Università degli Studi Roma Tre

Scuola Dottorale in Scienze Matematiche e Fisiche

Sezione Matematica

XXVII ciclo

PhD Thesis in Mathematics

by

Cihan Pehlivan

Some average results connected with reductions of groups of rational numbers

Supervisor

Prof. Francesco Pappalardi

Coordinator

Prof. Luigi Chierchia

ACADEMIC YEAR 2014-2015

Contents

Abstract **ii**

Acknowledgements **iii**

Notations and Terminology **iv**

1 Introduction **1**

2 Average Multiplicative Order of Γ Over Primes **9**

2.1 Preliminary Definitions and Results 9

2.2 Proof of Theorem 1.4 14

2.3 Density Calculations 18

2.4 Numerical Examples 25

3 Average r-rank Artin Conjecture **28**

3.1 Introduction 28

3.2 Preliminary Definitions and Lemmas 29

3.3 Proof of Theorem 1.8 42

4 Codes **55**

Bibliography **58**

Abstract

Let $\Gamma \subset \mathbb{Q}^*$ be a finitely generated subgroup and let p be a prime number such that the reduction group Γ_p is a well defined subgroup of the multiplicative group $\mathbb{F}_p^*$. Firstly, given that $\Gamma \subseteq \mathbb{Q}^*$, assuming the Generalized Riemann Hypothesis, we determine an asymptotic formula for the average over prime numbers, powers of the order of the reduction group modulo p. The problem was previously considered by Pomerance and Kurlberg for the rank 1 case. When Γ contains only positive numbers, we are also able to give an explicit expression for the involved density in terms of an Euler product. The first part is concluded with some numerical computations. In the second part, for any $m \in \mathbb{N}$ we prove an asymptotic formula for the average of the number of primes $p \leq x$ for which the index $[\mathbb{F}_p^* : \Gamma_p] = m$. The average is performed over all finitely generated subgroups $\Gamma = \langle a_1, \ldots, a_r \rangle \subset \mathbb{Q}^*$, with $a_i \in \mathbb{Z}$ and $a_i \leq T_i$ with a range of uniformity: $T_i > \exp(4(\log x \log\log x)^{\frac{1}{2}})$ for every $i = 1, \ldots, r$. We also prove an asymptotic formula for the mean square of the error terms in the asymptotic formula with a similar range of uniformity. The case of rank 1 and $m = 1$ corresponds to the classical Artin conjecture for primitive roots and has already been considered by Stephens in 1969.

Acknowledgements

I wish to express my gratitude to my advisor Prof. Francesco Pappalardi for his enlightening advices and his constant encouragement. I would also like to thank Prof. Luigi Chierchia, and my colleagues Giulio Meleleo, Stefano Guarino, Flavio Lombardi, Antonio Cigliola, Lorenzo Menici, Fabio Felici for their warm welcome to the department, I always felt like home in the department during the years I lived in Rome. I would also like to thank my committee members, Prof. Peter Stevenhagen, Prof. Pieter Moree.

A special thanks goes to my mother, my grandfather and my whole family members for their love and support. I would like to express my appreciation to my beloved friends Remzi Ay, Betül Perçinel and Necdet Perçinel and Ayhan Dil, their support was priceless. I also would like to thank my sincere friend Ümit Işlak for his help during my career and his proofreading of my thesis.

In addition, I would like express my thanks to my M.Sc. advisor Asst. Prof. Özlem Beyarslan and my B.Sc. advisor Prof. Alövsat Müslümov for their support and encouragement. Also, I would like to thank to all my friends in Turkey, for their confidence and support during my career. Last but not least, many thanks to the Nesin Mathematics Village, where I had wonderful experiences with amazing people.

Notations and Terminology

- $\mathbb{Z}$ - The ring of integers
- $\mathbb{N}$ - $\{1, 2, ...\}$
- $\mathbb{Z}/p\mathbb{Z}$ - The ring of integers modulo prime number p
- $\mathbb{F}_p^*$ - Multiplicative group of the field of p elements
- $\langle a \rangle$ - Subgroup of $\mathbb{F}_p^*$ generated by a
- $\gcd(a, b)$ - Greatest common divisor of the integers $a, b \in \mathbb{Z}$
- $\text{lcm}[a, b]$ - Least common multiple of the integers $a, b \in \mathbb{Z}$
- $\ell_a(p)$ - Order of an element $a \in \mathbb{F}_p^*$
- $\omega(n)$ - Number of distinct prime factors of n
- $\delta(\eta)$ - The field discriminant of $\mathbb{Q}(\sqrt{\eta})$
- $\varphi(n)$ - Euler totient function
- $\tau(n)$ - Denotes the number of positive divisors of n
- $\sigma_t(n)$ - $\sum_{d|n} d^t$
- $\mu(n)$ - Möbius function
- $\text{rad}(n)$ - Product of distinct prime numbers dividing n
- p, q, ℓ - Denotes prime numbers

- $\prod_p, \prod_q, \prod_\ell$ - Denotes the product taken over prime numbers
- $J_t(k)$ - Jordan's totient function: $k^t \prod_{p|k} \left(1 - \frac{1}{p^t}\right)$
- $f(x) = O(g(x))$ or $f(x) \ll g(x)$ - There exists a positive real number C and a real number x_0 such that $|f(x)| \leq C|g(x)|$ for all $x > x_0$
- $f(x) \sim g(x)$ - $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$
- $f(x) \ll_\lambda g(x)$ - Denotes that the implied constant depends on a given parameter λ
- $f(x) = o(g(x))$ - $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 0$
- $\pi(x)$ - Denotes the number of primes up to a number x
- $\mathrm{Li}(x)$ - $\int_2^x \frac{dt}{\log t}$

Chapter 1

Introduction

In his classic work *Disquisitones Arithmeticae,* Carl F. Gauss questioned why the rational number $\frac{1}{7}$ has a period of length 6, whereas $\frac{1}{11}$ has a period of length 2. In the same work, he observed that for any prime number $p \neq 2, 5$, $\frac{1}{p}$ has the same period with the order of 10 mod p, and that the period of $\frac{1}{p}$ is long when 10 is a primitive root modulo p, where an integer a is said to be a primitive root modulo p if $\langle a \pmod p \rangle = \mathbb{F}_p^*$. With this observation, Gauss further questioned whether 10 would be a primitive root for infinitely many prime numbers.

Later on, in 1927, Artin conjectured that any non-zero integer $a \neq \pm 1$, which is not a perfect square, is a primitive root for infinitely many primes. Letting p be a prime number, and denoting the multiplicative order of an integer a modulo p by $\ell_a(p)$, we say that the integer a is primitive root modulo p if $\ell_a(p) = p - 1$. Also defining $N_a(x)$ as the number of primes up to x for which $\ell_a(p) = p - 1$, we may formulate Artin's initial conjecture as:

Conjecture 1.1. *Let a be a fixed integer such that $a \neq \pm 1, 0$ or a perfect square. Write $a = b^h$ where $b \in \mathbb{Z}$ is not a perfect power and $h \in \mathbb{N}$. Then*

$$N_a(x) \sim A_h \frac{x}{\log x}$$

as $x \to \infty$ *where*

$$A_h = \prod_{\substack{q|h \\ q \text{ prime}}} \left(1 - \frac{1}{q-1}\right) \prod_{\substack{q\nmid h \\ q \text{ prime}}} \left(1 - \frac{1}{q(q-1)}\right).$$

Let us now briefly discuss Artin's heuristic argument towards the conjecture. First note that a is primitive root modulo p if and only if $a^{\frac{p-1}{q}} \not\equiv 1$ modulo p for all prime divisor q of $p-1$. Equivalently, a is a primitive root mod p if and only if the following two conditions are not satisfied simultaneously

$$p \equiv 1 \pmod{q} \tag{1.1}$$

$$a^{\frac{p-1}{q}} \not\equiv 1 \pmod{p}. \tag{1.2}$$

Fixing a prime q, by Dirichlet's Theorem, the number of primes p, that satisfies the first condition has frequency

$$\frac{1}{q-1}.$$

Also, the number of primes p that satisfy the second condition (except integers a that are q-th powers) has frequency $\frac{1}{q}$. Now, assuming that the two conditions in (1.1) and (1.2) are independent, one would expect that the probability of these two events occurring simultaneously is $\frac{1}{q(q-1)}$. Since we would like to have neither of these occur for any prime q, the natural guess for the probability that a is primitive root (mod p) then would be

$$\prod_{q} \left(1 - \frac{1}{q(q-1)}\right),$$

which is known as the Artin constant.

In 1957, Derrick H. Lehmer discovered some deviations from the constant suggested by Artin, and after some correspondence between Artin and Lehmer (see [26]), Artin added a correction factor to his initial conjecture. In 1967, Hooley [9] proved that Artin's conjecture is true and that we may obtain an asymptotic formula for $N_a(x)$, under the additional assumption that GRH (Generalized Riemann Hypothesis) holds.

Theorem 1.2. *[9] Suppose* $a \in \mathbb{Z} \setminus \{\pm 1, 0\}$ *which is not a perfect square. If the GRH holds for*

the Dedekind zeta functions for the fields $\mathbb{Q}(\zeta_k, a^{1/k})$ *with* $k \in \mathbb{N}$ *square-free, and where* ζ_k *is a primitive* k*-th root of unity, then*

$$N_a(x) = A(a)\pi(x) + O\left(\frac{x \log\log x}{(\log x)^2}\right)$$

where $A(a)$ *is a constant depending on* a*.*

Several generalizations of Artin's conjecture have been studied by various authors during the subsequent years (for an exhaustive survey see [16]).

Until so far, the best unconditional result about Artin's conjecture is due to Heath-Brown [8], Gupta and Murty [6]: One of 2, 3, or 5 is a primitive root modulo p for infinitely many primes p.

Next, we focus on results on average multiplicative order of an integer a. In 2005, V. I. Arnold [1] conjectured that on average $\ell_a(n) \sim c(a)\frac{n}{\log n}$, where $c(a)$ is a positive constant depending on a. His heuristic argument was based on the physical principle of turbulence, and it was noted by Arnold that his reasoning was supported by billions of numerical experiments. Given co-prime integers a, n with $n > 0$ and $|a| > 0$, if we define the average multiplicative order of a by

$$T_a(x) := \frac{1}{x} \sum_{\substack{n \leq x \\ (a,n)=1}} \ell_a(n),$$

then the conjecture of Arnold can be stated as: If $|a| > 1$ then

$$T_a(x) \sim c(a)\frac{x}{\log x},$$

for some constant $c(a)$.
However, in 2007, Shparlinski [23] showed under the GRH, if $|a| > 1$,

$$T_a(x) \gg \frac{x}{\log x} \exp(c(a)(\log\log\log x)^{\frac{3}{2}}),$$

for some constant $c(a) > 0$.

In 2012, Pomerance and Kurlberg [10], sharpened Shparlinski's result to

$$T_a(x) = \frac{x}{\log x} \exp\left(\frac{B \log\log x}{\log\log\log x}(1 + o(1))\right)$$

as $x \to \infty$, uniformly in a with $1 < |a| \leq \log x$. The upper bound implicit in this result holds unconditionally.

Our main interest in this thesis will be on average results over prime numbers. In this direction, in 1976, Stephens [25] proved that, again under the GRH assumption, if a is an integer which is not a perfect h power for any $h \geq 2$, then

$$\sum_{p \leq x} \frac{\ell_a(p)}{p-1} = c_a \cdot \frac{x}{\log x} + O\left(\frac{x \log\log x}{\log^2 x}\right),$$

where c_a is a constant depend on a.

As another related result, Pomerance and Kurlberg prove the following theorem in their aforementioned paper [10].

Theorem 1.3. *[10] Assume the GRH holds. Then for any given rational $a \neq 0, \pm 1$*

$$\frac{1}{\pi(x)} \sum_{p \leq x} \ell_a(p) = \frac{1}{2} c_a \cdot x + O\left(\frac{x}{(\log x)^{2-4/\log\log\log x}}\right),$$

where

$$c_a := \sum_{k=1}^{\infty} \frac{\varphi(k)\,\mathrm{rad}(k)(-1)^{\omega(k)}}{k^2[\mathbb{Q}(\zeta_k, a^{1/k}) : \mathbb{Q}]},$$

and the series c_a converges absolutely.

