ROMA TRE
UNIVERSITÀ DEGLI STUDI

DIPARTIMENTO DI MATEMATICA E FISICA

Densities related with groups of rational numbers

Tesi di dottorato in matematica
XXXIV Ciclo

Candidato:
Andam Ali Mustafa Firma:____________________________

Relatore di tesi:
Prof. Francesco Pappalardi Firma:____________________________

Coordinatore:
Prof. Alessandro Giuliani Firma:____________________________

Anno Accademico 2021-2022,
Dipartimento di Matematica e Fisica, Universit‘a degli Studi Roma Tre
Largo San Leonardo Murialdo 1, 00146, Roma

Densities related with groups of rational numbers

By: Andam Ali Mustafa

Supervisor: Prof. Francesco Pappalardi

January 31, 2022

Dedication

It is with genuine gratitude and warm regard that we dedicate this work to:

My wife Sayran, my son Ibrahim and my daughter Bella

My Parents and all my family Members

All my friends in Rome and Erbil.

With love and respect.

Andam Ali Mustafa
2022

Acknowledgments

First of all, I would like to express my special appreciation and thanks to my supervisor Prof. Francesco Pappalardi, you have been a tremendous mentor for me. I would like to thank you for encouraging my research and for allowing me to grow as a research scientist especially for acquainting me with the field of ”Analytic Number Theory”. Without his guidance, this research could not have been carried out, I could not have imagined having a better supervisor and mentor for my thesis.

Secondly, I would also like to express my thankfulness to the to all the staff members of the Mathematics Department in Roma Tre and Salahaddin Universities-Erbil for their help and offering the facilities. In particular, I extend all my gratefulness and sincere thanks to Asst. Prof. Herish O. Abdullah and Dr. Valerio Talamanca. Moreover, I would like to thank everyone who helped me in performing this work.

At the end, I would like to express appreciation to my beloved wife Sayran who spent sleepless nights with me and was always my support in the moments when there was no one to answer my queries.

Andam Ali Mustafa
2022

Summary

For a given finitely generated multiplicative subgroup of the rationals which possibly contain negative numbers, we derive, subject to GRH, formulas for the densities of primes for which the index of the reduction group has a given value. likewise, We completely classify the cases of rank one, torsion groups for which the density vanishes and the the set of primes for which the index of the reduction group has a given value, is finite. For higher rank groups we propose some partial results. Additionally, we present some computations comparing the approximated density computed with primes up to 10^{10} and those predicted by the Riemann Hypothesis.

Furthermore, We compute the density of the set of primes for which the order of the reduction group is divisible by a given integer. Consequently, we consider the general case. Moreover,In the second Section of the Chapter we test our formulas with several tables.

CONTENTS

Notations and Terminology

Symbol	Description
$\mathbb{N}$	$1, 2, ...$
$\mathbb{Z}$	Is the ring of integers.
p, q, ℓ	Denotes prime numbers.
$\mathbb{Q}^*$	Is the set of non-zero rational numbers.
F_p^*	Is the multiplicative group of the field of p elements.
L/K	L Is a field extension of K.
$\mathrm{Gal}(L/K)$	Is the Galois group of the field extension L/K.
$\mathcal{O}_K$	Is the ring of integers of the field K.
$\pi(x)$	Is the prime counting function.
$Li(x) = \int_2^x \frac{dt}{log(t)}$	Is the logarithmic integral function.
GRH	Generalized Riemann Hypothesis.
$f(x) \sim g(x)$	$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$
$\mu(n)$	Is Möbius function.
$\varphi(n)$	Is Euler totient function.
$\gcd(a, b)$	Greatest common divisor of the integers $a, b \in \mathbb{Z}$

Chapter 1

Introduction:

In this dissertation, we study the generalization of the Artin's primitive root conjecture, one of the most well-known unsolved problems in number theory. This Chapter motivates the problems we are investigating, outlines our goals, and gives an account of the contribution of this dissertation. We start with some historical background.

Artin's primitive root conjecture was formulated by E. Artin in 1927 during a conversation with H. Hasse (see[7]). Indeed, the conjecture was initiated due to Gauss when he thought of the answer to a question Why does the decimal expansions of the form $1/p$, where p is prime and distinct from 2 and 5, are different? For example:

$$1/3 = 0.\overline{3} \qquad 1/11 = 0.\overline{09} \qquad 1/17 = 0.\overline{0588235294117647}$$
$$1/7 = 0.\overline{142857} \quad 1/13 = 0.\overline{076923} \quad 1/19 = 0.\overline{052631578947368421}$$

So, in articles 315-317 of his Disquisitiones Arithmeticae (1801)[8], he showed that the period length match with the order of 10 in the cyclic group $\mathbb{F}_p^*$, that means the smallest positive integer k such that $10^k \equiv 1(\bmod p)$. This integer k is the multiplicative order of 10 modulo p and is denoted by $\mathrm{ord}_p(10)$. The integer k equals the order of the subgroup generated by 10 in $\mathbb{F}_p^*$, the multiplicative subgroup of residue classes modulo p. By Lagrange's theorem we conclude that $\mathrm{ord}_p(10)|p-1$. If $\mathrm{ord}_p(10) = p-1$, we say that 10 is a primitive root $\mathrm{mod} p$.

Since primes $p > 2$ are all odd, the groups $\mathbb{F}_p^*$ all have even order, so that squares cannot be cyclic generators. Clearly too, the number -1 has order dividing 2 in $\mathbb{F}_p^*$, so that -1 cannot be a cyclic generator when $p > 3$. Thus, a necessary condition on a for there to be infinitely many primes p with primitive root a is that a should not be a square and that a should not be -1. Artin's conjecture is that these trivially necessary conditions are also sufficient:

Weak Artin's conjecture: If the integer a is not a square and not-1, then there are infinitely many primes with the primitive root a.

Artin also formulated a strong form of this conjecture:

Strong Artin's conjecture: If the integer a is not a square and not -1. Furthermore, number of primes $p \leq x$ with primitive root a assumed $\rho_a(x)$, then there is a positive number $\delta(a)$ such that

$$\rho_a(x) \sim \delta\pi(x).$$

At the very beginning, his idea is a is a primitive root $(\bmod p)$ if and only if $a^{(p-1)}/\ell \not\equiv (\bmod p)$ for all prime divisors ℓ of $(p-1)$. However, according to a principle of Dedekind, p splits completely in $F_\ell = \mathbb{Q}(\zeta_\ell, a^{1/\ell})$, where $\zeta_\ell = e^{2\pi i/\ell}$ if and only if $a^{(p-1)}/\ell \equiv (\mathrm{mod} p)$. As a result, Artin deduced that a is a primitive root $(\bmod p)$ if and only if p does not split completely in any F_ℓ. Then he knew that the prime ideal theorem gives the density of primes which split completely in F_ℓ, as

$$\frac{1}{[F_\ell : \mathbb{Q}]},$$

Hence, the probability that p does not split completely is

$$1 - \frac{1}{[F_\ell : \mathbb{Q}]}.$$

So, one would expect

$$A(a) = \prod_\ell \left(l - \frac{1}{[F_\ell : \mathbb{Q}]} \right)$$

as the density of primes for which a is a primitive root. Until 1960, this expression was thought to be plausible, Then Lehmers [18] made some numerical calculations that did not seem always match with Artin's expression. Moreover, in 1968, Heilbronn Noticed that the events

”p does not split completely in F_ℓ”

are not necessarily independent as p and ℓ range through all primes and published a corrected quantitative conjecture. However, Artin made this correction much earlier, namely in 1958 in a letter to the Lehmers in a response to a letter of the Lehmers regarding his numerical work. Artin did not publish his corrected conjecture, nor did the Lehmers refer to Artin in their paper [18], although they give the correction factor. As late as 1964 Hasse provided a correction factor in the 1964 edition of his book [12] that is incorrect if $a \equiv 1 (\mathrm{mod} 4)$ is not a prime.

In 1937, Bilharz [3] proved the function field analogue of Artin's conjecture assuming the Riemann hypothesis for congruence zeta functions, which was subsequently proved by Weil. A natural question to raise is whether Artin's original conjecture could be proved assuming the generalized Riemann hypothesis (GRH) for the number fields involved. This was answered in the affirmative by Hooley [14] in 1967.

Theorem 1.1 (C. Hooley (1967)). *Let $\pi_{\langle a \rangle}(x)$ measures the number of primes for which a rational number a a primitive root $(\bmod\, p)$ such that $a \in \mathbb{Q} - \{-1, 0, 1\}$, and assume GRH for $\mathbb{Q}(\zeta_m, a^{1/m})$ with $m \in \mathbb{N}$, and squarefree, then the strong Artin Conjecture holds:*

$$\pi_{\langle a \rangle}(x) = \delta_a \frac{x}{\log(x)} + O\left(\frac{x \log(x) \log(x)}{\log^2(x)} \right).$$

In a remarkable work from 1977, Lenstra [21] adapted Hooley's method and, assuming GRH, proved a number field analogue of AC. His far reaching result again builds on an effective Cebotarev density theorem under GRH and he produced the five condition.

The work of Hooley was generalized by several authors. In 1983, Rajiv Gupta and Ram Murty [9] proved with out any hypothesis, that three is a set of 13 numbers such that, for at least one of these 13 numbers, Artin conjecture is true. Gupta, Kumar Murty, and Ram Murty [11] subsequently reduced the size of this set to 7.

Theorem 1.2. *Given $q, r, s \in \mathbb{Z}$ multiplicatively independent, such that none of $q, r, s, -3qr, -3qs, -3rs, qrs$ is a square,then there exist $a \in \{q, r, s\}$ with*

$$\pi_{\langle a \rangle}(x) := P_a \cap [1, x] \ll \frac{x}{(\log(x))^2}$$

Moreover, there exist $g \in \{2, 3, 5\}$ such that

$$\#\{p \leq x : p > 5, \langle g \mod p \rangle = \mathbb{F}_p^*\rangle \ll \frac{\pi(x)}{\log(x)}$$

In 1986, however, Heath-Brown [13] proved (improving on earlier fundamental work by Gupta, Ram Murty and Srinivasan [10, 27]) a result which implies that there are at most two primes ℓ_1 and ℓ_2 for which $\rho(\ell_1)$ and $\rho(\ell_1)$ are finite and at most three square free numbers a_1, a_2 and a_3 for which $\rho(a_1)$, $\rho(a_2)$ and $\rho(a_3)$ are finite.

Here, we couldn't list all the names and their works, but in order to get a full figure, we refer to Moree's Survey [25].

Given an integer $m \geq 1$, the prime counting function that counts the prime numbers p for which a is a near-primitive root modulo p of index m is:

$$\pi_\Gamma(x, m) := \#\{p \leq x : p \notin \operatorname{Supp} \Gamma, [\mathbb{F}_p^* : \Gamma_p] = m\}.$$

Many of anthers assuming the GRH, an asymptotic formula for $\pi_{\langle a \rangle}(x, m)$. In particular, Lenstra, Moree, and Stevenhagen, in [19], propose a complete characterization, assuming the GRH, of the pairs (a, m) for which there are no primes $p|a$ with $\operatorname{ind}_p(a) = m$.

Theorem 1.3. *Assume the GRH for $\mathbb{Q}(\sqrt[n]{a}), n \in \mathbb{N}$. Then*

$$\pi_{\langle a \rangle}(x, m) := \pi_{\langle a \rangle}(m) \cap [1, x] = \delta_{a,m} \frac{x}{\log(x)} + O_{a,m}\left(\frac{x}{(\log(x))^2}\right)$$

where

$$\delta_{a,m} = \sum_{n \in \mathbb{N}} \frac{\mu(n)}{[\mathbb{Q}[e^{\frac{2\pi i}{mn}}, \sqrt[mn]{a}] : \mathbb{Q}]}.$$

In another direction, L. Cangelmi and F. Pappalardi in [4, 29] determined, on GRH, an asymptotic formula for $\pi_\Gamma(x, 1)$, for which Γ_p contains a primitive root modulo p. Later for the higher rank Artin Quasi-primitive root Conjecturein in 2013 F. Pappalardi and A.Susa consider $\pi_\Gamma(x, m)$ in a general context.

Theorem 1.4. *Let $\Gamma \subset \mathbb{Q}^*$ has rank $r \geq 2$, let $m \in \mathbb{N}$ and assume GRH holds for $\mathbb{Q}(\zeta_k, \Gamma^{1/k})(k \in \mathbb{N})$. Then, $\forall \epsilon > 0$ and $m \leq x^{\frac{r-1}{(r+1)(4r+2)} - \epsilon}$,*

$$P_{\Gamma,m}(x) := P_{\Gamma,m} \cap [1, x] = \left(\delta_{\Gamma,m} + O\left(\frac{1}{\log^r(x)}\right)\right)\pi(x),$$

where

$$\delta_{\Gamma,m} = \sum_{k\geq 1} \frac{\mu}{[\mathbb{Q}(\zeta_{mk}, \Gamma^{1/mk}) : \mathbb{Q}]}.$$

Moreover, they were successfully For the case when Γ contains only positive rational number, and will mention later in the Chapter 3.

The goal of this dissertation is to obtain formulas for the densities of primes for which the index of the reduction group Γ_p has a given value. Moreover, find the density of the set of primes whose the reduction group Γ_p order is divisible by a certain integer.

In chapter two, some essential notes on multiplicative groups that it will be the inception step to understanding next chapters.

In chapter three, we derive formulas for the densities of primes for which the index of the reduction group has a certain value for a given a finitely generated multiplicative subgroup of the rationals that may contain negative integers, subject to GRH. We properly categorized the cases of rank one, torsion groups for which the density vanish, and the set of primes for which the reduction group's index has a given value. We provide some partial results for higher rank groups. Furthermore, we show some comparisons between the estimated density obtained with primes up to 10^{10} and those predicted by the Riemann Hypothesis.

In chapter four, We determine the density of the set of primes for which the order of the reduction group is divisible by a specified integer given a finitely generated multiplicative group of rational numbers. Moreover, we use many tables to test our formulas.

In Chapter 5, we will mention future work that will be about Densities related to average order of subgroups of $\mathbb{Q}^*$.

Chapter 2

Notes on Multiplicative Groups:

Let K be a number field and let Γ be a multiplicative subgroup of K^*. As usual we say that Γ is *finitely generated* if there exists $\alpha_1, \dots, \alpha_n \in \Gamma$ such that every other $\alpha \in \Gamma$ can be written in the form

$$\alpha = \alpha_1^{m_1} \cdots \alpha_n^{m_n} \qquad \text{with} \quad m_1, \dots, m_n \in \mathbb{Z}.$$

In such a case we write $\Gamma = \langle \alpha_1, \dots, \alpha_n \rangle$ and we refer to $\alpha_1, \dots, \alpha_r$ as *generators* of Γ. From the general theory of finitely generated groups, we know that if Γ is finitely generated, then

$$\Gamma \cong \mathbb{Z}^r \oplus T$$

where $r := \operatorname{rank} \Gamma$ is the *rank* and

$$T = \operatorname{Tor} \Gamma = \{\tau \in \Gamma : \tau^m = 1 \quad \text{for some } m \in \mathbb{N}\}$$

is the *torsion subgroup* of Γ. A *$\mathbb{Z}$–basis (modulo torsion)* if Γ is an ordered set of elements $(\gamma_1, \dots, \gamma_r)$ of Γ, such that for every $\alpha \in \Gamma$ there exists unique $m_1, \dots, m_r \in \mathbb{Z}$ and $\epsilon \in \operatorname{Tor} \Gamma$ such that $\alpha = \epsilon \cdot \gamma_1^{m_1} \cdots \gamma_r^{m_r}$. The elements of a $\mathbb{Z}$–basis are *multiplicatively independent* (i.e. $\gamma_1^{m_1} \cdots \gamma_r^{m_r} \in \operatorname{Tor} \Gamma$ with $m_1, \dots, m_r \in \mathbb{Z}$, implies $(m_1, \dots, m_r) = (0, \dots, 0)$). Viceversa, a set of multiplicatively independent generators forms a $\mathbb{Z}$–basis.

The torsion subgroup of Γ is known to be cyclic and we denote by ω_Γ its order. We say that Γ is *torsion free* if $\operatorname{Tor} \Gamma$ is trivial. In the event that K has at least one real embedding, we have that $\operatorname{Tor} \Gamma \subset \{-1, 1\}$. We also say that Γ is *unit–free* if it does not contain any infinite order unit of $\mathcal{O}_K^*$ (i.e. if $\Gamma \cap \mathcal{O}_K^* = \operatorname{Tor} \Gamma$). If $K = \mathbb{Q}$ or if K is an immaginary quadratic field, then necessarily every subgroup of K^* is unit–free. On the opposite side, we say that Γ is *unit–full* if $\mathcal{O}_K^* \subset \Gamma$.

We define *support* if Γ the following finite set of prime ideal of $\mathcal{O}_K$:

$$\operatorname{supp} \Gamma := \{\mathfrak{p} \text{ prime ideal of } \mathcal{O}_K : v_\mathfrak{p}(\alpha) \neq 0 \text{ for some } \alpha \in \Gamma\}.$$

Here $v_\mathfrak{p}(\alpha)$ denotes that $\mathfrak{p}$–*adic valuation* of α (i.e. if $(\alpha) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s}$ is the (unique) decomposition of the principal fractional ideal of K, (α) as the product of distinct prime powers, then $v_\mathfrak{p}(\alpha) = e_j$ if $\mathfrak{p} = \mathfrak{p}_j$ for some j and $v_\mathfrak{p}(\alpha) = 0$ otherwise).

If Γ is finitely generated, the support of Γ is finite. In fact, if $\alpha_1, \dots, \alpha_n \in \Gamma$ is a set of generators, then it is clear that a prime $\mathfrak{p}$ is in the support if and only if $v_\mathfrak{p}(\alpha_j) \neq 0$ for some $j = 1, \dots, n$. Furthermore we have the following

Proposition 2.1. *Let K be a number field and let $\Gamma \subset K^*$ be a unit–free finitely generated multiplicative subgroup. Then*

$$\operatorname{rank}\Gamma \geq \#\operatorname{supp}\Gamma.$$

Proof. Let $r = \operatorname{rank}\Gamma$ and $s = \#\operatorname{supp}\Gamma$. Suppose that $\gamma_1 \ldots, \gamma_r \in \Gamma$ is a $\mathbb{Z}$*–basis* of Γ. Also write $\operatorname{supp}\Gamma = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$ so that for all j, $(\gamma_j) = \mathfrak{p}_1^{e_{j1}} \cdots \mathfrak{p}_s^{e_{js}}$. If it was that $s > r$, then the matrix

$$E = E_{\gamma_1,\ldots\gamma_r} = \begin{pmatrix} e_{11} & \cdots & e_{1s} \\ \vdots & & \vdots \\ e_{r1} & \cdots & e_{rs} \end{pmatrix} \tag{2.1}$$

would have rank smaller or equal than r. This implies that there is a non trivial linear combination of the raws of E that vanishes. Hence there are integers $m_1, \ldots, m_r$ not all zero. such that

$$(\gamma_1)^{m_1} \cdots (\gamma_R)^{m_r} = (1).$$

Hence $\epsilon = \gamma_1^{m_1} \cdots \gamma_r^{m_r} \in \mathcal{O}_K^*$. Since $\mathcal{O}_K^* \cap \Gamma = \operatorname{Tor}\Gamma$, $\gamma_1, \ldots, \gamma_r$ are *multiplicatively dependent.* This is a contraddiction to the fact that $\gamma_1 \ldots, \gamma_r \in \Gamma$ is a $\mathbb{Z}$*–basis* of Γ. □

The following definition will be crucial for the application in the sequel.

Definition 2.2. Suppose $\Gamma = \langle \alpha_1, \ldots, \alpha_t \rangle \subset K^*$ is a finitely generated multiplicative subgroup, that $\operatorname{supp}\Gamma = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$ is the support and that the ordering of its elements is fixed. Let

$$E = E_{\alpha_1,\ldots\alpha_t} = \Big(e_{ij}\Big)_{\substack{i=1,\ldots,t \\ j=1,\ldots,s}}$$

be the matrix with integer entries defined (as in (2.1)) by $(a_j) = \mathfrak{p}_1^{e_{j1}} \cdots \mathfrak{p}_s^{e_{js}}$.

For any $j = 1, \ldots, \min\{s, t\}$, we define the *$j$–th elementary discriminant divisor* $\Delta_j = \Delta_j(\alpha_1, \ldots, \alpha_t)$ as the greatest common divisor of the determinants of all the $j \times j$ minors of E. We also define $\Delta_j(\alpha_1, \ldots, \alpha_t) := 0$ for $j > \min\{s, t\}$.

