UNIVERSITÀ DEGLI STUDI DI "ROMA TRE"
DIPARTIMENTO DI MATEMATICA

THESIS

Some analogous problems to Artin's Conjecture

Andrea Susa

Relatore
Prof. F. Pappalardi

Dottorato di Ricerca in Matematica: XVIII CICLO

Submitted: January 2006
Convocation: April 12, 2006

CONTENTS

NOTATIONS

$\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$	the set of natural, integer, rational, real and complex numbers
$\mathbb{Q}^+, \mathbb{Q}^*$	subgroups of rational numbers with respect to addition and multiplication
$\mathbb{Q}^{\geq 0}$, $\mathbb{R}^{\geq 0}$	the set of rational or real numbers greater or equal to zero
$\mathbb{F}_p$	finite field with $p-1$ elements (p is a prime)
d, n, m	integers (usually positive)
p, p_i, q, q_i, l, l_i	primes
$d \mid n$	d divides n
$d \nmid n$	d does not divide n
$p^m \parallel n$	p^m divides exactly n (i.e., $p^m \mid n$ and $p^{m+1} \nmid n$)
$v_p(a)$	p–adic valuation of a (i.e., $p^{v_p(a)} \parallel a$)
(a, b)	the greatest common divisor (gcd) of a and b
$[a, b]$	the least common multiple (lcm) of a and b
$n = \prod_{i=1}^{k} p_i^{\alpha_i}$	canonical primes factorization of an integer n
$\sum_{p \leq x}$	sum over all primes $\leq x$
$\sum_{d \mid n}$	sum over all positive divisors of n
$\sum_{p \mid n}$	sum over all primes dividing n
$\prod_p$	product over all primes
$P(t)$	product over all primes $p \leq t$
$\pi(x)$	the number of primes $p \leq x$
ζ_n	primitive n–th root of the unity
$\mathbb{Q}_n$	the field $\mathbb{Q}(\zeta_n)$ with ζ_n primitive n–th root of the unity

If $p \nmid a$, we define

$$\operatorname{ord}_p a = \min\left\{k \in \mathbb{N} :\ a^k \equiv 1 \bmod p\right\}, \quad \operatorname{ind}_p a = (p-1)/\operatorname{ord}_p a.$$

We denote by $\operatorname{li}(x)$ the *logarithmic integral:*

$$\operatorname{li}(x) = \int_2^x dt/\log t.$$

INTRODUCTION

The first that studied the problem to determine whether an integer (different to $0, \pm 1$ and a perfect square) is primitive root for infinitely many primes p, was Gauss. In articles 315-517 of his Disquisitiones Arithmeticae (1801), he showed the connection between the decimal expansion of the number $1/p$ with the multiplicative order of $10 \pmod p$. For any $p > 5$ prime, the decimal expansion of $1/p$ is purely periodic, with period equal to $\operatorname{ord}_p 10$. For example, $1/7 = 0.\overline{142857}$ has period (and order) equal to 6, so 10 is a primitive root $\pmod 7$. Gauss' table gives several other examples of primes p such that 10 is a primitive root $\pmod p$. Many authors ascribe to Gauss the following conjecture:

there exist infinitely many primes p such that 10 is primitive root.

In order to prove this conjecture, Chebichev showed that $\operatorname{ord}_p(10) \in \{1, 2, 4, p, 2p, 4p\}$ for any $p > 5$. In particular, he proved that, if $p \equiv 2 \pmod 5$ is a prime such that $q = 4p + 1$ is also prime, then 10 is a primitive root $\pmod q$. The Chebichev's argument is the following:

$$10^{2p} \equiv \left(\frac{10}{q}\right) = \left(\frac{2}{q}\right)\left(\frac{5}{q}\right) = (-1)^{(q^2-1)/8}\left(\frac{q}{5}\right) = -\left(\frac{4}{5}\right) \equiv -1 \pmod q.$$

Since the prime divisors of $10^4 - 1$ are $3, 11, 101 \neq 4p+1$ for any p, so $\operatorname{ord}_p 10 = q - 1$. But the problem to determine

$$\#\{p \leq x : p \equiv 2 \pmod 5 \text{ and } 4p + 1 \text{ is prime}\}$$

is hard. By a heuristic argument, the probability that both $n \equiv 2 \pmod 5$ and $4n + 1$ are primes ($n \leq x$) is at least $cx/\log^2 x$. Hence we can expect that the conjecture has affirmative answer.

No progress on this problem until 1927, when Emil Artin generalized the Gauss' conjecture in the the following:

for any integer a, different from $0, \pm 1$ and not a perfect square, there exist infinitely many primes p such that a is a primitive root.

In other words:

$$\mathcal{N}_a(x) = \#\{p \leq x \ : \ \langle a \rangle_p = \mathbb{F}_p^*\} = (A(a) + o(1))\,\mathrm{li}(x) \tag{0.1}$$

where $\mathrm{li}(x)$ is the *logarithmic integral*, defined as $\int_2^x dt/\log t$, and $A(a)$ is positive.

The Artin's approach to this problem is the following: a is a primitive root $(\mathrm{mod}\ p)$ if and only if for any prime q such that $q|p-1$, then $a^{(p-1)/q} \not\equiv 1 \pmod{p}$.

By a principle (due to Dedekind), the condition $a^{(p-1)/q} \equiv 1 \pmod{p}$ is equivalent to the condition that p splits completely in the kummerian extension $\mathbb{Q}(\zeta_q, a^{1/q})/\mathbb{Q}$ (with ζ_q a q–th primitive root of the unity). By Chebotarev's Density Theorem, the number of such primes is $1/[\mathbb{Q}(\zeta_q, a^{1/q}) : \mathbb{Q}]$.

Hence Artin deduce that a is primitive root $(\mathrm{mod}\ p)$ if and only if p don't splits completely in $\mathbb{Q}(\zeta_q, a^{1/q})/\mathbb{Q}$ for any $q|p-1$. Therefore, by Inclusion/Exclusion Principle, we can expect that

$$A(a) = \sum_{n \geq 1} \frac{\mu(n)}{[\mathbb{Q}(\zeta_n, a^{1/n}) : \mathbb{Q}]}.$$

More precisely, if we define:

$$A = \sum_{n \geq 1} \frac{\mu(n)}{n\varphi(n)} = \prod_l \left(1 - \frac{1}{l(l-1)}\right)$$

then $A > 0$ is well defined since the series converges, and $A(a)$ is a rational multiple of A.

So one can expect:

$$\#\{p \leq x \ : \ \langle a \rangle_p = \mathbb{F}_p^*\} \sim A(a)\pi(x), \qquad x \to \infty \tag{0.2}$$

where

$$A(a) = \prod_q \left(1 - \frac{1}{[\mathbb{Q}(\zeta_q, a^{1/q}) : \mathbb{Q}]}\right).$$

This value of $A(a)$ was believed true until 1960, when D.H. Lehmer made some numerical calculation and found out some discrepancies. Heilbronn showed

that the problem was born to consider the events p *does not split completely in* $\mathbb{Q}(\zeta_q, a^{1/q})$ as independents and published a correct value of the Artin's constant:

$$A(a) = \prod_{l \nmid h} \left(1 - \frac{1}{l(l-1)}\right) \prod_{l|h} \left(1 - \frac{1}{(l-1)}\right) C(a)$$

where h the largest integer such that $a = a_0^h$ with $a_0 \in \mathbb{Z}$ and

$$C(a) = \begin{cases} 1, & \text{if } a_0 \not\equiv 1 \pmod 4 \\ (1 + \mu(|a_0|) \prod_{q|(h,a_0)} \frac{1}{q-2} \prod_{\substack{q \nmid h \\ q|a_0)}} \frac{1}{q^2-q-1}, & \text{if } a_0 \equiv 1 \pmod 4. \end{cases}$$

His correction agreed with the Lehmer's calculation.

In 1965, Hooley proved in [6] the Artin's conjecture, with the term $A(a)$ as in the work of Heilbronn, using the Generalized Riemann Hypothesis. We give a sketch of the Hooley's proof following M. R. Murty [15].

