<a_r\leqslant T_r}} \underline{\chi}_0^{(p)}(\underline{a})\underline{\chi}_2(\underline{a})$$

$$= \sum_{\substack{p\leqslant x \\ p\equiv 1 \pmod m}} c_m(\underline{\chi}_0^{(p)}) \sum_{\substack{q\leqslant x \\ q\equiv 1 \pmod m \\ q\neq p}} \sum_{\underline{\chi}_2 \in (\widehat{\mathbb{F}_q^*})^r \setminus \{\underline{\chi}_0^{(q)}\}} c_m(\underline{\chi}_2) \sum_{\substack{\underline{a}\in\mathbb{Z}^r \\ 0<a_1\leqslant T_1 \\ \vdots \\ 0<a_r\leqslant T_r \\ p\nmid \prod_{i=1}^r a_i}} \underline{\chi}_2(\underline{a}) .$$

Identically to what was done in the proof of Theorem 1, the quantity

$$U_2 := \sum_{\substack{q\leqslant x \\ q\equiv 1 \pmod m}} \sum_{\underline{\chi}_2 \in (\widehat{\mathbb{F}_q^*})^r \setminus \{\underline{\chi}_0^q\}} \left| c_m(\underline{\chi}_2) \sum_{\substack{\underline{a}\in\mathbb{Z}^r \\ 0<a_1\leqslant T_1 \\ \vdots \\ 0<a_r\leqslant T_r}} \underline{\chi}_2(\underline{a}) \right|$$

can be estimated through Holder's inequality combined with the large sieve inequality, to get $U_2 \ll x/(\log x)^M$ for any constant $M > 1$. Moreover, Lemma 3.3.4 gives an upper bound for the following quantity:

$$\begin{aligned} V_2 \quad := \quad & \sum_{\substack{q\leqslant x \\ q\equiv 1 \pmod m}} \sum_{\underline{\chi}_2\in(\widehat{\mathbb{F}_q^*})^r\setminus\{\underline{\chi}_0^{(q)}\}} \left| c_m(\underline{\chi}_2) \sum_{\substack{\underline{a}\in\mathbb{Z}^r \\ 0<a_1\leqslant T_1 \\ \vdots \\ 0<a_r\leqslant T_r \\ p\mid\prod_{i=1}^r a_i}} \underline{\chi}_2(\underline{a}) \right| \\ \ll \quad & \frac{|\underline{T}|}{p^r} \sum_{\substack{q\leqslant x \\ q\equiv 1 \pmod m}} \sum_{\underline{\chi}_2\in(\widehat{\mathbb{F}_q^*})^r\setminus\{\underline{\chi}_0^{(q)}\}} |c_m(\underline{\chi}_2)| \\ \ll \quad & \frac{|\underline{T}|}{p^r} \sum_{\substack{q\leqslant x \\ q\equiv 1 \pmod m}} \tau\left(\frac{q-1}{m}\right) \ll \frac{|\underline{T}|x}{p^r m} . \end{aligned}$$

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

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

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. Given

$$H_3 = \sum_{\substack{p,q\leqslant x \\ p,q\equiv 1 \pmod m \\ p\neq q}} \sum_{\underline{\chi}_1\in(\widehat{\mathbb{F}_p^*})^r\setminus\{\underline{\chi}_0^{(p)}\}} \sum_{\underline{\chi}_2\in(\widehat{\mathbb{F}_q^*})^r\setminus\{\underline{\chi}_0^{(q)}\}} c_m(\underline{\chi}_1)c_m(\underline{\chi}_2) \sum_{\substack{\underline{a}\in\mathbb{Z}^r \\ 0<a_1\leqslant T_1 \\ \vdots \\ 0<a_r\leqslant T_r}} \underline{\chi}_1(\underline{a})\underline{\chi}_2(\underline{a})$$