Indeed, it is known that c_a is a rational multiple of $c = \prod_p (1 - \frac{p}{p^3-1})$, which is again a result of Pomerance and Kurlberg. To formulate this rigorously, we first need some further notation. Write $a = \pm(a_0)^h$ where h is a positive integer and $a_0 > 0$ is not an exact power of a rational number, and write $a_0 = a_1 a_2$ where a_1 is a square-free integer and a_2 is a rational number. Let $n = \mathrm{lcm}[2e+1; \delta(a_1)]$, for $a > 0$ and e be the 2-adic valuation $v_2(h)$. Also consider the multiplicative

function $f(k) = (-1)^{\omega(k)} \operatorname{rad}(k)(h,k)/k^3$, which for prime powers reduces to

$$f(p^j) = -p^{1-3j+\min(j,v_p(h))}.$$

Then defining

$$F(p,t) := \sum_{j=0}^{t-1} f(p^j), \qquad F(p) := \sum_{j=0}^{\infty} f(p^j),$$

the precise expression obtained for c_a, $a > 0$, obtained by Pomerance and Kurlberg in [10] is the following representation

$$c_a = c \prod_{p|h} \frac{F(p)}{1 - \frac{p}{p^3-1}} \left(1 + \prod_{p|n} \frac{F(p) - F(p, v_p(n))}{F(p)} \right). \tag{1.3}$$

In Chapter 2, we generalize the result of Pomerance and Kurlberg (see Theorem 1.3) to any finitely generated subgroup $\Gamma \subset \mathbb{Q}^*$ of $\mathbb{Q}^*$. This result is also submitted for publication [21].

Before stating our result rigorously, we need some other definitions. Let $\Gamma \subseteq \mathbb{Q}^*$ be a finitely generated multiplicative subgroup. The *support* of Γ is the (finite) set of prime numbers p for which the p–adic valuation $v_p(g) \neq 0$ for some $g \in \Gamma$. We denote this set by $\operatorname{Supp}\Gamma$ and define $\sigma_\Gamma = \prod_{p \in \operatorname{Supp}\Gamma} p$. For each prime number $p \nmid \sigma_\Gamma$, the reduction of Γ modulo p is well defined. That is,

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

If $\Gamma = \langle a_1, a_2, ..., a_r \rangle$ then we denote by $\Gamma^{\frac{1}{k}}$ the group generated by

$$\langle a_1^{\frac{1}{k}}, a_2^{\frac{1}{k}}, ..., a_r^{\frac{1}{k}} \rangle.$$

The following theorem is one of our main results in this thesis, and its proof will be included in Chapter 2.

Theorem 1.4. *Let $\Gamma \subseteq \mathbb{Q}^*$ be a finitely generated multiplicative subgroup with rank $r \geq 2$ and*

assume that the Generalized Riemann Hypothesis holds for $\mathbb{Q}(\zeta_k, \Gamma^{1/k})$, $k \in \mathbb{N}$. *Let*

$$C_{\Gamma,t} := \sum_{k\geq 1} \frac{J_t(k)(\mathrm{rad}(k))^t(-1)^{\omega(k)}}{k^{2t}[\mathbb{Q}(\zeta_k, \Gamma^{1/k}) : \mathbb{Q}]}. \tag{1.4}$$

Then the series $C_{\Gamma,t}$ *converges absolutely, and as* $x \to \infty$

$$\sum_{p\leq x} |\Gamma_p|^t = \mathrm{li}(x^{t+1}) \left(C_{\Gamma,t} + O_\Gamma\left(\frac{\log\log x}{(\log x)^r} \right) \right), \tag{1.5}$$

where the constant implied by the O_Γ*–symbol may depend on* Γ.

Moreover, again in Chapter 2, we give an explicit expression for the involved density in terms of an Euler product when Γ contains only positive numbers.

Let us next move to a discussion of Artin's conjecture without the GRH assumption for which we still do not have satisfactory results. Just one year after the work of Hooley, in 1968, Goldfeld [5] showed unconditionally that for each $D > 1$

$$N_a(x) = A \,\mathrm{li}\, x + O\left(\frac{x}{(\log x)^D} \right) \tag{1.6}$$

holds for all integers $a \leq N$ with at most $c_1 N^{\frac{9}{10}}(5\log x + 1)^{h+D+2}$ exceptions where $h = \frac{x}{\log N}$, A is Artin's constant, c_1 and constant of O-term are positive and depend on only D.

Later in 1969, Stephens [24] not only showed that in average the asymptotic formula 1.6 holds, but also making use of the normal order method of Turan, he proved that the number of exceptions is bounded by $O(N)$ when

$$N > \exp(6(\log x \log\log x)^{\frac{1}{2}})$$

and as N, x tends to infinity. The following theorems are again due to Stephens and they were used to prove his results just mentioned.

Theorem 1.5. *[24] If*

$$N > \exp(4(\log x \log\log x)^{\frac{1}{2}}),$$

then

$$\frac{1}{N}\sum_{a\leq N} N_a(x) = A\,\mathrm{li}\,x + O\left(\frac{x}{(\log x)^D}\right),$$

where A is Artin's constant, and the constant $D > 1$ is arbitrary.

Theorem 1.6. *[24] Let A be Artin's constant, and $E > 2$ be an arbitrary real number. Then for*

$$N > \exp(6(\log x \log\log x)^{\frac{1}{2}}),$$

we have

$$\frac{1}{N}\sum_{a\leq N} (N_a(x) - A\,\mathrm{li}\,x)^2 \ll \frac{x^2}{(\log x)^E}.$$

For any integer $|a| > 1$ which is not a perfect square, Artin's conjecture is about the number of primes which satisfy the relation $[F_p^* : \langle a \pmod p\rangle] = 1$. We can define a new counting function to enumerate the prime numbers which a generates a group of index $m \in \mathbb{N}$ in F_p^*,

$$N_a(x,m) = \#\{p \leq x : p \nmid a, [F_p^* : \langle a \pmod p\rangle] = m\}. \tag{1.7}$$

The following theorem was proven by Moree.

Theorem 1.7. *[17] Let m be an arbitrary positive integer. Then for $T > \exp(4(\log x \log\log x)^{1/2})$,*

we have

$$\frac{1}{T}\sum_{a\leq T} N_{a,m}(x) = \sum_{\substack{p\leq x \\ p\equiv 1 \pmod m}} \frac{\varphi((p-1)/m)}{p-1} + O\left(\frac{x}{(\log x)^E}\right) \tag{1.8}$$

for any constant $E > 2$.

In Chapter 3, we generalize the result of Moree given in Theorem 1.7 and the results of Stephens given in Theorems 1.5 and 1.6 to the r–rank case, which is part of a joint work with Lorenzo Menici [14]. Also, we prove an asymptotic formula for the average of the number of primes $p \leq x$ for which the index $[\mathbb{F}_p^* : \Gamma_p] = m$. The average is performed over all finitely generated subgroups $\Gamma =$

$\langle a_1, \ldots, a_r \rangle \subset \mathbb{Q}^*$, with $a_i \in \mathbb{Z}$ and $a_i \leq T_i$ with a range of uniformity: $T_i > \exp(4(\log x \log\log x)^{\frac{1}{2}})$ for every $i = 1, \ldots, r$. The main result of Chapter 3 is summarized in the following theorem.

Theorem 1.8. *Assume* $T^* := \min\{T_i : i = 1, \ldots, r\} > \exp(4(\log x \log\log x)^{\frac{1}{2}})$ *and* $m \leq (\log x)^D$ *for an arbitrary positive constant* D*. Then*

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

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

Furthermore, if $T^* > \exp(6(\log x \log\log x)^{\frac{1}{2}})$*, then*

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

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

Chapter 2

Average Multiplicative Order of Γ Over Primes

2.1 Preliminary Definitions and Results

We denote by $\mathbb{Q}(\zeta_k, \Gamma^{1/k})$ the extension of the cyclotomic field $\mathbb{Q}(\zeta_k)$ obtained by adding the k–th roots of all the elements in Γ. $\mathbb{Q}(\zeta_k, \Gamma^{1/k})$ is a finite Galois extension of $\mathbb{Q}$ and it is well known that

$$|\operatorname{Gal}(\mathbb{Q}(\zeta_k, \Gamma^{1/k})/Q(\zeta_k))| = |\Gamma(\mathbb{Q}(\zeta_k)^*)/\mathbb{Q}(\zeta_k)^*|.$$

For details on the Theory of Kummer's extensions see [12, Theorem 8.1]. If $\eta \in \mathbb{Q}^*$, by $\delta(\eta)$ we denote the *field discriminant* of $\mathbb{Q}(\sqrt{\eta})$. So, if $\eta \in \mathbb{Z}$ is square-free, $\delta(\eta) = \eta$ if $\eta = 1 \mod (4)$ and $\delta(\eta) = 4\eta$ otherwise. For any $k \in \mathbb{N}^+$,

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

For any square-free integer η, let

$$t_\eta = \begin{cases} \infty & \text{if for all } t \geq 0,\ \eta^{2^t}\mathbb{Q}^{*2^{t+1}} \notin \Gamma(2^{t+1}) \\ \min\{t \in \mathbb{N} : \eta^{2^t}\mathbb{Q}^{*2^{t+1}} \in \Gamma(2^{t+1})\} & \text{otherwise.} \end{cases} \tag{2.1}$$

We define the index of subgroup $\text{ind}(\Gamma_p) = \frac{p-1}{|\Gamma_p|}$. Let Γ be a finitely generated subgroup of $\mathbb{Q}^*$ of rank r and let $(a_1, ..., a_r)$ be a $\mathbb{Z}-$basis of Γ. We write $\text{Supp}(\Gamma) = \{p_1, ..., p_s\}$. Then we can construct the $s \times r-$matrix with coefficients in $\mathbb{Z}$:

$$M(a_1, ..., a_r) = A = \begin{pmatrix} \alpha_{1,1} & ... & \alpha_{1,r} \\ \vdots & & \vdots \\ \alpha_{s,1} & ... & \alpha_{s,r} \end{pmatrix}$$

defined by the property that $|a_i| = (p_1)^{\alpha_{1,i}}...(p_s)^{\alpha_{s,i}}$. It is clear that the rank of $M(a_1, ..., a_r)$ equals r. For all $i = 1, ..., r$ we define the $i-$th exponent of Γ by

$$\Delta_i = \Delta_i(\Gamma) = gcd(\text{ det } A : A \text{ is an } i \times i \text{ minor of } M(a_1, ..., a_r)).$$

For $m \in \mathbb{N}$, we have (see [3, Proposition 2])

$$|\Gamma(m)| = \frac{\varepsilon_{m,\Gamma} \times m^r}{gcd(m^r, m^{r-1}\Delta_1, ..., m\Delta_{r-1}, \Delta_r)}$$

where

$$\varepsilon_{m,\Gamma} = \begin{cases} 1 & \text{if } m \text{ is odd or if } -1 \notin \Gamma(\mathbb{Q}^*)^m \\ 2 & \text{if } m \text{ is even and if } -1 \in \Gamma(\mathbb{Q}^*)^m. \end{cases} \tag{2.2}$$

Then for every prime power p^α, we have (see [8])

$$|\Gamma(p^\alpha)| = p^{\max\{0, \alpha - v_p(\Delta_1), ..., (r-1)\alpha - v_p(\Delta_{r-1}), r\alpha - v_p(\Delta_r)\}}. \tag{2.3}$$

Proposition 2.1. *Let $g \in \mathbb{Q}^+ \setminus \{1\}$ and we write $g = (g_0)^h$ where h is a positive integer and g_0 is*

not a perfect power and let $g_0 = g_1 g_2^2$ *where* g_1 *is square free, then we have* $t_{g_1} = v_2(h)$ *and* $t_\eta = \infty$ *if* $\eta \neq g_1$.

Proof. Let $m = v_2(h)$ then,

$$|\Gamma(2^{t+1})| = 2^{t+1-\min(t+1,m)}.$$

The condition $\eta^{2^t}\mathbb{Q}^{*2^{t+1}} \in \Gamma(2^{t+1})$ is satisfied if the group $\Gamma(2^{t+1})$ has an element of order 2. It could happen if $t \geq m$, and in this case, the only element in $\Gamma(2^{t+1})$ of order 2 is $(g_1)^{2^t}\mathbb{Q}^{*2^{t+1}}$. So, $t_{g_1} = m = v_2(h)$ and $t_\eta = \infty$ for all other values of η. Note that t_η is defined if η is square-free.

□

The following statement is obtained using the effective version of the Chebotarev Density Theorem due to Serre (see [22, Theorem 4]).