The *Smith Normal Form* provides an efficient way to compute the elementary discriminant divisor. Given E, nonzero $m \times n$ matrix with integer entries. There exist invertible $m \times m$ and $n \times n$ matrices with integer entries (i.e. ±1 determinant) S, T so that the product

$$SET = \begin{pmatrix} e_1 & 0 & \cdots & 0 & \\ 0 & \ddots & & 0 & \\ \vdots & & e_r & \vdots & \\ 0 & & 0 & 0 & \\ 0 & & 0 & \ddots & \end{pmatrix}.$$

and the diagonal elements e_i are unique up to sign and satisfy $e_i \mid e_{i+1} \ \forall\ 1 \leq i < r$. Finally

$$\Delta_i = e_1 \cdots e_i.$$

From the Smith Normal Form decomposition, the basic properties of the elementary discriminant divisor are easily derived:

1. if $j > \operatorname{rank}\Gamma$, then $\Delta_j(\alpha_1, \ldots, \alpha_t) = 0$. In fact $r = \operatorname{rank}\Gamma$ is the largest index r such that $\Delta_r \neq 0$.
2. If $\Gamma = \langle \beta_1, \ldots, \beta_u \rangle$, then for all j

$$\Delta_j(\alpha_1, \ldots, \alpha_t) = \Delta_j(\beta_1, \ldots, \beta_u)$$

Hence the elementary discriminant divisor do not depend on the set of generators for Γ nor on the ordering of $\operatorname{supp}\Gamma$ chosen to define them. For this reason we shall denote the *j–th elementary discriminant divisor* by Δ_j.

3. $\Delta_{j_1} \cdot \Delta_{j_2} \mid \Delta_{j_1+j_2}$.

If $\Gamma \subset K^*$ is not finitely generated, the elementary discriminant divisor $(\Delta_j)_{j\in\mathbb{N}}$ could be defined is the natural way and they would costitute an infinite sequence of non negative integers.

Proposition 2.3. *Given $\Gamma \subset \mathbb{Q}^+$ finitely generated subgroup of rank r and $m \in \mathbb{N}$, we set*

$$\Gamma(m) := {}^{\Gamma \cdot (\mathbb{Q}^*)^m}\Big/_{(\mathbb{Q}^*)^m}.$$

Then

$$\#\Gamma\,(m) = \frac{m^r}{\gcd(m^r, m^{r-1}\Delta_1, \ldots, m\Delta_{r-1}, \Delta_r)}. \tag{2.2}$$

Proof. Since

$$\Gamma(m) \cong \prod_{\ell \mid m} \Gamma(\ell^{v_\ell(m)}),$$

and since the right hand side of the formula in (2.2) is multiplicative, it is enough to prove (2.2) in the case when m is the power of a prime ℓ. Let $\{p_1, \ldots, p_s\}$ be the support of Γ. Then

$$\begin{aligned}\Gamma(\ell^a) &= \frac{\langle a_1, \ldots, a_r, p_1^{\ell^a}, \ldots, p_s^{\ell^a}\rangle}{\langle p_1^{\ell^a}, \ldots, p_s^{\ell^a}\rangle} \\ &\cong \frac{\langle p_1, \ldots, p_s\rangle}{\langle p_1^{\ell^a}, \ldots, p_s^{\ell^a}\rangle} \Bigg/ \frac{\langle p_1, \ldots, p_s\rangle}{\langle a_1, \ldots, a_r, p_1^{\ell^a}, \ldots, p_s^{\ell^a}\rangle}.\end{aligned}$$

It is clear that $\langle p_1, \ldots, p_s\rangle / \langle p_1^{\ell^a}, \ldots, p_s^{\ell^a}\rangle$ has ℓ^{as} elements. We need to determine the size of the quotient $\langle p_1, \ldots, p_s\rangle / \langle a_1, \ldots, a_r, p_1^{\ell^a}, \ldots, p_s^{\ell^a}\rangle$. We consider the relations matrix $N = E_{a_1,\ldots,a_r,p_1^{\ell^a},\ldots,p_s^{\ell^a}}$ and $M =$

$E_{a_1,\ldots,a_r}$, then $N = (MmI_s)$. By the argument above, it follows that

$$\left|\frac{\langle p_1, \ldots, p_s\rangle}{\langle a_1, \ldots, a_r, p_1^{\ell^a}, \ldots, p_s^{\ell^a}\rangle}\right| = \ell^{a(s-r)}\,\mathrm{gcd}(\ell^{ar}, \ell^{a(r-1)}\Delta_1, \ldots, \ell^a\Delta_{r-1}, \Delta_r).$$

Hence the claim. □

Chapter 3

Densities of the "quasi r–rank Artin problem":

3.1 Introduction

The results of the present Chapter appeared in an article by Herish O. Abdullah, Andam Ali Mustafa and Francesco Pappalardi that was published in Funct. Approximation, Comment. Math. 65 No.1 73-93 (2021).

Let $\Gamma \subset \mathbb{Q}^*$ be a finitely generated multiplicative subgroup. We denote by $\operatorname{Supp}\Gamma$, the *support* of Γ, i.e. the finite set of those primes ℓ such that the ℓ–adic valuation of some elements of Γ is nonzero.

For any prime $p \notin \operatorname{Supp}\Gamma$, we can define the reduction group:

$$\Gamma_p = \{\gamma \bmod p : \gamma \in \Gamma\} \subset \mathbb{F}_p^*$$

and the prime counting function:

$$\pi_\Gamma(x, m) := \#\{p \leq x : p \notin \operatorname{Supp}\Gamma, [\mathbb{F}_p^* : \Gamma_p] = m\}.$$

We also define the density (if it exists) as

$$\rho(\Gamma, m) = \lim_{x \to \infty} \frac{\pi_\Gamma(x, m)}{\pi(x)}$$

which exists under the Generalized Riemann Hypothesis and it can be expressed by the following formula (see [31], [4], [32], [24]):

$$\rho(\Gamma, m) = \sum_{k \geq 1} \frac{\mu(k)}{[\mathbb{Q}(\zeta_{mk}, \Gamma^{1/mk}) : \mathbb{Q}]}. \tag{3.1}$$

Here $\zeta_d = e^{2\pi i/d}$ and $\Gamma^{1/d}$ denotes the set of real numbers α such that $\alpha^d \in \Gamma$.

If $\Gamma = \langle a \rangle$ with $a \in \mathbb{Q} \setminus \{-1, 0, 1\}$, the density in question is the density of primes p for which the index of a modulo p equals m. In the case $m = 1$, the statement that for a not a perfect square, $\rho(\langle a \rangle, 1)$ exists and it is not zero, is known as the classical Artin Conjecture for primitive roots which, in 1965, was shown, by C. Hooley [14], to be a consequence of the GRH. Hooley gave a formula for $\rho(\langle a \rangle, 1)$ in terms of an euler product which is consistent with (4.1).

If we write $a = \pm b^h$ with $b > 0$ not an exact power of a rational number, $d = \operatorname{disc}(\mathbb{Q}(\sqrt{b}))$ and $F_\ell = \mathbb{Q}(\zeta_\ell, a^{1/\ell})$ so that

$$[F_\ell : \mathbb{Q}] = \begin{cases} \ell(\ell-1)/\gcd(h, \ell) & \text{if } \ell > 2 \text{ or } a > 0 \\ 2 & \text{if } \ell = 2 \text{ and } a < 0, \end{cases}$$

then:

$$\rho(\langle a\rangle,1)=\left(1-\frac{1-(-1)^{hd}}{2}\prod_{\ell|d}\frac{-1}{[F_\ell:\mathbb{Q}]-1}\right)\times\prod_{\ell}\left(1-\frac{1}{[F_\ell:\mathbb{Q}]}\right).$$

In the above and in the sequel, ℓ will always denote prime numbers. The case when $m\geq 1$ has been considered by various authors [26],[15], [23]. In particular (Moree [23, Corollary 2.2]), if m is **odd**, then

$$\rho(\langle a\rangle,m)=\left(1-\frac{1-(-1)^{hd}}{2}\prod_{\substack{\ell|d\\ \ell\nmid 2m}}\frac{-1}{[F_\ell:\mathbb{Q}]-1}\right)\frac{(m,h)}{m^2}\times\prod_{\substack{\ell|m\\ h_\ell|m_\ell}}\left(1+\frac{1}{\ell}\right)\times\prod_{\ell\nmid m}\left(1-\frac{1}{[F_\ell:\mathbb{Q}]}\right). \tag{3.2}$$

In the above and in the sequel, m_ℓ will always denote the ℓ–part of m (i.e. $m_\ell=\ell^{v_\ell(m)}$ where v_ℓ is the ℓ–adic valuation). A formula for the remaining case, m **even**, can be found in [23, Theorem 2.2].

The case when the rank of Γ is greater than 1 was considered in [4, 24, 32, 29]. For $\Gamma\subset\mathbb{Q}^*$ finitely generated subgroup and $m\in\mathbb{N}$, we set $\Gamma(m):=\Gamma\cdot\mathbb{Q}^{*m}/\mathbb{Q}^{*m}$ and

$$A(\Gamma,m)=\frac{1}{\varphi(m)|\Gamma(m)|}\times\prod_{\substack{\ell>2\\ \ell|m}}\left(1-\frac{|\Gamma(m_\ell)|}{\ell|\Gamma(\ell m_\ell)|}\right)\times\prod_{\substack{\ell>2\\ \ell\nmid m}}\left(1-\frac{1}{(\ell-1)|\Gamma(\ell)|}\right). \tag{3.3}$$

For $\gamma\in\Gamma(m)$, $\gamma'\in\mathbb{Z}$ denotes the unique, up to sign, m–power free representative of γ ($\gamma=\gamma'\cdot\mathbb{Q}^{*m}$). The sign of γ' is chosen to be positive if m is odd or if $\gamma=\gamma'\cdot\mathbb{Q}^{*m}\subset\mathbb{Q}^+:=\{q\in\mathbb{Q}:q>0\}$ and is negative otherwise. If $\alpha>0$ and $\gamma\in\Gamma(2^\alpha)[2]$ (the 2-torsion subgroup of $\Gamma(2^\alpha)$) with $\gamma\neq\mathbb{Q}^{*2^\alpha}$, then $\gamma'=\pm\gamma_0^{2^{\alpha-1}}$ with $\gamma_0\in\mathbb{N},\gamma_0>1$ square free. We shall denote by $\delta(\gamma)=\operatorname{disc}\mathbb{Q}(\sqrt{\gamma_0})$ which is easily seen to depend only on γ.

For $\Gamma\subset\mathbb{Q}^+$, we define:

$$\tilde\Gamma(m):=\{\gamma\in\Gamma(m_2)[2]:v_2(\delta(\gamma))\leq v_2(m)\}. \tag{3.4}$$

It is easy to check that $\tilde\Gamma(m)$ is a 2–group and if $\Gamma\subset\mathbb{Q}^+$, then

$$\tilde\Gamma(m)=\begin{cases}\{1\} & \text{if } 2\nmid m\\ \{\gamma\in\Gamma(2):\gamma'\equiv 1\bmod 4\} & \text{if } 2\|m\\ \{\gamma\in\Gamma(4)[2]:2\nmid\gamma_0\} & \text{if } 4\|m\\ \Gamma(m_2)[2] & \text{if } 8\|m.\end{cases} \tag{3.5}$$

The group $\tilde\Gamma(m)$ will be defined also in the case when $\Gamma\not\subseteq\mathbb{Q}^+$ in (3.8).

Finally, we set:

$$B_{\Gamma,k} = \sum_{\gamma \in \tilde{\Gamma}(k)} \prod_{\substack{\ell \mid \delta(\gamma) \\ \ell \nmid k}} \frac{-1}{(\ell-1)|\Gamma(\ell)|-1}. \tag{3.6}$$

For the special case when Γ contains only positive rational numbers, in [32], it was proved the following:

Theorem 3.1. *Let $\Gamma \subset \mathbb{Q}^+$ be multiplicative subgroup of rank r and let $m \in \mathbb{N}$. Then*

$$\rho(\Gamma, m) = A(\Gamma, m) \times \left(B_{\Gamma,m} - \frac{|\Gamma(m_2)|}{(2,m)|\Gamma(2m_2)|} B_{\Gamma,2m} \right)$$

where $A(\Gamma, m)$ is defined as in (3.3) and $B_{\Gamma,k}$ is defined as in (3.6).

Note that, for m odd, $B_{\Gamma,m} = 1$ and the formula above specializes to

$$\begin{aligned} \rho(\Gamma, m) &= \frac{1}{\varphi(m)|\Gamma(m)|} \prod_{\ell \mid m} \left(1 - \frac{|\Gamma(m_\ell)|}{\ell |\Gamma(\ell m_\ell)|}\right) \prod_{\ell \nmid m} \left(1 - \frac{1}{(\ell-1)|\Gamma(\ell)|}\right) \times \\ &\quad \times \left(1 + \sum_{\substack{\gamma \in \Gamma(2) \setminus \{\mathbb{Q}^{*2}\} \\ \delta(\gamma) \equiv 1 \bmod 4}} \prod_{\substack{\ell \mid 2\delta(\gamma) \\ \ell \nmid m}} \frac{-1}{(\ell-1)|\Gamma(\ell)|-1} \right) \end{aligned} \tag{3.7}$$

which, for $m = 1$, should be compared with [24, 4.6. Theorem]. Furthermore, one can check that the formula in the above result from [32] coincides with that of Moree's [23, Theorem 2.2] in the case when $\Gamma = \langle a \rangle$ with $a \in \mathbb{Q}^+, a \neq 1$.

The goal of this Chapter is to extend the above Theorem by removing the constraint that $\Gamma \subset \mathbb{Q}^+$. We prove the following:

Theorem 3.2. *Let $\Gamma \subset \mathbb{Q}^*$ be multiplicative subgroup of rank $r \geq 1$ and let $m \in \mathbb{N}$. Let*

$$\tilde{\Gamma}(m) = \left\{ \gamma \in \Gamma(m_2)[2] : \begin{array}{l} \textit{if } \gamma \subset \mathbb{Q}^+ \textit{ then } v_2(\delta(\gamma)) \leq v_2(m); \\ \textit{if } \gamma \not\subseteq \mathbb{Q}^+ \textit{ then } v_2(\delta(\gamma)) = v_2(m) + 1 \end{array} \right\}. \tag{3.8}$$

Then, with $A(\Gamma, m)$ defined as in (3.3) and $B_{\Gamma,k}$ defined as in (3.6),

$$\rho(\Gamma, m) = A(\Gamma, m) \left(B_{\Gamma,m} - \frac{|\Gamma(m_2)|}{(2,m)|\Gamma(2m_2)|} B_{\Gamma,2m} \right).$$

Clearly, the definition of $\tilde{\Gamma}(m)$ in Theorem 3.2 reduces to the one in (3.4) when $\Gamma \subset \mathbb{Q}^+$. Furthermore, it is not hard to verify that:

$$\tilde{\Gamma}(m)=\begin{cases}\{1\} & \text{if } 2\nmid m;\\ \{\gamma\in\Gamma(2):\gamma'\equiv 1 \bmod 4\} & \text{if } 2\|m;\\ \{\gamma\in\Gamma(4):\text{either } \gamma'=\gamma_0^2, 2\nmid\gamma_0 \text{ or } \gamma'=-\gamma_0^2, 2\mid\gamma_0\} & \text{if } 4\|m;\\ \Gamma(m_2)[2]\cap\mathbb{Q}^+ & \text{if } 8\mid m.\end{cases} \tag{3.9}$$

Hence $\tilde{\Gamma}(m)$ is also a 2–group. The above identity should be compared with (3.5). If m is odd, then the formula for $\rho(\Gamma,m)$ in the statement of Theorem 3.2 simplifies to the same as in (3.7).

In Section 3.4 we specialize to the case when $\Gamma=\langle -1,a\rangle$ where $a\in\mathbb{Q}^*\setminus\{0,1,-1\}$ can be assumed to be positive. We deduce from Theorem 3.2 an explicit formulas for $\rho_{\langle -1,a\rangle,m}$ which is used in Section 3.5 to prove the following:

Theorem 3.3. *Let $a\in\mathbb{Q}^+, a\neq 1$, write $a=a_0^h$, where $a_0\in\mathbb{Q}^+$ not the exact power of any rational number and write $a_0=a_1a_2^2$ where $a_1>1$ is uniquely defined by the property to be a positive square free integer. The density $\rho(\langle -1,a\rangle,m)=0$ if and only if one of the following two (mutually exclusive) cases is verified:*

1. $3\mid h, 3\nmid m, 3\mid a_1, a_1\mid 3m, \quad 2\nmid h, 2\|m, 2\nmid a_1$;
2. $3\mid h, 3\nmid m, 3\mid a_1, a_1\mid 3m, \quad v_2(h)<v_2(m)\neq 1$.

Furthermore, on GRH, the set $\{p:\left[\mathbb{F}_p^*:\langle -1,a\rangle_p\right]=m\}$ is finite if and only if one of the above two conditions is satisfied.

Examples of pairs (a,m) satisfying 1. of Theorem 3.3 are $(a,m)=(3^3,2),(15^3,10),\cdots$ and examples of pairs satisfying 2. are $(a,m)=(3^6,4),(15^{12},40),\cdots$. A list of more values of (a,m) is presented in the second table of Section 3.7.

Next, in Section 3.6, we investigate the identity

$$\rho(\Gamma,m)=0$$

and the problem of determining whether

$$\mathcal{N}_{\Gamma,m}=\{p\notin\operatorname{Supp}\Gamma,\operatorname{ind}_p\Gamma=m\}$$

is finite.

If $\Gamma=\langle g\rangle$ with $g\in\mathbb{Q}\setminus\{0,1,-1\}$, this problem has been solved (on GRH) by Lenstra [20, (8.9)–(8.13)] (see also [23]). In fact,

Theorem 3.4. *Lenstra [23, Theorem 4] Let $g\in\mathbb{Q}\setminus\{-1,0,1\}$ and write $g=\pm g_0^h$, where $g_0\in\mathbb{Q}^+$ is not the power of any rational number. The density $\rho(\langle g\rangle,m)=0$ if and only if we are in one of the following six (mutually exclusive) cases:*

1. $2\nmid m$, $\operatorname{disc}(\mathbb{Q}(\sqrt{g}))\mid m$;

2. *$g > 0$, $v_2(m) > v_2(h)$, $3 \mid h$, $3 \nmid m$, $\operatorname{disc}(\mathbb{Q}(\sqrt{-3g_0})) \mid m$;*
3. *$g < 0$, $2 \nmid h$, $2 \| m$, $3 \nmid m$, $3 \mid h$, $\operatorname{disc}(\mathbb{Q}(\sqrt{3g_0})) \mid m$;*
4. *$g < 0$, $2\|h$, $2\|m$, $\operatorname{disc}(\mathbb{Q}(\sqrt{2g_0})) \mid 2m$;*
5. *$g < 0$, $2\|h$, $4\|m$, $3 \mid h$, $3 \nmid m$, $\operatorname{disc}(\mathbb{Q}(\sqrt{-6g_0})) \mid m$;*
6. *$g < 0$, $v_2(m) > 1 + v_2(h)$, $3 \mid h$, $3 \nmid m$, $\operatorname{disc}(\mathbb{Q}(\sqrt{-3g_0})) \mid m$.*

Furthermore, on GRH, $\mathcal{N}_{\langle g\rangle,m}$ is finite if and only if one of the above two conditions is satisfied.

In the higher rank case, we partially generalize the above in the following way:

Theorem 3.5. *Let $\Gamma \subset \mathbb{Q}^*$ be a non–trivial, finitely generated subgroup and let $m \in \mathbb{N}$. Then $\rho(\Gamma, m) = 0$ when one of the following three conditions is satisfied:*

A. $2 \nmid m$ and for all $g \in \Gamma, \operatorname{disc}(\mathbb{Q}(\sqrt{g})) \mid m$;
B. $2 \mid m$, $3 \nmid m$, $\Gamma(3)$ is trivial and there exists $\gamma_1 \in \tilde{\Gamma}(m)$ such that $3 \mid \delta(\gamma_1) \mid 6m$.
C. $2\|m$, $|\Gamma(2)| = 2, \tilde{\Gamma}(2m) = \Gamma(4)$ and for all $\gamma \in \tilde{\Gamma}(2m)$, $\delta(\gamma) \mid 4m$.

Remark. Regarding the last property of Theorem 3.5, note that Γ and m satisfy $2\|m$, then

$$|\Gamma(2)| = 2 \qquad \text{and} \qquad \tilde{\Gamma}(2m) = \Gamma(4)$$

if and only if

1. $\Gamma(2) = \{\mathbb{Q}^{*2}, -\mathbb{Q}^{*2}\}$;
2. the elements of $\Gamma(4)$ are of the form $\gamma_0^2\mathbb{Q}^{*4}$ or $-4\gamma_0^2\mathbb{Q}^{*4}$ with $\gamma_0 \in \mathbb{N}$ odd and square free;
3. $\Gamma(4)$ contains at least one element on the second form.

In fact, if $g\mathbb{Q}^{*2} \in \Gamma(2)$ with $g \in \Gamma$ and $|g|$ not a perfect square, then $g\mathbb{Q}^{*4} \in \Gamma(4)$ is an element of order 4 so that $\tilde{\Gamma}(2m)$ is proper subgroup of $\Gamma(4)$. The form of $\tilde{\Gamma}(m)$ is described in (3.9). Finally, at least one of the elements has to be of the form $-4\gamma_0^2\mathbb{Q}^{*4}$, otherwise $\Gamma(2) = \{\mathbb{Q}^{*2}\}$.