Let $L_q = \mathbb{Q}(\zeta_q, a^{1/q})$. We define the following functions:

$$\pi(x,k) = \#\{p \leq x : p \text{ splits completely in } L_q, \forall q|k\},$$
$$M(x,\eta_1,\eta_2) = \#\{p \leq x : p \text{ splits completely in some } L_q, \eta_1 < q < \eta_2\}.$$

By Chebotarev Density Theorem (under GRH), we have:

$$\pi(x,d) = \frac{\mathrm{li}(x)}{[L_d : \mathbb{Q}]} + O(\sqrt{x}\log(xd)). \tag{0.3}$$

We have, by Inclusion/Exclusion Principle:

$$\mathcal{N}_a(x) = \sum_{k \geq 1} \mu(k)\pi(x,k),$$

but we cannot use directly (0.3), because the contribution of the error term is too large. For this reason, if we set $P(t) = \prod_{l \leq t} l$, we obtain:

$$\mathcal{N}_a(x) \leq \sum_{d|P(t)} \mu(d)\pi(x,d),$$
$$\mathcal{N}_a(x) \geq \sum_{d|P(t)} \mu(d)\pi(x,d) - M(x,z,x-1).$$

If we set $z = \frac{1}{6}\log x$, by (0.3), we obtain:

$$\mathcal{N}_a(x) = A(a)\,\mathrm{li}(x) + O\left(\frac{x}{\log^2 x}\right) + O\left(M(x, z, x-1)\right).$$

To estimate the term $M(x, z, x-1)$, we ca use:

$$M(x, z, x-1) \leq M(x, z, \eta_1) + M(x, \eta_1, \eta_2) + M(x, \eta_2, x-1),$$

with $\eta_1 = \sqrt{x}/\log^2 x$ and $\eta_2 = \sqrt{x}\log x$. The first two terms are shown to be $O\left(\frac{x\log\log x}{\log^2 x}\right)$ using (0.3) and some sieve methods. The last term is more difficult to estimate. The idea is the following: if $a^{(p-1)/q} \equiv 1 \pmod p$ for some $q > \eta_2$, then $p | \prod_{m<\sqrt{x}/\log x}(a^m - 1)$. But the number of prime divisors of $a^m - 1$ is at most $m\log a$, so:

$$\sum_{m<\sqrt{x}/\log x} m\log a = O\left(\frac{x\log\log x}{\log^2 x}\right),$$

and we obtain the thesis:

$$N_a(x) = A(a)\,\mathrm{li}(x) + O\left(\frac{x\log\log x}{\log^2 x}\right).$$

In 1976, Matthews studied a generalization of the Artin's conjecture:

> *Given $a_1, \ldots, a_r \in \mathbb{Z} \setminus \{0, \pm 1\}$ and not a perfect square, do there exist infinity many primes p such that a_i is a primitive root $\pmod p$ for any $i = 1, \ldots, r$?*

He proved the following theorem:

Theorem (Matthews, [11])**.** *Given $a_1, \ldots, a_r \in \mathbb{Z}^*$, there exists a positive constant $C = C(a_1, \ldots, a_r)$ such that if the Generalized Riemann Hypothesis holds, then*

$$\#\left\{p \leq x \mid \mathrm{ord}_p\, a_i = p-1\ \forall i = 1, \ldots, r\right\} = C\,\mathrm{li}(x) + O\left(x\frac{(\log\log x)^{2^r-1}}{(\log x)^2}\right).$$

□

In 1983, Gupta and Murty proved, without any hypothesis, that there is a set of 13 numbers such that, for a least one of these 13 elements, Artin's conjecture is true. This result was later sharpened in 1986 by Heath-Brown to a set of 3 elements:

Theorem (Heath-Brown, [5])**.** *One of $2, 3, 5$ is a primitive root $\pmod p$ for infinitely many primes p.* □

0.1 Analogous problems to Artin's conjecture

Many analogous problems to Artin's conjecture are been studied (and solved) in this last years. The first problem has been addressed by H. Lenstra ([9]) and solved by Murata in [14] and Wagstaff in [21]:

> *Let $a, m \in \mathbb{N}^+$, with $a \geq 2$ squarefree. Do there exist infinitely many primes p such that $\operatorname{ind}_p a = m$?*

Theorem (Murata, [14])**.** *Let $a \geq 2$ be a squarefree natural number and assume that the GRH holds. Then we have, for any $\epsilon > 0$*

$$\#\{p \leq x \ : \ \operatorname{ind}_p a = m\} = \left(c_{a,m} + O\left(\frac{m^{\epsilon}\log\log x + \log a}{\log x}\right)\right)\operatorname{li}(x)$$

where $c_{a,m}$ is a suitable non negative constant, and the constant implied in the O–symbol may depend on ϵ. □

A general expression for the constant $c_{a,m}$ has been obtained by S. Wagstaff. Our Theorem 1,(see cap 1.) generalizes Matthews's Theorem and it is an analogue of Murata's Theorem.

Several authors studied the most general problem:

> *Let $a, k \in \mathbb{N}^+$. Do there exist infinitely many primes p such that $k|\operatorname{ord}_p a$?*

Wiertelak [22] was the first to obtain an asymptotic formula for

$$\mathcal{N}_a(x,k) = \#\{p \leq x : \ k|\operatorname{ord}_p a\}.$$

Moree proved the following result.

Theorem (Moree, [12])**.** *Let $k \in \mathbb{N}^+$ be squarefree and $a \in \mathbb{Q} \setminus \{0, \pm 1\}$. Then the following asymptotic formula holds:*

$$\mathcal{N}_a(x,k) = \left(\kappa_{a,k} + O_{a,k}\left(\frac{(\log\log x)^{\omega(k)+3}}{(\log x)^2}\right)\right)\operatorname{li}(x).$$

where $\kappa_{a,k}$ is a positive rational constant. □

Another problem solved (under GRH) is the so-called *two-variable Artin conjecture*.

> *Let $a, b \in \mathbb{Q}^*$ multiplicatively independent. Do there exist infinitely many primes p such that $\operatorname{ord}_p a | ord_p(b)$?*

This problem was studied by Stephens in 1976 and completely solved by Moree and Stevenhagen that proved the following theorem:

Theorem (Moree & Stevenhagen, [13])**.** *Let $a, b \in \mathbb{Q}^*$ multiplicatively independent. If we assume GRH, then:*

$$\lim_{x\to\infty} \frac{\#\{p \leq x : \operatorname{ord}_p a | ord_p(b)\}}{\pi(x)} = c_{a,b} \prod_p \left(1 - \frac{p}{p^3 - 1}\right)$$

for some positive rational constant $c_{a,b}$. □

In this Thesis we study the following problem, due to Schinzel–Wojcik.

> *Let $\{a_1, \ldots, a_r\} \subset \mathbb{Q} \setminus \{0, \pm 1\}$. The Schinzel–Wojcik's problem for $\{a_1, \ldots, a_r\}$ is to determine whether there are infinitely many primes p such that*
>
> $$\operatorname{ord}_p a_1 = \cdots = \operatorname{ord}_p a_r$$
>
> *and if their density is positive.*

We define:

$$\mathcal{N}_{a_1,\ldots,a_r}(x) = \#\{p \leq x : \ v_p(a_i) = 0 \ \forall\ i = 1, \ldots, r, \ \operatorname{ord}_p a_1 = \cdots = \operatorname{ord}_p a_r\}.$$

The main results are the following two theorems:

Theorem. *Let $\{a_1, \ldots, a_r\} \subset \mathbb{Q} \setminus \{0, \pm 1\}$, $\Gamma = \langle a_1, \ldots, a_r \rangle$ as subgroup of $\mathbb{Q}^*$ and assume that the Generalized Riemann Hypothesis holds for the fields $\mathbb{Q}(\zeta_n, a_1^{1/n_1}, \ldots, a_r^{1/n_r})$ ($n, n_1, \ldots, n_r \in \mathbb{N}$) and that $\operatorname{rank}(\Gamma) \geq 2$. Then*

$$\mathcal{N}_{a_1,\ldots,a_r}(x) = \left(\delta_{a_1,\ldots,a_r} + O_{a_1,\ldots,a_r}\left(\frac{(\log\log x)^{2^r-2}}{\log x}\right)\right) \operatorname{li}(x)$$

where $\delta_{a_1,\ldots,a_r}$ is a rational constant. □

Unfortunately, in this general case we are unable to determine whether the SW problem has affirmative answer. However it is reasonable to expect that SW problem has affirmative answer if and only if $\delta_{a_1,\ldots,a_r} \neq 0$. In the particular case in which the group $\langle a_1, \ldots, a_r \rangle$ has rank one and each $a_i = a^{h_i}$ for some $a \in \mathbb{Q}$, we can show, without applying Generalized Riemann Hypothesis, the following result.