Lemma 2.2. *[Chebotarev Density Theorem] Let* $\Gamma \subset \mathbb{Q}^*$ *be a finitely generated subgroup of rank* r *and* $k \in \mathbb{N}^+$. *The GRH for the Dedekind zeta function of* $\mathbb{Q}(\zeta_k, \Gamma^{1/k})$ *implies that*

$$\#\left\{p \leq x : p \notin \operatorname{Supp}\Gamma,\ k \mid \operatorname{ind}(\Gamma_p)\right\} = \frac{\operatorname{li}(x)}{\left[\mathbb{Q}(\zeta_k, \Gamma^{1/k}) : \mathbb{Q}\right]} + O\big(\sqrt{x}\log(xk^{r+1}\sigma_\Gamma)\big). \tag{2.4}$$

The following Lemma describes explicitly the degree of $[\mathbb{Q}(\zeta_k, \Gamma^{1/k}) : \mathbb{Q}]$ (see [19, Lemma 1 and Corollary 1]).

Lemma 2.3. *Let* $k \geq 1$ *be an integer. With the notation above, we have*

$$\left[\mathbb{Q}(\zeta_k, \Gamma^{1/k}) : \mathbb{Q}(\zeta_k)\right] = |\Gamma(k)|/|\widetilde{\Gamma}(k)|,$$

where

$$\widetilde{\Gamma}(k) = (\Gamma \cap \mathbb{Q}(\zeta_k)^{2^{v_2(k)}}) \cdot \mathbb{Q}^{*2^{v_2(k)}}/\mathbb{Q}^{*2^{v_2(k)}}.$$

Furthermore, in the special case when $\Gamma \subset \mathbb{Q}^+$,

$$\widetilde{\Gamma}(k) = \{\eta \mid \sigma_\Gamma, \eta^{2^{v_2(k)-1}} \mathbb{Q}^{*2^{v_2(k)}} \in \Gamma(2^{v_2(k)}),\ \delta(\eta) \mid k\}.$$

The next results follows from Lemma 2.3, see also [19, Equation 7].

Corollary 2.4. *Let* $\Gamma \subset \mathbb{Q}^*$ *be a subgroup with* $r = \mathrm{rank}_{\mathbb{Z}}(\Gamma)$ *and let* $k \in \mathbb{N}$. *Then*

$$2k^r \geq [\mathbb{Q}(\zeta_k, \Gamma^{1/k}) : \mathbb{Q}(\zeta_k)] \geq \frac{(k/2)^r}{\Delta_r(\Gamma)}. \tag{2.5}$$

Next Lemma is implicit in the work of C. R. Matthews (see [13]).

Lemma 2.5. *Assume that* $\Gamma \subseteq \mathbb{Q}^*$ *is a multiplicative subgroup of rank* $r \geq 2$ *and assume that* $(a_1, \ldots, a_r)$ *is a* $\mathbb{Z}$*–basis of* Γ. *Let* $t \in \mathbb{R}$, $t > 1$. *We have the following estimate*

$$\#\{p \notin \mathrm{Supp}\,\Gamma : |\Gamma_p| \leq t\} \ll_\Gamma \frac{t^{1+1/r}}{\log t}. \tag{2.6}$$

Theorem 2.6. *Assume the GRH. Let* Γ *be a multiplicative subgroup of* $\mathbb{Q}^*$ *of rank* $r \geq 2$. *Then for* $1 \leq L \leq \log x$, *we have*

$$\#\left\{p \leq x : p \notin \mathrm{Supp}\,\Gamma, |\Gamma_p| \leq \frac{p-1}{L}\right\} \ll_\Gamma \frac{\pi(x)}{L^r}. \tag{2.7}$$

The proof of the above is routine and easier than the main theorem in [9] and the one in [1, Theorem 6]. Hence, we will skip some of the details.

Proof. Let t, $L \leq t \leq x$, be a parameter that will be chosen later.

- *first step*: First consider primes $p \notin \operatorname{Supp}\Gamma$ such that $|\Gamma_p| \leq \frac{p-1}{t}$. By Lemma 2.5, we have

$$\#\left\{p \notin \operatorname{Supp}\Gamma : |\Gamma_p| \leq \frac{x}{t}\right\} \ll_\Gamma \frac{(x/t)^{1+1/r}}{\log(x/t)}. \tag{2.8}$$

- *second step*: Next consider the primes $p \notin \operatorname{Supp}\Gamma$ such that there exists a prime q, $L \leq q \leq t$ such that $q \mid \operatorname{ind}(\Gamma_p) = \frac{p-1}{|\Gamma_p|}$. If we apply Lemma 2.2, we obtain

$$\begin{aligned}\#\{p \leq x : p \notin \operatorname{Supp}\Gamma, q \mid \operatorname{ind}(\Gamma_p)\} &= \frac{\operatorname{li}(x)}{\left[\mathbb{Q}(\zeta_q, \Gamma^{1/q}) : \mathbb{Q}\right]} + O_\Gamma\left(\sqrt{x}\log(xq)\right) \\ &\ll_\Gamma \frac{\pi(x)}{q^r\varphi(q)} + \sqrt{x}\log(xq) \end{aligned} \tag{2.9}$$

where in the latter estimate we have applied Corollary 2.4. If we sum the above over primes q: $L \leq q \leq t$, we obtain

$$\begin{aligned}\#\{p \leq x : p \notin \operatorname{Supp}\Gamma, \exists q \mid \operatorname{ind}(\Gamma_p), L \leq q \leq t\} &\ll_\Gamma \sum_{\substack{q \text{ prime} \\ L \leq q \leq t}} \left(\frac{\pi(x)}{q^r\varphi(q)} + \sqrt{x}\log(xq)\right) \\ &\ll_\Gamma \frac{\pi(x)}{L^r} + x^{1/2}t\log x. \end{aligned} \tag{2.10}$$

- *third step*: The primes p that were not counted in previous steps, have the property that all the prime divisors of $\operatorname{ind}(\Gamma_p)$ belong to the interval $[1, L]$. Hence, for such primes p, $\operatorname{ind}(\Gamma_p)$ is divisible for some integer d in $[L, L^2]$.

  Applying again Lemma 2.2 and Corollary 2.4, and taking the sum over d we deduce that the total number of such primes is

$$\ll_\Gamma \sum_{\substack{d \in \mathbb{N} \\ L < d \leq L^2}} \left(\frac{\pi(x)}{d^r\varphi(d)} + x^{\frac{1}{2}}\log(xd)\right) \ll_\Gamma \frac{\pi(x)}{L^r} + x^{1/2}L^2\log x. \tag{2.11}$$

A choice of $t = \frac{x^{1/2}}{L^r \log^2 x}$ allows us to conclude the proof. □

The Theorem of Wirsing [28] is formulated as follows.

Lemma 2.7. *Assume that a real valued multiplicative function $h(n)$ satisfies the following conditions.*

- $h(n) \geq 0, n = 1, 2, ..;$
- $h(p^n) \leq c_1 {c_2}^n, n = 2, 3...,$ *for some constants* c_1, c_2 *with* $c_2 < 2;$
- *there exists a constant* $\tau > 0$ *such that*

$$\sum_{p \leq x} h(p) = (\tau + o(1)) \frac{x}{\log x}. \tag{2.12}$$

Then for any $x \geq 0$,

$$\sum_{n \leq x} h(n) = \left(\frac{1}{e^{\gamma\tau}\Gamma(\tau)} + o(1) \right) \frac{x}{\log x} \prod_{p \leq x} \sum_{\nu \geq 0} \frac{h(p^\nu)}{p^\nu} \tag{2.13}$$

where γ *is the Euler constant, and*

$$\Gamma(s) = \int_0^\infty e^{-t} t^{s-1} dt \tag{2.14}$$

is the gamma function.

2.2 Proof of Theorem 1.4

The proof use the methods of Kurlberg and Pomerance [1, Theorem 2].

Proof of Theorem 1.4. Let $z = \log x$. We have

$$\sum_{p\le x} |\Gamma_p|^t = \sum_{\substack{p\le x\\ \mathrm{ind}(\Gamma_p)\le z}} |\Gamma_p|^t + \sum_{\substack{p\le x\\ \mathrm{ind}(\Gamma_p)> z}} |\Gamma_p|^t = A + E.$$

We write $|\Gamma_p|^t = \frac{(p-1)^t}{\mathrm{ind}^t(\Gamma_p)}$ and use the identity $\frac{1}{\mathrm{ind}^t(\Gamma_p)} = \sum_{uv|\,\mathrm{ind}(\Gamma_p)} \frac{\mu(v)}{u^t}$, after splitting the sum we have

$$\begin{aligned} A &= \sum_{\substack{p\le x\\ \mathrm{ind}(\Gamma_p)\le z}} (p-1)^t \sum_{uv|\,\mathrm{ind}(\Gamma_p)} \frac{\mu(v)}{u^t} \\ &= \sum_{p\le x} (p-1)^t \sum_{\substack{uv|\,\mathrm{ind}(\Gamma_p)\\ uv\le z}} \frac{\mu(v)}{u^t} - \sum_{\substack{p\le x\\ \mathrm{ind}(\Gamma_p)> z}} (p-1)^t \sum_{\substack{uv|\,\mathrm{ind}(\Gamma_p)\\ uv\le z}} \frac{\mu(v)}{u^t} \\ &= A_1 - E_1. \end{aligned}$$

The main term A_1 is

$$A_1 = \sum_{uv\le z} \frac{\mu(v)}{u^t} \sum_{\substack{uv|\mathrm{ind}(\Gamma_p)\\ p\le x}} (p-1)^t.$$

Applying partial summation and using Lemma 2.2 on GRH, we can write the inner some as

$$\frac{\mathrm{li}(x^{t+1})}{[\mathbb{Q}(\zeta_{uv}, \Gamma^{1/uv}) : \mathbb{Q}]} + O\Big(x^{t+\frac{1}{2}} \log x\Big).$$

Then it follows,

$$A_1 = \mathrm{li}(x^{t+1}) \sum_{uv\le z} \frac{\mu(v)}{u^t[\mathbb{Q}(\zeta_{uv}, \Gamma^{1/uv}) : \mathbb{Q}]} + O\left(x^{t+\frac{1}{2}} \log x \sum_{n\le z} \left| \sum_{uv=n} \frac{\mu(v)}{u^t} \right| \right).$$

The inner sum in the O-term is bounded by $\frac{\varphi(n)}{n}$ so that the O-term above is $O\Big(x^{t+\frac{1}{2}} \log^2(x)\Big)$.

Next we use the elementary fact $J_t(\mathrm{rad}(k)) = J_t(k)\left(\frac{\mathrm{rad}(k)}{k}\right)^t$ and $\sum_{v|k}\mu(v)v^t = \prod_{p|k}(1-p^t) = (-1)^{\omega(k)}J_t(\mathrm{rad}(k)) = (-1)^{\omega(k)}\frac{J_t(k)(\mathrm{rad}(k))^t}{k^t}$. So

$$\sum_{uv=k}\frac{\mu(v)}{u^t[\mathbb{Q}(\zeta_{uv},\Gamma^{1/uv}):\mathbb{Q}]} = \sum_{v|k}\frac{\mu(v)v^t}{k^t[\mathbb{Q}(\zeta_k,\Gamma^{1/k}):\mathbb{Q}]} = \frac{(-1)^{\omega(k)}J_t(k)(\mathrm{rad}(k))^t}{k^{2t}[\mathbb{Q}(\zeta_k,\Gamma^{1/k}):\mathbb{Q}])}.$$

Let $C_{\Gamma,t} := \sum_{k\geq 1}\frac{J_t(k)(\mathrm{rad}(k))^t(-1)^{\omega(k)}}{k^{2t}[\mathbb{Q}(\zeta_k,\Gamma^{1/k}):\mathbb{Q}]}$, then we have

$$\sum_{uv\leq z}\frac{\mu(v)}{u^t[\mathbb{Q}(\zeta_{uv},\Gamma^{1/uv}):\mathbb{Q}]} = C_{\Gamma,t} - \sum_{k>z}\frac{J_t(k)(\mathrm{rad}(k))^t(-1)^{\omega(k)}}{k^{2t}[\mathbb{Q}(\zeta_k,\Gamma^{1/k}):\mathbb{Q}]}.$$