The result in Theorem 3.5 is compatible with the result of Lenstra. In fact

Proposition 3.6. *Suppose $\Gamma = \langle g\rangle$ and $m \in \mathbb{N}$. Then condition A. of Theorem 3.5 reduces to condition 1. of Lenstra's Theorem, condition C. reduces to condition 4 and condition B. reduced to one of conditions 2, 3, 5 or 6 according to the following:*

2.	*if $g > 0$*
3.	*if $g < 0$, $v_2(m) = 1$ and $v_2(h) = 0$*
5.	*if $g < 0$, $v_2(m) = 2$ and $v_2(h) = 1$*
6.	*if $g < 0$ and $v_2(m) > v_2(h) + 1$*

where $g = \pm g_0^h$ with $g_0 \neq 1$ not the power of a rational number.

When $\operatorname{rank}\Gamma > 2$, we do not know in general if $\rho(\Gamma, m) = 0$ implies that at least one of the conditions of Theorem 3.5 is satisfied. Possibly the approach due to Lenstra, Moree and Stevenhagen [19] could provide a complete characterization of the pairs Γ, m with $\rho(\Gamma, m) = 0$ also in the case when Γ contains some negative rational numbers. The techniques of [19] have been adapted to the context of higher rank groups by Moree and

Stevenhagen in [24] where the case $m = 1$ is considered. On the other hand, a least in the case when m is odd, condition 1. of Theorem 3.5 is also necessary. In fact we have the following:

Proposition 3.7. *Assume that* $2 \nmid m$ *and* $\rho(\Gamma, m) = 0$. *Then condition 1. of Theorem 3.5 is satisfied.*

We conclude with the following:

Proposition 3.8. *Assume that* $\Gamma \subset \mathbb{Q}^*$ *and* m *satisfy one of the three conditions of Theorem 3.5, then* $\mathcal{N}_{\Gamma,m}$ *is finite. In particular, on GRH, if* $2 \nmid m$,

$$\mathcal{N}_{\Gamma,m} \textit{ finite} \iff \forall \gamma {\mathbb{Q}^*}^2 \in \Gamma(2), \operatorname{disc}(\mathbb{Q}(\sqrt{\gamma})) \mid m.$$

3.2 The degree of Kummer extensions

In this section we determine an explicit formula for the order of the Galois group

$$\#\operatorname{Gal}(\mathbb{Q}(\zeta_m, \Gamma^{1/d})/\mathbb{Q}) = [\mathbb{Q}(\zeta_m, \Gamma^{1/d}) : \mathbb{Q}]$$

where $d \mid m$, $\zeta_m = e^{2\pi i/m}$ and $\Gamma^{1/d} = \{\sqrt[d]{\alpha} \in \mathbb{R} : \alpha \in \Gamma\}$.

By the standard properties of Kummer extensions (see for example [17, Theorem 8.1]), if we denote by $K_m = \mathbb{Q}(\zeta_m)$ the cyclotomic field, we have that

$$\operatorname{Gal}(K_m(\Gamma^{1/d})/K_m) \cong \Gamma(d)/\tilde{\Gamma}_{m,d} \tag{3.10}$$

where $\Gamma(d) := \Gamma \cdot \mathbb{Q}^{*d}/\mathbb{Q}^{*d}$ and $\tilde{\Gamma}_{m,d} := \left(\Gamma \cdot \mathbb{Q}^{*d} \cap {K_m^*}^d\right)/\mathbb{Q}^{*d}$. Note that if $d > 1$ is odd, then ${K_m^*}^d \cap \mathbb{Q}^* = \mathbb{Q}^{*d}$, and

$$\tilde{\Gamma}_{m,d} \cong \prod_{\ell \mid d} \tilde{\Gamma}_{m,d_\ell} = \tilde{\Gamma}_{m,d_2}.$$

We recall that for $\gamma \in \Gamma(d)$, $\gamma' \in \mathbb{Z}$ denotes the unique, up to sign, d–power free representative of γ ($\gamma = \gamma' \cdot \mathbb{Q}^{*d}$). The sign of γ' is chosen to be positive if d is odd or if $\gamma = \gamma' \cdot \mathbb{Q}^{*d} \subset \mathbb{Q}^+$ and is negative otherwise. Therefore

$$\tilde{\Gamma}_{m,2^\alpha} = \{\gamma \in \Gamma(2^\alpha) : \; \gamma' \in \Gamma \cdot {\mathbb{Q}^*}^{2^\alpha} \cap {K_m^*}^{2^\alpha}\}. \tag{3.11}$$

It was observed in [31, Corollary 1] that, for $2^\alpha \mid m$,

$$\text{if } \Gamma \subset \mathbb{Q}^+ \qquad \text{then} \qquad \tilde{\Gamma}_{m,2^\alpha} = \{\gamma \in \Gamma(2^\alpha)[2] : \delta(\gamma) \mid m\}. \tag{3.12}$$

In fact, if $\Gamma \subset \mathbb{Q}^+$ and $\gamma' \in \Gamma(2^\alpha)[2]$, then $\gamma' = \gamma_0^{2^{\alpha-1}}$ and $\delta(\gamma) = \operatorname{disc}\mathbb{Q}(\sqrt{\gamma_0})$ divides m if and only if $\gamma' \in {K_m^*}^{2^\alpha}$ (see for example Weiss [36, page 264]).

Furthermore, if $\alpha = 0$, then $\tilde{\Gamma}_{m,1}$ is the trivial group and in [4, page 124, (24)] is was proven that if $\alpha = 1$

then,

$$\text{if } m \text{ is squarefree} \quad \text{then} \quad \tilde{\Gamma}_{m,2} = \{\gamma \in \Gamma(2) : \operatorname{disc}\mathbb{Q}(\sqrt{\gamma'}) \mid m \text{ and } \operatorname{disc}\mathbb{Q}(\sqrt{\gamma'}) \equiv 1 (\bmod 4)\}. \quad (3.13)$$

Note that for $4 \nmid m$, the condition $\operatorname{disc}\mathbb{Q}(\sqrt{\gamma'}) \equiv 1(\bmod 4)$ above is irrelevant as it is implied by the condition that $\operatorname{disc}\mathbb{Q}(\sqrt{\gamma'}) \mid m$. Hence, for m square free, the formula in (3.13) and that in (3.12) coincide.

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

Proposition 3.1. *Let $\Gamma \subset \mathbb{Q}^*$ be a finitely generated subgroup, let $m \in \mathbb{N}$ be even. Then*

$$\tilde{\Gamma}_{m,2} = \{\gamma \in \Gamma(2) : \operatorname{disc}\mathbb{Q}(\sqrt{\gamma'}) \mid m\}$$

Although the proof of the Proposition is the same as the proof of Corollary 1 in [31], we add it here for completeness.

Proof of the Proposition. Let us start from the definition in (3.11):

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

where $K_m = \mathbb{Q}(\zeta_m)$. If $\gamma' \in \Gamma \cdot \mathbb{Q}^{*2}$ is a squarefree integer, then $\gamma' \in {K_m^*}^2$ if and only if $\sqrt{\gamma'} \in {K_m}^*$ and this happens if and only if $\operatorname{disc}\mathbb{Q}(\sqrt{\gamma'}) \mid m$ (see for example Weiss [36, page 264]). This completes the proof. □

We have the general

Lemma 3.2. *Let $\Gamma \subset \mathbb{Q}^*$ be a finitely generated group. Let $m \in \mathbb{N}$ and let $\alpha \in \mathbb{N}$, $\alpha \neq 0$ be such that $2^\alpha \mid m$. Finally set*

$$\tilde{\Gamma}^+_{m,2^\alpha} = \{\gamma \in \Gamma(2^\alpha)[2] : \gamma \subset \mathbb{Q}^+, \delta(\gamma) \mid m\}$$

and

$$\tilde{\Gamma}^-_{m,2^\alpha} = \begin{cases} \{\gamma \in \Gamma(2^\alpha)[2] : \gamma \not\subseteq \mathbb{Q}^+, \delta(\gamma) \mid m\} & \text{if } 2^{\alpha+1} \mid m \\ \{\gamma \in \Gamma(2^\alpha)[2] : \gamma \not\subseteq \mathbb{Q}^+, \delta(\gamma) \mid 2m \text{ but } \delta(\gamma) \nmid m\} & \text{if } 2^\alpha \| m \end{cases}$$

where, if $\gamma' = \pm\gamma_0^{2^{\alpha-1}}$, $\delta(\gamma) := \operatorname{disc}(\mathbb{Q}(\sqrt{\gamma_0})$. Then

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

The proof is, in spirit, the same as the proof of [34, Lemma 4].

Proof. We start from the definition:

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

Suppose first $\gamma = \gamma'\mathbb{Q}^{*2^\alpha} \subset \mathbb{Q}^+$ with $\gamma' \in \mathbb{N}$, 2^α–power free and that $\sqrt[2^\alpha]{\gamma'} \in \mathbb{Q}(\zeta_m)$. Then $\mathbb{Q}(\sqrt[2^\alpha]{\gamma'})$ is a Galois, real, extension of $\mathbb{Q}$ and this can only happen if its degree over $\mathbb{Q}$ is at most 2. Hence $\gamma' = \gamma_0^{2^{\alpha-1}}$ for some square free $\gamma_0 \in \mathbb{N}$ so that $\delta(\gamma) = \operatorname{disc}\mathbb{Q}(\sqrt{\gamma_0}) \mid m$ and $\gamma \in \Gamma(2^\alpha)[2]$. Hence $\gamma \in \tilde{\Gamma}^+_{m,2^\alpha}$.

Next suppose that $\gamma = \gamma'\mathbb{Q}^{*2^\alpha} \not\subseteq \mathbb{Q}^+$, $\gamma' \in \mathbb{Z}$ and $\gamma' < 0$. The condition $\gamma' \in {K_m^*}^{2^\alpha}$ implies that $\gamma'^2 \in {K_m^*}^{2^{\alpha+1}}$ is positive. Therefore, by the argument above, $\gamma'^2 = \gamma_0^{2^\alpha}$ for some square free $\gamma_0 \in \mathbb{N}$. Finally $\gamma' = -\gamma_0^{2^{\alpha-1}} \in {K_m^*}^{2^\alpha}$.

From this property we deduce that

$$\sqrt[2^\alpha]{\gamma'} = \varepsilon\sqrt{\gamma_0} \in K_m^*$$

for some primitive $2^{\alpha+1}$–root of unity ε. We need to distinguish two cases: $2^{\alpha+1} \mid m$ or $2^\alpha \| m$.

If $2^{\alpha+1} \mid m$, $\varepsilon \in K_m$. So $\sqrt{\gamma_0} \in K_m$ which is equivalent to $\delta(\gamma) \mid m$.

If $2^\alpha \| m$, $\varepsilon \in K_{2m} \setminus K_m$. $\sqrt{\gamma_0} \in K_{2m} \setminus K_m$ which is equivalent to $\delta(\gamma) \mid 2m$ but $\delta(\gamma) \nmid m$.

This discussion proves that

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

Viceversa, suppose that $\gamma \in \tilde{\Gamma}^+_{m,2^\alpha} \cup \tilde{\Gamma}^-_{m,2^\alpha}$ and that $\gamma \neq \mathbb{Q}^{*2^\alpha}$. Then $\gamma = \pm\gamma_0^{2^{\alpha-1}}\mathbb{Q}^{*2^\alpha}$ and the condition $\delta(\gamma) = \operatorname{disc}\mathbb{Q}(\sqrt{\gamma_0}) \mid m$ is equivalent to $\sqrt{\gamma_0} \in K_m$.

Finally, if $\gamma \in \tilde{\Gamma}^+_{m,2^\alpha}$, $\gamma' = \gamma_0^{2^{\alpha-1}} = \left(\sqrt{\gamma_0}\right)^{2^\alpha} \in {K_m^*}^{2^\alpha}$ and hence $\gamma' \in \mathbb{Q}^{*2^\alpha} \cap {K_m^*}^{2^\alpha}$ so that $\tilde{\Gamma}^+_{m,2^\alpha} \subset \tilde{\Gamma}_{m,2^\alpha}$, while if $\gamma \in \tilde{\Gamma}^-_{m,2^\alpha}$, $\gamma' = -\gamma_0^{2^{\alpha-1}} = \left(\varepsilon\sqrt{\gamma_0}\right)^{2^\alpha}$, for some primitive $2^{\alpha+1}$–root of unity ε.

If $2^{\alpha+1} \mid m$, then $\varepsilon \in K_m^*$ and hence $\gamma' \in \Gamma \cdot \mathbb{Q}^{*2^\alpha} \cap {K_m^*}^{2^\alpha}$ so that $\tilde{\Gamma}^-_{m,2^\alpha} \subset \tilde{\Gamma}_{m,2^\alpha}$.

Suppose $2^\alpha \| m$. If $\gamma \in \tilde{\Gamma}^-_{m,2^\alpha}$, then $\gamma' = -\gamma_0^{2^{\alpha-1}}$ and $\gamma'^2 = \gamma_0^{2^\alpha} = (\sqrt{-\gamma_0})^{2^{\alpha+1}} \in K_m^{2^{\alpha+1}}$ since the condition $\delta(\gamma) \mid 2m$ but $\delta(\gamma) \nmid m$ implies that $\sqrt{-\gamma_0} \in K_m^*$. Therefore either $\gamma' \in {K_m^*}^{2^\alpha}$ or $-\gamma' \in {K_m^*}^{2^\alpha}$. If it was that $-\gamma' = \gamma_0^{2^{\alpha-1}} \in {K_m^*}^{2^\alpha}$ we would deduce that $\sqrt{\gamma_0} \in K_m^*$ and this would contradic $\delta(\gamma) \nmid m$. Finally $\gamma' \in \Gamma \cdot \mathbb{Q}^{*2^\alpha} \cap {K_m^*}^{2^\alpha}$ so that $\tilde{\Gamma}^-_{m,2^\alpha} \subset \tilde{\Gamma}_{m,2^\alpha}$. □

Remark. Let $\gamma_0 \in \mathbb{N}$ be square free and suppose that $2\|m$. Then the condition $\operatorname{disc}(\mathbb{Q}(\sqrt{-\gamma_0})) \mid m$ is equivalent to $\operatorname{disc}(\mathbb{Q}(\sqrt{\gamma_0})) \mid 2m$ and $\operatorname{disc}(\mathbb{Q}(\sqrt{\gamma_0})) \nmid m$. In fact with the given assumption on γ_0 and m, $\operatorname{disc}(\mathbb{Q}(\sqrt{-\gamma_0})) \mid m$ if and only if $\gamma_0 \equiv 3 \bmod 4$ and $\gamma_0 \mid m/2$ so that $\operatorname{disc}(\mathbb{Q}(\sqrt{\gamma_0})) = 4\gamma_0 \mid 2m$ and $\operatorname{disc}(\mathbb{Q}(\sqrt{\gamma_0})) = 4\gamma_0 \nmid m$. This explains why the formula in Lemma 4.1 reduces to the one in Proposition 3.1 in the case when $\alpha = 1$.

3.3 Proof of Theorem 3.2

Let us start by writing $m = 2^{v_2(m)}n$ with $2 \nmid n$ and note that

$$\begin{aligned}
\rho(\Gamma, m) &= \sum_{k\geq 1} \frac{\mu(k)}{[\mathbb{Q}(\zeta_{mk}, \Gamma^{1/mk}) : \mathbb{Q}]} = \sum_{k\geq 1} \frac{\mu(k)\left|\tilde{\Gamma}_{mk,m_2k_2}\right|}{\varphi(mk)\left|\Gamma(mk)\right|} \\
&= \sum_{\alpha=0}^{\infty} \frac{\mu(2^\alpha)}{\varphi(2^{\alpha+v_2(m)})\left|\Gamma(2^{\alpha+v_2(m)})\right|} \sum_{\substack{k\geq 1\\ 2\nmid k}} \frac{\mu(k)\left|\tilde{\Gamma}_{2^{\alpha+v_2(m)}nk,2^{\alpha+v_2(m)}}\right|}{\varphi(nk)\left|\Gamma(nk)\right|} \\
&= \sum_{\alpha=v_2(m)}^{\infty} \frac{\mu(2^{\alpha-v_2(m)})}{\varphi(2^\alpha)\left|\Gamma(2^\alpha)\right|} \left(\sum_{\substack{k\geq 1\\ 2\nmid k}} \frac{\mu(k)\left|\tilde{\Gamma}^{+}_{2^\alpha nk,2^\alpha}\right|}{\varphi(nk)\left|\Gamma(nk)\right|} + \sum_{\substack{k\geq 1\\ 2\nmid k}} \frac{\mu(k)\left|\tilde{\Gamma}^{-}_{2^\alpha nk,2^\alpha}\right|}{\varphi(nk)\left|\Gamma(nk)\right|} \right) \\
&= \sum_{\alpha=v_2(m)}^{\infty} \frac{\mu(2^{\alpha-v_2(m)})}{\varphi(2^\alpha)\left|\Gamma(2^\alpha)\right|} \left(\sum_{\substack{\gamma\in\Gamma(2^\alpha)[2]\\ \gamma\subset\mathbb{Q}^+}} \sum_{\substack{k\geq 1, 2\nmid k\\ \delta(\gamma)\mid 2^\alpha kn}} \frac{\mu(k)}{\varphi(nk)\left|\Gamma(nk)\right|} + \sum_{\substack{\gamma\in\Gamma(2^\alpha)[2]\\ \gamma\not\subseteq\mathbb{Q}^+}} \sum_{\substack{k\geq 1, 2\nmid k\\ \delta(\gamma)\mid 2^{1+\alpha}kn\\ \delta(\gamma)\nmid 2^\alpha kn}} \frac{\mu(k)}{\varphi(nk)\left|\Gamma(nk)\right|} \right).
\end{aligned}$$

Lemma 3.1. *Suppose that δ is a squarefree odd integer, that n is an odd integer and set:*

$$A_{\Gamma,n} = \frac{1}{\varphi(n)|\Gamma(n)|} \times \prod_{\substack{\ell>2\\ \ell\mid n}} \left(1 - \frac{|\Gamma(n_\ell)|}{\ell|\Gamma(\ell n_\ell)|}\right) \times \prod_{\substack{\ell>2\\ \ell\nmid n}} \left(1 - \frac{1}{(\ell-1)|\Gamma(\ell)|}\right).$$

Then the following identity holds

$$\sum_{\substack{k\geq 1, 2\nmid k\\ \delta\mid kn}} \frac{\mu(k)}{\varphi(nk)\left|\Gamma(nk)\right|} = A_{\Gamma,n} \prod_{\substack{\ell\mid\delta\\ \ell\nmid n}} \frac{-1}{(\ell-1)|\Gamma(\ell)| - 1}.$$

Proof. Observe that $\delta \mid kn$ if and only if $d := \delta/\gcd(\delta, n) \mid k$. If we write $k = dt$, then $\gcd(d, n) = \gcd(d, t) = 1$, so that $\varphi(ndt)|\Gamma(ndt)| = \varphi(d)|\Gamma(d)| \times \varphi(nt)|\Gamma(nt)|$ and

$$\begin{aligned}
\sum_{\substack{k\geq 1, 2\nmid k\\ \delta\mid kn}} \frac{\mu(k)}{\varphi(nk)\left|\Gamma(nk)\right|} &= \sum_{\substack{t\geq 1,\\ \gcd(t,2d)=1}} \frac{\mu(dk)}{\varphi(ndt)|\Gamma(ndt)|} \\
&= \frac{1}{\varphi(n)|\Gamma(n)|} \times \frac{\mu(d)}{\varphi(d)|\Gamma(d)|} \times \sum_{\substack{t\geq 1,\\ \gcd(t,2d)=1}} \frac{\mu(t)\varphi(t,n)|\Gamma(n)|}{\gcd(n,t)\varphi(t)|\Gamma(nt)|}
\end{aligned}$$

where we used the identity $\varphi(tn) = \varphi(t)\varphi(n)\gcd(t,n)/\varphi(\gcd(t,n))$. Since $\frac{|\Gamma(n)|}{|\Gamma(nt)|}$ is a multiplicative function of t, the above equals:

$$\begin{aligned}
&= \frac{1}{\varphi(n)|\Gamma(n)|} \times \frac{\mu(d)}{\varphi(d)|\Gamma(d)|} \times \prod_{\ell \nmid 2d} \left(1 - \frac{\varphi(\gcd(\ell, n))|\Gamma(n_\ell)|}{\varphi(\ell)\gcd(n,\ell)|\Gamma(\ell n_\ell)|}\right) \\
&= \frac{1}{\varphi(n)|\Gamma(n)|} \times \frac{\mu(d)}{\varphi(d)|\Gamma(d)|} \times \prod_{\ell \nmid 2d, \ell | n} \left(1 - \frac{|\Gamma(n_\ell)|}{\ell|\Gamma(\ell n_\ell)|}\right) \times \prod_{\ell \nmid 2dn} \left(1 - \frac{1}{(\ell-1)|\Gamma(\ell n_\ell)|}\right) \\
&= A_{\Gamma,n} \times \frac{\mu(d)}{\varphi(d)|\Gamma(d)|} \times \prod_{\ell | d, \ell > 2} \left(1 - \frac{1}{(\ell-1)|\Gamma(\ell)|}\right)^{-1} \\
&= A_{\Gamma,n} \times \prod_{\substack{\ell | \delta \\ \ell \nmid 2n}} \frac{-1}{(\ell-1)|\Gamma(\ell)|-1}.
\end{aligned}$$

□

From Lemma 3.1, we deduce that

$$\begin{aligned}
\rho(\Gamma, m) &= A_{\Gamma,n} \sum_{v_2(m) \le \alpha \le v_2(m)+1} \frac{\mu(2^{\alpha - v_2(m)})}{\varphi(2^\alpha)\,|\Gamma(2^\alpha)|} \times \\
&\quad \times \left(\sum_{\substack{\gamma \in \Gamma(2^\alpha)[2] \\ \gamma \subset \mathbb{Q}^+ \\ v_2(\delta(\gamma)) \le \alpha}} \prod_{\substack{\ell | \delta(\gamma) \\ \ell \nmid 2n}} \frac{-1}{(\ell-1)|\Gamma(\ell)|-1} + \sum_{\substack{\gamma \in \Gamma(2^\alpha)[2] \\ \gamma \not\subseteq \mathbb{Q}^+ \\ v_2(\delta(\gamma)) = \alpha+1}} \prod_{\substack{\ell | \delta(\gamma) \\ \ell \nmid 2n}} \frac{-1}{(\ell-1)|\Gamma(\ell)|-1} \right) \\
&= A_{\Gamma,n} \times \left(B_{\Gamma,m} - \frac{|\Gamma(m_2)|}{(2,m)|\Gamma(2m_2)|} B_{\Gamma,2m} \right)
\end{aligned}$$

where

$$B_{\Gamma,m} = \sum_{\gamma \in \tilde{\Gamma}(m)} \prod_{\substack{\ell | \delta(\gamma) \\ \ell \nmid 2m}} \frac{-1}{(\ell-1)|\Gamma(\ell)|-1} \tag{3.14}$$

and

$$\tilde{\Gamma}(m) = \left\{ \gamma \in \Gamma(m_2)[2] : \begin{array}{l} \text{if } \gamma \subset \mathbb{Q}^+ \text{ then } v_2(\delta(\gamma)) \le v_2(m); \\ \text{if } \gamma \not\subseteq \mathbb{Q}^+ \text{ then } v_2(\delta(\gamma)) = v_2(m)+1 \end{array} \right\}. \tag{3.15}$$

Note that in the product in (3.14), the position $\ell \nmid 2m$ is equivalent to $\ell \nmid m$. In fact, when m is odd, then necessarily, for $\gamma \in \tilde{\Gamma}(m)$, $\delta(\gamma)$ is also odd.