we will apply again Holder's inequality and the large sieve (Lemma 5 in [31]) to obtain an upper bound. In order to do that, since the r-tuples of characters, $\underline{\chi}_1$ and $\underline{\chi}_2$, appearing in H_3 are both non-principal, we indicate with χ_1 the i-th component of the r-tuple $\underline{\chi}_1$ of Dirichlet characters to the modulus p (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 χ_1 and $\chi_{2,i}$ are non-principal) and a "non-diagonal" term H_3^{nd} (in which for none of the indices $i \in \{1,\dots,r\}$ is possible to have χ_1 and $\chi_{2,i}$ both non-principal). Analogously to what was done for the estimate of the error term (3.12) in the proof of Theorem 1, the main contributions to H_3^d and H_3^{nd} derive from the cases in which, for a certain r-tuple of characters modulo p or q, we pick just one character non-principal and the other $r-1$ all principal. Explicitly, $H_3^d = \sum_{i=1}^r H_{3,i}$, where

$$H_{3,i} := \sum_{\substack{p,q\leqslant x \\ p,q\equiv 1 \pmod m \\ p\neq q}} \sum_{\substack{\underline{\chi}_1\in(\widehat{\mathbb{F}_p^*})^r \\ \chi_1\in\widehat{\mathbb{F}_p^*}\setminus\{\chi_0^{(p)}\}}} \sum_{\substack{\underline{\chi}_2\in(\widehat{\mathbb{F}_q^*})^r \\ \chi_2\in\widehat{\mathbb{F}_q^*}\setminus\{\chi_0^{(q)}\}}} c_m(\underline{\chi}_1)c_m(\underline{\chi}_2) \sum_{\substack{\underline{a}\in\mathbb{Z}^r \\ 0<a_1\leqslant T_1 \\ \vdots \\ 0<a_r\leqslant T_r}} \underline{\chi}_1(\underline{a})\underline{\chi}_2(\underline{a})$$

$$\ll \frac{|\underline{T}|}{T_i} \sum_{\substack{p,q\leqslant x \\ p,q\equiv 1 \pmod m \\ p\neq q}} \sum_{\chi_1\in\widehat{\mathbb{F}_p^*}\setminus\{\chi_0^{(p)}\}} \sum_{\chi_2\in\widehat{\mathbb{F}_q^*}\setminus\{\chi_0^{(q)}\}} d_{m.i}(\chi_1)d_{m,i}(\chi_2) \left| \sum_{\substack{a_i\in\mathbb{Z} \\ 0<a_i\leqslant T_i}} \chi_1(a_i)\chi_2(a_i) \right|$$

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

$$H_{3,ij} := \sum_{\substack{p,q\leqslant x \\ p,q\equiv 1 \pmod m \\ p\neq q}} \sum_{\substack{\underline{\chi}_1\in(\widehat{\mathbb{F}_p^*})^r \\ \chi_1\in\widehat{\mathbb{F}_p^*}\setminus\{\chi_0^{(p)}\}}} \sum_{\substack{\underline{\chi}_2\in(\widehat{\mathbb{F}_q^*})^r \\ \chi_2\in\widehat{\mathbb{F}_q^*}\setminus\{\chi_0^{(q)}\}}} c_m(\underline{\chi}_1)c_m(\underline{\chi}_2) \sum_{\substack{\underline{a}\in\mathbb{Z}^r \\ 0<a_1\leqslant T_1 \\ \vdots \\ 0<a_r\leqslant T_r}} \underline{\chi}_1(\underline{a})\underline{\chi}_2(\underline{a})$$

$$\ll \frac{|\underline{T}|}{T_iT_j} \sum_{\substack{p,q\leqslant x \\ p,q\equiv 1 \pmod m \\ p\neq q}} \sum_{\chi_1\in\widehat{\mathbb{F}_p^*}\setminus\{\chi_0^{(p)}\}} \sum_{\chi_2\in\widehat{\mathbb{F}_q^*}\setminus\{\chi_0^{(q)}\}} d_{m,i}(\chi_1)d_{m,j}(\chi_2) \left| \sum_{\substack{a_i,a_j\in\mathbb{Z} \\ 0<a_i\leqslant T_i \\ 0<a_j\leqslant T_j}} \chi_1(a_i)\chi_2(a_j) \right| .$$

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

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

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

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

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

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

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 in two products and through the same methods used for (3.13) we have