Since $[\mathbb{Q}(\zeta_k,\Gamma^{1/k}):\mathbb{Q}] = [\mathbb{Q}(\zeta_k,\Gamma^{1/k}):\mathbb{Q}(\zeta_k)]\varphi(k)$, if we use Corollary 2.4, we have

$$\frac{J_t(k)(\mathrm{rad}(k))^t(-1)^{\omega(k)}}{k^{2t}[\mathbb{Q}(\zeta_k,\Gamma^{1/k}):\mathbb{Q}]} \ll \frac{(\mathrm{rad}(k))^t}{k^{t+1}k^r}.$$

Finally, we have

$$A_1 = \mathrm{li}(x^{t+1})\left(C_{\Gamma,t} + O\left(\frac{1}{z^r}\right)\right).$$

It remains to estimate the error terms E and E_1. Applying Theorem 2.6:

$$E \ll \frac{x^t}{z^t}\frac{\pi(x)}{z^r}.$$

In order to estimate E_1, we calculate

$$\left|\sum_{\substack{uv|n\\ uv\leq z}}\frac{\mu(v)}{u^t}\right| \leq \sum_{u|n}\frac{1}{u^t}\sum_{\substack{v|n\\ v\leq z}}1 \leq \frac{\tau(n)\sigma_t(n)}{n^t}$$

so

$$E_1 \leq \sum_{n>z} \frac{\tau(n)\sigma_t(n)}{n^t} \sum_{\substack{p\leq x \\ n|\mathrm{ind}(\Gamma_p)}} (p-1)^t.$$

Then applying Lemma 2.2 and Corollary 2.4 we obtain that

$$E_1 \quad \ll \quad x^t\pi(x)\sum_{n>z}\frac{\tau(n)\sigma_t(n)}{n^t\varphi(n)n^r}.$$

Let $g(n) := \frac{\tau(n)\sigma_t(n)}{n^{t-1}\varphi(n)}$, $\sum_{p\leq x} g(p) = (2+o(1))\frac{x}{\log x}$. Using Lemma 2.7(in our case τ is 2), we have

$$\sum_{n\leq x} g(n) \quad = \quad \left(\frac{1}{e^{\gamma 2}}+o(1)\right)\frac{x}{\log x}\prod_{p\leq x}\left(1+\frac{p}{(p-1)(p^t-1)}\sum_{\nu\geq 1}\frac{(\nu+1)(p^{\nu t+t}-1)}{p^{\nu t+\nu}}\right).$$

To make the product convergent we add a correction factor, and invoke Merten's third formula, we have

$$\sum_{n\leq x} g(n) \sim \quad x\log x.$$

Let $G(n) := \sum_{n\leq x} g(n)$ using partial summation, we have

$$\sum_{n>z}\frac{g(n)}{n^{r+1}} = \lim_{T\to\infty}\left(\frac{G(T)}{T^{r+1}}-\frac{G(z)}{z^{r+1}}\right) - \int_z^\infty G(u)\frac{d}{du}\left(\frac{1}{u^{r+1}}\right) \ll \frac{\log z}{z^r}.$$

Therefore, we obtain

$$E_1 \ll x^t\pi(x)\frac{\log z}{z^r}.$$

We have chosen $z = \log x$, finally we have

$$\sum_{p \le x} |\Gamma_p|^t = \mathrm{li}(x^{t+1}) C_{\Gamma,t} + O\left(\frac{x^{t+1} \log\log x}{(\log x)^{r+1}}\right).$$

□

2.3 Density Calculations

Further on, for the case $t = 1$ we use C_Γ instead of $C_{\Gamma,1}$. Kurlberg and Pomerance in [1] consider the case when $\Gamma = \langle g \rangle$ has rank 1. In the special case when $\Gamma \subset \mathbb{Q}^+$, we express the value of C_Γ as an Euler product.

Theorem 2.8. *Assume that Γ is a finitely generated subgroup of $\mathbb{Q}^+$. Then*

$$\begin{aligned} C_{\Gamma,t} \quad &= \prod_p \left(1 - \sum_{\alpha \ge 1} \frac{p^t - 1}{p^{\alpha(t+1)-1} |\Gamma(p^\alpha)| (p-1)}\right) \\ &\times \left(1 + \sum_{\substack{\eta \mid \sigma_\Gamma \\ \eta \ne 1}} S_\eta \prod_{p \mid 2\eta} \left(1 - \left(\sum_{\alpha \ge 1} \frac{p^t - 1}{p^{\alpha(t+1)-1} |\Gamma(p^\alpha)| (p-1)}\right)^{-1}\right)^{-1}\right) \end{aligned} \tag{2.15}$$

where

$$S_\eta = \frac{\displaystyle\sum_{\alpha \ge \gamma_\eta} \frac{2^t - 1}{2^{\alpha(t+1)-1} |\Gamma(2^\alpha)|}}{\displaystyle\sum_{\alpha \ge 1} \frac{2^t - 1}{2^{\alpha(t+1)-1} |\Gamma(2^\alpha)|}} \tag{2.16}$$

and $\gamma_\eta = \max\{1 + t_\eta, v_2(\delta(\eta))\}$.

Proof of Theorem 2.8. We start by splitting the sum $C_{\Gamma,t}$ as

$$C_{\Gamma,t} := \sum_{k \ge 1} \frac{J_t(k) (\mathrm{rad}(k))^t (-1)^{\omega(k)}}{k^{2t} [\mathbb{Q}(\zeta_k, \Gamma^{1/k}) : \mathbb{Q}]} = A_1 + A_2. \tag{2.17}$$

where A_1 is the sum of the terms corresponding to odd values of k and A_2 is the sum of the terms corresponding to even values of k. Note that if $\Gamma \subseteq \mathbb{Q}^+$ by Lemma 2.3, we have

$$[\mathbb{Q}(\zeta_k, \Gamma^{1/k}) : \mathbb{Q}] = \frac{\varphi(k)|\Gamma(k)|}{|\widetilde{\Gamma}(k)|} \tag{2.18}$$

and if k is even,

$$\widetilde{\Gamma}(k) = \{\eta \mid \sigma_\Gamma, \eta^{2^{v_2(k)-1}}\mathbb{Q}^{*2^{v_2(k)}} \in \Gamma(2^{v_2(k)}),\ \delta(\eta) \mid k\} \tag{2.19}$$

while if k is odd $\widetilde{\Gamma}(k) = \{1\}$. We define

$$f_t(k) = \frac{J_t(k)(\mathrm{rad}(k))^t(-1)^{\omega(k)}}{k^{2t}\varphi(k)|\Gamma(k)|}.$$

Note that if $D \in \mathbb{N}^+$ is even, since $f_t(k)$ is multiplicative in k, then

$$\sum_{\substack{k\geq 1\\ \gcd(k,D)=1}} f_t(k) = \prod_{p\nmid D}\left(1 + \sum_{\alpha\geq 1} f_t(p^\alpha)\right) = \prod_{p\nmid D}\left(1 - \sum_{\alpha\geq 1}\frac{p^t-1}{p^{\alpha(t+1)-1}|\Gamma(p^\alpha)|(p-1)}\right). \tag{2.20}$$

Therefore, we have the identity

$$A_1 := \prod_{p>2}\left(1 + \sum_{\alpha\geq 1} f_t(p^\alpha)\right) = \prod_{p>2}\left(1 - \sum_{\alpha\geq 1}\frac{p^t-1}{p^{\alpha(t+1)-1}|\Gamma(p^\alpha)|(p-1)}\right). \tag{2.21}$$

We can write A_2 as,

$$\begin{aligned} A_2 &= \sum_{\eta|\sigma_\Gamma} \sum_{\substack{k\geq 1,2|k \\ \widetilde{\Gamma}(k)\ni\eta}} \frac{J_t(k)(\mathrm{rad}(k))^t(-1)^{\omega(k)}}{k^{2t}\varphi(k)|\Gamma(k)|} \\ &= \sum_{\eta|\sigma_\Gamma} \sum_{\substack{\alpha\geq 1 \\ \eta^{2^{\alpha-1}}\mathbb{Q}^{*2^\alpha}\in\Gamma(2^\alpha)}} \sum_{\substack{k\geq 1 \\ v_2(k)=\alpha \\ \delta(\eta)|k}} f_t(k) \\ &= \sum_{\eta|\sigma_\Gamma} \sum_{\substack{\alpha\geq 1 \\ \eta^{2^{\alpha-1}}\mathbb{Q}^{*2^\alpha}\in\Gamma(2^\alpha) \\ \alpha\geq v_2(\delta(\eta))}} \frac{-(2^t-1)}{2^{\alpha(t+1)-1}|\Gamma(2^\alpha)|} \sum_{\substack{k\geq 1 \\ 2\nmid k \\ \delta(\eta)|8k}} f_t(k). \end{aligned} \tag{2.22}$$

Now write $\delta(\eta) = 2^{v_2(\delta(\eta))}M$. Then

$$\begin{aligned} \sum_{\substack{k\geq 1 \\ 2\nmid k \\ \delta(\eta)|8k}} f_t(k) &= \prod_{\substack{p>2 \\ p\nmid M}} \left(1+\sum_{\alpha\geq 1} f_t(p^\alpha)\right) \prod_{\substack{p>2 \\ p|M}} \left(\sum_{\alpha\geq 1} f_t(p^\alpha)\right) \\ &= A_1 \prod_{\substack{p>2 \\ p|M}} \left(\left(1+\sum_{\alpha\geq 1} f_t(p^\alpha)\right)^{-1} \left(\sum_{\alpha\geq 1} f_t(p^\alpha)\right)\right). \end{aligned} \tag{2.23}$$

Hence, if t_η is the quantity defined in (2.1), then

$$C_{\Gamma,t} := A_1 \times \left(1+\sum_{\eta|\sigma_\Gamma} \sum_{\substack{\alpha\geq 1 \\ \alpha\geq t_\eta+1 \\ \alpha\geq v_2(\delta(\eta))}} \frac{-(2^t-1)}{2^{\alpha(t+1)-1}|\Gamma(2^\alpha)|} \prod_{\substack{p>2 \\ p|M}} \left(1+\left(\sum_{\alpha\geq 1} f_t(p^\alpha)\right)^{-1}\right)^{-1}\right).$$

Now let

$$\delta_\Gamma := \prod_{p \text{ prime}} \left(1+\sum_{\alpha\geq 1} f_t(p^\alpha)\right) = \prod_{p \text{ prime}} \left(1-\sum_{\alpha\geq 1} \frac{p^t-1}{p^{\alpha(t+1)-1}|\Gamma(p^\alpha)|(p-1)}\right)$$

and deduce that

$$C_{\Gamma,t} = \delta_\Gamma \left(1 + \sum_{\substack{\eta | \sigma_\Gamma \\ \eta \neq 1}} \frac{\displaystyle\sum_{\alpha \geq \gamma_\eta} \frac{2^t - 1}{2^{\alpha(t+1)-1} |\Gamma(2^\alpha)|}}{\displaystyle\sum_{\alpha \geq 1} \frac{2^t - 1}{2^{\alpha(t+1)-1} |\Gamma(2^\alpha)|}} \prod_{p | 2\eta} \left(1 + \left(\sum_{\alpha \geq 1} f_t(p^\alpha) \right)^{-1} \right)^{-1} \right)$$

where $\gamma_\eta = \max\{1 + t_\eta, v_2(\delta(\eta))\}$ and this completes the proof. □

In the special case when Γ consists of prime numbers and $t = 1$, the above formula can be considerably simplified:

Corollary 2.9. *Let $\Gamma = \langle p_1, \ldots, p_r \rangle$ where all the p_i's are prime numbers and $r \geq 1$, with the notation above, we have*

$$\begin{aligned} C_{\langle p_1, \ldots, p_r \rangle} &= \prod_p \left(1 - \frac{p}{p^{r+2} - 1} \right) \\ &\quad \times \left(1 + \sum_{\substack{\eta | p_1 \cdots p_r \\ \eta \neq 1}} \frac{1}{2^{\max\{0, v_2(\delta(\eta)/2)\}(r+2)}} \prod_{\ell | 2\eta} \frac{\ell}{\ell + 1 - \ell^{r+2}} \right). \end{aligned} \tag{2.24}$$

The quantity

$$C_r = \prod_p \left(1 - \frac{p}{p^{r+2} - 1} \right) \tag{2.25}$$

can be computed with arbitrary precision:

r	C_r
1	$0.57595996889294543964316337549249669251\cdots$
2	$0.82357659279814332395380438513901050177\cdots$
3	$0.92190332088740008067545348360869076931\cdots$
4	$0.96388805107176946676374437726734997946\cdots$
5	$0.98282912014687261524345691713313004185\cdots$
6	$0.99168916383630008819101294319807859837\cdots$
7	$0.99593155027181927318700546733612700362\cdots$
8	$0.99799372275691129752727433560285572887\cdots$
9	$0.99900593591154969071253065973483263501\cdots$
10	$0.99950593624928276115384423618416539651\cdots$

Table 2.1: Approximated values of some of the C_r's.