3.4 The case $\Gamma = \langle -1, a\rangle$ with $a \in \mathbb{Q}^+ \setminus \{0,1\}$

In this section we consider the special case when $\Gamma = \langle -1, a\rangle$ with $a \in \mathbb{Q}^+ \setminus \{0,1,-1\}$. The rank of Γ is 1 and we write $a = a_0^h$ with $a_0 \in \mathbb{Q}^+$ not an exact power of a rational number. Further we write $a_0 = a_1 a_2^2$ where $a_1, a_2 \in \mathbb{Q}^+$ are uniquely defined by the property that $a_1 \in \mathbb{N}$ and $a_1 > 1$ is square free. We have the following:

Theorem 3.1. *With the above notation, let* $A = \prod_\ell \left(1 - \frac{1}{\ell^2-\ell}\right) = 0.37395581361920228805 4\ldots$ *be the Artin Canstant,*

$$\rho(\langle -1, a\rangle, m) = \frac{(m,h)}{2m^2} \prod_{\ell \mid 2m} \frac{\ell^2-\ell}{\ell^2-\ell-1} \prod_{\substack{\ell \mid h \\ \ell \nmid 2m}} \frac{\ell^2-2\ell}{\ell^2-\ell-1} \prod_{\substack{\ell \mid 2m \\ v_\ell(m/h)\geq 0}} \frac{\ell+1}{\ell} \left(1 + \tau_{a,m} \prod_{\substack{\ell \mid a_1 \\ \ell \nmid 2m}} \frac{-(\ell,h)}{\ell^2-\ell-(\ell,h)}\right) A$$

where

$$\tau_{a,m} = \begin{cases} 0 & \textit{if } v_2(h) > v_2(m), \textit{ or} \\ & \textit{if } v_2(h) = v_2(m) = 0 \textit{ and } 2 \mid ha_1; \\ & \\ -\frac{1}{3} & \textit{if } v_2(h) = v_2(m) = 0 \textit{ and } 2 \nmid ha_1, \textit{ or} \\ & \textit{if } v_2(h) = v_2(m) > 0, \textit{ or} \\ & \textit{if } v_2(h) < v_2(m) = 1 \textit{ and } 2 \mid ha_1; \\ & \\ 1 & \textit{if } v_2(h) < v_2(m) = 1 \textit{ and } 2 \nmid ha_1, \textit{ or} \\ & \textit{if } v_2(h) < v_2(m) \neq 1. \end{cases}$$

Proof. For $m \in \mathbb{N}$ (see [32, equation (5) page 6]) we have that,

$$|\langle -1, a\rangle(m)| = \left|\langle -1, a_0^h\rangle \mathbb{Q}^{*m}/\mathbb{Q}^{*m}\right| = \frac{(2,m)m}{(m,h)}. \tag{3.16}$$

Hence $A_{\langle -1,a\rangle,m}$, as in Theorem 3.2, equals

$$\frac{(m,h)}{(m,2)\varphi(m^2)} \times \prod_{\ell \nmid 2hm} \left(1 - \frac{1}{(\ell-1)\ell}\right) \times \prod_{\substack{\ell \nmid 2m \\ \ell \mid h}} \left(1 - \frac{1}{\ell-1}\right) \times \prod_{\substack{\ell > 2 \\ \ell \mid m \\ v_\ell(h/m)\geq 1}} \left(1 - \frac{1}{\ell}\right) \times \prod_{\substack{\ell > 2 \\ \ell \mid m \\ v_\ell(h/m)\leq 0}} \left(1 - \frac{1}{\ell^2}\right).$$

We recall that

$$\widetilde{\langle -1, a\rangle}(m) = \begin{cases} \{1\} & \text{if } 2 \nmid m; \\ \{\gamma \in \Gamma(2) : \gamma' \equiv 1 \bmod 4\} & \text{if } 2 \| m; \\ \{\gamma \in \Gamma(4) : \text{either } \gamma' = \gamma_0^2, 2 \nmid \gamma_0 \text{ or } \gamma' = -\gamma_0^2, 2 \mid \gamma_0\} & \text{if } 4 \| m; \\ \Gamma(m_2)[2] \cap \mathbb{Q}^+ & \text{if } 8 \mid m. \end{cases}$$

Furthermore, if $\alpha \in \mathbb{N}$, then

$$\langle -1, a\rangle(2^\alpha)[2] = \begin{cases} \{\mathbb{Q}^{*2^\alpha}, -\mathbb{Q}^{*2^\alpha}, a_1^{2^{\alpha-1}}\mathbb{Q}^{*2^\alpha}, -a_1^{2^{\alpha-1}}\mathbb{Q}^{*2^\alpha}\} & \text{if } v_2(h) < \alpha \\ \{\mathbb{Q}^{*2^\alpha}, -\mathbb{Q}^{*2^\alpha}\} & \text{if } v_2(h) \geq \alpha. \end{cases}$$

Therefore, if $v_2(m) = 1$,

$$\widetilde{\langle -1, a\rangle}(m) = \begin{cases} \{\mathbb{Q}^{*2}\} & \text{if } 2 \mid ha_1; \\ \{\mathbb{Q}^{*2}, \left(\frac{-1}{a_1}\right) a_1\mathbb{Q}^{*2}\} & 2 \nmid ha_1, \end{cases}$$

if $v_2(m) = 2$,

$$\widetilde{\langle -1, a\rangle}(m) = \begin{cases} \{\mathbb{Q}^{*4}\} & \text{if } 4 \mid h; \\ \{\mathbb{Q}^{*4}, a_1^2\mathbb{Q}^{*4}\} & \text{if } 2 \nmid a_1 \text{ and } 4 \nmid h; \\ \{\mathbb{Q}^{*4}, -a_1^2\mathbb{Q}^{*4}\} & \text{if } 2 \mid a_1 \text{ and } 4 \nmid h \end{cases}$$

and if $\alpha = v_2(m) \geq 3$,

$$\widetilde{\langle -1, a\rangle}(m) = \begin{cases} \{\mathbb{Q}^{*2^\alpha}\} & \text{if } v_2(h) \geq v_2(m) \\ \{\mathbb{Q}^{*2^\alpha}, a_1^{2^{\alpha-1}}\mathbb{Q}^{*2^\alpha}\} & \text{if } v_2(h) < v_2(m). \end{cases}$$

From this, we deduce that

$$B_{\langle -1,a\rangle,m} = \sum_{\gamma \in \widetilde{\langle -1,a\rangle}(m)} \prod_{\substack{\ell \mid \delta(\gamma) \\ \ell \nmid 2m}} \frac{-1}{(\ell-1)|\widetilde{\langle -1, a\rangle}(\ell)| - 1} = 1 + \varepsilon_{m,a} \prod_{\substack{\ell \mid a_1 \\ \ell \nmid 2m}} \frac{-(\ell, h)}{\ell^2 - \ell - (\ell, h)}$$

where

$$\varepsilon_{m,a} = \begin{cases} 0 & \text{if } v_2(m) \leq v_2(h); \\ 0 & \text{if } 2 \| m \text{ and } 2 \mid ha_1; \\ 1 & \text{otherwise.} \end{cases}$$

Therefore

$$B_{\langle -1,a\rangle,m}-\frac{\langle -1,a\rangle(m_2)}{(2,m_2)\langle -1,a\rangle(2m_2)}B_{\langle -1,a\rangle,2m}=$$

$$\left(1-\frac{\gcd(h,2m_2)}{4\gcd(h,m_2)}\right)\left(1+\prod_{\substack{\ell\mid a_1\\ \ell\nmid 2m}}\frac{-(\ell,h)}{\ell^2-\ell-(\ell,h)}\times\frac{\varepsilon_{m,a}-\frac{\gcd(h,2m_2)}{4\gcd(h,m_2)}\varepsilon_{2m,a}}{1-\frac{\gcd(h,2m_2)}{4\gcd(h,m_2)}}\right).$$

Finally

$$\begin{aligned}\tau_{m,a}&=\frac{\varepsilon_{m,a}-\frac{\gcd(h,2m_2)}{4\gcd(h,m_2)}\varepsilon_{2m,a}}{1-\frac{\gcd(h,2m_2)}{4\gcd(h,m_2)}}=\begin{cases}0 & \text{if } v_2(m)<v_2(h);\\ \frac{-\varepsilon_{2m,a}}{3} & \text{if } v_2(m)=v_2(h)\\ \frac{4\varepsilon_{m,a}-\varepsilon_{2m,a}}{3} & \text{if } v_2(m)>v_2(h);\end{cases}\\
&=\begin{cases}0 & \text{if } v_2(h)>v_2(m), \text{ or}\\ & \text{if } v_2(h)=v_2(m)=0 \text{ and } 2\mid ha_1;\\ \\ -\frac{1}{3} & \text{if } v_2(h)=v_2(m)=0 \text{ and } 2\nmid ha_1, \text{ or}\\ & \text{if } v_2(h)=v_2(m)>0, \text{ or}\\ & \text{if } v_2(h)<v_2(m)=1 \text{ and } 2\mid ha_1;\\ \\ 1 & \text{if } v_2(h)<v_2(m)=1 \text{ and } 2\nmid ha_1, \text{ or}\\ & \text{if } v_2(h)<v_2(m)\neq 1;\end{cases}\end{aligned}$$

and this concludes the proof. □

3.5 The vanishing of $\rho(\langle -1,a\rangle,m)$ and the proof of Theorem 3.3

In this section we consider the equation:

$$\rho(\langle -1,a\rangle,m)=0.$$

In virtue of Theorem 3.1, we deduce that for every $a\in\mathbb{Q}^+\setminus\{0,1\}$ and $m\in\mathbb{N}$, $\rho(\langle -1,a\rangle,m)=0$ is satisfied if and only if:

$$C_{a,m}=1+\tau_{a,m}\prod_{\substack{\ell\mid a_1\\ \ell\nmid 2m}}\frac{-(\ell,h)}{\ell^2-\ell-(\ell,h)}=0.$$

Furthermore, for ℓ odd,

$$\frac{(\ell,h)}{\ell^2-\ell-(\ell,h)} \leq 1$$

and the equality holds if and only if $\ell = 3 \mid h$. Hence the equation $C_{a,m} = 0$ is equivalent to: $\tau_{a,m} = 1, 3 \mid h$ and 3 is the only odd prime that divides a_1 but it does not divide m. This happens exactly in one the following cases:

$$3 \mid h, 3 \nmid m, 3 \mid a_1, a_1 \mid 3m, \quad 2 \nmid h, 2 \| m, 2 \nmid a_1,$$

or

$$3 \mid h, 3 \nmid m, 3 \mid a_1, a_1 \mid 3m, \quad v_2(h) < v_2(m) \neq 1.$$

Proof of Theorem 3.3. From the above discussion, it is clear that $\rho_{\langle -1,a\rangle,m} = 0$ is satisfied if and only if one the the above properties are satisfied. In all other cases $\rho_{\langle -1,a\rangle,m} \neq 0$. So, on GRH by [32, Theorem 1], there are infinitely primes p such that $\left[\mathbb{F}_p^* : \langle -1, a\rangle_p\right] = m$.

Suppose next that a, m are such

$$3 \mid h, 3 \nmid m, 3 \mid a_1, a_1 \mid 3m \text{ and } 2 \mid m$$

and let p be a prime such that $\left[\mathbb{F}_p^* : \langle -1, a\rangle_p\right] = m$. From the fact that $2 \mid \left[\mathbb{F}_p^* : \langle -1, a\rangle_p\right]$ we deduce that -1 and a are squares in $\mathbb{F}_p*$ and that $p \equiv 1 \bmod 2m$. Furthermore, if $\ell > 3$ is any other prime that divides a_1. Then $\ell \mid m \mid p-1$. So, by quadratic reciprocity,

$$\left(\frac{\ell}{p}\right) = \left(\frac{p}{\ell}\right) = \left(\frac{1}{\ell}\right) = 1.$$

If the first of the properties in the statement of Theorem 3.3 is satisfied, then, since $2 \nmid h$, also a_1 is a square in $\mathbb{F}_p^*$. The property that $2 \nmid a_1$ implies that every $\ell \mid a_1$ is such that $\left(\frac{\ell}{p}\right) = 1$. Thus

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = \left(\frac{3}{p}\right)\prod_{\ell \mid a_1, \ell \neq 3}\left(\frac{\ell}{p}\right) = \left(\frac{a_1}{p}\right) = 1.$$

This implies that $p \equiv 1 \bmod 3$. Hence both -1 and a are cubes in $\mathbb{F}_p^3$ which implies that $3 \mid m$ and this is a contradiction.

In the case when a, m are such that the second properties in the statement of Theorem 3.3 is satisfied we let p be a prime such that $\left[\mathbb{F}_p^* : \langle -1, a\rangle_p\right] = m$. Then, since $v_2(h) < v_2(m)$ and $m \mid p-1$,

$$\left(\frac{a_1}{p}\right) = \left(\frac{a_0}{p}\right)^{h/h_2} \equiv a_0^{h/h_2 \frac{p-1}{2}} = a^{\frac{p-1}{2^{h_2+1}}} = a^{\frac{p-1}{m} m/2^{h_2+1}} \equiv 1 \bmod p.$$

So that again a_1 is a square modulo p. Furthermore, since $v_2(m) \geq 2$ and $p \equiv 1 \bmod 2m$, then $8 \mid p-1$. Thus

$$\left(\frac{2}{p}\right) = 1$$

Finally, a similar argument as above shows that $\left(\frac{-3}{p}\right) = 1$ and $3 \mid p-1$. Again both -1 and a are cubes in $\mathbb{F}_p^3$ which implies that $3 \mid m$ and this is a contradiction. □

3.6 The vanishing of $\rho(\Gamma, m)$

Proof of Theorem 3.5. We start from the identity

$$\rho(\Gamma, m) = A(\Gamma, m)\left(B_{\Gamma,m} - \frac{|\Gamma(m_2)|}{(2,m)|\Gamma(2m_2)|}B_{\Gamma,2m}\right).$$

It is easy to check, by the definition in (3.3), that $A(\Gamma, m) \neq 0$ for all m and all Γ. So, the equation $\rho(\Gamma, m) = 0$ is equivalent to

$$B_{\Gamma,m} = \frac{|\Gamma(m_2)|}{(2,m)|\Gamma(2m_2)|}B_{\Gamma,2m}. \tag{3.17}$$

1. If $2 \nmid m$, then $B_{\Gamma,m} = 1$ and $|\Gamma(m_2)| = 1$. So the identity in (3.17) specializes to

$$|\Gamma(2)| = B_{\Gamma,2m} = \sum_{\gamma \in \tilde{\Gamma}(2m)} \prod_{\substack{\ell \mid \delta(\gamma) \\ \ell \nmid 2m}} \frac{-1}{(\ell-1)|\Gamma(\ell)|-1}. \tag{3.18}$$

   Note that the hypothesis that $\mathrm{disc}(\mathbb{Q}(\sqrt{g})) \mid m$ for all $g \in \Gamma$, we deduce that $\mathrm{disc}(\mathbb{Q}(\sqrt{g})) = \delta(g\mathbb{Q}^{*2}) \equiv 1 \bmod 4$. Hence each of the products in (3.18) is empty. Finally $\Gamma(2) = \tilde{\Gamma}(2m)$ so that the identity in (3.18) is satisfied.

2. Next assume that the condition in *2.* is satisfied. We claim that $B_{\Gamma,m} = B_{\Gamma,2m} = 0$ which implies that (3.17) is an identity. Observe that, if $\gamma_1 \in \tilde{\Gamma}(m)$ is as in the statement, then

$$\prod_{\substack{\ell \mid \delta(\gamma_1) \\ \ell \nmid 2m}} \frac{-1}{(\ell-1)|\Gamma(\ell)|-1} = \frac{-1}{2|\Gamma(3)|-1} = -1.$$

   Therefore, since $\tilde{\Gamma}(m)$ is a group, $3 \nmid m$ and $3 \mid \delta(\gamma_1\gamma)$ if and only of $3 \nmid \delta(\gamma)$,

$$B_{\Gamma,m} = -\sum_{\gamma \in \tilde{\Gamma}(m)} \prod_{\substack{\ell \mid \delta(\gamma_1\gamma) \\ \ell \nmid 2m}} \frac{-1}{(\ell-1)|\Gamma(\ell)|-1} = -B_{\Gamma,m}$$

   which immediately implies that $B_{\Gamma,m} = 0$. We observe that, if $\gamma_1 = \pm\gamma_0^{m_2/2}\mathbb{Q}^{*m_2}$, then $\gamma_2 = \gamma_0^{m_2}\mathbb{Q}^{*2m_2} \in$

$\tilde{\Gamma}(2m_2)$ since it satisfies $\delta(\gamma_1) = \delta(\gamma_2)$ and $v_2(\gamma_2) \leq v_2(2m)$. So, by the same argument, we deduce that $B_{\Gamma,2m} = 0$.

3. By the remark after the statement Theorem 3.5, the third condition implies that $B_{\Gamma,m} = 1$ and $|\Gamma(m_2)| = 2$. So, identity (3.17) reduces to $B_{\Gamma,2m} = |\Gamma(2m_2)|$. The hypothesis that $\Gamma(4) = \tilde{\Gamma}(2m)$ and that, for every $\gamma \in \tilde{\Gamma}(2m)$, $\delta(\gamma) \mid 4m$, implies that

$$\prod_{\substack{\ell \mid \delta(\gamma) \\ \ell \nmid 2m}} \frac{-1}{(\ell-1)|\Gamma(\ell)|-1} = 1$$

so that $B_{\Gamma,2m} = |\tilde{\Gamma}(2m)|$ and identity (3.17) is satisfied.

□

Proof of Proposition 3.6. If $\Gamma = \langle g \rangle$, then $3 \mid h$ if and only if $\Gamma(3)$ is trivial and that $v_2(h)$ is the largest α such that $\Gamma(2^\alpha)$ is trivial.