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

We choose $s_i = \left\lfloor \frac{2\log x}{\log T_i} \right\rfloor + 1$ and $s_j = \left\lfloor \frac{2\log x}{\log T_j} \right\rfloor + 1$, 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 3.1.2. □

Chapter 4

Work in progress

In this Chapter we present the current results of a joint work with Francesco Pappalardi that, given a finitely generated subgroup $\Gamma \subset \mathbb{Q}^*$, allow to determine an explicit formula for the order of the Galois group $\#\,\mathrm{Gal}(\mathbb{Q}(\zeta_m, \Gamma^{1/d})/\mathbb{Q})$ where $d \mid m$, $\zeta_m = e^{2\pi i/m}$ and $\Gamma^{1/d} = \{\alpha \in \mathbb{C} : \alpha^d \in \Gamma\}$. In this way, we can generalize equation (1.5) and, consequently, every result which makes use of that formula, like those in Section 2.3 or formula (1.11) from [26].

By the standard properties of Kummer extensions (see for example [13, Theorem 8.1]), we have that

$$\mathrm{Gal}(\mathbb{Q}(\zeta_m, \Gamma^{1/d})/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \oplus \Gamma(d)/\tilde{\Gamma}_{m,d}$$

where

$$\Gamma(d) := \Gamma \cdot \mathbb{Q}^{*d}/\mathbb{Q}^{*d} \qquad \text{and} \qquad \tilde{\Gamma}_{m,d} := \{\gamma \in \Gamma(d) : \ \gamma' \in \Gamma \cdot \mathbb{Q}^{*d} \cap (\mathbb{Q}(\zeta_m)^*)^d\},$$

where for $\gamma \in \Gamma(d)$, $\gamma' \in \mathbb{Z}$ denotes the unique d–power free representative of γ ($\gamma = \gamma' \cdot \mathbb{Q}^{*d}$). This notation will be used extensively throughout this paper. Note that the sign of γ' is chosen to be positive if d is odd or if $\gamma = \gamma' \cdot \mathbb{Q}^{*d} \subset \mathbb{Q}^+$ and is negative otherwise. Furthermore if $d > 1$ is odd, then $(\mathbb{Q}(\zeta_m)^*)^d \cap \mathbb{Q}^* = \mathbb{Q}^{*d}$. Hence, if for ℓ prime, $v_\ell(d)$ denotes the ℓ–adic valuation of d, then

$$\tilde{\Gamma}_{m,d} \cong \prod_{\ell \mid d} \tilde{\Gamma}_{m,\ell^{v_\ell(d)}} = \tilde{\Gamma}_{m,2^{v_2(d)}}.$$

If $\eta \in \mathbb{Z}$, we denote by $\delta(\eta) = \mathrm{disc}(\mathbb{Q}(\sqrt{\eta})$ the field discriminant. So, if η is squarefree, then $\delta(\eta) = \eta$ or 4η according with $\eta \equiv 1 \bmod 4$ or not. It was observed in [25, Corollary 1] that, in the case when $\Gamma \subset \mathbb{Q}^+$, then if $2^\alpha \mid m$,

$$\tilde{\Gamma}_{m,2^\alpha} = \{\gamma \in \Gamma(2^\alpha) : \ \gamma' = \eta^{2^{\alpha-1}}, \ \delta(\eta) \mid m\}.^1 \tag{4.1}$$

[1] Note that if we denote by $\mathrm{Supp}\,\Gamma$ the *support* of Γ, i.e. the finite set of those primes ℓ such that the ℓ–adic

In particular, if $\alpha = 0$, then $\tilde{\Gamma}_{m,1}$ is the trivial group and if $\alpha = 1$ and m is squarefree, then in [2, page 124, (24)] is was proven that

$$\tilde{\Gamma}_{m,2} = \{\gamma \in \Gamma(2) : \delta(\gamma') \mid m \text{ and } \delta(\gamma') \equiv 1 \bmod (m)\}.$$

Note that for $4 \nmid m$, the condition $\delta(\gamma') \equiv 1(\mathrm{mod} m)$ above is irrelevant as it is implied by the condition that $\delta(\gamma') \mid m$. So that the formula for $\tilde{\Gamma}_{m,2}$ and that in (4.1) coincide.