Proof of Corollary 2.9. Let Γ be generated by prime numbers $p_1, ..., p_r$, since Δ_i's are 1 we have $|\Gamma(k)| = k^r$ and $t_\eta = 0$ for all $\eta \mid \sigma_\Gamma = p_1 \cdots p_r$ and

$$\gamma_\eta = \begin{cases} 1 & \text{if } \eta \equiv 1 \bmod 4 \\ 2 & \text{if } \eta \equiv 3 \bmod 4 \\ 3 & \text{if } \eta \equiv 2 \bmod 4. \end{cases}$$

Furthermore,

$$\sum_{\alpha \geq \gamma_\eta} \frac{1}{2^{2\alpha-1}|\Gamma(2^\alpha)|} = \frac{1}{2^{(\gamma_\eta - 1)(r+2)}} \sum_{\alpha \geq 1} \frac{1}{2^{2\alpha-1}|\Gamma(2^\alpha)|}$$

and since $|\Gamma(k)| = k^r$ for all $k \in \mathbb{N}^+$, we have that

$$\sum_{\alpha \geq 1} \frac{1}{p^{2\alpha-1}|\Gamma(p^\alpha)|} = \frac{p}{p^{r+2}-1}.$$

Hence, if we let

$$C_r = \prod_p \left(1 - \frac{p}{p^{r+2}-1}\right)$$

then

$$C_{\langle p_1,\ldots,p_r\rangle} = C_r \left(1 + \sum_{\substack{\eta \mid p_1 \cdots p_r \\ \eta \neq 1}} \frac{1}{2^{(\gamma_\eta - 1)(r+2)}} \prod_{\ell \mid 2\eta} \frac{\ell}{\ell + 1 - \ell^{r+2}} \right)$$

and this completes the proof. □

Furthermore, we have the following Corollary.

Corollary 2.10. *Let Γ be a finitely generated subgroup of $\mathbb{Q}^+$ with rank r. Then C_Γ is a non zero rational multiple of C_r.*

Proof of Corollary 2.10. If we set $k_p = \max\{v_p(\Delta_r/\Delta_{r-1}), \cdots, v_p(\Delta_1/\Delta_0)\}$ then for $\alpha \geq k_p$, $|\Gamma(p^\alpha)| = p^{r\alpha - v_p(\Delta_r)}$. Hence

$$\sum_{\alpha \geq 1} \frac{1}{p^{2\alpha-1}|\Gamma(p^\alpha)|} = \sum_{\alpha=1}^{k_p} \frac{1}{p^{2\alpha-1}|\Gamma(p^\alpha)|} + \frac{p^{v_p(\Delta_r)+1-(r+2)k_p}}{p^{r+2}-1} \in \mathbb{Q}.$$

In particular, if $p \nmid \Delta_r$, then $k_p = 0$ and $|\Gamma(p^\alpha)| = p^{\alpha r}$ for all $\alpha \geq 0$ and

$$\sum_{\alpha \geq 1} \frac{1}{p^{2\alpha-1}|\Gamma(p^\alpha)|} = \frac{p}{p^{r+2}-1}.$$

Therefore

$$C_\Gamma = r_\Gamma \prod_{p \nmid \Delta_r} \left(1 - \frac{p}{p^{r+2}-1} \right)$$

where

$$\begin{aligned} r_\Gamma \quad &= \prod_{p \mid \Delta_r} \left(1 - \sum_{\alpha \geq 1} \frac{1}{p^{2\alpha-1}|\Gamma(p^\alpha)|} \right) \\ &\quad \times \left(1 + \sum_{\substack{\eta \mid \sigma_\Gamma \\ \eta \neq 1}} S_\eta \prod_{p \mid 2\eta} \left(1 - \left(\sum_{\alpha \geq 1} \frac{1}{p^{2\alpha-1}|\Gamma(p^\alpha)|} \right)^{-1} \right)^{-1} \right) \in \mathbb{Q}. \end{aligned} \tag{2.26}$$

Finally C_Γ is a rational multiple of

$$C_r = \prod_p \left(1 - \frac{p}{p^{r+2}-1}\right)$$

and this concludes the proof. □

A calculation shows that, in the case when $\Gamma = \langle g \rangle$, the above expression for $C_{\langle g \rangle}$ coincides with the density c_g of Pomerance and Kurlberg (see equation 1.3). We will give the proof for $g > 0$, in the following Corollary.

Corollary 2.11. *Let $\Gamma = \langle g \rangle$ where $g \in \mathbb{Q}^+ \setminus \{1\}$ and we write $g = (g_0)^h$ where h is a positive integer and g_0 is not a perfect power and let $g_0 = g_1 g_2^2$ where g_1 is square free, we have $C_\Gamma = c_g$.*

Proof. By Proposition 2.1, we have $t_\eta = \infty$ unless $\eta = g_1$, so S_η is different than 0 only when $\eta = g_1$, then we have

$$C_{\langle g \rangle} = \prod_p \left(1 - \sum_{\alpha \geq 1} \frac{1}{p^{2\alpha-1}|\Gamma(p^\alpha)|}\right) \left(1 + S_{g_1} \prod_{p|2g_1} \left(1 - \left(\sum_{\alpha \geq 1} \frac{1}{p^{2\alpha-1}|\Gamma(p^\alpha)|}\right)^{-1}\right)^{-1}\right).$$

When the rank is 1, for prime powers we have $|\Gamma(p^\alpha)| = p^{\max(0,\alpha - v_p(\Delta_1))}$. Since $\Delta_1 = h$, then

$$\begin{aligned} C_{\langle g \rangle} &= \prod_p \left(1 - \sum_{\alpha \geq 1} \frac{1}{p^{2\alpha-1} p^{\max\{0,\alpha - v_p(h)\}}}\right) \\ &\quad \times \left(1 + S_{g_1} \prod_{p|2g_1} \left(1 - \left(\sum_{\alpha \geq 1} \frac{1}{p^{2\alpha-1}|\Gamma(p^\alpha)|}\right)^{-1}\right)^{-1}\right) \\ &= \prod_p \left(1 - \sum_{\alpha \geq 1} \frac{1}{p^{3\alpha-1}}\right) \prod_{p|h} \frac{\left(1 - \sum_{\alpha \geq 1} \frac{1}{p^{2\alpha-1+\max(0,\alpha-v_p(h))}}\right)}{\left(1 - \sum_{\alpha \geq 1} \frac{1}{p^{3\alpha-1}}\right)} \\ &\quad \times \left(1 + S_{g_1} \prod_{p|2g_1} \left(1 - \left(\sum_{\alpha \geq 1} \frac{1}{p^{2\alpha-1}|\Gamma(p^\alpha)|}\right)^{-1}\right)^{-1}\right). \end{aligned}$$

If we use the notation of Pomerance and Kurlberg, which we defined previously in introduction and noting that $j - \min(j, v_p(h)) = \max(0, j - v_p(h))$, we have

$$\begin{aligned} C_{\langle g \rangle} &= c \prod_{p|h} \frac{F(p)}{1 - \frac{p}{p^3-1}} \left(1 + \frac{F(2) - F(2, \gamma_{g_1})}{F(2) - 1} \prod_{p|2g_1} (1 + (F(p) - 1)^{-1})^{-1} \right) \\ &= c \prod_{p|h} \frac{F(p)}{1 - \frac{p}{p^3-1}} \left(1 + \frac{F(2) - F(2, \gamma_{g_1})}{F(2) - 1} \prod_{p|2g_1} \frac{F(p) - 1}{F(p)} \right) \\ &= c \prod_{p|h} \frac{F(p)}{1 - \frac{p}{p^3-1}} \left(1 + \frac{F(2) - S(2, \gamma_{g_1})}{F(2)} \prod_{p|g_1, p>2} \frac{F(p) - 1}{F(p)} \right) \\ &= c \prod_{p|h} \frac{F(p)}{1 - \frac{p}{p^3-1}} \left(1 + \prod_{p|n} \frac{F(p) - F(p, v_p(n))}{S(p)} \right) \end{aligned} \tag{2.27}$$

where $n = \text{lcm}[2e+1; \delta(a_1)]$, to get last equality we used the equation $\gamma_{g_1} = \max(1+t_{g_1}, v_2(\delta(g_1))) = v_2(n)$ and the property $v_p(n) = 1$ except for $p = 2$. □

2.4 Numerical Examples

In this section we compare some numerical data. The following table compares the value of C_Γ as predicted by Corollary 2.9 with

$$A_\Gamma = \frac{\sum_{p \leq 10^{10}} |\Gamma_p|}{\sum_{p \leq 10^{10}} p}.$$

We consider the following cases:

- $\Gamma_r = \langle 2, ..., p_r \rangle$, the group generated by the first r primes
- $\Gamma'_r = \langle 3, ..., p_{r+1} \rangle$, the group generated by the first r odd primes
- $\Gamma''_r = \langle 5, ..., p''_r \rangle$, the group generated by the first r primes congruent to 1 modulo 4.

r	1	2	3	4	5	6	7
A_{Γ_r}	0.5723625220	0.8234145762	0.9219692467	0.9638944667	0.9828346715	0.9916961670	0.9959388895
C_{Γ_r}	0.5723602190	0.8234094709	0.9219688310	0.9638925514	0.9828293379	0.9916891587	0.9959315465
$A_{\Gamma'_r}$	0.5797271743	0.8249081874	0.9220326599	0.9639044730	0.9828352799	0.9916947130	0.9959372205
$C_{\Gamma'_r}$	0.5797162295	0.8249060912	0.9220306381	0.9639002343	0.9828302996	0.9916892783	0.9959315614
$A_{\Gamma''_r}$	0.5856374600	0.8246697078	0.9220170449	0.9639045923	0.9828329969	0.9916930151	0.9959357111
$C_{\Gamma''_r}$	0.5856399683	0.8246572843	0.9220082264	0.9638982767	0.9828301305	0.9916892643	0.9959315465

Table 2.2: Comparison of the results

Example 2.12. *We will use the same example in [19]. Let*

$$\Gamma = \langle 3^3.11^{15}, 3^3.11^3, 3^7.13^7, 2^2.5^2.11.13 \rangle.$$

Then $\mathrm{Supp}(\Gamma) = (2, 3, 5, 11, 13)$ *and the matrix associated to* Γ *is*

$$\begin{pmatrix} 0 & 0 & 0 & 2 \\ 3 & 3 & 7 & 0 \\ 0 & 0 & 0 & 2 \\ 15 & 3 & 0 & 1 \\ 0 & 0 & 7 & 1 \end{pmatrix}$$

$\Delta_4(\Gamma) = 2^3.3^2.7$, $\Delta_3(\Gamma) = 2.3$, $\Delta_2(\Gamma) = \Delta_1(\Gamma) = 1$ *where for* $i = 1, ..., r$, Δ_i *is the* i*'th exponent of* Γ. *Using this identity (2.3)*

$$|\Gamma(\ell^j)| = l^{max\{0, j-v_l(1), 2j-v_l(1), 3j-v_l(2.3), 4j-v_l(2^3.3^2.7)\}}.$$

After some calculations (see [19])

$$t_\eta = \begin{cases} 0 & \text{if } \eta \in \{1, 33, 29, 143\} \\ 1 & \text{if } \eta \in \{30, 110, 130, 4290\} \\ 2 & \text{if } \eta \in \{3, 11, 10, 13, 330, 390, 1430\} \\ \infty & \text{otherwise.} \end{cases}$$

Then we have

$$s_\eta = \begin{cases} 1 & \text{if } \eta \in \{1, 33, 29\} \\ 2 & \text{if } \eta \in \{143\} \\ 3 & \text{if } \eta \in \{3, 11, 10, 13, 30, 110, 130, 330, 390, 1430, 4290\} \\ \infty & \text{otherwise.} \end{cases}$$

For specific Γ *in the example, we have the following results* $A_\Gamma = 0.838115336148$, $C_\Gamma = 0.838100746276$.