To analyze precisely the special case when $\Gamma = \langle g \rangle$, $g = \pm g_0^h$ with $g_0 \neq 1$ not the power of a rational number, we observe that $\#\Gamma(m) = m/\gcd(m,h)$ and

$$\Gamma(m)[2] = \begin{cases} \{\mathbb{Q}^{*m_2}, g_0^{m_2/2}\mathbb{Q}^{*m_2}\} & \text{if } g > 0 \text{ and } v_2(m) > v_2(h), \text{ or} \\ & \text{if } g < 0 \text{ and } v_2(m) > v_2(h)+1; \\ \{\mathbb{Q}^{*m_2}, -g_0^{m_2/2}\mathbb{Q}^{*m_2}\} & \text{if } g < 0 \text{ and } v_2(m) = v_2(h)+1; \\ \{\mathbb{Q}^{*m_2}, -\mathbb{Q}^{*m_2}\} & \text{if } g < 0 \text{ and } v_2(m) = v_2(h); \\ \{\mathbb{Q}^{*m_2}\} & \text{if } g > 0 \text{ and } v_2(m) = v_2(h), \text{ or} \\ & \text{if } v_2(m) < v_2(h). \end{cases}$$

A. If $2 \nmid m$ and for all $\gamma \in \Gamma, \operatorname{disc}(\mathbb{Q}(\sqrt{\gamma})) \mid m$, then, in particular $\operatorname{disc}(\mathbb{Q}(\sqrt{g}) \mid m$ which is the first property in Lenstra's Theorem.

B. If $3 \mid \delta(g) \mid 6m$, $v_2(\delta(g)) \leq v_2(m)+1$. Thus

$$\tilde{\Gamma}(m) = \begin{cases} \{\mathbb{Q}^{*m_2}, g_0^{m_2/2}\mathbb{Q}^{*m_2}\} & \text{if } g > 0, v_2(\delta(g)) \leq v_2(m) \text{ and } v_2(m) > v_2(h), \text{ or} \\ & \text{if } g < 0, v_2(\delta(g)) \leq v_2(m) \text{ and } v_2(m) > v_2(h)+1; \\ \{\mathbb{Q}^{*m_2}, -g_0^{m_2/2}\mathbb{Q}^{*m_2}\} & \text{if } g < 0 \text{ and } v_2(\delta(g))-1 = v_2(m) = v_2(h)+1; \\ \{\mathbb{Q}^{*m_2}\} & \text{otherwise.} \end{cases} \tag{3.19}$$

Note that, in order for $v_2(\delta(g)) - 1 = v_2(m)$, necessarely $v_2(m) = 1$ of $v_2(m) = 2$ and in the latter case $2 \mid g_0$. The condition $3 \mid \delta(g) \mid 6m$ which implies:

$$\begin{aligned} \operatorname{disc}(\mathbb{Q}(\sqrt{-3g_0})) \mid m & \quad \text{in the first case of (3.19);} \\ \operatorname{disc}(\mathbb{Q}(\sqrt{3g_0})) \mid m & \quad \text{in the second case of (3.19), with } v_2(m) = 1; \\ \operatorname{disc}(\mathbb{Q}(\sqrt{-6g_0})) \mid m & \quad \text{in the second case of (3.19), with } v_2(m) = 2. \end{aligned}$$

We conclude that the second case of Theorem 3.5 specializes, in the case $\Gamma = \langle g \rangle$, to following cases of the Theorem of Lenstra.

2.	if $g > 0$
3.	if $g < 0$, $v_2(m) = 1$ and $v_2(h) = 0$
5.	if $g < 0$, $v_2(m) = 2$ and $v_2(h) = 1$
6.	if $g < 0$ and $v_2(m) > v_2(h) + 1$.

C. The third property in the above statement means that. every element $\gamma \in \tilde{\Gamma}(4)$ is either of the form $\gamma_0^2 \mathbb{Q}^{*4}$ or $-4\gamma_0^2 \mathbb{Q}^{*4}$ with $\gamma_0 \mid m$ odd and square free and at least one of them is of the second form. Hence, necessarily, $g = -g_0^2$ with g_0 even, not a fourth power and $v_2(g_0)$ odd. This implies that $2 \| h$ and that $\operatorname{disc}(\mathbb{Q}(\sqrt{2g_0})) \mid 2m$.

□

Proof of Proposition 3.7. Assume that $2 \nmid m$ and $\rho(\Gamma, m) = 0$, then by (3.17), $|\Gamma(2)| = B_{\Gamma,2m}$. Furthermore

$$|B_{\Gamma,2m}| \leq |\tilde{\Gamma}(2m)| \leq |\Gamma(2)|.$$

This implies that $\tilde{\Gamma}(2m) = \Gamma(2)$ and that for every $\gamma \in \Gamma$, $\gamma' \equiv 1 \bmod 4$ and

$$\prod_{\substack{\ell \mid \delta(\gamma) \\ \ell \nmid 2m}} \frac{-1}{(\ell - 1)|\Gamma(\ell)| - 1} = 1.$$

Thus $\delta(\gamma) \mid m$ for all $\gamma \in \Gamma(2)$. Hence the property in *1.* holds for Γ and m. □

Proof of Proposition 3.8. Suppose that Γ and m satisfy the first condition in the statement of Theorem 3.5. Let $p \notin \operatorname{Supp} \Gamma$ be such that $|\Gamma_p| = (p-1)/m$, then $p \equiv 1 \bmod m$ and by, quadratic reciprocity, for all $g \in \Gamma$, since $\delta(g\mathbb{Q}^{*2}) \mid m$, $\left(\frac{g}{p}\right) = 1$. Hence $\Gamma_p \subset \mathbb{F}_p^*$ is contained in the subgroup of squares which implies that $2 \mid m$, a contradiction.

Next suppose that Γ and m satisfy the second condition in the statement of Theorem 3.5. First note that, if $p \notin \operatorname{Supp} \Gamma$ is a prime such that $|\Gamma_p| = (p-1)/m$, then $p \equiv 2 \bmod 3$ since $3 \nmid m$ and since all elements of Γ are perfect cubes. Furthermore the hypothesis m even implies that all elements of Γ_p are squares modulo p.

Let $\gamma_1 \in \tilde{\Gamma}(m)$ be such that $3 \mid \delta(\gamma_1) \mid 6m$. Then

$$\left(\frac{\gamma_1}{p}\right) = \left(\frac{\delta(\gamma_1)}{p}\right) = \left(\frac{3}{p}\right)\left(\frac{\delta(\gamma_1)/3}{p}\right) = -1,$$

which is a contradiction to the property that all the elements of Γ are squares modulo p.

Finally suppose that Γ and m satisfy the third condition in the statement of Theorem 3.5. Let $-4\gamma_0^2\mathbb{Q}^{*4} \in \Gamma(4)$ with γ_0 odd and square free as in the Remark after the statement of Theorem 3.5. Since $2\|m$, $-4\gamma_0^2$ is a square modulo p. Hence $p \equiv 1 \bmod 2m$. We have also that $p \not\equiv 1 \bmod 4m$, otherwise the quartic symbol

$$\left[\frac{-4\gamma_0^2}{p}\right]_4 = \left[\frac{-1}{p}\right]_4 \left(\frac{2}{p}\right)\left(\frac{\gamma_0}{p}\right) = 1,$$

since $\gamma_0 \mid m$. Furthermore $\gamma_0 \mid m$ also implies, by quadratic reciprocity that $\left(\frac{\gamma_0}{p}\right) = 1$, hence the Legendre symbol:

$$\left(\frac{2\gamma_0}{p}\right) = \left(\frac{2}{p}\right) = 1$$

if and only if $p \equiv 1 \bmod 8$ (since $p \not\equiv -1 \bmod 4$). So a contradiction. □

3.7 Numerical Examples

In this section we compare numerical data. The density $\rho_{\Gamma,m}$ can be explicitly computed once a set of generators of Γ is given. The tables in this section have been computed using Pari-GP [35].

The first table compares the values of $\rho_{\langle -1,a\rangle,m}$ as in Theorem 3.1 (second row) and

$$\frac{\pi_{\langle -1,a\rangle}(10899719603, m)}{\pi(10899719603)} \qquad \text{(first row)}$$

with $a = 2, \dots, 21$, $m = 1, \dots, 20$. All values have been truncated to the first decimal digits.

$a\backslash m$	1	2	3	4	5	6	7	8	9	10
2	0.5609316	0.09349469	0.09972896	0.07011468	0.02834563	0.01661614	0.01340015	0.01753052	0.01108010	0.00472355
	0.5609337	0.09348895	0.09972155	0.07011672	0.02834191	0.01662026	0.01340210	0.01752918	0.01108017	0.00472365
3	0.5983436	0.1121961	0.06648385	0.02804691	0.03023376	0.04986213	0.01429211	0.007009285	0.007383818	0.00566415
	0.5983293	0.1121867	0.06648103	0.02804669	0.03023138	0.04986078	0.01429557	0.007011672	0.007386782	0.00566838
4	0.3739585	0.1869731	0.06648425	0.1402365	0.01889511	0.03324471	0.008932948	0.03505868	0.007385783	0.00945051
	0.3739558	0.1869779	0.06648103	0.1402334	0.01889461	0.03324052	0.008934733	0.03505836	0.007386782	0.00944730
5	0.5707797	0.1328580	0.1014608	0.03321178	0.01889962	0.02361663	0.01363818	0.008306253	0.01127759	0.0141702
	0.5707747	0.1328527	0.1014711	0.03321318	0.01889461	0.02361826	0.01363722	0.008303295	0.01127456	0.0141709
6	0.5609309	0.1495846	0.09972773	0.02804226	0.02834054	0.01662218	0.01340140	0.007010532	0.01108035	0.00756130
	0.5609337	0.1495823	0.09972155	0.02804669	0.02834191	0.01662026	0.01340210	0.007011672	0.01108017	0.00755784
7	0.5655185	0.1368145	0.1005323	0.03419843	0.02856917	0.02432134	0.008929491	0.008552522	0.01116960	0.00691573
	0.5654942	0.1368131	0.1005323	0.03420328	0.02857234	0.02432233	0.008934733	0.008550819	0.01117025	0.00691266
8	0.3365588	0.05609852	0.2991703	0.04207116	0.01700431	0.04985612	0.008041882	0.01051791	0.03324158	0.00283249
	0.3365602	0.05609337	0.2991647	0.04207003	0.01700515	0.04986078	0.008041260	0.01051751	0.03324052	0.00283419
9	0.3739683	0.2991733	0.06648385	0.05609534	0.01889393	0.03323814	0.008931910	0.01402027	0.007383818	0.0151180
	0.3739558	0.2991647	0.06648103	0.05609337	0.01889461	0.03324052	0.008934733	0.01402334	0.007386782	0.0151156
10	0.5609298	0.1427061	0.09972107	0.03321470	0.02834725	0.02536964	0.01340418	0.008301758	0.01108199	0.00471766
	0.5609337	0.1426937	0.09972155	0.03321318	0.02834191	0.02536776	0.01340210	0.008303295	0.01108017	0.00472365
11	0.5626496	0.1389491	0.1000259	0.03473188	0.02843085	0.02469908	0.01344676	0.008686747	0.01111246	0.00701644
	0.5626491	0.1389469	0.1000265	0.03473672	0.02842859	0.02470167	0.01344308	0.008684180	0.01111406	0.00702047
12	0.5983387	0.1121865	0.06648742	0.02804858	0.03023264	0.04986241	0.01429060	0.007011669	0.007378899	0.00566779
	0.5983293	0.1121867	0.06648103	0.02804669	0.03023138	0.04986078	0.01429557	0.007011672	0.007386782	0.00566838
13	0.5621469	0.1393328	0.09993109	0.03483086	0.02840633	0.02476879	0.01343573	0.008701322	0.01110203	0.00704395
	0.5621400	0.1393287	0.09993601	0.03483217	0.02840286	0.02476955	0.01343092	0.008708044	0.01110400	0.00703976
14	0.5609384	0.1413718	0.09973011	0.03419959	0.02833696	0.02513520	0.01340095	0.008548704	0.01107725	0.00714109
	0.5609337	0.1413735	0.09972155	0.03420328	0.02834191	0.02513307	0.01340210	0.008550819	0.01108017	0.00714308
15	0.5589555	0.1417091	0.1014805	0.03543326	0.03024462	0.02362492	0.01335049	0.008858559	0.01127789	0.00566780
	0.5589655	0.1417096	0.1014711	0.03542739	0.03023138	0.02361826	0.01335507	0.008856848	0.01127456	0.00566838
16	0.3739585	0.1869731	0.06648425	0.09348516	0.01889511	0.03324471	0.008932948	0.07012322	0.007385783	0.00945051
	0.3739558	0.1869779	0.06648103	0.09348895	0.01889461	0.03324052	0.008934733	0.07011672	0.007386782	0.00944730
17	0.5616273	0.1397238	0.09985219	0.03493080	0.02838022	0.02484125	0.01341405	0.008729947	0.01109205	0.00705916
	0.5616237	0.1397160	0.09984421	0.03492899	0.02837678	0.02483839	0.01341858	0.008732248	0.01109380	0.00705933
18	0.5609340	0.09348952	0.09972808	0.07011901	0.02834935	0.01661992	0.01340618	0.01753497	0.01108209	0.00472335
	0.5609337	0.09348895	0.09972155	0.07011672	0.02834191	0.01662026	0.01340210	0.01752918	0.01108017	0.00472365
19	0.5614939	0.1398239	0.09982117	0.03495974	0.02836823	0.02486121	0.01341314	0.008741045	0.01108672	0.00706348
	0.5614820	0.1398222	0.09981903	0.03495555	0.02836962	0.02485728	0.01341520	0.008738887	0.01109100	0.00706470
20	0.5707806	0.1328471	0.1014829	0.03322058	0.01889355	0.02362051	0.01363731	0.008299904	0.01127612	0.0141725
	0.5707747	0.1328527	0.1014711	0.03321318	0.01889461	0.02361826	0.01363722	0.008303295	0.01127456	0.0141709
21	0.5600268	0.1409286	0.1005350	0.03522960	0.02829520	0.02431948	0.01429444	0.008803046	0.01116625	0.00711351
	0.5600216	0.1409175	0.1005323	0.03522937	0.02829583	0.02432233	0.01429557	0.008807343	0.01117025	0.00712004

$a\backslash m$	11	12	13	14	15	16	17	18	19	20
2	0.00510744	0.0124679	0.00359997	0.00222978	0.00503516	0.00438153	0.00206209	0.00184754	0.00164031	0.00354257
	0.00510365	0.0124652	0.00359751	0.00223368	0.00503856	0.00438229	0.00206270	0.00184670	0.00164041	0.00354274
3	0.00544021	0.0124616	0.00383648	0.00268420	0.00336011	0.00175025	0.00220027	0.00553765	0.00174867	0.00141870
	0.00544389	0.0124652	0.00383735	0.00268042	0.00335904	0.00175292	0.00220022	0.00554009	0.00174977	0.00141710
4	0.00340434	0.0249248	0.00239988	0.00446720	0.00335940	0.00876508	0.00137414	0.00369432	0.00109360	0.00708846
	0.00340243	0.0249304	0.00239834	0.00446737	0.00335904	0.00876459	0.00137514	0.00369339	0.00109361	0.00708548
5	0.00519359	0.00590447	0.00366198	0.00317556	0.00336173	0.00207477	0.00210207	0.00262178	0.00166963	0.00354352
	0.00519319	0.00590457	0.00366063	0.00317418	0.00335904	0.00207582	0.00209889	0.00262425	0.00166919	0.00354274
6	0.00510627	0.0124629	0.00359992	0.00357324	0.00504114	0.00175411	0.00206171	0.00184493	0.00163881	0.00141912
	0.00510365	0.0124652	0.00359751	0.00357389	0.00503856	0.00175292	0.00206270	0.00184670	0.00164041	0.00141710
7	0.00513631	0.00607994	0.00362347	0.00669896	0.00507949	0.00213845	0.00207716	0.00269970	0.00165395	0.00172480
	0.00514514	0.00608058	0.00362676	0.00670105	0.00507953	0.00213770	0.00207947	0.00270248	0.00165375	0.00172817
8	0.00306486	0.0373951	0.00216091	0.00133867	0.0151169	0.00262701	0.00123701	0.00554338	0.000983628	0.00212638
	0.00306219	0.0373956	0.00215851	0.00134021	0.0151157	0.00262938	0.00123762	0.00554009	0.000984246	0.00212564
9	0.00340005	0.0249340	0.00239661	0.00715018	0.00336011	0.00350570	0.00137538	0.00369255	0.00109416	0.00283125
	0.00340243	0.0249304	0.00239834	0.00714779	0.00335904	0.00350584	0.00137514	0.00369339	0.00109361	0.00283419
10	0.00510461	0.00590093	0.00360070	0.00340683	0.00503538	0.00207639	0.00206380	0.00281799	0.00164099	0.00354335
	0.00510365	0.00590457	0.00359751	0.00340931	0.00503856	0.00207582	0.00206270	0.00281864	0.00164041	0.00354274
11	0.00340353	0.00617265	0.00361100	0.00331679	0.00505721	0.00216874	0.00206702	0.00274380	0.00164561	0.00175059
	0.00340243	0.00617542	0.00360852	0.00331979	0.00505397	0.00217105	0.00206901	0.00274463	0.00164543	0.00175512
12	0.00544441	0.0124649	0.00383767	0.00268083	0.00336152	0.00175182	0.00219725	0.00554242	0.00175120	0.00141594
	0.00544389	0.0124652	0.00383735	0.00268042	0.00335904	0.00175292	0.00220022	0.00554009	0.00174977	0.00141710
13	0.00511588	0.00619055	0.00239962	0.00332478	0.00504846	0.00217509	0.00206879	0.00274989	0.00164528	0.00175839
	0.00511463	0.00619239	0.00239834	0.00332891	0.00504940	0.00217701	0.00206714	0.00275217	0.00164394	0.00175994
14	0.00510613	0.00608177	0.00359234	0.00223823	0.00503918	0.00213949	0.00206543	0.00279089	0.00163908	0.00172924
	0.00510365	0.00608058	0.00359751	0.00223368	0.00503856	0.00213770	0.00206270	0.00279256	0.00164041	0.00172817
15	0.00508856	0.00590030	0.00358190	0.00338418	0.00335933	0.00221683	0.00205424	0.00262339	0.00162967	0.00141946
	0.00508574	0.00590457	0.00358489	0.00338579	0.00335904	0.00221421	0.00205547	0.00262425	0.00163465	0.00141710
16	0.00340434	0.0166159	0.00239988	0.00446720	0.00335940	0.0175294	0.00137414	0.00369432	0.00109360	0.00472694
	0.00340243	0.0166203	0.00239834	0.00446737	0.00335904	0.0175292	0.00137514	0.00369339	0.00109361	0.00472365
17	0.00510339	0.00620499	0.00359956	0.00333673	0.00504253	0.00218122	0.00137517	0.00275780	0.00164143	0.00176759
	0.00510993	0.00620960	0.00360194	0.00333816	0.00504476	0.00218306	0.00137514	0.00275982	0.00164243	0.00176483
18	0.00510607	0.0124616	0.00359556	0.00223293	0.00504174	0.00438445	0.00206104	0.00184680	0.00163940	0.00353899
	0.00510365	0.0124652	0.00359751	0.00223368	0.00503856	0.00438229	0.00206270	0.00184670	0.00164041	0.00354274
19	0.00510559	0.00621063	0.00360779	0.00333827	0.00504638	0.00218332	0.00206461	0.00276301	0.00109126	0.00176729
	0.00510864	0.00621432	0.00360103	0.00334070	0.00504349	0.00218472	0.00206472	0.00276192	0.00109361	0.00176618
20	0.00519737	0.00589984	0.00366014	0.00317452	0.00336146	0.00207540	0.00209665	0.00262335	0.00166906	0.00353976
	0.00519319	0.00590457	0.00366063	0.00317418	0.00335904	0.00207582	0.00209889	0.00262425	0.00166919	0.00354274
21	0.00509391	0.00607751	0.00358806	0.00268179	0.00508293	0.00220359	0.00206029	0.00270407	0.00163689	0.00178045
	0.00509535	0.00608058	0.00359166	0.00268042	0.00507953	0.00220184	0.00205935	0.00270248	0.00163774	0.00178001

Next table lists the first few values of a (first raw), its factorization (second raw) and m (third raw) such that $\rho(\langle -1, a\rangle, m) = 0$.

a	27	216	729	1728	3375	9261	13824	19683	27000	35937	46656	59319	74088	110592	132651	185193	216000
	3^3	6^3	3^6	12^3	15^3	21^3	24^3	3^9	30^3	33^3	6^6	39^3	42^3	48^3	51^3	57^3	60^3
m	2	4	4	2	10	14	4	2	20	22	4	26	28	2	34	38	10

Next table compares the values of $\rho_{\Gamma,m}$ as in Theorem 3.2 (second row) and

$$\frac{\pi_\Gamma(10^{10}, m)}{\pi(10^{10})} \qquad \text{(first row)}$$

for some groups Γ of rank 2 and $m = 1, \ldots, 20$. All values have been truncated to the first decimal digits.