Theorem. *Let $a \in \mathbb{Q} \setminus \{0, \pm 1\}$, $h_1, \ldots, h_r \in \mathbb{N}^+$ with $(h_1, \ldots, h_r) = 1$ and $h = [h_1, \ldots, h_r]$. Then the following asymptotic formula holds:*

$$\mathcal{N}_{a^{h_1},\ldots,a^{h_r}}(x) = \left(\delta_{a^{h_1},\ldots,a^{h_r}} + O_{a,h}\left(\frac{(\log\log x)^{\omega(h)+3}}{(\log x)^2}\right)\right)\operatorname{li}(x)$$

where $\omega(h)$ denotes the number of distinct primes factors of h and $\delta_{a^{h_1},\ldots,a^{h_r}}$ is a rational constant. □

In this case we can give a complete answer to the SW problem.

Corollary. *Let $a \in \mathbb{Q} \setminus \{0, \pm 1\}$ and $h_1, \ldots, h_r \in \mathbb{N}^+$. Then $\delta_{a^{h_1},\ldots,a^{h_r}} \neq 0$. Therefore the SW problem for $\{a^{h_1}, \ldots, a^{h_r}\}$ has an affirmative answer.*

0.2 Analogous problems to Artin's conjecture for subgroups

Pappalardi in [16], studied the problem to determine (under GRH) an asymptotic formula for the number of primes for which $\mathbb{F}_p^*$ can be generated by r given multiplicatively independent rational numbers. In particular, if Γ is generated by a single element, then this problem coincides with Artin's Conjecture. His result:

Theorem (Pappalardi, [17])**.** *Let $\Gamma = \langle a_1, \ldots a_r \rangle \subset \mathbb{Q}^*$, be a finitely generated subgroup with $\operatorname{rank}(\Gamma) = r > 1$. Assume that the GRH holds. Then*

$$\#\{p \leq x : \ [\mathbb{F}_p^* : \Gamma_p] = 1\} = \delta_\Gamma \operatorname{li}(x) + O\left(\frac{x \log(a_1 \cdots a_r)}{\log^2 x}\right)$$

where

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

and the error term is uniform with respect to $r \leq \frac{1}{3\log 2}\log x$ and $a_1, \ldots, a_r$.

In particular, if $a_1, \dots, a_r$ are primes, then

$$\{p \le x : \ p \notin \mathcal{S}_\Gamma, \ [\mathbb{F}_p^* : \Gamma_p] = 1\} = \delta_\Gamma \operatorname{li}(x) + O\left(\frac{x4^r \log(xa_1 \cdots a_r)}{\log^{r+2} x}\right)$$

uniformly with respect to $r \le \frac{1}{4}\log x/\log\log x$ and $a_1, \dots, a_r$. □

Cangelmi & Pappalardi in [3], have determined the number of primes p such that the image of $\Gamma \pmod p$ contains a promitive root, and so $[\mathbb{F}_p^* : \Gamma_p] = 1$. Their results:

Theorem (Cangelmi & Pappalardi, [3])**.** *Let $\Gamma \subset \mathbb{Q}^*$, be a finitely generated subgroup with $\operatorname{rank}(\Gamma) = s > 1$. Assume that the GRH holds. Then*

$$\{p \le x : \ [\mathbb{F}_p^* : \Gamma_p] = 1\} = \left(\delta_\Gamma + O\left(\frac{1}{\log^s(x)(\log\log x)^s}\right)\right) \operatorname{li}(x)$$

where δ_Γ is a suitable non negative constant, and the constant implied in the O–symbol depends only on Γ. □

The most general problem is the following.

> *Let $\Gamma \subseteq \mathbb{Q}^*$ be a finitely generated subgroup such that Γ be torsion free with support $\mathcal{S}_\Gamma$ and $m \in \mathbb{N}^+$. Do there exist infinity many primes p for which the index of the group generated by the reduction of $\Gamma \pmod p$ is m?.*

The associate function is the following:

$$\mathcal{N}_\Gamma(x; m) = \#\{p \le x : \ p \notin \mathcal{S}_\Gamma, \text{ and } [\mathbb{F}_p^* : \Gamma_p] = m\}.$$

We prove, in chapter 3, the theorem:

Theorem. *Let Γ as above and $m = o(x^{1/6})$. Assume that the GRH holds for the fields of the form $\mathbb{Q}(\zeta_M, \Gamma^{1/M})$ with $M \in \mathbb{N}^+$. Then*

$$\mathcal{N}_\Gamma(x; m) = \left(\rho(\Gamma, m) + O\left(\frac{\log x}{m \log^2(x/m)}\right)\right) \operatorname{li}(x)$$

where if $M = mk$, then

$$\rho(\Gamma, m) = \sum_{k \ge 1} \frac{\mu(k)}{\varphi(M)} \frac{1}{|\Gamma \cdot \mathbb{Q}_M^{*M}/\mathbb{Q}_M^{*M}|}. \tag{0.4}$$

□

1. ON A PROBLEM OF SCHINZEL & WÓJCIK

1.1 Introduction

If $a \in \mathbb{Q}^*$ and p is an odd prime such that the p–adic valuation $v_p(a) = 0$ then we define the *order* of a modulo p by

$$\operatorname{ord}_p a = \min\left\{k \in \mathbb{N} \,:\, a^k \equiv 1 \pmod{p}\right\}.$$

In 1992 Schinzel and Wójcik [19] proved the following theorem.

Theorem (Schinzel & Wójcik, 1992, [19])**.** *Let $a, b \in \mathbb{Q} \setminus \{0, \pm 1\}$. Then exist infinitely many primes p such that the following two conditions are satisfied:*

(i) $v_p(a) = v_p(b) = 0$*;*

(ii) $\operatorname{ord}_p a = \operatorname{ord}_p b$*.*

Clearly the first condition is satisfied for all but finitely many primes and the second is the important one. Whenever we use the symbol $\operatorname{ord}_p a$, we always assume that $v_p(a) = 0$. The proof of Schinzel and Wójcik's result is very ingenious and uses Dirichlet's Theorem for primes in arithmetic progressions. In the last line of their paper, Schinzel and Wójcik conclude by stating the following problem:

> *Given $a, b, c \in \mathbb{Q} \setminus \{0, \pm 1\}$, do there exist infinitely many primes such that*
>
> $$\operatorname{ord}_p a = \operatorname{ord}_p b = \operatorname{ord}_p c?$$

We refer to the above as the Schinzel–Wójcik (SW for short) problem for a, b, c. In general, if $\{a_1, \dots, a_r\} \subset \mathbb{Q} \setminus \{0, \pm 1\}$, the SW problem for $\{a_1, \dots, a_r\}$ is to determine whether there are infinitely many primes p such that

$$\operatorname{ord}_p a_1 = \cdots = \operatorname{ord}_p a_r.$$

It is easy to produce examples having no odd primes with the wanted property. Indeed let $a = e, b = e^2, c = -e^2$. For any $p \geq 3$, if $\delta = \operatorname{ord}_p e = \operatorname{ord}_p -e^2$, then we have $e^{2\delta} \equiv (-e^2)^\delta \equiv 1 \pmod{p}$. Therefore $(-1)^\delta \equiv 1 \pmod{p}$ so that $2 \mid \delta$ and $(e^2)^{\delta/2} \equiv 1 \pmod{p}$. This implies $\operatorname{ord}_p e^2 \mid \delta/2$ contradicting $\operatorname{ord}_p e^2 = \delta$. However we have the following result due to Wójcik [24]:

Theorem (Wójcik, 1996 [24]). *Let $K/\mathbb{Q}$ be a finite extension and $\alpha_1, \dots, \alpha_r \in K \setminus \{0, 1\}$ be such that the multiplicative group $\langle \alpha_1, \dots, \alpha_r \rangle \subset K$ is torsion free. Then the Schinzel's* Hypothesis H *implies that there exist infinitely many primes $\mathfrak{p}$ of K of degree 1 such that*

$$\operatorname{ord}_{\mathfrak{p}} \alpha_1 = \cdots = \operatorname{ord}_{\mathfrak{p}} \alpha_r.$$

It is an immediate corollary that if $a, b, c \in \mathbb{Q} \setminus \{0, 1\}$ are such that $-1 \notin \langle a, b, c \rangle \subset \mathbb{Q}^*$, then Hypothesis H (see [18]) implies that the SW problem for $\{a, b, c\}$ has an affirmative answer. Note, however, that the sufficient condition $-1 \notin \langle a, b, c \rangle$ is not always necessary. Indeed consider SW problem for $\{2, 3, -6\}$. The above theorem does not apply although for $p = 19, 211, 499, 907$ and for many more primes p, we find that $\operatorname{ord}_p 2 = \operatorname{ord}_p 3 = \operatorname{ord}_p -6$. Moreover, empirical data suggest that the SW problem has an affirmative answer. Observe that Hypothesis H never answers the SW problem for sets of the form $\{a, b, -ab\} \subset \mathbb{Q} \setminus \{0, \pm 1\}$. For completeness, we recall the famous

Hypothesis H (Schinzel, 1959 [18]) *Let $f_1, \dots, f_k \in \mathbb{Z}[x]$ be irreducible polynomials with positive coefficients and such that $\gcd(f_1(n) \cdots f_k(n) \mid n \in \mathbb{N}) = 1$. Then there are infinitely many $t \in \mathbb{N}$ such that $f_1(t), \dots, f_k(t)$ are all prime.*

The condition on the greatest common divisor of the values of the polynomials is needed to avoid situations like the one of the polynomial $x^2 + x + 2$ that takes only even values.