Our first task is to extend the above formula for $\tilde{\Gamma}_{m,2}$ in the case when m is not necessarily squarefree.

Proposition 4.0.1. *Let $\Gamma \subset \mathbb{Q}^*$ be a finitely generated subgroup, let $m \in \mathbb{N}$ be even. Then*

$$\tilde{\Gamma}_{m,2} = \{\gamma \in \Gamma(2) : \delta(\gamma') \mid m\}$$

Although the proof of the Proposition is the same as the proof of Corollary 1 in [25], we add it here for completeness.

Proof of the Proposition. Let us start from the definition:

$$\tilde{\Gamma}_{m,2} := \{\gamma \in \Gamma(2) : \ \gamma' \in \Gamma \cdot \mathbb{Q}^{*2} \cap (\mathbb{Q}(\zeta_m)^*)^2\}.$$

and note that if $\gamma' \in \Gamma \cdot \mathbb{Q}^{*2}$ is squarefree, then $\gamma' \in (\mathbb{Q}(\zeta_m)^*)^2$ if and only if $\sqrt{\gamma'} \in \mathbb{Q}(\zeta_m)^*$ and this happens if and only if $\delta(\gamma') \mid m$ (see for example Weiss [35, page 264]). This completes the proof. $\square$

So we are left with the case $\alpha \geqslant 2$. We have the general

Proposition 4.0.2. *Let $\Gamma \subset \mathbb{Q}^*$ be a finitely generated group. Let $m \in \mathbb{N}$ and let $\alpha \in \mathbb{N}$, $\alpha \neq 0$ be such that $2^\alpha \mid m$. Finally set*

$$\tilde{\Gamma}^+_{m,2^\alpha} = \{\gamma \in \Gamma(2^\alpha) : \gamma' = u^{2^{\alpha-1}} \text{ and } \delta(u) \mid m\}$$

and

$$\tilde{\Gamma}^-_{m,2^\alpha} = \begin{cases} \{\gamma \in \Gamma(2^\alpha) : \gamma' = -u^{2^{\alpha-1}} \text{ and } \delta(u) \mid m\} & \text{if } 2^{\alpha+1} \mid m \\ \{\gamma \in \Gamma(2^\alpha) : \gamma' = -u^{2^{\alpha-1}} \text{ and } \delta(u) \mid 2m \text{ but } \delta(u) \nmid m\} & \text{if } 2^{\alpha+1} \nmid m. \end{cases}$$

Then

$$\tilde{\Gamma}_{m,2^\alpha} = \tilde{\Gamma}^+_{m,2^\alpha} \cup \tilde{\Gamma}^-_{m,2^\alpha}.$$

---

valuation of some elements of Γ is nonzero and we set

$$\sigma_\Gamma := \prod_{\ell \in \mathrm{Supp}\,\Gamma} \ell,$$

then $\gamma \in \tilde{\Gamma}_{m,2^\alpha}$ such that $\gamma' = \eta^{2^{\alpha-1}}$, implies that $\eta \mid \gcd(m, \sigma_\Gamma)$.

The proof is, in spirit, the same as the proof of [29, Lemma 4].

Proof. From the discussion above, we can restrict ourselves to the case when $\alpha \geqslant 2$. Suppose that $\gamma' \in \mathbb{Z}$, $\gamma' > 0$ is 2^α–power free and that $\sqrt[2^\alpha]{\gamma'} \in \mathbb{Q}(\zeta_m)$. Then $\mathbb{Q}(\sqrt[2^\alpha]{\gamma'})$ is a Galois, real, extension of $\mathbb{Q}$ and this can only happen if its degree over $\mathbb{Q}$ is at most 2. Hence $\gamma' = u^{2^{\alpha-1}}$ for some $u \in \mathbb{N}$.