$\Gamma\backslash m$	1	2	3	4	5	6	7	8	9	10
$\langle -1,2,3\rangle$	0.820596	0.082060	0.0395175	0.0239324	0.00822387	0.0098772	0.00279091	0.0029907	0.0014603	0.0008217
	0.820590	0.082059	0.0395099	0.0239339	0.00822248	0.0098774	0.00279248	0.0029917	0.0014633	0.0008222
$\langle 2,3\rangle$	0.697505	0.205153	0.0395175	0.0205123	0.00698931	0.0098772	0.00237151	0.0059838	0.0014603	0.0020563
	0.697501	0.205147	0.0395099	0.0205147	0.00698910	0.0098774	0.00237361	0.0059834	0.0014633	0.0020556
$\langle 2,-3\rangle$	0.711182	0.191476	0.0263467	0.0205125	0.00712861	0.0230480	0.00241891	0.0059831	0.0009733	0.0019170
	0.711178	0.191471	0.0263399	0.0205147	0.00712615	0.0230474	0.00242015	0.0059834	0.0009755	0.0019185
$\langle -2,3\rangle$	0.697509	0.205148	0.0395175	0.0205138	0.00699074	0.0098772	0.00237228	0.0059827	0.0014603	0.0020548
	0.697501	0.205147	0.0395099	0.0205147	0.00698910	0.0098774	0.00237361	0.0059834	0.0014633	0.0020556
$\langle -2,-3\rangle$	0.711187	0.191471	0.0263420	0.0205148	0.00712694	0.0230528	0.00241881	0.0059807	0.0009757	0.0019186
	0.711178	0.191471	0.0263399	0.0205147	0.00712615	0.0230474	0.00242015	0.0059834	0.0009755	0.0019185

$\Gamma\backslash m$	11	12	13	14	15	16	17	18	19	20
$\langle -1,2,3\rangle$	0.000679	0.002879	0.0004043	0.0002789	0.000396198	0.000373124	0.000176883	0.000364441	0.000126355	0.000239328
	0.000678	0.002880	0.0004046	0.0002792	0.000395897	0.000373967	0.000177465	0.000365832	0.000126284	0.000239822
$\langle 2,3\rangle$	0.000577	0.002468	0.0003435	0.0006983	0.000396198	0.000747096	0.000150315	0.000364441	0.000107638	0.000205653
	0.000576	0.002469	0.0003439	0.0006981	0.000395897	0.000747933	0.000150846	0.000365832	0.000107342	0.000205562
$\langle 2,-3\rangle$	0.000588	0.002469	0.0003505	0.0006509	0.000263545	0.000747221	0.000153294	0.000851385	0.000109579	0.000205082
	0.000587	0.002469	0.0003506	0.0006515	0.000263931	0.000747933	0.000153803	0.000853609	0.000109447	0.000205562
$\langle -2,3\rangle$	0.000576	0.002469	0.0003436	0.0006975	0.000396198	0.000746852	0.000150279	0.000364441	0.000107482	0.000205266
	0.000576	0.002469	0.0003439	0.0006981	0.000395897	0.000747933	0.000150846	0.000365832	0.000107342	0.000205562
$\langle -2,-3\rangle$	0.000588	0.002467	0.0003507	0.0006510	0.000263912	0.000747661	0.000153299	0.000848999	0.000109390	0.000204851
	0.000587	0.002469	0.0003506	0.0006515	0.000263931	0.000747933	0.000153803	0.000853609	0.000109447	0.000205562

Chapter 4

Divisibility of reduction in groups of rational numbers

4.1 Introduction

The results of the present Chapter have been collected in an article by Herish O. Abdullah, Andam Ali Mustafa and Francesco Pappalardi that has been submitted for publication.

Let $\Gamma \subset \mathbb{Q}^*$ be a finitely generated multiplicative group of rank r. We denote by $\operatorname{Supp}\Gamma$, the *support* of Γ, i.e. the finite set of those primes ℓ such that the ℓ–adic valuation of some elements of Γ is nonzero. For any prime $p \notin \operatorname{Supp}\Gamma$, we consider the reduction group:

$$\Gamma_p = \{\gamma \bmod p : \gamma \in \Gamma\} \subset \mathbb{F}_p^*$$

and, for $m \in \mathbb{N}$, the prime counting function:

$$\pi(x, \Gamma, m) := \#\{p \leq x : p \notin \operatorname{Supp}\Gamma, m \mid \#\Gamma_p\}.$$

We also define the density as

$$\varrho(\Gamma, m) = \lim_{x\to\infty} \frac{\pi(x,\Gamma,m)}{\pi(x)}$$

which in [31, Theorem 1] was proven to exists and to be expressed by the following formula:

$$\varrho(\Gamma, m) = \sum_{n\in\mathcal{S}_m} \sum_{\substack{d|n \\ f|n}} \frac{\mu(d)\mu(f)}{[\mathbb{Q}(\zeta_{nd}, \Gamma^{1/\gamma(f,\frac{n}{m})}) : \mathbb{Q}]} \tag{4.1}$$

where $\mathcal{S}_m = \{n \in \mathbb{N} : \operatorname{Rad}(n) \mid m \text{ and } m \mid n\}$ and for $n \in \mathbb{N}$, $\operatorname{Rad}(n)$ denotes the *radical of* n, the largest squarefree integer dividing n and $\gamma(f,k) = \prod_{\ell|f} \ell^{v_\ell(k)+1}$. Here $\zeta_d = e^{2\pi i/d}$ and $\Gamma^{1/d}$ denotes the set of real numbers α such that $\alpha^d \in \Gamma$.

If $\Gamma = \langle a\rangle$ with $a \in \mathbb{Q}\setminus\{-1,0,1\}$, then the density in question is the density of primes p for which $\operatorname{ord}_p(a)$, the order of a modulo p, is divisible by m. Expessions for $\varrho(\langle a\rangle, m)$ have been proposed by several authors ([5, 6, 28, 22, 30, 37]). The most general formula is due to Moree in [22, Theorem 2]. He has shown the following:

Theorem 4.1. *Let $a \in \mathbb{Q}\setminus\{-1,0,1\}$, write $a = \pm a_0^h$ with $a_0 > 0$ not the exact power of a rational number. Set $\delta(a) = \operatorname{disc}(\mathbb{Q}(\sqrt{a_0}))$, denote by $v_\ell(h)$ the ℓ–adic valuation of h and $(h, m^\infty) = \prod_{\ell|m} \ell^{v_\ell(h)}$, where ℓ always denotes a prime number. Finally set $\mathbf{v} = v_2(\delta(a)/mh)$. Then*

$$\varrho(\langle a\rangle, m) = \frac{\nu_{a,m}}{m(h,m^\infty)} \prod_{\ell|m} \left(\frac{\ell^2}{\ell^2-1}\right)$$

$$\varepsilon_{a,m}=\begin{cases}-\frac{1}{2} & \textit{if } a>0, \mathbf{v}\le 0, \textit{ or}\\ & \textit{if } a<0, \mathbf{v}=1;\\ \frac{1}{4} & \textit{if } a<0, \mathbf{v}\le 0, \textit{ or}\\ & \textit{if } a>0, \mathbf{v}=1;\\ \frac{1}{16} & \textit{if } \mathbf{v}>1,\end{cases}\quad \nu_{a,m}=\begin{cases}1 & \textit{if } 2\nmid m;\\ 1+3(1-\frac{a}{|a|})(2^{v_2(h)}-1)/4 & \textit{if } 2\| m, \delta(a)\nmid 4m;\\ 1+3(1-\frac{a}{|a|})(2^{v_2(h)}-1)/4+\varepsilon_{a,m} & \textit{if } 2\| m, \delta(a)\mid 4m;\\ 1 & \textit{if } 4\mid m, \delta(a)\nmid 4m;\\ 1+\varepsilon_{|a|,m} & \textit{if } 4\mid m, \delta(a)\mid 4m.\end{cases}$$

In particular, if $a>0$, then

$$\nu_{a,m}=\begin{cases}1+(-1/2)^{2^{\max\{0,\mathbf{v}\}}} & \textit{if } 2\mid m, \delta(a)\mid 4m;\\ 1 & \textit{otherwise.}\end{cases}$$

Regarding the higher rank case, for $k\in\mathbb{N}$, we set

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

which is a finite group with order dividing $2\cdot k^r$.

In [31] it was proved the following:

Theorem 4.2. *Assume that Γ is a finitely generated subgroup of $\mathbb{Q}^+$ and that $m\in\mathbb{N}$. For any squarefree integer η, let $t_\eta=\infty$ if either m is odd or for all $t\ge 0$, $\eta^{2^t}\mathbb{Q}^{*2^{t+1}}\notin\Gamma(2^{t+1})$ and $t_\eta=\min\left\{t\in\mathbb{N}:\eta^{2^t}\mathbb{Q}^{*2^{t+1}}\in\Gamma(2^{t+1})\right\}$ otherwise. Furthermore let $s_\eta=v_2\left(\frac{\delta(\eta)}{m}\right)$, where $\delta(\eta)$ is the discriminant of $\mathbb{Q}(\sqrt{\eta})$ and let $\sigma_\Gamma=\prod_{\ell\in\operatorname{Supp}\Gamma}\ell$. Then*

$$\varrho_{\Gamma,m}=\frac{1}{\varphi(m)}\prod_{\substack{\ell\mid m\\ \ell>2}}\left(1-\sum_{j\ge 1}\frac{\ell-1}{\ell^j|\Gamma(\ell^j)|}\right)\left(1-\sum_{\eta\mid\gcd(m,\sigma_\Gamma)}\psi_\eta\right),$$

where

$$\psi_\eta=\begin{cases}0 & \textit{if } t_\eta=\infty;\\ \displaystyle\sum_{k>t_\eta}\frac{1}{2^k\left|\Gamma(2^k)\right|} & \textit{if } s_\eta\le t_\eta<\infty;\\ -\frac{1}{2^{s_\eta}|\Gamma(2^{s_\eta})|}+\displaystyle\sum_{k>s_\eta}\frac{1}{2^k\left|\Gamma(2^k)\right|} & \textit{if } s_\eta>t_\eta.\end{cases}$$

It is not difficult to check that:

- since $\sum_{j\ge 1}\frac{1}{\ell^j|\Gamma(\ell^j)|}$ is rational for any prime ℓ, $\varrho_{\Gamma,m}$ is also rational;
- in the special case when $\Gamma=\langle a\rangle$ with $a>0$, the formulas of the above Theorems coincide. See for example [30, page 333–Remark 4].

The goal of this Chapter is to extend the above Theorem by removing the constraint that $\Gamma \subset \mathbb{Q}^+$. We prove the following:

Theorem 4.3. *Let Γ be a finitely generated subgroup of $\mathbb{Q}^*$ and that $m \in \mathbb{N}$. We assume the following notations:*

- *for $\beta \geq 1$, $\Gamma_2(2^\beta)$ is the 2–torsion subgroup of $\Gamma(2^\beta) = \Gamma \cdot (\mathbb{Q}^*)^{2^\beta} / (\mathbb{Q}^*)^{2^\beta}$;*
- *for $\gamma = \pm(\gamma_0)^{2^{\beta-1}} (\mathbb{Q}^*)^{2^\beta} \in \Gamma_2(2^\beta)$, with $\gamma_0 \in \mathbb{N}$ square free , $\delta(\gamma)$ denotes the field discriminant of $\mathbb{Q}(\sqrt{\gamma_0})$;*
- $\Gamma_2(2^\beta, m) = \{\gamma \in \Gamma_2(2^\beta) : \delta(\gamma) \mid 4m\}$;
- *for $\gamma \in \Gamma(2^\beta)$, $\operatorname{sgn}(\gamma) = \begin{cases} 1 & \textit{if } \gamma \subset \mathbb{Q}^>; \\ -1 & \textit{otherwise.} \end{cases}$*

Then

$$\varrho_{\Gamma,m} = \frac{1}{\varphi(m)} \prod_{\substack{\ell \mid m \\ \ell > 2}} \left(1 - \sum_{j \geq 1} \frac{\ell - 1}{\ell^j |\Gamma(\ell^j)|}\right) \times (1 - X_{\Gamma,m})$$

where,

- *if $2 \nmid m$, or, if $2 \| m$ and $-1 \in \Gamma$, $X_{\Gamma,m} = 0$;*
- *if $2 \| m$, $X_{\Gamma,m} = \sum_{\beta \geq 1} \frac{1}{2^\beta |\Gamma(2^\beta)|} \sum_{\gamma \in \Gamma_2(2^\beta, m)} \varepsilon(\beta, \gamma) \operatorname{sgn}(\gamma)$.*
  with $\varepsilon(1, \gamma) := \left(\frac{-4}{\gamma_0}\right)$, $\qquad \varepsilon(2, \gamma) := (-1)^{\gamma_0 + 1}$, $\qquad \varepsilon(\beta, \gamma) := 1$ for $\beta \geq 3$;
- *if $4 \| m$, $X_{\Gamma,m} = \sum_{\beta \geq 1} \frac{\left|\Gamma_2(2^\beta, m)\right|}{2^\beta \left|\Gamma(2^\beta)\right|} - \frac{|\{\gamma \in \Gamma_2(2, m) : 8 \mid \delta(\gamma)\}|}{|\Gamma(2)|}$;*
- *if $8 \mid m$, $X_{\Gamma,m} = \sum_{\beta \geq 1} \frac{\left|\Gamma_2(2^\beta, m)\right|}{2^\beta \left|\Gamma(2^\beta)\right|}$.*

4.2 The degree of Kummer extensions

In order to prove the Theorem, we need an explicit formula for the degree $[\mathbb{Q}(\zeta_m, \Gamma^{1/d}) : \mathbb{Q}]$ where $d \mid m$. A result with the correct level of generality can be found in [2]:

Lemma 4.1. *Let $\Gamma \subset \mathbb{Q}^*$ be a finitely generated group. Let $m, d \in \mathbb{N}$ with $d \mid m$. Then*

$$[\mathbb{Q}(\zeta_m, \Gamma^{1/d}) : \mathbb{Q}] = |\Gamma(d)| \times |\tilde{\Gamma}_{m,d}|^{-1} \tag{4.2}$$

where $\Gamma(d) := \Gamma \cdot \mathbb{Q}^{*d} / \mathbb{Q}^{*d}$ and

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

Here, if we let $\Gamma_2(d) = \Gamma(2^{v_2(d)})[2]$, the 2–torsion group and, for $\gamma = \pm\gamma_0^{2^{v_2(d)-1}} {\mathbb{Q}^*}^{2^{v_2(d)}} \in \Gamma_2(d)$, with $\gamma_0 > 0$ not the exact power of any rational number, we let $\delta(\gamma) := \operatorname{disc}(\mathbb{Q}(\sqrt{\gamma_0})$, then

$$\tilde{\Gamma}^+_{m,d} = \{\gamma \in \Gamma_2(d) : \gamma \subset \mathbb{Q}^+, \delta(\gamma) \mid m\}$$

and

$$\tilde{\Gamma}^{-}_{m,d} = \begin{cases} \{\gamma \in \Gamma_2(d) : \gamma \not\subseteq \mathbb{Q}^+, \delta(\gamma) \mid m\} & \textit{if } v_2(d) < v_2(m) \\ \{\gamma \in \Gamma_2(d) : \gamma \not\subseteq \mathbb{Q}^+, \delta(\gamma) \mid 2m \textit{ but } \delta(\gamma) \nmid m\} & \textit{if } v_2(d) = v_2(m). \end{cases}$$

4.3 Proof of Theorem 4.3

Proof. We use the formulas for the degrees of Lemma 4.1 which lead to the following identity:

$$[\mathbb{Q}(\zeta_{nd}, \Gamma^{1/\gamma(f,\frac{n}{m})}) : \mathbb{Q}] = \frac{d\varphi(n)}{|\tilde{\Gamma}_{nd,\gamma(f,\frac{n}{m})}|} \prod_{\ell \mid f} \left| \Gamma(\ell^{v_\ell(n/m)+1}) \right|,$$

where $\gamma(f, \frac{n}{m}) = \prod_{\ell \mid f} \ell^{v_\ell(\frac{n}{m})+1}$. Note that $\tilde{\Gamma}_{nd,\gamma(f,\frac{n}{m})}$ is trivial if f is odd while if $2 \mid f$, then $v_2(\gamma(f, \frac{n}{m})) = v_2(\frac{n}{m}) + 1$, so that (if $2 \mid f$) $\tilde{\Gamma}_{nd,\gamma(f,\frac{n}{m})} = \tilde{\Gamma}_{nd,2n/m}$. Also note that, if $2 \mid n$, $2n/m$ is a divisor of nd. Thus, the sum defining $\varrho_{\Gamma,m}$ in (4.1), equals

$$\begin{aligned} & \sum_{n \in \mathcal{S}_m} \frac{1}{\varphi(n)} \sum_{d \mid n} \frac{\mu(d)}{d} \sum_{\substack{f \mid n \\ f \text{ odd}}} \mu(f) \prod_{\ell \mid f} \frac{1}{\left|\Gamma(\ell^{v_\ell(\frac{\ell n}{m})})\right|} \\ + & \sum_{n \in \mathcal{S}_m} \left(\sum_{\substack{f \mid n \\ f \text{ even}}} \mu(f) \prod_{\ell \mid f} \frac{1}{\left|\Gamma(\ell^{v_\ell(\frac{\ell n}{m})})\right|} \right) \left(\frac{1}{\varphi(n)} \sum_{d \mid n} \frac{\mu(d)}{d} \# \tilde{\Gamma}_{nd,2n/m} \right) \\ = & \ S_1 + S_2, \end{aligned}$$

say. To compute S_1, we use the identity

$$\frac{1}{\varphi(n)} \sum_{d \mid n} \frac{\mu(d)}{d} = \frac{1}{n}.$$

So that

$$\begin{aligned} S_1 &= \sum_{n \in \mathcal{S}_m} \frac{1}{n} \prod_{\substack{\ell \mid m \\ \ell \geq 3}} \left(1 - \left| \Gamma(\ell^{v_\ell(n/m)+1}) \right|^{-1} \right) \\ &= \left(\sum_{\alpha \geq v_2(m)} \frac{1}{2^\alpha} \right) \times \prod_{\substack{\ell \mid m \\ \ell \geq 3}} \sum_{j \geq v_\ell(m)} \frac{1}{\ell^j} \left(1 - \left| \Gamma(\ell^{j - v_\ell(m)+1}) \right|^{-1} \right) \qquad (4.3) \\ &= \frac{2}{m} \prod_{\substack{\ell \mid m \\ \ell \geq 3}} \sum_{j \geq 0} \frac{1}{\ell^j} \left(1 - \left| \Gamma(\ell^{j+1}) \right|^{-1} \right) = \frac{1}{\varphi(m)} \prod_{\substack{\ell \mid m \\ \ell \geq 3}} \left(1 - (\ell - 1) \sum_{j \geq 1} \frac{1}{\ell^j \left| \Gamma(\ell^j) \right|} \right). \end{aligned}$$

We also deduce that for m odd, $S_2 = 0$, since the sum over f is empty, and

$$\varrho_{\Gamma,m} = \frac{1}{\varphi(m)} \prod_{\substack{\ell \mid m \\ \ell \geq 3}} \left(1 - \sum_{j \geq 1} \frac{\ell - 1}{\ell^j \, |\Gamma(\ell^j)|} \right).$$

When m is even, in order to compute

$$\begin{aligned} S_2 &= \sum_{n \in \mathcal{S}_m} \left(\sum_{\substack{f \mid n \\ f \text{ odd}}} \mu(f) \prod_{\ell \mid f} \frac{1}{\left| \Gamma\big(\ell^{v_\ell(\frac{\ell n}{m})}\big) \right|} \right) \frac{-1}{\left| \Gamma\big(2^{v_2(2n/m)}\big) \right|} \left(\frac{1}{\varphi(n)} \sum_{d \mid n} \frac{\mu(d)}{d} \# \tilde{\Gamma}_{nd,2n/m} \right) \\ &= \sum_{n \in \mathcal{S}_m} \left(\prod_{\substack{\ell \mid m \\ \ell \geq 3}} 1 - \frac{1}{\left| \Gamma\big(\ell^{v_\ell(\frac{\ell n}{m})}\big) \right|} \right) \frac{-1}{\left| \Gamma\big(2^{v_2(2n/m)}\big) \right|} \left(\frac{1}{\varphi(n)} \sum_{d \mid n} \frac{\mu(d)}{d} \# \tilde{\Gamma}_{nd,2n/m} \right), \end{aligned} \tag{4.4}$$

we observe that if, for $k \in \mathbb{N}$ we write $k = 2^{v_2(k)} k'$, then

$$\# \tilde{\Gamma}_{nd,2n/m} = \# \tilde{\Gamma}_{2^{v_2(dn)} m', 2^{v_2(2n/m)}}.$$

Hence

$$\begin{aligned} \frac{1}{\varphi(n)} \sum_{d \mid n} \frac{\mu(d)}{d} \# \tilde{\Gamma}_{nd,2n/m} &= \frac{1}{\varphi(n')} \sum_{d \mid n'} \frac{\mu(d)}{d} \times \frac{1}{2^{v_2(n)-1}} \left(\# \tilde{\Gamma}_{2^{v_2(n)} m', 2^{v_2(2n/m)}} - \frac{1}{2} \# \tilde{\Gamma}_{2^{v_2(2n)} m', 2^{v_2(2n/m)}} \right) \\ &= \frac{2}{n} \left(\# \tilde{\Gamma}_{2^{v_2(n)} m', 2^{v_2(2n/m)}} - \frac{1}{2} \# \tilde{\Gamma}_{2^{v_2(2n)} m', 2^{v_2(2n/m)}} \right). \end{aligned}$$