The *Generalized Riemann Hypothesis* (GRH for short) can be applied to the SW problem. Indeed, we have the following:

Theorem (Matthews, 1976 [11]). *Given $a_1, \dots, a_r \in \mathbb{Z}^*$, there exists a positive constant $C = C(a_1, \dots, a_r)$ such that if the Generalized Riemann Hypothesis*

holds, then

$$\#\{p \le x \mid \operatorname{ord}_p a_i = p-1 \ \forall i = 1,\dots,r\} = C\,\mathrm{li}(x) + O\left(x\frac{(\log\log x)^{2^r-1}}{(\log x)^2}\right).$$

This result is known as the *simultaneous primitive roots Theorem* and admits as an immediate consequence the following:

Corollary. *With the above notation, if $C(a_1,\dots,a_r) \neq 0$ and the GRH holds, then the SW problem has an affirmative answer for $a_1,\dots,a_r$.*

Further results in [11] imply that:

1. $C(a_1,\dots,a_r) = 0$ if and only if at least one of the following conditions is satisfied:

   (a) there exists $1 \le i_1 < \ldots < i_{2s+1} \le n$ such that

   $$a_{i_1}\cdots a_{i_{2s+1}} \in (\mathbb{Q}^*)^2;$$

   (b) there exists $1 \le i_1 < \ldots < i_{2s} \le n$ such that

   $$a_{i_1}\cdots a_{i_{2s}} \in -3(\mathbb{Q}^*)^2$$

   and the set of primes $q \equiv 1 \pmod 3$ for which each a_i is not a cube modulo q is finite.

   Furthermore each of the conditions above implies that $a_1,\dots,a_n$ cannot be simultaneously primitive roots for infinitely many primes.

2. Using the above it can be checked that $C(2,3,-6) \neq 0$ so that GRH implies that the SW problem has an affirmative answer in this case.

3. For any $a, b \in \mathbb{Q}\setminus\{0,\pm1\}$ it is easy to see that $C(a,b,ab) = 0$. Indeed, if $\operatorname{ord}_p a = \operatorname{ord}_p b = p-1$, then the Legendre symbols $\left(\frac{a}{p}\right)$ and $\left(\frac{b}{p}\right)$ are both equal to -1. Therefore $\left(\frac{ab}{p}\right) = 1$ and this implies that $\operatorname{ord}_p ab \mid \frac{p-1}{2}$.

4. The SW problem for $\{4,3,-12\}$ is still open both on Hypothesis H and on GRH.

For given rational numbers $a_1, \dots, a_r$ not 0 or ± 1, we consider the following function:

$$\mathcal{N}_{a_1,\dots,a_r}(x) = \{p \le x \ : \ \operatorname{ord}_p a_1 = \cdots = \operatorname{ord}_p a_r\}. \tag{1.1}$$

We denote by $\langle a_1, \dots, a_r\rangle$ the subgroup of $\mathbb{Q}^*$ generated by $a_1, \dots, a_r$, and by $r(a_1, \dots, a_r) = \operatorname{rank}_{\mathbb{Z}}\langle a_1, \dots, a_r\rangle$ its rank as abelian group. Clearly

$$1 \le r(a_1, \dots, a_r) \le r.$$

The main results are the following two theorems.

Theorem 1. *Let $\{a_1, \dots, a_r\} \subset \mathbb{Q} \setminus \{0, \pm 1\}$ and assume that the Generalized Riemann Hypothesis holds for the fields $\mathbb{Q}(\zeta_n, a_1^{1/n_1}, \dots, a_r^{1/n_r})$ ($n, n_1, \dots, n_r \in \mathbb{N}$) and that $r(a_1, \dots, a_r) \ge 2$. Then*

$$\mathcal{N}_{a_1,\dots,a_r}(x) = \left(\delta_{a_1,\dots,a_r} + O_{a_1,\dots,a_r}\left(\frac{(\log\log x)^{2^r-2}}{\log x}\right)\right)\operatorname{li}(x)$$

where if $k_1, \dots, k_r \in \mathbb{N}$, $k = [k_1, \dots, k_r]$,

$$\Gamma = \langle a_1^{\frac{k}{k_1}}, \dots, a_r^{\frac{k}{k_r}}\rangle, \qquad \mathcal{A} = \Gamma \cdot \mathbb{Q}^{*mk}/\mathbb{Q}^{*mk},$$

$N = 2^{v_2(mk)}$ *and*

$$\mathcal{B} = \left\{\xi\mathbb{Q}^{*N} \in \Gamma\mathbb{Q}^{*N}/\mathbb{Q}^{*N} : \ [\mathbb{Q}(\sqrt[N]{\xi}) : \mathbb{Q}] \le 2 \text{ and } \operatorname{disc}(\mathbb{Q}(\sqrt[N]{\xi})) \mid mk\right\},$$

then

$$\delta_{a_1,\dots,a_r} = \sum_{\substack{m\in\mathbb{N}\\ k_1,\dots,k_r\in\mathbb{N}}} \frac{\mu(k_1)\cdots\mu(k_r)}{\varphi(mk)}\frac{\#\mathcal{B}}{\#\mathcal{A}}. \tag{1.2}$$

When each a_i is the power of the same rational number, the group $\langle a_1, \dots, a_r\rangle$ has rank one. In this case we write $a_i = a^{h_i}$ for each $i = 1, \dots, r$ and we note that we can assume that the greatest common divisor $(h_1, \dots, h_r) = 1$ otherwise we can replace a with $a^{(h_1,\dots,h_r)}$. Here the Generalized Riemann Hypothesis can be avoided.

Theorem 2. *Let $a \in \mathbb{Q} \setminus \{0, \pm 1\}$, $h_1, \dots, h_r \in \mathbb{N}^+$ with $(h_1, \dots, h_r) = 1$ and $h = [h_1, \dots, h_r]$. Then the following asymptotic formula holds:*

$$\mathcal{N}_{a^{h_1},\dots,a^{h_r}}(x) = \left(\delta_{a^{h_1},\dots,a^{h_r}} + O_{a,h}\left(\frac{(\log\log x)^{\omega(h)+3}}{(\log x)^2}\right)\right)\operatorname{li}(x)$$

where $\omega(h)$ denotes the number of distinct prime factors of h. If $a = \pm b^d$ with $b > 0$ not a power of any rational number and $D(b) = \operatorname{disc}(\mathbb{Q}\sqrt{b})$, then

$$\delta_{a^{h_1},\dots,a^{h_r}} = \prod_{l|h}\left(1 - \frac{l^{1-v_l(d)}}{l^2-1}\right)\times\left[1 + t_{2,h}\times\left(s_a + t_{D(b),4h}\times\varepsilon_a \prod_{l|2D(b)} \frac{1}{1-\frac{l^2-1}{l^{1-v_l(d)}}}\right)\right]$$

where

$$s_a = \begin{cases} 0 & \text{if } a > 0; \\ -\frac{3\cdot 2^{v_2(d)}-3}{3\cdot 2^{v_2(d)}-2} & \text{if } a < 0; \end{cases} \qquad t_{x,y} = \begin{cases} 1 & \text{if } x \mid y; \\ 0 & \text{otherwise;} \end{cases}$$

and

$$\varepsilon_a = \begin{cases} \left(-\frac{1}{2}\right)^{2^{\max\{0,v_2(D(b)/d)-1\}}} & \text{if } a > 0; \\ \left(-\frac{1}{2}\right)^{2^{2-\max\{1,v_2(D(b)/d)\}}} & \text{if } a < 0 \text{ and } v_2(D(b)) \neq v_2(8d); \\ \frac{1}{16} & \text{if } a < 0 \text{ and } v_2(D(b)) = v_2(8d). \end{cases}$$

In this degenerate case we can give a complete answer to the SW problem.