Chapter 3

Average r-rank Artin Conjecture

3.1 Introduction

In the present work, we will discuss the average version of the *r–rank Artin quasi primitive root conjecture*. Let $\Gamma \subset \mathbb{Q}^*$ be a multiplicative subgroup of finite rank r. We define

$$N_{\Gamma,m}(x) := \#\{p \leq x : |\Gamma_p| = \frac{p-1}{m}\}.$$

It was proven by Cangelmi, Pappalardi and Susa in [18], [3] and [20], assuming the GRH for $\mathbb{Q}(\zeta_k, \Gamma^{1/k})$, $k \in \mathbb{N}$, that for any $\varepsilon > 0$, if $m \leq x^{\frac{r-1}{(r+1)(4r+2)}-\varepsilon}$,

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

where δ_Γ^m is a rational multiple of

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

Here we restrict ourselves to study subgroups $\Gamma = \langle a_1, \cdots, a_r\rangle$ with $a_i \in \mathbb{Z}$ for all $i = 1, \ldots, r$.

Notice that, since $\varphi(mn) = \varphi(m)\varphi(n)\gcd(m,n)/\varphi(\gcd(m,n))$

$$C_{r,m} = \frac{1}{m^r\varphi(m)}\sum_{n\geq 1}\frac{\mu(n)}{n^r\varphi(n)}\prod_{p|\gcd(m,n)}\left(1-\frac{1}{p}\right) = \frac{1}{m^{r+1}}\prod_{p|m}\left(1-\frac{p}{p^{r+1}-1}\right)^{-1} C_r\ .$$

The proof of Theorem 1.8 (see equation (3.5) and Lemma 3.6) will lead to a side product to the asymptotic identity, for $T_i > \exp(4(\log x \log\log x)^{\frac{1}{2}})$ for all $i = 1,\dots,r$, $m \leq (\log x)^D$ and any constant $M > 2$:

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

where $J_r(n) = n^r\prod_{\ell|n}(1-1/\ell^r)$ is the so called *Jordan's totient function*. This provides a natural generalization of Moree's result in [17].

3.2 Preliminary Definitions and Lemmas

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 $\underline{a}\cdot\underline{n} = a_1n_1 + \cdots + a_rn_r$. 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 $\underline{\chi}(\underline{a}) = \chi_1(a_1)\cdots\chi_r(a_r) \in \mathbb{C}$.

Additionally, $(q,\underline{a}) := (q,a_1,\dots,a_r) = \gcd(q,a_1,\dots,a_r)$; 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 $\langle\underline{a}\rangle_p := \Gamma_p$, where $\Gamma = \langle a_1,\dots,a_r\rangle$, the reduction modulo p of the subgroup $\langle\underline{a}\rangle = \langle a_1,\dots,a_r\rangle \subset \mathbb{Q}$. Given a finite field $\mathbb{F}_p$, $\widehat{\mathbb{F}_p^*}$ will denote its relative dual group (or character group).

Let $\mathbb{C}$ be the set of complex numbers and $\mathbb{C}^*$ be the set of non-zero complex numbers. A homomorphism from Abelian group G to $\mathbb{C}^*$ is called a character of group G. A character χ is called Dirichlet character if χ is a function from $\mathbb{Z}$ to $\mathbb{C}^*$ which satisfies the following properties for

a fixed integer q:

- $\chi(n+q) = \chi(n)$ for any integer n
- $\chi(n) \neq 0$ if $\gcd(n,q) = 1$ and $\chi(n) = 0$ otherwise
- $\chi(nm) = \chi(n)\chi(m)$ for all integers n and m.

Let χ be a character modulo q. We called χ is primitive if there is no positive integer $n < q$ such that $n \mid q$ and $\chi(m) = \chi(m \pmod n)$ for all m. The proof of the following result can be found in any standard text book on analytic number theory.

Lemma 3.1. *Let χ be a character modulo q, and $C(\chi) = \frac{1}{\varphi(q)} \sum_b^{'} \chi(b)$ where the sum is over primitive roots modulo q. Then we have*

$$\sum_{\chi \pmod q} C(\chi) \cdot \chi(a) = \begin{cases} 1 & \text{if } a \text{ is primitive root} \mod q \\ 0 & \text{otherwise.} \end{cases} \tag{3.1}$$

Theorem 3.2. *[Large Sieve] For each character χ modulo q, let*

$$S(\chi) = \sum_{n=M+1}^{M+N} a_n \chi(n)$$

where $a_n \in \mathbb{C}$ and $M, N \in \mathbb{Z}$. Then we have

$$\sum_{q \leq K} \sum_{\chi \pmod q}^{'} |S(\chi)|^2 \ll (K^2 + N) \sum_{n=M+1}^{M+N} |a_n|^2,$$

where $\sum^{'}$ denotes summation over primitive characters, $K \in \mathbb{Z}^+$ and $k \geq 1$.

We refer to Gallagher [4] for the proof.
Using Theorem 3.2, Stephens [24] proved the following Theorem.

Theorem 3.3. *Let $N \in \mathbb{Z}$, $K \in \mathbb{Z}^+$ and $k \geq 1$ we have*

$$\sum_{k \leq K} \sum_{\chi \pmod{k}}{}' \left| \sum_{a \leq N} \chi(a) \right|^{2r} \ll (K^2 + N^r) N^r (\log(eN^{r-1}))^{r^2-1},$$

where $\sum'$ denotes summation over primitive characters.

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 [7, Theorem 272]) that, given any integer n,

$$c_q(n) = \mu\left(\frac{q}{(q,n)}\right) \frac{\varphi(q)}{\varphi\left(\frac{q}{(q,n)}\right)}. \tag{3.2}$$

In the following Lemma, we prove a similar equation for multiple Ramanujan sum.

Lemma 3.4. *Let*

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

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 of Lemma 3.4. Let us start by considering the case when $q = \ell$ is prime. Then

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

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

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

Then

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

If we apply equation (3.2), 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 $k \geq 2$, 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 fist 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

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

Hence,

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

In the second case, we go back to the definition of $c_q(\underline{n})$ and we have

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

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

We also 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 amount in saying that the *multiple Ramanujan sum* is multiplicative in q. Indeed

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

since $\gcd(q',q'')=1$, the result follows from the following remarks:

- for all $j=1,\dots r$, 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 $\underline{b}\in(\mathbb{Z}/q''\mathbb{Z})^r$,

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

The proof of the Lemma now follows from the multiplicativity of μ and of J_r. □

From the above statement we deduce the following:

Corollary 3.5. *Let p be an odd prime, let $m\in\mathbb{N}$ be a divisor of $p-1$. If $\underline{\chi}=(\chi_1,\dots,\chi_r)$ is a r-tuple of Dirichlet characters modulo p and 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

$$c_m(\underline{\chi}) = \frac{1}{(p-1)^r}\,\mu\left(\frac{p-1}{m\gcd\left(\frac{p-1}{m},\frac{p-1}{\mathrm{ord}(\chi_1)},\dots,\frac{p-1}{\mathrm{ord}(\chi_r)}\right)}\right)\frac{J_r\left(\frac{p-1}{m}\right)}{J_r\left(\frac{p-1}{m\gcd\left(\frac{p-1}{m},\frac{p-1}{\mathrm{ord}(\chi_1)},\dots,\frac{p-1}{\mathrm{ord}(\chi_r)}\right)}\right)}\,. \quad (3.3)$$

Proof of Corollary 3.5. 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

$$\begin{aligned} c_m(\underline{\chi}) &= \frac{1}{(p-1)^r}\sum_{\substack{\underline{a}\in(\mathbb{F}_p^*)^r\\(p-1,\underline{a})=m}}\chi_1(g)^{a_1}\cdots\chi_r(g)^{a_r}\\ &= \frac{1}{(p-1)^r}\sum_{\substack{\underline{a}'\in(\mathbb{Z}/t\mathbb{Z})^r\\(t,\underline{a}')=1}}e^{2\pi i\underline{a}'\cdot\underline{n}/t}\\ &= \frac{1}{(p-1)^r}\,c_{\frac{p-1}{m}}(\underline{n}). \end{aligned} \quad (3.4)$$

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

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

and this concludes the proof. □

For a fixed rank r, define $R_p(m) := \#\{\underline{a} \in (\mathbb{Z}/(p-1)\mathbb{Z})^r : (\underline{a}, p-1) = m\}$. Then using well-known properties of the Möbius function, we can write

$$R_p(m) = \sum_{\underline{a} \in (\mathbb{Z}/(p-1)\mathbb{Z})^r} \sum_{\substack{n \mid \frac{a_1}{m} \\ \vdots \\ n \mid \frac{a_r}{m} \\ n \mid \frac{p-1}{m}}} \mu(n) = \sum_{n \mid \frac{p-1}{m}} \mu(n)[h_m(n)]^r$$

where

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

so that

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

Defining

$$S_m(x) := \frac{1}{m^r} \sum_{\substack{p \le x \\ p \equiv 1 \pmod m}} \sum_{n \mid \frac{p-1}{m}} \frac{\mu(n)}{n^r} = \sum_{\substack{p \le x \\ p \equiv 1 \pmod m}} \frac{1}{(p-1)^r} J_r\left(\frac{p-1}{m}\right) \tag{3.5}$$

we have the following Lemma.

Lemma 3.6. *If $m \le (\log x)^D$ with D arbitrary positive constant, then*

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

where M is an arbitrary constant greater than 1 and $C_{r,m} = \sum_{n \ge 1} \frac{\mu(n)}{(nm)^r \varphi(nm)}$.

Proof. We choose an arbitrary positive constant B and for every co-prime integers a and b, we

denote $\pi(x;a,b) = \#\{p \le x : p \equiv a \pmod b\}$, then

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

The sum in the error term is

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

For the main term we apply the Siegel–Walfisz Theorem [27], which states that for every arbitrary positive constants B and C, if $a \le (\log x)^B$, then

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

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

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

where we have used the elementary inequality $\varphi(mn) \geq \varphi(m)\varphi(n)$. Since

$$\frac{n}{\varphi(n)} \ll \log\log n \ ,$$

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

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

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

Lemma 3.7. *Let τ be the divisor function and $m \in \mathbb{N}$. For x sufficiently large, $x > m$, we have the following inequality:*

$$\sum_{\substack{p \leq x \\ p \equiv 1 \pmod{m}}} \tau\left(\frac{p-1}{m} \right) \leq \frac{2x}{m}.$$

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

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

So we have the identity:

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

Using the Montgomery–Vaughan [15] version of the Brun–Titchmarsh Theorem:

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

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

$$\sum_{\substack{p\le x\\ p\equiv 1 \pmod m}} \tau\left(\frac{p-1}{m}\right) \le 2\sum_{k\le Q} \frac{2x}{\varphi(km)\log(x/km)} \le \frac{2x}{\log(x/m)} \sum_{k\le Q} \frac{1}{\varphi(km)}.$$

Now substitute the elementary inequality $\varphi(km) \geq m\varphi(k)$ and use the result of Montgomery [15]

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

where

$$A = \frac{\zeta(2)\zeta(3)}{\zeta(6)} = 1.94360\cdots \quad \text{and} \quad B = A\gamma - \sum_{n=1}^{\infty} \frac{\mu^2(n) \log n}{n\varphi(n)} = -0.06056\ldots ,$$

which in particular implies that for Q large enough

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

Finally

$$\sum_{\substack{p \leq x \\ p \equiv 1 \pmod{m}}} \tau\left(\frac{p-1}{m}\right) \leq \frac{2x}{m} .$$

□

Lemma 3.8. *Let p be an odd prime number and let*

$$d_m(\chi) = \sum_{\substack{\underline{\chi} \in \left(\widehat{\mathbb{F}_p^*}\right)^r \\ \chi_1 = \chi \neq \chi_0}} |c_m(\underline{\chi})| ;$$

then

$$d_m(\chi) \leq \frac{1}{m} \prod_{\ell \mid \frac{p-1}{m}} \left(1 + \frac{1}{\ell}\right) .$$