By replacing the above in (4.4), we obtain, for m even:

$$\begin{aligned}
S_2 &= \sum_{n\in\mathcal{S}_m}\left(\prod_{\substack{\ell\mid m\\ \ell\geq 3}} 1-\frac{1}{\left|\Gamma\left(\ell^{v_\ell(\frac{\ell n}{m})}\right)\right|}\right)\frac{-1}{\left|\Gamma\left(2^{v_2(2n/m)}\right)\right|}\frac{2}{n}\left(\#\tilde{\Gamma}_{2^{v_2(n)}m',2^{v_2(2n/m)}}-\frac{1}{2}\#\tilde{\Gamma}_{2^{v_2(2n)}m',2^{v_2(2n/m)}}\right)\\
&= \sum_{n'\in\mathcal{S}_{m'}}\frac{1}{n'}\left(\prod_{\substack{\ell\mid m\\ \ell\geq 3}} 1-\frac{1}{\left|\Gamma\left(\ell^{v_\ell(\frac{\ell n}{m})}\right)\right|}\right)\times\sum_{\alpha\geq v_2(m)}\frac{-1}{2^{\alpha-1}\left|\Gamma\left(2^{\alpha-v_2(m/2)}\right)\right|}\left(\#\tilde{\Gamma}_{2^{\alpha}m',2^{\alpha-v_2(m/2)}}\right.\\
&\quad\left.-\frac{1}{2}\#\tilde{\Gamma}_{2^{\alpha+1}m',2^{\alpha-v_2(m/2)}}\right)\\
&= S_1\times\sum_{\beta\geq 1}\frac{-1}{2^{\beta}\left|\Gamma(2^{\beta})\right|}\left(2\#\tilde{\Gamma}_{2^{\beta-1}m,2^{\beta}}-\#\tilde{\Gamma}_{2^{\beta}m,2^{\beta}}\right)\\
&= S_1\times\sum_{\beta\geq 1}\frac{-1}{2^{\beta}\left|\Gamma(2^{\beta})\right|}\sum_{\gamma\in\Gamma_2(2^{\beta})}\tau_{\gamma,m,2^{\beta}}
\end{aligned}$$

where,

$$\tau_{\gamma,m,2^{\beta}}=\begin{cases}2 & \text{if } \gamma\in\tilde{\Gamma}_{2^{\beta-1}m,2^{\beta}}\setminus\tilde{\Gamma}_{2^{\beta}m,2^{\beta}}\\ 1 & \text{if } \gamma\in\tilde{\Gamma}_{2^{\beta-1}m,2^{\beta}}\cap\tilde{\Gamma}_{2^{\beta}m,2^{\beta}}\\ 0 & \text{if } \gamma\notin\tilde{\Gamma}_{2^{\beta-1}m,2^{\beta}}\cup\tilde{\Gamma}_{2^{\beta}m,2^{\beta}}\\ -1 & \text{if } \gamma\in\tilde{\Gamma}_{2^{\beta}m,2^{\beta}}\setminus\tilde{\Gamma}_{2^{\beta-1}m,2^{\beta}}.\end{cases}$$

Clearly $\tau_{\gamma,2^{\beta},m}=0$ if $\delta(\gamma)'\nmid m'$. Therefore we can write:

$$S_2=S_1\times\sum_{\beta\geq 1}\frac{-1}{2^{\beta}\left|\Gamma(2^{\beta})\right|}\sum_{\substack{\gamma\in\Gamma_2(2^{\beta})\\ \delta(\gamma)'\mid m'}}\tau_{\gamma,m,2^{\beta}}.$$

First assume that $\delta(\gamma)'\mid m'$ and that $4\mid m$. Then

$$\tau_{\gamma,m,2^{\beta}}=\begin{cases}1 & \text{if } \beta\geq 2, \text{ or}\\ & \text{if } \beta=1 \text{ and } v_2(\delta(\gamma))\leq v_2(m);\\ -1 & \text{if } \beta=1 \text{ and } v_2(\delta(\gamma))=v_2(m)+1.\end{cases}$$

Note that it is impossible that $v_2(\delta(\gamma))>v_2(m)+1$ since $4\mid m$.

Second assume that $\delta(\gamma)' \mid m'$ and that $2 \| m$.

$$\tau_{\gamma,m,2^\beta} = \begin{cases} 1 & \text{if } v_2(\delta(\gamma)) \leq \beta; \\ -1 & \text{if } v_2(\delta(\gamma)) = \beta+1; \\ 0 & \text{if } v_2(\delta(\gamma)) > \beta+1 \end{cases} \text{ if } \gamma \subset \mathbb{Q}^{>}, \qquad \tau_{\gamma,m2^\beta} = \begin{cases} -1 & \text{if } v_2(\delta(\gamma)) \leq \beta; \\ 1 & \text{if } v_2(\delta(\gamma)) = \beta+1; \\ 0 & \text{if } v_2(\delta(\gamma)) > \beta+1 \end{cases} \text{ if } \gamma \not\subset \mathbb{Q}^{>}.$$

In the case when $-1 \in \Gamma$, $\gamma \in \Gamma_2(2^\beta)$ if and only if $-\gamma \in \Gamma_2(2^\beta)$. Hence, if $2\|m$ and $-1 \in \Gamma$,

$$\sum_{\substack{\gamma \in \Gamma_2(2^\beta) \\ \delta(\gamma)' | m'}} \tau_{\gamma,m,2^\beta} = 0.$$

We are left to consider the case $2\|m$ and $-1 \notin \Gamma$.

It is not easy to check that if $\operatorname{sgn}\gamma = 1$ if $\gamma \subset \mathbb{Q}^{>}$ and -1 otherwise, then

$$\tau_{\gamma,m,2} = \begin{cases} \operatorname{sgn}\gamma & \text{if } \gamma_0 \equiv 1 \bmod 4 \\ -\operatorname{sgn}(\gamma) & \text{if } \gamma_0 \equiv 3 \bmod 4 \\ 0 & \text{if } \gamma_0 \equiv 2 \bmod 4, \end{cases} \qquad \tau_{\gamma,m,4} = \begin{cases} \operatorname{sgn}\gamma & \text{if } \gamma_0 \equiv \pm 1 \bmod 4 \\ -\operatorname{sgn}\gamma & \text{if } \gamma_0 \equiv 2 \bmod 4. \end{cases}$$

and

$$\tau_{\gamma,m,2^\beta} = \operatorname{sgn}\gamma \text{ if } \beta \geq 3.$$

Therefore

$$S_2 = -S_1 \times \left(\frac{1}{2\,|\Gamma(2)|} \sum_{\gamma \in \Gamma_2(2,m)} \left(\frac{-4}{\gamma_0}\right) \operatorname{sgn}\gamma + \frac{1}{4\,|\Gamma(4)|} \sum_{\gamma \in \Gamma_2(4,m)} (-1)^{\gamma_0+1} \operatorname{sgn}\gamma \right.$$
$$\left. + \sum_{\beta \geq 3} \frac{1}{2^\beta \left|\Gamma(2^\beta)\right|} \sum_{\gamma \in \Gamma_2(2^\beta,m)} \operatorname{sgn}\gamma \right)$$

and this completes the proof. □

4.4 How to explicitely compute $\varrho(\Gamma, m)$

The crucial step to compute the density $\varrho(\Gamma, m)$ is the calculation of the sizes of the groups:

$$\Gamma(\ell^a) := \Gamma \cdot (\mathbb{Q}^*)^{\ell^a} / (\mathbb{Q}^*)^{\ell^a}$$

for various primes ℓ. This is done to some extent in [**?**]. Let $\|\Gamma\| = \{|g| : g \in \Gamma\} \subset \mathbb{Q}^{>}$. If ℓ is odd, then we have that

$$\#\Gamma(\ell^a) = \#\|\Gamma\|(\ell^a).$$

If $\ell = 2$, then

$$\#\Gamma(2^a) = \begin{cases} 2 \times \#\|\Gamma\|(2^a) & \text{if } -(\mathbb{Q}^*)^{2^a} \in \Gamma(2^a) \\ \#\|\Gamma\| & \text{otherwise.} \end{cases}$$

Suppose that $\Gamma \subset \mathbb{Q}^{>}$ and $n \in \mathbb{N}$. Then

$$\#\Gamma\,(n) = \frac{n^r}{\gcd(n^r, n^{r-1}\Delta_1, \ldots, n\Delta_{r-1}, \Delta_r)}.$$

where the elementary divisors $\Delta_1, \ldots, \Delta_r$ are defined as follows: Let $\operatorname{Supp}\Gamma = \{p_1, \ldots, p_r\}$ be the support of Γ, suppose that r is its rank and that $a_1, \ldots, a_r$ is a free set of generators of Γ. Write

$$a_i = p_1^{e_{i1}} \cdot p_2^{e_{i2}} \cdots p_r^{e_{ir}}.$$

Then Δ_k is the $\gcd$ of all the $k \times k$ minors of the matrix (e_{ij}).

- If $\gcd(\Delta_r, m) = 1$, then $\Gamma(\ell^a) = \ell^{ra}$ and

$$\frac{1}{\varphi(m)}\prod_{\ell|m}\left(1 - \sum_{\beta\geq 1}\frac{\ell-1}{\ell^\beta\#\Gamma(\ell^\beta)}\right) = \frac{1}{m}\prod_{\ell|}\left(\frac{\ell}{\ell-1} - \frac{\ell}{\ell^{r+1}-1}\right) = \frac{1}{m}\prod_{\ell|m}\frac{\ell^2(\ell^r-1)}{(\ell-1)(\ell^{r+1}-1)}$$

- Suppose $r = 2$ and set $x_1 = v_2(\Delta_1)$ and $x_2 = v_2(\Delta_2)$.

$$\begin{aligned}
\frac{\ell}{\ell-1} - \ell\left\{\sum_{\beta\geq 1}\frac{\ell^{\max\{\beta^2, x_1\beta, x_2\}}}{\ell^{3\beta}}\right\} &= \frac{\ell}{\ell-1} - \ell\left\{\sum_{1\leq\alpha\leq x_1}\frac{1}{\ell^\alpha} + \sum_{x_1<\alpha\leq x_2-x_1}\frac{\ell^{x_1}}{\ell^{2\alpha}} + \sum_{\alpha>x_2-x_1}\frac{\ell^{x_2}}{\ell^{3\alpha}}\right\} \\
&= \frac{\ell}{\ell-1} - \ell\left\{\frac{1}{\ell}\frac{\ell^{-x_1}-1}{\ell^{-1}-1} + \ell^{-x_1}\sum_{0<\alpha\leq x_2-2x_1}\frac{1}{\ell^{2\alpha}} + \ell^{2x_2-3x_1}\sum_{\alpha>0}\frac{1}{\ell^{3\alpha}}\right\} \\
&= \frac{\ell}{\ell-1} - \ell\left\{\frac{1-\ell^{-x_1}}{\ell-1} + \ell^{-x_1}\frac{1-\ell^{-2x_2+4x_1}}{\ell^2-1} + \ell^{-2x_2+3x_1}\frac{1}{\ell^3-1}\right\} \\
&= \frac{1}{\ell^{x_1}}\frac{\ell^2}{\ell^2-1} - \frac{1}{\ell^{2x_2-3x_1}}\frac{\ell^4-\ell^3}{(\ell^2-1)(\ell^3-1)}.
\end{aligned}$$

Hence

$$\frac{1}{\varphi(m)}\prod_{\ell|m}\left(1 - \sum_{\beta\geq 1}\frac{\ell-1}{\ell^\beta\#\Gamma(\ell^\beta)}\right) = \frac{1}{m}\prod_{\ell|m}\left(\frac{1}{\ell^{x_1}}\frac{\ell^2}{\ell^2-1} - \frac{1}{\ell^{2x_2-3x_1}}\frac{\ell^4-\ell^3}{(\ell^2-1)(\ell^3-1)}\right).$$

More complicated formulas can be derived also for the case when $r \geq 3$.

4.4.1 Comparison with Moree's formulas

Suppose $r = 1$ and $\Gamma = \langle a \rangle$ with $a \in \mathbb{Q} \setminus \{-1, 0, 1\}$, we write $a = \pm a_0^h$ with $a_0 > 0$ not the exact power of a rational number. Then $h = \Delta_1$ and $\#\langle a \rangle(m) = m/\gcd(m, h)$. A quick calculation shows that

$$\frac{1}{\varphi(m)} \prod_{\substack{\ell | m \\ \ell > 3}} \left(1 - \sum_{\beta \geq 1} \frac{\ell - 1}{\ell^\beta \# \Gamma(\ell^\beta)}\right) = \frac{2^{v_2(h)+1}}{m \gcd(h, m^\infty)} \prod_{\substack{\ell | m \\ \ell > 3}} \frac{\ell^2}{\ell^2 - 1}.$$

In fact, if $x_1 = v_2(h)$, then

$$\frac{\ell}{\ell - 1} - \ell \left(\sum_{\beta \geq 1} \frac{\ell^{\max\{\beta, x_1\}}}{\ell^{2\beta}}\right) = \frac{1}{\ell^{x_1}} \frac{\ell^2}{\ell^2 - 1}.$$

Hence, for m odd, the formulas of Theorem 4.3 and of Theorem 4.1 coincides. We also deduce that for $2 \mid m$

$$\varrho(\Gamma, m) = \frac{1}{m \gcd(h, m^\infty)} \prod_{\ell | m} \frac{\ell^2}{\ell^2 - 1} \times \frac{3}{2} \times 2^{v_2(h)} \left(1 - X_{\Gamma, m}\right).$$

If $2 \mid m$, then

$$\Gamma(2^\beta) = \begin{cases} \{\mathbb{Q}^{*2^\beta}, -\mathbb{Q}^{*2^\beta}\} & \text{if } a < 0 \text{ and } v_2(h) \geq \beta; \\ \{\mathbb{Q}^{*2^\beta}\} & \text{if } a > 0 \text{ and } v_2(h) \geq \beta; \\ \{a^j \mathbb{Q}^{*2^\beta} : j = 0, \ldots, 2^{\beta - v_2(h)} - 1\} & \text{if } \beta > v_2(h). \end{cases}$$

Assume that $\delta(a) \nmid 4m$. Then

$$\Gamma_2(2^\beta, m) = \begin{cases} \{\mathbb{Q}^{*2^\beta}, -\mathbb{Q}^{*2^\beta}\} & \text{if } a < 0 \text{ and } v_2(h) \geq \beta; \\ \{\mathbb{Q}^{*2^\beta}\} & \text{otherwise.} \end{cases}$$

Hence

$$1 - \sum_{\beta \geq 1} \frac{|\Gamma_2(2^\beta, m)|}{2^\beta |\Gamma(2^\beta)|} = \frac{2}{3 \times 2^{v_2(h)}}$$

Finally

$$\frac{3}{2} \times 2^{v_2(h)} \left(1 - X_{\Gamma, m}\right) = \begin{cases} 1 & \text{if } a > 0 \text{ or if } 4 | m; \\ \frac{3}{2} \times 2^{v_2(h)} \left(1 - \frac{1}{3 \times 2^{v_2(h)}}\right) & \text{if } a < 0 \text{ and } 2 \| m. \end{cases}$$

Hence, for m odd or for $\delta(a) \nmid 4m$, the formulas of Theorem 4.3 and of Theorem 4.1 coincides.

Next assume that $2 \mid m$, $a > 0$ and that $\delta(a) \mid 4m$. Then

$$\Gamma_2(2^\beta, m) = \begin{cases} \{\mathbb{Q}^{*2^\beta}\} & \textit{if } v_2(h) \geq \beta \\ \{\mathbb{Q}^{*2^\beta}, a_0^{2^{\beta-1}}\mathbb{Q}^{*2^\beta}\} & \textit{if } v_2(h) < \beta. \end{cases}$$

Hence

$$1 - \sum_{\beta \geq 1} \frac{|\Gamma_2(2^\beta, m)|}{2^\beta |\Gamma(2^\beta)|} = \frac{1}{3 \times 2^{v_2(h)}}.$$

Finally

$$\frac{3}{2} \times 2^{v_2(h)} \left(1 - X_{\Gamma,m}\right) = \begin{cases} 17/16 & \text{if } 2\|m, v_2(h) = 0 \text{ and } 8 \mid \delta(a); \\ 5/4 & \text{if } 4\|m, 8 \mid \delta(a) \text{ and } v_2(h) = 0; \\ & \text{if } 2\|m, v_2(h) = 1 \text{ and } 8 \mid \delta(a); \\ & \text{if } 2\|m, v_2(h) = 0 \text{ and } 4\|\delta(a); \\ 1/2 & \text{if } 8 \mid m, \text{ or} \\ & \text{if } 4\|m, 8 \nmid \delta(a) \text{ or } v_2(h) > 0; \\ & \text{if } 2\|m, v_2(h) > 1; \\ & \text{if } 2\|m, v_2(h) = 1, 8 \nmid \delta(a); \\ & \text{if } 2\|m, v_2(h) = 0, 2 \nmid \delta(a). \end{cases}$$

Hence, for m odd or for $\delta(a) \nmid 4m$ or for $a > 0$, the formulas of Theorem 4.3 and of Theorem 4.1 coincides.

Last assume that $2 \mid m$, $a < 0$ and that $\delta(a) \mid 4m$. Then

$$\Gamma_2(2^\beta, m) = \begin{cases} \{\mathbb{Q}^{*2^\beta}, -\mathbb{Q}^{*2^\beta}\} & \textit{if } v_2(h) \geq \beta \\ \{\mathbb{Q}^{*2^\beta}, -a_0^{2^{\beta-1}}\mathbb{Q}^{*2^\beta}\} & \textit{if } v_2(h) = \beta - 1 \\ \{\mathbb{Q}^{*2^\beta}, a_0^{2^{\beta-1}}\mathbb{Q}^{*2^\beta}\} & \textit{if if } v_2(h) < \beta - 1. \end{cases}$$

Hence

$$1 - \sum_{\beta \geq 1} \frac{|\Gamma_2(2^\beta, m)|}{2^\beta |\Gamma(2^\beta)|} = \frac{1}{3 \times 2^{v_2(h)}}.$$

Finally, if $4 \mid m$, then

$$\frac{3}{2} \times 2^{v_2(h)} \left(1 - X_{\Gamma,m}\right) = \begin{cases} 5/4 & \text{if } 4\|m, 8 \mid \delta(a) \text{ and } v_2(h) = 0; \\ 1/2 & \text{if } 8 \mid m \\ & \text{if } 4\|m, 8 \nmid \delta(a) \text{ or } v_2(h) > 0, \end{cases}$$

and, if $2\|m$,then

$$\frac{3}{2}\times 2^{v_2(h)}\left(1-X_{\Gamma,m}\right)=\begin{cases}17/16 & \text{if } v_2(\delta(a)=3 \text{ and } v_2(h)=0;\\ 1/2 & \text{if } v_2(\delta(a))=2 \text{ and } v_2(h)=0;\\ 5/4 & \text{if } v_2(\delta(a))=0 \text{ and } v_2(h)=0;\\ 2 & \text{if } v_2(\delta(a))=3 \text{ and } v_2(h)=1;\\ 11/4 & \text{if } v_2(\delta(a))<3 \text{ and } v_2(h)=1;\\ \frac{3}{2}\times 2^{v_2(h)}-1/4 & \text{if } v_2(h)\geq 2.\end{cases}$$

Hence, in all cases when $\Gamma=\langle a\rangle$, the formulas of Theorem 4.3 and of Theorem 4.1 coincides.

4.5 Numerical Data

In this section we compare numerical data. The density $\varrho(\Gamma,m)$ can be explicitely computed once a set of generators of Γ is given. The first table compares the values of $\varrho(\langle -1,a\rangle,m)$ as in Theorem 4.3 (second row) and $\frac{\pi(10^9,\langle -1,a\rangle,m)}{\pi(10^9)}$ (first row) with $2\leq a\leq 10$ and $m=2,\ldots,10$. All values have been truncated to 7 decimal digits.