Next suppose that $\gamma' \in \mathbb{Z}$, $\gamma' < 0$ and that $\eta \in \mathbb{Q}(\zeta_m)$ is such that $\eta^{2^\alpha} = \gamma'$. We claim that $\gamma' = -u^{2^{\alpha-1}}$ for some $u \in \mathbb{N}$. In fact $\gamma'^2 > 0$ and $\gamma'^2 = \eta^{2^{\alpha+1}}$. Hence we can apply the argument above to deduce that $\gamma'^2 = u^{2^\alpha}$ so that $\gamma' = -u^{2^{\alpha-1}}$. From this property we dedce that $\eta = \zeta_{2^{\alpha+1}}^k \sqrt{u}$ for some $k \in \mathbb{N}$, $\leqslant 2^{\alpha+1}$, k odd. Clearly we can assume that $k = 1$ so that $\eta = \zeta_{2^{\alpha+1}}\sqrt{u} \in \mathbb{Q}(\zeta_m)$. We need to distinguish two cases: $2^{\alpha+1} \mid m$ or $2^\alpha \| m$. In the first case, $\zeta_{2^{\alpha+1}} \in \mathbb{Q}(\zeta_m)$ so that the condition $\eta \in \mathbb{Q}(\zeta_m)$ is equivalent to $\sqrt{u} \in \mathbb{Q}(\zeta_m)$ which is equivalent to $\delta(u) \mid m$. In the second case we have that $\zeta_{2^{\alpha+1}} \notin \mathbb{Q}(\zeta_m)$. So $\sqrt{u} \notin \mathbb{Q}(\zeta_m)$ but $\zeta_{2^{\alpha+1}} \in \mathbb{Q}(\zeta_{2m})$, hence $\sqrt{u} \in \mathbb{Q}(\zeta_{2m}) \backslash \mathbb{Q}(\zeta_m)$. Viceversa, if $\sqrt{u} \in \mathbb{Q}(\zeta_{2m}) \backslash \mathbb{Q}(\zeta_m)$, we have that

$$\mathbb{Q}(\zeta_{2m}) = \mathbb{Q}(\zeta_m)(\sqrt{u}) = \mathbb{Q}(\zeta_m)(\sqrt{\zeta_{2^\alpha}}) = \mathbb{Q}(\zeta_m)(\zeta_{2^{\alpha+1}}).$$

Hence $\sqrt{u} = \alpha\zeta_{2^{\alpha+1}}$ for some $\alpha \in \mathbb{Q}(\zeta_m)$. So $\zeta_{2^{\alpha+1}}\sqrt{u} \in \mathbb{Q}(\zeta_m)$.

Finally $\sqrt{u} \in \mathbb{Q}(\zeta_{2m}) \backslash \mathbb{Q}(\zeta_m)$ is equivalent to $\delta(u) \mid 2m$ but $\delta(u) \nmid m$. □

Corollary 4.0.3. *Let $\Gamma \subset \mathbb{Q}^*$ be a finitely generated subgroup. Suppose that $m, d \in \mathbb{N}$ with $d \mid m$. Then*

$$\# \operatorname{Gal}(\mathbb{Q}(\zeta_m, \Gamma^{1/d})/\mathbb{Q}) = [\mathbb{Q}(\zeta_m, \Gamma^{1/d}) : \mathbb{Q}] = \varphi(m) \times |\Gamma(d)| \times \left|\tilde{\Gamma}_{m,2^{v_2(d)}}\right|^{-1}.$$

Bibliography

[1] L. Bach and F. Shallit, *Algorithmic Number Theory (Vol I: Efficient Algorithms).* MIT Press Series in the Foundations of Computing, Cambridge, 1996.

[2] L. Cangelmi and F. Pappalardi, *On the r-rank Artin Conjecture, II.* J. Number Theory **75** (1999),120–132.

[3] N. G. Chebotarëv, *Opredelenie plotnosti sovokupnosti prostykh chisel, prinadlezhashchikh zadannomu klassu podstanovok*, Izv. Ross. Akad. Nauk (1923), 205–250.

[4] A. T. Felix, *Generalizing the Titchmarsh divisor problem.* Int. J. Number Theory **8** (2012), 613–629.

[5] A. Fiorilli, *On a theorem of Bombieri, Friedlander and Iwaniec.* Canad. J. Math. **64** (2012), 1019–1035.