Corollary 3. *Let $a \in \mathbb{Q} \setminus \{0, \pm 1\}$ and $h_1, \dots, h_r \in \mathbb{N}^+$. Then $\delta_{a^{h_1},\dots,a^{h_r}} \neq 0$. Therefore the SW problem for $\{a^{h_1}, \dots, a^{h_r}\}$ has an affirmative answer.*

Corollary 3 will be proven at the end of Section 1.4.

1.2 Lemmata

In this section we present some useful results for setting up the proofs.

Let $\Gamma \subseteq \mathbb{Q}^*$ be a finitely generated multiplicative subgroup. The *support* of Γ is the finite set of primes defined as

$$S_\Gamma = \{p : \exists g \in \Gamma,\ v_p(g) \neq 0\}.$$

Furthermore for each prime $p \notin S_\Gamma$, we define the *order* $\operatorname{ord}_p \Gamma$ of Γ modulo p as the maximum order modulo p of the elements of Γ and the *index* of Γ modulo p by

$$\operatorname{ind}_p \Gamma = (p-1)/\operatorname{ord}_p \Gamma.$$

If we write $\operatorname{ind}_p \Gamma$ or $\operatorname{ord}_p \Gamma$, we always implicitly assume that $p \notin S_\Gamma$. In particular the *index* of a_i modulo p is defined as $\operatorname{ind}_p a_i = (p-1)/\operatorname{ord}_p a_i$. Once again, if we write $\operatorname{ind}_p a_i$, we assume that $v_p(a_i) = 0$.

We start from an elementary result:

Lemma 4. *Let $a_1 \ldots, a_r \in \mathbb{Q}^* \setminus \{\pm 1\}$, $m \in \mathbb{N}$, $k_1, \ldots, k_r \in \mathbb{N}$ be squarefree and set $k = [k_1, \ldots, k_r]$. If $p \notin S_{\langle a_1, \ldots, a_r \rangle}$, then the conditions*

i. $mk_i \mid \operatorname{ind}_p a_i$ *for* $i = 1, \ldots, r$*;*

ii. $mk \mid \operatorname{ind}_p \langle a_1^{k/k_1}, \ldots, a_r^{k/k_r} \rangle$

are equivalent.

Proof. First note that

$$(mk_i \mid \operatorname{ind}_p a_i \forall i = 1, \ldots, r) \quad \Longleftrightarrow \quad (mk \mid \operatorname{ind}_p a_i^{k/k_i} \forall i = 1, \ldots, r).$$

Indeed, if g is a primitive root modulo p and $a_i \equiv g^{\alpha_i} \pmod p$, then $\operatorname{ind}_p a_i = (p-1, \alpha_i)$. Furthermore $mk_i \mid (p-1, \alpha_i)$ for $i = 1, \ldots, r$ if and only if $mk \mid p-1$ and $mk \mid \alpha_i k/k_i$ for $i = 1, \ldots, r$. This happens if and only if $mk \mid (p-1, \alpha_i k/k_i)$ for $i = 1, \ldots, r$ or equivalently if $mk \mid \operatorname{ind}_p a_i^{k/k_i}$ for $i = 1, \ldots, r$. Finally

$$\operatorname{ind}_p \langle a_1^{k/k_1}, \ldots, a_r^{k/k_r} \rangle = (\operatorname{ind}_p a_1^{k/k_1}, \ldots, \operatorname{ind}_p a_r^{k/k_r}).$$

So $mk \mid \operatorname{ind}_p a_i^{k/k_i}$ for $i = 1, \ldots, r$ if and only if $mk \mid \operatorname{ind}_p \langle a_1^{k/k_1}, \ldots, a_r^{k/k_r} \rangle$. □

The proof of Theorem 1 uses the Chebotarev Density Theorem. The following version is obtained using the effective version due to Lagarias and Odlyzko [7].

Lemma 5 (Chebotarev Density Theorem)**.** *Let $M \in \mathbb{N}$. Then the Generalized Riemann Hypothesis for the Dedekind zeta function of the field $\mathbb{Q}(\zeta_M, \Gamma^{1/M})$ implies*

$$\#\{p \le x : \ M \mid \operatorname{ind}_p \Gamma\} = \frac{\operatorname{li}(x)}{[\mathbb{Q}(\zeta_M, \Gamma^{1/M}) : \mathbb{Q}]} + O\big(\sqrt{x} \log(xM \# S_\Gamma)\big). \qquad \square \tag{1.3}$$

To compute the degree $\big[\mathbb{Q}(\zeta_M, \Gamma^{1/M}) : \mathbb{Q}\big] = \# \operatorname{Gal}(\mathbb{Q}(\zeta_M, \Gamma^{1/M}) : \mathbb{Q})$ we need to employ Kummer Theory (see [8, Chapter VIII, section 8] and also [3]) that allows us to deduce the next result.

Lemma 6. *Let $M \geq 1$ be an integer and set $K = 2^{v_2(M)}$. With the notation above, we have that*

$$\left[\mathbb{Q}(\zeta_M, \Gamma^{1/M}) : \mathbb{Q}\right] = \#\mathcal{A}/\#\mathcal{B}$$

where

$$\mathcal{A} = \Gamma \cdot \mathbb{Q}^{*M}/\mathbb{Q}^{*M}$$

and

$$\mathcal{B} = \left\{\xi\mathbb{Q}^{*K} \in \Gamma\mathbb{Q}^{*K}/\mathbb{Q}^{*K} : \ [\mathbb{Q}(\sqrt[K]{\xi}) : \mathbb{Q}] \leq 2 \text{ and } \operatorname{disc}(\mathbb{Q}(\sqrt[K]{\xi})) \mid M\right\}. \square$$

The next lemma is implicit in the work of C. R. Matthews [10]:

Lemma 7. *Assume that $\Gamma \subseteq \mathbb{Q}^*$ is a multiplicative subgroup of rank $s \geq 2$. Let $t \in \mathbb{R}$, $t > 1$. We have the following estimate*

$$\#\left\{p \mid \operatorname{ord}_p \Gamma \leq t\right\} \ll \frac{t^{1+1/s}}{\log t}, \tag{1.4}$$

where the implied constants may depend on Γ. $\square$

The invariant $\Delta_s(\Gamma)$ of a multiplicative subgroup $\Gamma \subseteq \mathbb{Q}^*$ with $\operatorname{rank}_{\mathbb{Z}}(\Gamma) = s$, is defined as the great common divisor of all the minors of size s of the relation matrix of the group of absolute values of Γ (see [3, Section 3.1] for some details or chapter 2, section 1).

The next result follows immediately from a result in [3, Section 3.3], where it is stated in the case when M is squarefree. However, it is clear that the proof does not depend on this property.

Lemma 8. *Let Γ and M as above, and $s = \operatorname{rank}_{\mathbb{Z}}(\Gamma)$. Then*

$$[\mathbb{Q}(\zeta_M, \Gamma^{1/M}) : \mathbb{Q}] \geq \varphi(M)\frac{(M/2)^s}{\Delta_s(\Gamma)}. \qquad \square$$

Lemma 9. *Let $r \geq 2$ and let $\Gamma = \langle a_1^{k/k_1}, \ldots, a_r^{k/k_r}\rangle$ where $k_1, \ldots, k_r \in \mathbb{N}$ and $k = [k_1, \ldots, k_r]$. Further let $P(t)$ be the product of all primes up to t. Then we have the following identity*

$$\sum_{m \leq z} \sum_{k_1, \ldots, k_r \mid P(t)} \frac{\mu(k_1)\cdots\mu(k_r)}{[\mathbb{Q}(\zeta_{mk}, \Gamma^{1/km}) : \mathbb{Q}]} = \delta_{a_1,\ldots,a_r} + O\left(\frac{(\log t)^{2^r-2}}{t} + \frac{1}{z^s}\right) \tag{1.5}$$

where the implied constant may depend on $a_1, \ldots, a_r$.