Proof. From equation (3.4), we have

$$d_m(\chi) = \frac{1}{(p-1)^r} \sum_{\substack{\underline{n} \in \left(\frac{\mathbb{Z}}{(p-1)\mathbb{Z}}\right)^r \\ n_1 \neq 0}} \mu^2 \left(\frac{(p-1)/m}{\left(\frac{p-1}{m}, \underline{n}\right)} \right) \frac{J_r\left(\frac{p-1}{m}\right)}{J_r\left(\frac{(p-1)/m}{\left(\frac{p-1}{m}, \underline{n}\right)}\right)} ,$$

thus naming $t = \frac{p-1}{m}$ and $u = \gcd(t, n_1)$ we get

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

where

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

Denoting $\alpha = v_\ell(t)$, then

$$\begin{aligned} d_m(\chi) &= \frac{1}{(p-1)} \sum_{d|t} \mu^2\left(\frac{t}{d}\right) \frac{J_r(t)}{d^{r-1} J_r\left(\frac{t}{d}\right)} \sum_{k \mid \frac{u}{d}} \frac{\mu(k)}{k^{r-1}} \\ &\leq \frac{1}{p-1} \sum_{d|t} \mu^2\left(\frac{t}{d}\right) d = \frac{t}{p-1} \sum_{k|t} \frac{\mu^2(k)}{k} \\ &= \frac{1}{m} \prod_{\ell|t} \left(1 + \frac{1}{l}\right). \end{aligned}$$

□

3.3 Proof of Theorem 1.8

Proof. We will follow the method of Stephens [24]. By exchanging the order of summation we obtain that

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

where $M_p^m(\underline{T})$ is the number of r-tuples $\underline{a} \in \mathbb{Z}^r$, with $0 < a_i \le T_i$ 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

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

where

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

It is easy to show that, given a r-tuple $\underline{\chi}$ of characters mod p, then

$$t_{p,m}(\underline{a}) = \sum_{\underline{\chi}\in(\widehat{\mathbb{F}_p^*})^r} c_m(\underline{\chi})\underline{\chi}(\underline{a})\,; \tag{3.6}$$

so we have

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

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

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

$$= \frac{1}{(p-1)^r} R_p(m) \ .$$

Denoting $|\underline{T}| := \prod_{i=1}^r T_i$ and using (3.5), we can write the main term as

$$\frac{1}{|\underline{T}|} \sum_{\substack{p \le x \\ p \equiv 1 \pmod m}} \sum_{\substack{\underline{a} \in \mathbb{Z}^r \\ 0 < a_1 \le T_1 \\ \vdots \\ 0 < a_r \le T_r}} c_m(\underline{\chi}_0) \underline{\chi}_0(\underline{a}) = \frac{1}{|\underline{T}|} \sum_{\substack{p \le x \\ p \equiv 1 \pmod m}} c_m(\underline{\chi}_0) \prod_{i=1}^r \{\lfloor T_i \rfloor - \lfloor T_i/p \rfloor\}$$

$$= \sum_{\substack{p \le x \\ p \equiv 1 \pmod m}} c_m(\underline{\chi}_0) \left(1 - \frac{r}{p} + \cdots + \frac{1}{p^r} + \sum_{i=1}^r O\left(\frac{1}{T_i}\right) \right)$$

$$= \sum_{\substack{p \le x \\ p \equiv 1 \pmod m}} c_m(\underline{\chi}_0) + O\left(\sum_{\substack{p \le x \\ p \equiv 1 \pmod m}} \frac{1}{p} \right) + O\left(\frac{x}{T^* \log x} \right)$$

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

Since $m \le (\log x)^D$, $D > 0$, and $T^* > \exp(4(\log x \log\log x)^{1/2})$, we can apply Lemma 3.6:

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

where $M > 1$.

For the error term we need to estimate the sum;

$$E_{r,m}(x) := \frac{1}{|\underline{T}|} \sum_{\substack{p\le x\\ p\equiv 1 \pmod m}} \sum_{\underline{\chi}\in\left(\widehat{\mathbb{F}_p^*}\right)^r\setminus\{\underline{\chi}_0\}} \left| c_m(\underline{\chi}) \sum_{\substack{\underline{a}\in\mathbb{Z}^r\\ 0<a_1\le T_1\\ \vdots\\ 0<a_r\le T_r}} \underline{\chi}(\underline{a}) \right|$$
$$\ll \sum_{i=1}^{r} \frac{1}{T_i} \sum_{\substack{p\le x\\ p\equiv 1 \pmod m}} \sum_{\chi_i\in\widehat{\mathbb{F}_p^*}\setminus\{\chi_0\}} d_m(\chi_i) \left| \sum_{\substack{a\in\mathbb{Z}\\ 0<a\le T_i}} \chi_i(a) \right|$$

where

$$d_m(\chi) = \sum_{\substack{\underline{\chi}\in\left(\widehat{\mathbb{F}_p^*}\right)^r\\ \chi_1=\chi\neq\chi_0}} |c_m(\underline{\chi})| \,.$$

Define

$$E_{r,m}^j(x) := \sum_{\substack{p\le x\\ p\equiv 1 \pmod m}} \sum_{\chi_i\in\widehat{\mathbb{F}_p^*}\setminus\{\chi_0\}} d_m(\chi_i) \left| \sum_{\substack{a\in\mathbb{Z}\\ 0<a\le T_i}} \chi_i(a) \right| \tag{3.7}$$

then using Holder's inequality

$$\left\{E_{r,m}^j(x)\right\}^{2s_i} \le \left\{ \sum_{\substack{p\le x\\ p\equiv 1 \pmod m}} \sum_{\chi_i\in\widehat{\mathbb{F}_p^*}\setminus\{\chi_0\}} \{d_m(\chi_i)\}^{\frac{2s_i}{2s_i-1}} \right\}^{2s_i-1}$$
$$\times \sum_{\substack{p\le x\\ p\equiv 1 \pmod m}} \sum_{\chi_i\in\widehat{\mathbb{F}_p^*}\setminus\{\chi_0\}} \left| \sum_{\substack{a\in\mathbb{Z}\\ 0<a\le T_i}} \chi_i(a) \right|^{2s_i} . \tag{3.8}$$

If g is a primitive root modulo p, then for every $j = 1, \dots, r$ we write again $\chi_j(g) = e^{2\pi i n_j/(p-1)}$ for

a certain $n_j \in \mathbb{Z}/(p-1)\mathbb{Z}$, by equation (3.4) so that

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

Thus, using Lemma 3.4 and indicating again $t = (p-1)/m$ we have

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

Calling $D_m(p) = \max_{\chi\in\widehat{\mathbb{F}_p^*}\setminus\{\chi_0\}}\{d_m(\chi)\}$ and using Lemmas 3.8 and 3.7 in equation (3.8) we have

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

To estimate the other term in (3.8) we use Theorem 3.3 :

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

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

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

where

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

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

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

Now, if $T_i>x^2$ for all $i=1,\dots,r$, then $s_1=\cdots=s_r=1$ 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 $M>1$. If $T_j\le x^2$ for some $j\in\{1,\dots,r\}$, then $s_j\ge 2$ and the corresponding contribution to $E_{r,m}(x)$ will be

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

By hypothesis

$$T^* > \exp(4(\log x \log\log x)^{1/2}) \,, \tag{3.9}$$

so

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

also in this case, using (3.9), we have $E_{r,m}(x) \ll x/(\log x)^M$ for every $M > 1$. This proves the first statement of the Theorem.

In order to prove the second statement of the Theorem, we now consider

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

where $M^m_{p,q}(\underline{T})$ denotes the number of r-tuples $\underline{a} \in \mathbb{Z}^r$, with $a_i \le T_i$ and $v_p(a_i) = v_q(a_i) = 0$ for each $i = 1, \dots, r$, whose reductions modulo p and q satisfy $[\mathbb{F}_p^* : \langle \underline{a}\rangle_p] = m$ and $[\mathbb{F}_q^* : \langle \underline{a}\rangle_q] = m$ simultaneously. Then by applying the first result of the statement, we obtain, for every constant $M' > 2$,

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

If we write

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

we can apply again the first result of the statement to get

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

where $M > 1$. In the same spirit as in the proof of the first part of the statement, we use (3.6). Hence

$$\begin{aligned}\sum_{\substack{p,q\le x\\ p,q\equiv 1 \pmod m\\ p\neq q}} M_{p,q}^m(\underline{T}) &= \sum_{\substack{p,q\le x\\ p,q\equiv 1 \pmod m\\ p\neq q}} \sum_{\substack{\underline{a}\in\mathbb{Z}^r\\ 0<a_1\le T_1\\ \vdots\\ 0<a_r\le T_r}} t_{p,m}(\underline{a})t_{q,m}(\underline{a})\\ &= \sum_{\substack{p,q\le x\\ p,q\equiv 1 \pmod m\\ p\neq q}} \sum_{\underline{\chi}_1\in(\widehat{\mathbb{F}_p})^r}\sum_{\underline{\chi}_2\in(\widehat{\mathbb{F}_q})^r} c_m(\underline{\chi}_1)c_m(\underline{\chi}_2) \sum_{\substack{\underline{a}\in\mathbb{Z}^r\\ 0<a_1\le T_1\\ \vdots\\ 0<a_r\le T_r}} \underline{\chi}_1(\underline{a})\underline{\chi}_2(\underline{a}) \ .\end{aligned}$$

Therefore,

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

where H_1, H_2, H_3 are the contributions to the double sum 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 a r-tuples whose all entries are principal characters

(mod p) and (mod q) respectively, so that

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

Then for every constant $M'>2$, Lemma 3.6 gives

$$\begin{aligned}
H_1 &= \sum_{\substack{p,q\le x \\ p,q\equiv 1 \pmod m \\ p\neq q}} c_m(\underline{\chi}_0^p)c_m(\underline{\chi}_0^q) \sum_{\substack{\underline{a}\in\mathbb{Z}^r \\ 0<a_1\le T_1 \\ \vdots \\ 0<a_r\le T_r}} \underline{\chi}_0^p(\underline{a})\underline{\chi}_0^q(\underline{a}) \\
&= |\underline{T}| \sum_{\substack{p,q\le x \\ p,q\equiv 1 \pmod m \\ p\neq q}} c_m(\underline{\chi}_0^p)c_m(\underline{\chi}_0^q)\left(1-\frac{r}{p}-\frac{r}{q}+\cdots+\frac{1}{(pq)^r}+\sum_{i=1}^{r}O\left(\frac{1}{T_i}\right)\right) \\
&= |\underline{T}|\left(\left(\sum_{\substack{p\le x \\ p\equiv 1 \pmod m}} c_m(\underline{\chi}_0)\right)^2 - \sum_{\substack{p\le x \\ p\equiv 1 \pmod m}} (c_m(\underline{\chi}_0^p))^2\right)\left(1+O\left(\frac{1}{T^*}\right)\right) + |\underline{T}|O\left(\frac{x\log\log x}{\log x}\right) \\
&= |\underline{T}|\left(S_m^2(x)+O\left(\frac{x^2}{T^*(\log x)^2}\right)+O\left(\frac{x\log\log x}{\log x}\right)\right) \\
&= |\underline{T}|\left(C_{r,m}^2\,\mathrm{Li}^2(x)+O\left(\frac{x^2}{m^r(\log x)^{M'}}\right)\right).
\end{aligned}$$

Focusing on H_2 and supposing $\underline{\chi}_1 = \underline{\chi}_0 \neq \underline{\chi}_2$, then

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

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

The quantity

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

can be estimated as before through Holder's inequality combined with the large sieve inequality to get $U_2 \ll x/(\log x)^M$ with $M > 1$, while Lemma 3.7 gives the following upper bound:

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

$$\ll \frac{|\underline{T}|}{p^r} \sum_{\substack{q\le x\\ q\equiv 1 \pmod m}} \tau\left(\frac{q-1}{m}\right) \ll \frac{|\underline{T}|x}{p^r m} \, .$$

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

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

Finally, we notice that for $\chi_1 \in \widehat{\mathbb{F}_p^*} \setminus \{\chi_0^p\}$ 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. Consequently, given