[6] M. Goldfeld, *Artin's conjecture on the average.* Mathematika **15** (1968), 223–226.

[7] R. Gupta and M. Ram Murty, *A remark on Artin's conjecture.* Invent. Math. **78**, (1984), 127–130.

[8] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers.* Oxford University Press, 4th edition, London, 1975.

[9] C. Hooley, *On Artin's conjecture.* J. Reine Angew. Math. **225** (1967), 209–220.

[10] D. R. Heath-Brown, *Artin's conjecture for primitive roots.* Quart. J. Math. Oxford (2) **37** (1986), 27–38.

[11] P. Kurlberg and C. Pomerance, *On a problem of Arnold: the average multiplicative order of a given integer.* Algebra and Numb. Th. **7** (2013), 981–999.

[12] J. C. Lagarias and A. M. Odlyzko, *Effective versions of the Chebotarev density theorem.* Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975), pp. 409–464. Academic Press, London, 1977.

[13] S. Lang, Algebra, 2nd edition, Addison-Wesley, U.S.A., 1984.

[14] D. H. Lehmer and E. Lehmer, *Heuristics, anyone?.* Studies in Mathematical Analysis and Related Topics, Stanford Univ. Press (1962), 202–210.

[15] C. R. Matthews, *Counting points modulo p for some finitely generated subgroups of algebraic groups.* Bull. London Math. Soc. **14** (1982), 149–154.

[16] L. Menici, *Weights on reduction of groups of rational numbers.* To be submitted.

[17] L. Menici and C. Pehlivan, *Average r-rank Artin's conjecture.* To appear in Acta Arith.

[18] L. Menici and F. Pappalardi, *Densities related to subgroups of* $\mathbb{Q}^*$. In preparation.

[19] H. Montgomery, *Primes in arithmetic progressions.* Michigan Math. J. **17** (1970), 33–39.

[20] P. Moree, *Artin's primitive root conjecture -a survey-,* Integers **12A** (2012), A13, 100pp.

[21] P. Moree, *Asymptotically exact heuristics for (near) primitive roots.* J. Numb. Th. **83** (2000), 155–181.

[22] L. Murata. *A problem analogous to Artin's conjecture for primitive roots and its applications.* Arch. Math. (Basel) **57** (1991), no. 6, 555–565.

[23] Pappalardi, F., *On Hooley's theorem with weights.* Rend. Sem. Mat. Univ. Pol. Torino **53**, 4 (1995), 375-388.

[24] F. Pappalardi, *The r-rank Artin conjecture.* Math. Comp. **66** (1997), 853-868.

[25] F. Pappalardi *Divisibility of Reduction in Groups of Rational Numbers.* Math. Comp. **84**, 291 (2015), 385–407.

[26] F. Pappalardi and A. Susa, *An analogue of Artin's conjecture for multiplicative subgroups of the rationals.* Arc. der Math. **101**, 4 (2013), 319–330.

[27] C. Pehlivan *The average multiplicative order of a finitely generated subgroup of the rationals modulo primes.* To appear in Int. J. Numb. Th.

[28] J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers.* Illinois J. Math. **6** (1962), 64–94.

[29] A. Schinzel, *A refiniment of a Theorem of Gerst on power residues.* Acta Arith. **17** (1970), 161–168.

[30] J. P. Serre, *Quelques applications du théorème de densité de Chebotarev.* Inst. Hautes Études Sci. Publ. Math. No. 54 (1981), 323–401.

[31] P. J. Stephens, *An average result for Artin's conjecture.* Mathematika **16** (1969), 178–188.

[32] P. J. Stephens, *Prime divisors of second order linear recurrences. II.* J. Numb. Th. **8** (1976), 333–345.

[33] E. C. Titchmarsh, *A divisor problem.* Rend. Circ. Mat. Palermo **54** (1930), 414–429.

[34] A. Walfisz, *Zur additiven zahlentheorie II.* Mathematische Zeitschrift **40** (1936), 592–607.

[35] E. Weiss, *Algebraic Number Theory.* McGraw-Hill, New York (1963).