Proof. Let us start by observing that if $s = \mathrm{rank}_{\mathbb{Z}}(\Gamma)$, then

$$\Delta_s(\langle a_1^{k/k_1}, \dots, a_r^{k/k_r}\rangle) \le k^{s-1} \times \Delta_s(\langle a_1, \dots, a_r\rangle).$$

Therefore, by Lemma 8 and since $\varphi(mk) \ge \varphi(m)\varphi(k)$, we have

$$\frac{1}{[\mathbb{Q}(\zeta_{mk}, \Gamma^{1/km}) : \mathbb{Q}]} \le \frac{1}{\varphi(m)m^s} \times \frac{2^s\Delta_s(\Gamma)}{\varphi(k)k^s} \ll \frac{1}{\varphi(m)m^s} \times \frac{1}{\varphi(k)\cdot k}.$$

Hence

$$\begin{aligned} S_0 &= \sum_{m>z} \sum_{k_1,\dots,k_r | P(t)} \frac{\mu(k_1)\cdots\mu(k_r)}{[\mathbb{Q}(\zeta_{mk}, \Gamma^{1/km}) : \mathbb{Q}]} \\ &\ll \sum_{m>z} \frac{1}{\varphi(m)m^s} \sum_{k|P(t)} \mu(k)^2 \sum_{\substack{k_1,\dots,k_r \\ k=[k_1,\dots,k_r]}} \frac{1}{\varphi(k)\cdot k} = O\left(\frac{1}{z^s}\right) \end{aligned} \tag{1.6}$$

since for k squarefree

$$\#\{k_1, \dots, k_r \in \mathbb{N} :\ k = [k_1, \dots, k_r]\} = (2^r - 1)^{\omega(k)}$$

and the series

$$\sum_{k|P(t)} \frac{(2^r-1)^{\omega(k)}}{\varphi(k)\cdot k}$$

converges as $t \to \infty$.

For a similar reason,

$$\begin{aligned} S_1 &= \sum_{m\le z} \sum_{k>t} \mu(k)^2 \sum_{\substack{k_1,\dots,k_r \\ k=[k_1,\dots,k_r]}} \frac{1}{[\mathbb{Q}(\zeta_{mk}, \Gamma^{1/km}) : \mathbb{Q}]} \\ &\ll \sum_{k>t} \mu(k)^2 \frac{(2^r-1)^{\omega(k)}}{\varphi(k)\cdot k} = O\left(\frac{(\log t)^{2^r-2}}{t}\right). \end{aligned} \tag{1.7}$$

The last estimate can be obtained for example as an application of the Ikeara Tauberian Theorem (see for example Delange [4]) and by partial summation, observing that

$$\sum_{n=1}^{\infty} \frac{\mu(k)^2(2^r-1)^{\omega(n)}}{\varphi(n)\cdot n^{s-1}} \cdot \zeta(s)^{1-2^r}.$$

is a meromorphic function, analytic and non zero at $s = 1$.

Finally, since

$$\sum_{m\leq z}\sum_{k_1,\dots,k_r|P(t)}\frac{\mu(k_1)\cdots\mu(k_r)}{[\mathbb{Q}(\zeta_{mk},\Gamma^{1/km}):\mathbb{Q}]}=\delta_{a_1,\dots,a_r}+O(S_0)+O(S_1),$$

we obtain the claim on summing the estimates of (1.6) and (1.7). □

1.3 General case: proof of Theorem 1

Let m be a positive integer. We need to consider the auxiliary function:

$$\mathcal{N}_{a_1,\dots,a_r}(x,m)=\{p\leq x\ :\ \mathrm{ind}_p\, a_1=\cdots=\mathrm{ind}_p\, a_r=m\}\,.$$

It is immediate that

$$\mathcal{N}_{a_1,\dots,a_r}(x)=\sum_{m\in\mathbb{N}}\mathcal{N}_{a_1,\dots,a_r}(x,m). \tag{1.8}$$

Note that for $r = 1$, the function $\mathcal{N}_a(x, m)$ was considered by L. Murata in 1991 [14], who proved:

Theorem 10 (Murata)**.** *Let $a \geq 2$ be a squarefree natural number and assume that the GRH holds. Then we have, for any $\epsilon > 0$*

$$\#\{p\leq x\ :\ \mathrm{ind}_p\, a=m\}=\left(c_{a,m}+O\left(\frac{m^\epsilon\log\log x+\log a}{\log x}\right)\right)\mathrm{li}(x)$$

where $c_{a,m}$ is a suitable non negative constant, and the constant implied in the O–symbol may depend on ϵ.

The problem of determining when $c_{a,m} = 0$ has been addressed by H. Lenstra [9]. A general expression for the constant $c_{a,m}$ has been obtained by S. Wagstaff [21]. These results and also Theorem 1 are proved using the classical method of Hooley [6].

As a side-product of our Theorem 1, we prove implicitly the following result that generalizes Matthews's Theorem and it is an analogue of Murata's Theorem:

Theorem 11. *Let $\{a_1, \dots, a_r\} \subset \mathbb{Q} \setminus \{0, \pm 1\}$, $m \in \mathbb{N}$, assume that GRH holds and that $r(a_1, \dots, a_r) \geq 2$. Then*

$$\mathcal{N}_{a_1,\dots,a_r}(x,m) = \left(c_{a_1,\dots,a_r,m} + O_{a_1,\dots,a_r,m}\left(\frac{(\log\log x)^{2^r-2}}{\log x} \right) \right) \mathrm{li}(x)$$

where

$$c_{a_1,\dots,a_r,m} = \sum_{k_1,\dots,k_r \in \mathbb{N}} \frac{\mu(k_1)\cdots\mu(k_r)}{\varphi(mk)} \frac{\#\mathcal{B}}{\#\mathcal{A}} \tag{1.9}$$

and the notations are the same as in the statement of Theorem 1. □

Proof of Theorem 1. We estimate the lowerbound and the upperbound separately. For the upperbound note that if $y \in \mathbb{R}$, with $0 \leq y \leq x$, then

$$\sum_{m \geq y} \mathcal{N}_{a_1,\dots,a_r}(x,m) \ll \left(\frac{x}{y}\right)^{1+1/s} \frac{1}{\log(x/y)}.$$

Indeed if $\mathrm{ind}_p\, a_1 = \cdots = \mathrm{ind}_p\, a_r$, then each a_i generates the same group modulo p. Hence in particular, for each $i = 1, \dots, r$, we have that $\mathrm{ind}_p\, a_i = \mathrm{ind}_p \langle a_1, \dots, a_r \rangle$. So

$$\begin{aligned}
\sum_{m \geq y} \mathcal{N}_{a_1,\dots,a_r}(x,m) &\leq \#\left\{ p \leq x \,:\, \mathrm{ind}_p\langle a_1, \dots, a_r\rangle > y \right\} \\
&\leq \#\left\{ p \leq x : \, \mathrm{ord}_p\langle a_1, \dots, a_r\rangle < \frac{x}{y} \right\} \\
&\ll \left(\frac{x}{y}\right)^{1+1/s} \frac{1}{\log(x/y)}
\end{aligned}$$

by Lemma 7. Therefore we can take $y = (x \log^s x)^{1/(s+1)}$ obtaining

$$\begin{aligned}
\mathcal{N}_{a_1,\dots,a_r}(x) &\leq \sum_{m \leq y} \mathcal{S}_{a_1,\dots,a_r}(x,m) + O\left(\left(\frac{x}{y}\right)^{1+1/s} \frac{1}{\log(x/y)} \right) \\
&= \sum_{m \leq y} \mathcal{N}_{a_1,\dots,a_r}(x,m) + O\left(\frac{x}{(\log x)^2} \right).
\end{aligned}$$

For each $t \in \mathbb{R}$, $1 \leq t \leq x$, we further set

$$\mathcal{N}_{a_1,\dots,a_r}(x,m,t) = \#\left\{ p \leq x : \, \forall i = 1, \dots, r, \; m | \, \mathrm{ind}_p\, a_i \text{ and } \left(\frac{\mathrm{ind}_p\, a_i}{m}, P(t) \right) = 1 \right\}$$

where, as usual, $P(t)$ denotes the product of all primes p up to t.