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

once again we can apply Holder's inequality and Theorem 3.3 (large Sieve) to obtain an upper bound for H_3. First, notice that since the r-tuple of characters, $\underline{\chi}_1$ and $\underline{\chi}_2$, appearing in H_3 are both non-principal and indicating with $\chi_{1,i}$ the i-th component of the r-tuple $\underline{\chi}_1$ of Dirichlet characters of modulus p (similarly for $\chi_{2,i}$), the estimate for H_3 comes from a diagonal part H_3^d (in which for a certain $i \in \{1, \ldots, r\}$ both $\chi_{1,i}$ and $\chi_{2,i}$ are non-principal) plus a non-diagonal part H_3^{nd} (in which for none of the indices $i \in \{1, \ldots, r\}$ is possible to have $\chi_{1,i}$ and $\chi_{2,i}$ both non-principal): explicitly, $H_3^d = \sum_{i=1}^r H_{3,i}$, where

$$\begin{aligned} H_{3,i} :=& \sum_{\substack{p,q \leq x \\ p,q \equiv 1 \pmod m \\ p \neq q}} \sum_{\substack{\underline{\chi}_1 \in (\widehat{\mathbb{F}_p^*})^r \setminus \{\underline{\chi}_0^p\} \\ \chi_{1,i} \in \widehat{\mathbb{F}_p^*} \setminus \{\chi_0^p\}}} \sum_{\substack{\underline{\chi}_2 \in (\widehat{\mathbb{F}_q^*})^r \setminus \{\underline{\chi}_0^q\} \\ \chi_{2,i} \in \widehat{\mathbb{F}_q^*} \setminus \{\chi_0^q\}}} c_m(\underline{\chi}_1) c_m(\underline{\chi}_2) \sum_{\substack{\underline{a} \in \mathbb{Z}^r \\ 0 < a_1 \leq T_1 \\ \vdots \\ 0 < a_r \leq T_r}} \underline{\chi}_1(\underline{a}) \underline{\chi}_2(\underline{a}) \\ \leq& \frac{|\underline{T}|}{T_i} \sum_{\substack{p,q \leq x \\ p,q \equiv 1 \pmod m \\ p \neq q}} \sum_{\chi_{1,i} \in \widehat{\mathbb{F}_p^*} \setminus \{\chi_0^p\}} \sum_{\chi_{2,i} \in \widehat{\mathbb{F}_q^*} \setminus \{\chi_0^q\}} d_m(\chi_{1,i}) d_m(\chi_{2,i}) \left| \sum_{0 < a_i \leq T_i} \chi_{1,i}(a_i) \chi_{2,i}(a_i) \right|, \end{aligned}$$

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

$$H_{3,ij} := \sum_{\substack{p,q\le x\\ p,q\equiv 1 \pmod m\\ p\neq q}} \sum_{\substack{\underline{\chi}_1\in(\widehat{\mathbb{F}_p^*})^r\setminus\{\underline{\chi}_0^p\}\\ \chi_{1,i}\in\widehat{\mathbb{F}_p^*}\setminus\{\chi_0^p\}}} \sum_{\substack{\underline{\chi}_2\in(\widehat{\mathbb{F}_q^*})^r\setminus\{\underline{\chi}_0^q\}\\ \chi_{2,j}\in\widehat{\mathbb{F}_q^*}\setminus\{\chi_0^q\}}} c_m(\underline{\chi}_1)c_m(\underline{\chi}_2) \sum_{\substack{\underline{a}\in\mathbb{Z}^r\\ 0<a_1\le T_1\\ \vdots\\ 0<a_r\le T_r}} \underline{\chi}_1(\underline{a})\underline{\chi}_2(\underline{a})$$

$$\le \frac{|\underline{T}|}{T_iT_j} \sum_{\substack{p,q\le x\\ p,q\equiv 1 \pmod m\\ p\neq q}} \sum_{\chi_{1,i}\in\widehat{\mathbb{F}_p^*}\setminus\{\chi_0^p\}} \sum_{\chi_{2,j}\in\widehat{\mathbb{F}_q^*}\setminus\{\chi_0^q\}} d_m(\chi_{1,i})d_m(\chi_{2,j}) \left| \sum_{\substack{0<a_i\le T_i\\ 0<a_j\le T_j}} \chi_{1,i}(a_i)\chi_{2,j}(a_j)\right| .$$

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

$$\frac{H_{3,i}}{|\underline{T}|} \ll \frac{1}{T_i} \left\{ \sum_{\substack{p,q\le x\\ p,q\equiv 1 \pmod m\\ p\neq q}} \sum_{\substack{\chi_{1,i}\in\widehat{\mathbb{F}_p^*}\setminus\{\chi_0^p\}\\ \chi_{2,i}\in\widehat{\mathbb{F}_q^*}\setminus\{\chi_0^q\}}} [d_m(\chi_{1,i})d_m(\chi_{2,i})]^{\frac{2s_i}{2s_i-1}} \right\}^{\frac{2s_i-1}{2s_i}}$$

$$\times \left\{ \sum_{\substack{p,q\le x\\ p,q\equiv 1 \pmod m\\ p\neq q}} \sum_{\eta \pmod{pq}} \left| \sum_{0<a_i\le T_i} \eta(a_i)\right|^{2s_i} \right\}^{\frac{1}{2s_i}}$$

$$\ll \frac{1}{T_i} \left\{ \left(\frac{x\log\log x}{m^2}\right)^{4s_i-2} (x^4+T_i^{s_i})T_i^{s_i}(\log(eT_i^{s_i-1}))^{s_i^2-1} \right\}^{\frac{1}{2s_i}} .$$

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

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

Now, if $T_i > x^4$ then $s_i = 1$ and $H_{3,i}/|\underline{T}| \ll x(\log\log x)^2$. Otherwise, if $T_i \le x^4$ then $s_i \ge 2$ and, if $T_i > \exp(6(\log x\log\log x)^{1/2})$, similar to what was done to prove the first statement of the

Theorem, 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 $H_{3,ij}$, with $i \neq j$: it can be factorized in two products, and after using same methods in (3.7), we have

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

Similar to what was done to estimate the error term (3.7), 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 $H_3 \leq H_3^d + H_3^{nd}$, summing the upper bounds for H_1, H_2 and H_3 we get the proof of second part of the Theorem 1.4. □

Corollary 3.9. *For any $\epsilon > 0$, let*

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

then, supposing $T_i > \exp(6(\log x \log\log x)^{1/2})$ *for every* $i = 1, \ldots, r$*, we have*

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

for every positive constant F*.*

Proof. See [24] (Corollary, page 187). □

Chapter 4

Codes

In this chapter, we include some sample codes that were used to generate the tables in this thesis, they were written in Pari.

The first code we include generates the data for A_{Γ_r}, where $\Gamma_r = \langle 2, ..., p_r \rangle$ is the group generated by the first r primes. The results are given in the first row of Table 2.2.

```
{P=2+3+5+7+11+13+17;
A=vector(7);
A[1]=znorder(Mod(2,3))+znorder(Mod(2,5))+znorder(Mod(2,7))+znorder(Mod(2,11))
+znorder(Mod(2,13))+znorder(Mod(2,17));
A[2]=lcm(znorder(Mod(2,5)),znorder(Mod(3,5)))+lcm(znorder(Mod(2,7)),
znorder(Mod(3,7)))+lcm(znorder(Mod(2,11)),znorder(Mod(3,11)))
+lcm(znorder(Mod(2,13)),znorder(Mod(3,13)))
+lcm(znorder(Mod(2,17)),znorder(Mod(3,17)));
A[3]=lcm(lcm(znorder(Mod(2,7)),znorder(Mod(3,7))),znorder(Mod(5,7)))
+lcm(lcm(znorder(Mod(2,11)),znorder(Mod(3,11))),znorder(Mod(5,11)))
```

```
+lcm(lcm(znorder(Mod(2,13)),znorder(Mod(3,13))),znorder(Mod(5,13)))
+lcm(lcm(znorder(Mod(2,17)),znorder(Mod(3,17))),znorder(Mod(5,17)));
A[4]=lcm(lcm(lcm(znorder(Mod(2,11)),znorder(Mod(3,11))),
znorder(Mod(5,11))),znorder(Mod(7,11)))
+lcm(lcm(lcm(znorder(Mod(2,13)),znorder(Mod(3,13))),znorder(Mod(5,13))),
znorder(Mod(7,13)))
+lcm(lcm(lcm(znorder(Mod(2,17)),znorder(Mod(3,17))),znorder(Mod(5,17))),
znorder(Mod(7,17)));
A[5]=lcm(lcm(lcm(lcm(znorder(Mod(2,13)),znorder(Mod(3,13))),
znorder(Mod(5,13))),znorder(Mod(7,13))),znorder(Mod(11,13)))
+lcm(lcm(lcm(lcm(znorder(Mod(2,17)),znorder(Mod(3,17))),znorder(Mod(5,17))),
znorder(Mod(7,17))),znorder(Mod(11,17)));
A[6]=lcm(lcm(lcm(lcm(lcm(znorder(Mod(2,17)),znorder(Mod(3,17))),
znorder(Mod(5,17))),znorder(Mod(7,17))),znorder(Mod(11,17))),
znorder(Mod(13,17)));
print(A);
forprime(p=19,10000000000,
         P=P+p;
         a=znorder(Mod(2,p));
         b=lcm(a,znorder(Mod(3,p)));
         c=lcm(b,znorder(Mod(5,p)));
          d=lcm(c,znorder(Mod(7,p)));
          e=lcm(d,znorder(Mod(11,p)));
```

```
 f=lcm(e,znorder(Mod(13,p)));

 g=lcm(f,znorder(Mod(17,p)));

 A[1]=A[1]+a;

 A[2]=A[2]+b;

 A[3]=A[3]+c;

 A[4]=A[4]+d;

 A[5]=A[5]+e;

 A[6]=A[6]+f;

A[7]=A[7]+g;

);print(A*1./P)}
```

The second code below generates the data for C_{Γ_r}, where $\Gamma_r = \langle 2, ..., p_r \rangle$ is the group generated by the first r primes which were given in the first row of Table 2.2.

```
\read(cohen)

K(j,r)=j/(j+1-j^(r+2));

kk(ee,r)=RIS=1;fordiv(ee,X,if(isprime(X),RIS=RIS*K(X,r)));RIS;

{

for(r=1,7,U=1;P=round(prodeuler(Z=2,prime(r),Z));

fordiv(P,T,if(T>1,U=U+kk(2*T,r)/2^((r+2)*max(0,valuation(quaddisc(T)/2,2)))));

print(U*prodeulerrat(1-x/(x^(r+2)-1))))

}
```

Bibliography

[1] Arnold, I. V., *Number-theoretical turbulence in Fermat Euler arithmetics and large Young diagrams geometry statistics.* Journal of Fluid Mechanics, **7** (2005), S4–S50.

[2] Artin, E., Collected Papers, Reading, MA:Addison-Wesley (1965).

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

[4] Gallagher, P. X., *The large sieve.* Mathematika, **14** (1967), 14-20.

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

[6] Gupta, R., Murty, R.M.*A remark on Artins conjecture*, Invent. Math. **78** (1984) 127130.

[7] Hardy, G.H. and Wright, E.M., *An Introduction to the Theory Of Numbers.* Oxford University Press, fourth edition, London, 1975.

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

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

[10] Kurlberg, P. and Pomerance, C., *On a problem of Arnold: the average multiplicative order of a given integer.* Algebra and Number Theory, **7** (2013), 981-999.

[11] Lagarias, J. C. and Odlyzko, A. M., *Effective versions of the Chebotarev density Theorem.* Algebraic number fields, ed. A. Frohlich, Academic Press, New York, 1977, 409-464

[12] Lang, S. Algebra. Second edition. *Addison-Wesley*, U.S.A, 1984.

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

[14] Menici, L., Pehlivan, C. *Average r–rank Artin Conjecture.* submitted.

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

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

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

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

[19] Pappalardi, F., *Divisibility of reduction in groups of rational numbers.* Math. Comp., (2012).

[20] Pappalardi, F. and Susa, A., *An analogue to Artin's Conjecture for multiplicative subgroups of the rationals.* Arch. Math., **101** (2013), 319–330.

[21] Pehlivan, C. , *Average multiplicative order of finitely generated subgroup of rational numbers over primes* submitted.

[22] Serre, J. P., *Quelques applications du theor'eme de densite de Chebotarev.* Inst. Hautes Etudes Sci. Publ. Math., **54** (1981), 323-401.

[23] Shparlinski, I. E., *On some dynamical systems in finite fields and residue rings.* Discrete and continuous dynamical systems, Series **A17** (2007), 901–917.

[24] Stephens, P. J., *An Average Result For Artin's Conjecture.* Mathematika, **16** (1969), 178–188.

[25] Stephens, P. J., *Prime divisors of second-order linear recurrences. I.* J. Number Theory, **8** (1976), 313-332

[26] Stevenhagen, P., *The correction factor in Artin's primitive root conjecture.* Journal de thorie des nombres de Bordeaux, **15** no.1 (2003), 383-391.

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

[28] Wirsing, E., *Das asymptotische Verhalten von Summen uber multiplikative Funktionen.* Math. Ann., **143** (1961), 75–102.