$m\backslash a$	2	3	4	5	6	7	8	9	10
2	0.9999999	0.9999999	0.9999999	0.9999999	0.9999999	0.9999999	0.9999999	0.9999999	0.9999999
	1.0000000	1.0000000	1.0000000	1.0000000	1.0000000	1.0000000	1.0000000	1.0000000	1.0000000
3	0.3750162	0.3749919	0.3750162	0.3749945	0.3750245	0.3749809	0.1249966	0.3749919	0.3749708
	0.3750000	0.3750000	0.3750000	0.3750000	0.3750000	0.3750000	0.1250000	0.3750000	0.3750000
4	0.4166745	0.3333555	0.0833265	0.3333396	0.3333192	0.3333367	0.4166745	0.1666562	0.3333669
	0.4166666	0.3333333	0.0833333	0.3333333	0.3333333	0.3333333	0.4166666	0.1666666	0.3333333
5	0.2083311	0.2083280	0.2083311	0.2083616	0.2083418	0.2083259	0.2083311	0.2083280	0.2083098
	0.2083333	0.2083333	0.2083333	0.2083333	0.2083333	0.2083333	0.2083333	0.2083333	0.2083333
6	0.3750162	0.3749919	0.3750162	0.3749945	0.3750245	0.3749809	0.1249966	0.3749919	0.3749708
	0.3750000	0.3750000	0.3750000	0.3750000	0.3750000	0.3750000	0.1250000	0.3750000	0.3750000
7	0.1458489	0.1458220	0.1458489	0.1458239	0.1458389	0.1458159	0.1458489	0.1458220	0.1458463
	0.1458333	0.1458333	0.1458333	0.1458333	0.1458333	0.1458333	0.1458333	0.1458333	0.1458333
8	0.0833265	0.1666562	0.0416661	0.1666921	0.1666536	0.1666561	0.0833265	0.0833204	0.1666902
	0.0833333	0.1666666	0.0833333	0.1666666	0.1666666	0.1666666	0.0833333	0.0833333	0.1666666
9	0.1249966	0.1250027	0.1249966	0.1249958	0.1250068	0.1250054	0.0416750	0.1250027	0.1249969
	0.1250000	0.1250000	0.1250000	0.1250000	0.1250000	0.1250000	0.0416666	0.1250000	0.1250000
10	0.2083311	0.2083280	0.2083616	0.2083616	0.2083418	0.2083259	0.2083311	0.2083280	0.2083098
	0.2083333	0.2083333	0.2083333	0.2083333	0.2083333	0.2083333	0.2083333	0.2083333	0.2083333

The next table compares the values of $\varrho(\langle -a,b\rangle,m)$ as in Theorem 4.3 (second row) and $\frac{\pi(10^9,\langle -a,b\rangle,m)}{\pi(10^9)}$ (first row) with $2\leq a,b\leq 5$ and $\langle -a,b\rangle$ of rank 2. All values have been truncated to 7 decimal digits.

$m\backslash(-a,b)$	(-2,3)	(-2,5)	(-3,2)	(-3,4)	(-3,5)	(-4,3)	(-4,5)	(-5,2)	(-5,3)	(-5,4)
2	0.8705485	0.8705288	0.8705338	0.7410800	0.8571489	0.9285638	0.9285677	0.8705286	0.8571464	0.7410777
	0.8705457	0.8705457	0.8705457	0.7410714	0,8571428	0.9285714	0.9285714	0.8705457	0,8571428	0.7410714
3	0.4615489	0.4615368	0.4615489	0.4615489	0.4615306	0.4615489	0.4615368	0.4615368	0.4615306	0.4615368
	0.4615384	0.4615384	0.4615384	0.4615384	0.4615384	0.4615384	0.4615384	0.4615384	0.4615384	0.4615384
4	0.4821469	0.4821530	0.4821469	0.3392994	0.4285866	0.3392994	0.3392914	0.4821530	0.4285866	0.3392914
	0.4821428	0.4821428	0.4821428	0.3392857	0.4285714	0.3392857	0.3392857	0.4821428	0.4285714	0.3392857
5	0.2419332	0.2419311	0.2419332	0.2419332	0.2419252	0.2419332	0.2419311	0.2419311	0.2419252	0.2419311
	0.2419354	0.2419354	0.2419354	0.2419354	0.2419354	0.2419354	0.2419354	0.2419354	0.2419354	0.2419354
6	0.4574275	0.4017685	0.3420480	0.2225239	0.3296714	0.3956073	0.4285727	0.4017794	0.4450531	0.3420354
	0.4574175	0.4017857	0.3420329	0.2225274	0.3296703	0.3956043	0.4285714	0.4017857	0.4450549	0,3420329
7	0.1637375	0.1637373	0.1637375	0.1637375	0.1637352	0.1637375	0.1637373	0.1637373	0.1637352	0.1637373
	0.1637426	0.1637426	0.1637426	0.1637426	0.1637426	0.1637426	0.1637426	0.1637426	0.1637426	0.1637426
8	0.1785587	0.1785900	0.1785587	0.1696331	0.2142934	0.1696331	0.1696659	0.1785900	0.2142934	0.1696659
	0.1785714	0.1785714	0.1785714	0.1696428	0.2142857	0.1696428	0.1696428	0.1785714	0.2142857	0.1696428
9	0.1538451	0.1538464	0.1538451	0.1538451	0.1538590	0.1538451	0.1538464	0.1538464	0.1538590	0.1538464
	0.1538461	0.1538461	0.1538461	0.1538461	0.1538461	0.1538461	0.1538461	0.1538461	0.1538461	0.1538461
10	0.2106084	0.1792937	0.2106117	0.1792846	0.1728040	0.2246538	0.2073685	0.2397705	0.2332921	0.2376132
	0.2106134	0.1792914	0.2106134	0.1792914	0.1728110	0.2246543	0.2073732	0.2397753	0.2332949	0.2376152

The next table compares the values of $\varrho(\langle -a,-b\rangle, m)$ as in Theorem 4.3 (second row) and $\frac{\pi(10^9,\langle -a,-b\rangle,m)}{\pi(10^9)}$ (first row) with $2 \leq a < b \leq 5$ and $\langle -a,-b\rangle$ of rank 2 which do not appear in the table above. All values have been truncated to 7 decimal digits.

$m\backslash(-a,b)$	(-2,-3)	(-2,-5)	(-3,-4)	(-3,-5)	(-4,-5)
2	0.8705314	0.8705488	0.9285885	0.8571462	0.9285705
	0.8705357	0.8705357	0.9285714	0.8571428	0.8705357
3	0.4615489	0.4615368	0.4615489	0.4615306	0.4615368
	0.4615384	0.4615384	0.4615384	0.4615384	0.4615384
4	0.4821469	0.4821530	0.3392994	0.4285866	0.3392914
	0.4821428	0.4821428	0.3392857	0.4285714	0.3392857
5	0.2419332	0.2419311	0.2419332	0.2419252	0.2419311
	0.2419332	0.2419311	0.2419332	0.2419332	0.2419252
6	0.3420248	0.4017928	0.3956284	0.3296539	0.4285691
	0.34203296	0.4017857	0.3956043	0.3296703	0.4285714
7	0.1637375	0.1637373	0.1637375	0.1637352	0.1637373
	0.1637426	0.1637426	0.1637426	0.1637426	0.1637426
8	0.1785587	0.1785900	0.1696331	0.2142934	0.1696659
	0.1785714	0.1785714	0.1696428	0.2142857	0.1696428
9	0.1538451	0.1538464	0.1538451	0.1538590	0.1538464
	0.1538461	0.1538461	0.1538461	0.1538461	0.1538461
10	0.2106062	0.2397738	0.2246562	0.2332870	0.2073765
	0.2106134	0.2397753	0.2246543	0.2332949	0.2073732

The next table compares the values of $\varrho(\langle \pm 2, \pm 3, \pm 5\rangle, m)$ as in Theorem 4.3 (second row) and $\frac{\pi(10^9,\langle \pm 2,\pm 3,\pm 5\rangle,m)}{\pi(10^9)}$ (first row) and $m = 2,\ldots,10$. All values have been truncated to 7 decimal digits.

$m\backslash(\pm a, \pm b, \pm c)$	(-2,3,5)	(2,-3,5)	(2,3,-5)	(-2,-3,5)	(-2,3,-5)	(2,-3,-5)	(-2,-3,-5)
2	09369727	0.9369867	0.9369780	0.9369753	0.9369809	0.9369824	0.9369852
	0.9369791	0.9369791	0.9369791	0.9369791	0.9369791	0.9369791	0.9369791
3	0.4874978	0.4874978	0.4874978	0.4874978	0.4874978	0.4874978	0.4874978
	0.4875000	0.4875000	0.4875000	0.4875000	0.4875000	0.4875000	0.4875000
4	0.4958488	0.4958488	0.4958488	0.4958488	0.4958488	0.4958488	0.4958488
	0.4958333	0.4958333	0.4958333	0.4958333	0.4958333	0.4958333	0.4958333
5	0.2483914	0.2483914	0.2483914	0.2483914	0.2483914	0.2483914	0.2483914
	0.2483974	0.2483974	0.2483974	0.2483974	0.2483974	0.2483974	0.2483974
6	0.4869885	0.4260683	0.4869926	0.4260422	0.4869911	0.4260532	0.4260539
	0.4869921	0.4260546	0.4869921	0.4260546	0.4869921	0.4260546	0.4260546
7	0.1662449	0.1662449	0.1662449	0.1662449	0.1662449	0.1662449	0.1662449
	0.1662500	0.1662500	0.1662500	0.1662500	0.1662500	0.1662500	0.1662500
8	0.2166697	0.2166697	0.2166697	0.2166697	0.2166697	0.2166697	0.2166697
	0.2166666	0.2166666	0.2166666	0.2166666	0.2166666	0.2166666	0.2166666
9	0.1625054	0.1625054	0.1625054	0.1625054	0.1625054	0.1625054	0.1625054
	0.1625000	0.1625000	0.1625000	0.1625000	0.1625000	0.1625000	0.1625000
10	0.2170817	0.2170833	0.2481338	0.2170819	0.2481318	0.2481331	0.2481336
	0.2170890	0.2170890	0.2481386	0.2170890	0.2481386	0.2481386	0.2481386
11	0.0999258	0.0999258	0.0999258	0.0999258	0.0999258	0.0999258	0.0999258
	0.0999316	0.0999316	0.0999316	0.0999316	0.0999316	0.0999316	0.0999316
12	0.2396969	0.2396969	0.2396969	0.2396969	0.2396969	0.2396969	0.2396969
	0.2396875	0.2396875	0.2396875	0.2396875	0.2396875	0.2396875	0.2396875
13	0.0832971	0.0832971	0.0832971	0.0832971	0.0832971	0.0832971	0.0832971
	0.0832983	0.0832983	0.0832983	0.0832983	0.0832983	0.0832983	0.0832983
14	0.1557722	0.1557708	0.1557699	0.1557610	0.1557671	0.1557703	0.1557664
	0.1557727	0.1557727	0.1557727	0.1557727	0.1557727	0.1557727	0.1557727
15	0.1210907	0.1210907	0.1210907	0.1210907	0.1210907	0.1210907	0.1210907
	0.1210937	0.1210937	0.1210937	0.1210937	0.1210937	0.1210937	0.1210937
16	0.1083288	0.1083288	0.1083288	0.1083288	0.1083288	0.1083288	0.1083288
	0.1083333	0.1083333	0.1083333	0.1083333	0.1083333	0.1083333	0.1083333

Chapter 5

Future work-Densities related to average order of subgroups of $\mathbb{Q}^*$

5.1 Introduction

Let $g \in \mathbb{Q} \setminus \{0, \pm 1\}$ and consider a prime p not dividing the numerator or denominator of g, let $\ell_g(p)$ denote the multiplicative order of g modulo p. For simplicity, when p does divide the numerator or denominator of g, we let $\ell_g(p) = 1$. Define

$$c_g := \sum_{k=1}^{\infty} \frac{\varphi(k)\operatorname{Rad}(k)(-1)^{\omega(k)}}{k^2[\mathbb{Q}(g^{1/k}, e^{2\pi i/k}) : \mathbb{Q}]}.$$

Assuming GRH, Kurlberg and Pomerance [16, Theorem 2] proved that the series for c_g converges absolutely, and,

$$\frac{1}{\pi(x)} \sum_{p \le x} \ell_g(p) = \frac{1}{2} c_g \cdot x + O\left(\frac{x}{(\log x)^{1/2 - 1/\log\log\log x}}\right).$$

Further, with $g = a/b$ where $a, b \in \mathbb{Z}$, the error estimate holds uniformly for $|a|, |b| \le x$. Here $\operatorname{Rad}(k)$ denotes the largest squarefree divisor of k and $\omega(k)$ the number of primes dividing $\operatorname{Rad}(k)$.

The authors of [16] gave a more explicit formula for c_g. Write $g = \pm g_0^h$ where h is a positive integer and g_0 >0 is not an exact power of a rational number. Let $\delta(g)$ be the field discriminant of $\mathbb{Q}(\sqrt{g_0})$.

$$n = \begin{cases} \operatorname{lcm}[2^{v_2(h)+1}, \delta(g)] & \text{if } g > 0; \\ \delta(g)/2 & \text{if } g < 0, v_2(h) = 0 \text{ and } 4 \| \delta(g); \\ \delta(g)/4 & \text{if } g < 0, v_2(h) = 1 \text{ and } 8 \mid \delta(g); \\ \operatorname{lcm}[2^{v_2(h)+2}, \delta(g)] & \text{otherwise.} \end{cases}$$

Then

$$c_g = \prod_{\ell \text{ prime}} F(\ell) \times \left(H - \prod_{\ell | 2\delta(g)} 1 - \frac{G(\ell)}{F(\ell)}\right)$$

where

$$F(\ell) = 1 - \frac{\ell}{\ell^2 - 1} + \frac{\ell^3}{\ell^{2v_\ell(h)}(\ell+1)(\ell^3 - 1)} \quad , G(\ell) = \left(1 - \sum_{j=1}^{v_2(n)-1} \ell^{1-3j+\min(j, v_\ell(h))}\right)$$

and

$$H = \begin{cases} \frac{29}{21 \cdot 4^{v_2(h)} + 8} & \text{if } v_2(h) > 0 \text{ and } g < 0; \\ 1 & \text{otherwise.} \end{cases}$$

which is easily seen to be a rational multiple of

$$c := \prod_{\ell} \left(1 - \frac{\ell}{\ell^3 - 1}\right) = 0.5759599689....$$

Let $\Gamma \subset \mathbb{Q}^*$ be a finitely generated multiplicative group of rank r. We denote by $\operatorname{Supp}\Gamma$, the *support* of Γ, i.e. the finite set of those primes ℓ such that the ℓ–adic valuation of some elements of Γ is nonzero. For any prime $p \notin \operatorname{Supp}\Gamma$, we consider the reduction group:

$$\Gamma_p = \{\gamma \bmod p : \gamma \in \Gamma\} \subset \mathbb{F}_p^*.$$

C. Pelhivan in [33] proved he following result:

Theorem 5.1. *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*

$$C_\Gamma := \sum_{k \geq 1} \frac{\varphi(k) \operatorname{Rad}(k)(-1)^{\omega(k)}}{k^2[\mathbb{Q}(\zeta_k, \Gamma^{1/k}) : \mathbb{Q}]}.$$

Then the series C_Γ converges absolutely and as $x \to \infty$,

$$\frac{1}{\pi(x)} \sum_{p \leq x} |\Gamma_p| = \frac{1}{2} C_\Gamma \cdot x + O_\Gamma\left(\frac{x(\log\log x)}{(\log x)^r}\right)$$

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

In the same paper derived the following identity:

Theorem 5.2. *Assume that Γ is a finitely generated subgroup of $\mathbb{Q}^+$. Then*

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

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

$$t_\eta = \begin{cases} \infty & \textit{if for all } t \geq 0,\ \eta^{2^t} \mathbb{Q}^{*2^{t+1}} \notin \Gamma(2^{t+1}) \\ \min\{t \in \mathbb{N} : \eta^{2^t} \mathbb{Q}^{*2^{t+1}} \in \Gamma(2^{t+1})\} & \textit{otherwise.} \end{cases} \tag{5.1}$$

From the above result it is not difficult to deduce that C_Γ is a rational multiple of

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

So, in the particular case when $\Gamma = \langle g \rangle$ ha rank 1 and we write $g = g_0^h$ where $g_0 > 0$ is not the power of any rational number and $g_0 = g_1 g_2^2$ where g_1 is square free, then it is not difficult to check that $t_{g_1} = v_2(h)$ and $t_\eta = \infty$ if $\eta \neq g_1$.

It is our plan to extend the Theorem above to the case when Γ is not necessarily contained in $\mathbb{Q}^+$. The tool of the previous chapters will be used in this future project.

References

[1] H. Abdullah, A. A. Mustafa, and F. Pappalardi. Divisibility of reduction in groups of rational numbers. *Manuscript submitted for publication*.

[2] H. Abdullah, A. A. Mustafa, and F. Pappalardi. Density of the ”quasi r-rank artin problem”. *Functiones et Approximatio, Commentarii Mathematici*, 65(1):73–93, 2021.

[3] Herbert Bilharz. Primdivisoren mit vorgegebener primitivwurzel. *Mathematische Annalen*, 114(1):476–492, 1937.

[4] Leonardo Cangelmi and Francesco Pappalardi. On ther-rank artin conjecture, ii. *Journal of Number Theory*, 75(1):120–132, 1999.

[5] K. Chinen and L. Murata. On a distribution property of the residual order of $a(\mod p)$. *Journal of Number Theory*, 105:60–81, 2004.

[6] K. Chinen and L. Murata. On a distribution property of the residual order of $a(\bmod p)$ ii. *Journal of Number Theory*, 105:82–100, 2004.

[7] Günther Frei, P Roquette, and F Lemmermeyer. Emil artin and helmut hasse. *Their correspondence*, 1934:294, 1923.

[8] Carl Friedrich Gauss. *Disquisitiones arithmeticae*. Yale University Press, 1966.

[9] Rajiv Gupta and M Ram Murty. A remark on artin’s conjecture. *Inventiones mathematicae*, 78(1):127–130, 1984.

[10] Rajiv Gupta and M Ram Murty. Primitive points on elliptic curves. *Compositio mathematica*, 58(1): 13–44, 1986.

[11] Rajiv Gupta, V Kumar Murty, and M Ram Murty. The euclidian algorithm for s integers. In *CMS Conference Proceedings*, pages 189–202, 1985.

[12] Helmut Hasse. *Vorlesungen über Zahlentheorie*, volume 59. Springer-Verlag, 2013.

[13] DR Heath-Brown. Artin’s conjecture for primitive roots. *The Quarterly Journal of Mathematics*, 37(1): 27–38, 1986.

[14] C. Hooley. On artin’s conjecture. *Journal für die reine und angewandte Mathematik*, 225:209–220, 1967.

[15] Samuel S. Wagstaff Jr. Pseudoprimes and a generalization of artin’sconjecture. *Acta Arithmetica*, 2(41): 141–150, 1982.

[16] Pär Kurlberg and Carl Pomerance. On a problem of arnold: the average multiplicative order of a given integer. *Algebra & Number Theory*, 7(4):981–999, 2013.

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

[18] Derrick H Lehmer and Emma Lehmer. Heuristics, anyone. *Studies in mathematical analysis and related topics*, pages 202–210, 1962.

[19] H. Lenstra, P. Moree, and P. Stevenhagen. Character sums for primitive root densities. *Mathematical Proceedings of the Cambridge Philosophical Society*, 157(3):489–511, 2014.

[20] H. W. Lenstra and Jr. On artin's conjecture and euclid's algorithm in global fields. *Inventiones Mathematicae*, 42:201–224, 1977.

[21] Hendrik W Lenstra. On artin's conjecture and euclid's algorithm in global fields. 1977.

[22] P. Moree. On primes p for which d divides $\mathrm{ord}_p(g)$. *Functiones et Approximatio, Commentarii Mathematici*, 33:85–95, 2005.

[23] P. Moree. Near-primitive roots. *Functiones et Approximatio, Commentarii Mathematici*, 48(1):133–145, 2013.

[24] P. Moree and P. Stevenhagen. Computing higher rank primitive root densities. *Acta Arithmetica*, 163(1): 15–32, 2014.

[25] Pieter Moree. Artin's primitive root conjecture–a survey. *Integers*, 12(6):1305–1416, 2012.

[26] L. Murata. A problem analogous to artin's conjecture for primitive roots and its applications. *Archiv der Mathematik*, 57:555–565, 1991.

[27] M Ram Murty and Seshadri Srinivasan. Some remarks on artin's conjecture. *Canadian Mathematical Bulletin*, 30(1):80–85, 1987.

[28] R. W. K. Odoni. A conjecture of krishnamurthy on decimal periods and some allied problems. *Journal of Number Theory*, 13:303–319, 1981.

[29] F. Pappalardi. The r-rank artin conjecture. *Mathematics of Computation*, 66(218):853–868, 1997.

[30] F. Pappalardi. Squarefree values of the order function. *New York Journal of Mathematics*, 9:331–344, 2003.

[31] F. Pappalardi. Divisibility of reduction in groups of rational numbers. *Mathematics of Computation*, 84 (291):385–407, 2015.

[32] F. Pappalardi and A. Susa. An analogue of artin's conjecture for multiplicative subgroups. *Archiv der Mathematik*, 101(4):319–330, 2013.

[33] Cihan Pehlivan. The average multiplicative order of a finitely generated subgroup of the rationals modulo primes. *International Journal of Number Theory*, 12(08):2147–2158, 2016.

[34] A. Schinzel. A refiniment of a theorem of gerst on power residues. *Acta Arithmetica*, 17(2):161–168, 1970.

[35] *PARI/GP version* 2.11.2. The PARI Group, Univ. Bordeaux, 2019. available from http://pari.math.u-bordeaux.fr/.

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

[37] K. Wiertelak. On the density of some sets of primes, iv. *Acta Arithmetica*, 43(2):177—190, 1984.