Note that

$$\mathcal{N}_{a_1,\dots,a_r}(x,m) \le \mathcal{N}_{a_1,\dots,a_r}(x,m,t).$$

Furthermore the Inclusion/Exclusion Principle yields

$$\sum_{m\le y}\mathcal{N}_{a_1,\dots,a_r}(x,m,t) = \sum_{m\le y}\sum_{k_1,\dots,k_r|P(t)}\mu(k_1)\cdots\mu(k_r)C_m(x;k_1,\dots,k_r) \quad (1.10)$$

where

$$C_m(x;k_1,\dots,k_r) = \#\{p\le x:\ mk_i \mid \operatorname{ind}_p a_i\ \forall i=1,\dots,r\}.$$

Let $k=[k_1,\dots,k_r]$, apply Lemma 4 so that $mk_i \mid \operatorname{ind}_p a_i$ for $i=1,\dots,r$ if and only if $mk \mid \operatorname{ind}_p\langle a_1^{k/k_1},\dots,a_r^{k/k_r}\rangle$. Therefore

$$C_m(x;k_1,\dots,k_r) = \#\{p\le x:\ mk \mid \operatorname{ind}_p\langle a_1^{k/k_1},\dots,a_r^{k/k_r}\rangle\}.$$

The Chebotarev Density Theorem in Lemma 5, implies that (1.10) equals

$$\sum_{m\le y}\sum_{k_1,\dots,k_r|P(t)}\mu(k_1)\cdots\mu(k_r)\left[\frac{\operatorname{li}(x)}{[\mathbb{Q}(\zeta_{mk},\Gamma^{1/km}):\mathbb{Q}]}+O_{a_1,\dots,a_r}(\sqrt{x}\log(xmk))\right]$$

where $\Gamma=\langle a_1^{k/k_1},\dots,a_r^{k/k_r}\rangle$. Here we used the fact that $S_\Gamma = S_{\langle a_1,\dots,a_r\rangle}$. It is easy to see that:

$$\begin{aligned}\sum_{m\le y}\sum_{k_1,\dots,k_r|P(t)}\sqrt{x}\log(xmk) &= \sum_{m\le y}O\big(\sqrt{x}2^{tr}\log(xmP(t))\big)\\ &= O\big(x^{(s+3)/(2s+2)}2^{tr}\log^2(xP(t))\big).\end{aligned}$$

Therefore, since $s\ge 2$,

$$\begin{aligned}\mathcal{N}_{a_1,\dots,a_r}(x) &\le \left[\sum_{m\le y}\sum_{k_1,\dots,k_r|P(t)}\frac{\mu(k_1)\cdots\mu(k_r)}{[\mathbb{Q}(\zeta_{mk},\Gamma^{1/km}):\mathbb{Q}]}+O\left(\frac{1}{\log x}\right)\right]\operatorname{li}(x)\\ &= \left[\delta_{a_1,\dots,a_r}+O\left(\frac{(\log t)^{2^r-2}}{t}+\frac{2^{tr}\log^3(xP(t))}{x^{(s-1)/(2s+2)}}+\frac{1}{\log x}\right)\right]\operatorname{li}(x)\end{aligned} \quad (1.11)$$

in virtue of Lemma 9 and of the previous discussion. If we choose $t = \log x/(7r\log 2)$, we obtain the upperbound estimate.

As for the lowerbound let $z \in \mathbb{R}$, with $1 \leq z \leq x$. It is clear that

$$\mathcal{N}_{a_1,\dots,a_r}(x) \geq \sum_{m\leq z} \mathcal{S}_{a_1,\dots,a_r}(x,m). \tag{1.12}$$

From a similar argument as above we deduce that

$$\sum_{m\leq z} \mathcal{N}_{a_1,\dots,a_r}(x,m) = \left[\delta_{a_1,\dots,a_r} + O\left(\frac{(\log\log x)^{2^r-2}}{\log x} + \frac{1}{z^s} + \frac{z\log^3 x}{x^{1/42}}\right)\right]\mathrm{li}(x) + E(x,z). \tag{1.13}$$

where if $t = \log x/(7r\log 2)$, then

$$E(x,z) = O\left(\sum_{m\leq z} \#\left\{p\leq x:\ \exists i, l > t, lm \mid \mathrm{ind}_p\, a_i\right\}\right).$$

In order to estimate the above for each η_1, η_2 with $t \leq \eta_1 < \eta_2 \leq x$, we define:

$$E_i(x,m;\eta_1,\eta_2) = \#\left\{p\leq x:\ \exists l\in(\eta_1,\eta_2],\ lm \mid \mathrm{ind}_p\, a_i\right\}.$$

So

$$E(x,z) \leq \sum_{m\leq z}\sum_{i=1}^{r}[E_i(x,m;t,\eta) + E_i(x,m;\eta,x)].$$

Note that

$$E_i(x,m;\eta,x) \leq \left\{p\leq x:\ \mathrm{ord}_p\, a_i < \frac{x}{m\eta}\right\}.$$

Applying Lemma 7, we deduce that

$$\sum_{i=1}^{r}\sum_{m\leq z} E_i(x,m;\eta,x) \ll \sum_{m\leq z}\left(\frac{x}{m\eta}\right)^{1+1/s}\frac{1}{\log(x/m\eta)} = O\left(\frac{x}{\log^2(x/z)}\right), \tag{1.14}$$

if we choose $\eta = (x\log^s x)^{1/(s+1)}$.

To estimate the first term, we use again the Chebotarev Density Theorem in the form given by Theorem 1.3. So

$$\begin{aligned}\sum_{i=1}^{r}\sum_{m\le z} E_i(x,m;t,\eta) &\le \sum_{i=1}^{r}\sum_{m\le z}\sum_{l\in(t,\eta]}\left(\frac{\mathrm{li}(x)}{[\mathbb{Q}(\zeta_{ml},a_i^{1/ml}):\mathbb{Q}]}+O(\sqrt{x}\log(xml))\right)\\ &= O_{a_1,\dots a_r}\left(\mathrm{li}(x)\sum_{m\le z}\sum_{l>t}\frac{1}{m\varphi(m)}\frac{1}{l^2-l}+\sum_{l<\eta}\sqrt{x}z\log(xzl)\right)\\ &= O_{a_1,\dots a_r}\left(\frac{\mathrm{li}(x)}{t}+\eta\sqrt{x}\log(xz\eta)\right).\end{aligned}$$

To conclude the proof of Theorem 1 it is enough to choose $z=\log x$. □

1.4 Degenerate case: proof of Theorem 2 and Corollary 3.

Let

$$\mathcal{N}_a(x,k)=\#\{p\le x:\ k|\operatorname{ord}_p a\}.$$

The function $\mathcal{N}_a(x,k)$ has been studied by several authors: Ballot, Hasse, Moree, Odoni, Pappalardi, Wiertelak and maybe others. Wiertelak [22] was the first to obtain an asymptotic formula for $\mathcal{N}_a(x,k)$ (see also [16]). The proof of Theorem 2 requires the most general result due to Moree [12, Theorem 2].

Lemma 12. *Let $k\in\mathbb{N}^+$ be squarefree and $a\in\mathbb{Q}\setminus\{0,\pm1\}$. Then the following asymptotic formula holds:*

$$\mathcal{N}_a(x,k)=\left(\kappa_{a,k}+O_{a,k}\left(\frac{(\log\log x)^{\omega(k)+3}}{(\log x)^2}\right)\right)\mathrm{li}(x).$$

Here

$$\kappa_{a,k}=(1+\varepsilon)\prod_{l|k}\frac{l^{1-v_l(d)}}{l^2-1} \tag{1.15}$$

where if we write $a = \pm b^d$ *with* $b \in \mathbb{Q}^{>0}$ *not a perfect power,* $D(b) = \mathrm{disc}(\mathbb{Q}(\sqrt{b}))$,

$$\varepsilon = \begin{cases} \frac{3(1-\mathrm{sgn}(a))(2^{v_2(d)}-1)}{4} + \varepsilon_a, & \text{if } 2 \mid k \text{ and } D(b) \mid 4k; \\ \frac{3(1-\mathrm{sgn}(a))(2^{v_2(d)}-1)}{4}, & \text{if } 2 \mid k \text{ and } D(b) \nmid 4k; \\ 0, & \text{if } 2 \nmid k; \end{cases}$$

and

$$\varepsilon_a = \begin{cases} \left(-\frac{1}{2}\right)^{2^{\max\{0, v_2(D(b)/d)-1\}}}, & \text{if } a > 0; \\ \left(-\frac{1}{2}\right)^{2^{2-\max\{1, v_2(D(b)/d)\}}}, & \text{if } a < 0 \text{ and } v_2(D(b)) \neq v_2(8d); \\ \frac{1}{16}, & \text{if } a < 0 \text{ and } v_2(D(b)) = v_2(8d). \end{cases}$$

Proof of Theorem 2. We use the general property:

$$\mathrm{ord}_p\, a^s = \mathrm{ord}_p\, a/(s, \mathrm{ord}_p\, a)$$

and we observe that when $(h_1, \ldots, h_r) = 1$, the condition

$$(h_i, \mathrm{ord}_p\, a) = (h_j, \mathrm{ord}_p\, a) \text{ for all } i, j = 1, \ldots, r$$

is equivalent to $(h_i, \mathrm{ord}_p\, a) = 1$ for $i = 1, \ldots, r$. The latter condition is equivalent to $(h, \mathrm{ord}_p\, a) = 1$ where $h = [h_1, \ldots, h_r]$. Therefore by the Inclusion/Exclusion Principle,

$$\begin{aligned} \mathcal{N}_{a^{h_1}, \ldots, a^{h_r}}(x) &= \{p \leq x : \ (h, \mathrm{ord}_p\, a) = 1\} \\ &= \sum_{k \mid h} \mu(k) \#\{p \leq x : \ k \mid \mathrm{ord}_p\, a\}. \end{aligned}$$

The function above has also been considered by Wiertelak [23] in the special case when a is a positive integer. By Lemma 12, we have

$$\begin{aligned} S_{a^{h_1}, \ldots, a^{h_r}}(x) &= \sum_{k \mid\mid h} \mu(k) \left(\kappa_{a,k} + O_{a,h}\left(\frac{(\log\log x)^{\omega(h)+3}}{(\log x)^2} \right) \right) \mathrm{li}(x) \\ &= \left(\delta_{a^{h_1}, \ldots, a_r^{h_r}} + O_{a,h}\left(\frac{(\log\log x)^{\omega(h)+3}}{(\log x)^2} \right) \right) \mathrm{li}(x) \end{aligned}$$

where

$$\delta_{a^{h_1}, \ldots, a_r^{h_r}} = \sum_{k \mid h} \mu(k)(1+\varepsilon) \prod_{l \mid k} \frac{l^{1-v_l(d)}}{l^2 - 1}.$$

The above is equal to $\Sigma_1 + \Sigma_2 + \Sigma_3$ where

$$\Sigma_1 = \sum_{k|h} \mu(k) \prod_{l|k} \frac{l^{1-v_l(d)}}{l^2-1} = \prod_{l|h} \left(1 - \frac{l^{1-v_l(d)}}{l^2-1}\right), \tag{1.16}$$

$$\begin{aligned} \Sigma_2 &= \frac{(3(1-\mathrm{sgn}(a))(2^{v_2(d)}-1)}{4} \sum_{\substack{k|h \\ 2|k}} \mu(k) \prod_{l|k} \frac{l^{1-v_l(d)}}{l^2-1} \\ &= t_{2,h} \times \frac{\mathrm{sgn}(a)-1}{2} \times \frac{3 \cdot 2^{v_2(d)}-3}{3 \cdot 2^{v_2(d)}-2} \times \prod_{l|h} \left(1 - \frac{l^{1-v_l(d)}}{l^2-1}\right) \\ &= t_{2,h} \times s_a \times \prod_{l|h} \left(1 - \frac{l^{1-v_l(d)}}{l^2-1}\right) \end{aligned} \tag{1.17}$$

and

$$\Sigma_3 = \varepsilon_a \times \sum_{\substack{k|h \\ 2|k \\ D(b)|4k}} \mu(k) \prod_{l|k} \frac{l^{1-v_l(d)}}{l^2-1}. \tag{1.18}$$

The conditions $2 \mid k$ and $D(b) \mid 4k$ are equivalent to the condition $[2, D(b)/(D(b),4)] \mid k$. Furthermore the integer $[2, D(b)/(D(b),4)]$ is squarefree and equals to the product of the primes dividing $2D(b)$. Therefore the sum on the right hand side above equals

$$t_{2,h} \times t_{D(b),4h} \times \prod_{l|2D(d)} \frac{-l^{1-v_l(d)}}{l^2-1} \left(1 - \frac{l^{1-v_l(d)}}{l^2-1}\right)^{-1} \times \prod_{l|h} \left(1 - \frac{l^{1-v_l(d)}}{l^2-1}\right). \tag{1.19}$$

Adding up the expression in (1.16), (1.17), (1.18) and ε_a times (1.19) we obtain the formula for $\delta_{a^{h_1},\ldots,a^{h_r}}$ in the statement of Theorem 2. □

Proof of Corollary 3. Note that

$$\prod_{l|h} \left(1 - \frac{l^{1-v_l(d)}}{l^2-1}\right) \neq 0$$

so, in order for $\delta_{a^{h_1},\ldots,a^{h_r}} = 0$ we should have $2 \mid h$ so that $t_{2,h} = 1$ and

$$s_a + t_{D(b),4h} \times \varepsilon_a \prod_{l|2D(b)} \frac{1}{\left(1 - \frac{l^2-1}{l^{1-v_l(d)}}\right)} = -1. \tag{1.20}$$

In the case $a > 0$, then $s_a = 0$ and identity (1.20) boils down to

$$\prod_{l|2D(b)} \left(\frac{l - l^{v_l(d)}(l^2-1)}{l} \right) = -t \times \varepsilon_a = -t \times \left(-\frac{1}{2} \right)^{2^\nu} \tag{1.21}$$

where $\nu \in \{0, 1, 2\}$ and $t \in \{0, 1\}$. First note that the left hand side of (1.21) is larger than $1/2$ in absolute value. Indeed, we have that

$$\frac{l^{v_l(d)}(l^2-1) - l}{l} \begin{cases} > 1 & \text{if } l > 2 \text{ or if } l = 2 \text{ and } v_2(d) > 0 \\ = \frac{1}{2} & \text{if } l = 2 \text{ and } v_2(d) = 0. \end{cases}$$

This implies that in order for equality (1.21) to be satisfied we must have $\nu = 0$ and $t = 1$. But this also implies that $2D(b) = 16$ and therefore the left hand side of (1.21) is equal to $-1/2$ while the right hand side is equal to $1/2$.

In the case $a < 0$, after some calculations, identity (1.20) boils down to

$$\prod_{\substack{l|D(b) \\ l>2}} \left(\frac{l - l^{v_l(d)}(l^2-1)}{l} \right) = 2t \times \left(-\frac{1}{2} \right)^{2^\nu}, \tag{1.22}$$

where $\nu \in \{0, 1, 2\}$, $t \in \{0, 1\}$. This forces $t = 1$ and $\nu = 0$ for otherwise the right hand side of (1.22) would have as denominator a power of 2 which cannot happen on the left hand side. By a similar argument as above we arrive to a contradiction. This concludes the proof of Corollary 3. □

1.5 Numerical Examples

In this section we compare numerical data. The table compares the densities $\delta_{a,a^2,\ldots,a^r}$ with the quantities $\mathcal{S}_{a,a^2\ldots,a^r}(10^8)/\pi(10^8)$ for $r = 2, 3, \ldots, 8$ and $a \in \mathbb{Q} \setminus \{0, \pm 1\}$ with natural height up to 8. Both quantities have been truncated at the fifth decimal digit.

$\mathcal{N}_{a,a^2\ldots,a^r}(10^8)/\pi(10^8)$ $\delta_{a,a^2,\ldots,a^r}$,							
$a \setminus r$	2	3	4	5	6	7	8
2	0.29165	0.18226	0.18226	0.14429	0.14429	0.12325	0.12325
	0.29166	0.18229	0.18229	0.14431	0.14431	0.12326	0.12326
-2	0.29164	0.18228	0.18228	0.14429	0.14429	0.12325	0.12325
	0.29166	0.18229	0.18229	0.14431	0.14431	0.12326	0.12326
3	0.33336	0.27084	0.27084	0.21445	0.21445	0.18322	0.18322
	0.33333	0.27083	0.27083	0.21440	0.21440	0.18314	0.18314
-3	0.33335	0.08334	0.08334	0.06597	0.06597	0.05635	0.05635
	0.33333	0.08333	0.08333	0.06597	0.06597	0.05635	0.05635
3/2	0.33338	0.22401	0.22401	0.17732	0.17732	0.15145	0.15145
	0.33333	0.22395	0.22395	0.17730	0.17730	0.15144	0.15144
-3/2	0.33331	0.22398	0.22398	0.17729	0.17729	0.15152	0.15152
	0.33333	0.22395	0.22395	0.17730	0.17730	0.15144	0.15144
4	0.58330	0.36454	0.36454	0.28858	0.28858	0.24651	0.24651
	0.58333	0.36458	0.36458	0.28862	0.28862	0.24653	0.24653
-4	0.33333	0.20832	0.20832	0.16490	0.16490	0.14082	0.14082
	0.33333	0.20833	0.20833	0.16493	0.16493	0.14087	0.14087
3/4	0.33330	0.27083	0.27083	0.21443	0.21443	0.18323	0.18323
	0.33333	0.27083	0.27083	0.21440	0.21440	0.18134	0.18134
-3/4	0.33335	0.08332	0.08332	0.06593	0.06593	0.05634	0.05634
	0.33333	0.08333	0.08333	0.06597	0.06597	0.05635	0.05635
5	0.33323	0.20826	0.20826	0.12157	0.12157	0.10384	0.10384
	0.33333	0.20833	0.20833	0.12152	0.12152	0.10380	0.10380
-5	0.33342	0.20833	0.20833	0.18661	0.18661	0.15941	0.15941
	0.33333	0.20833	0.20833	0.18663	0.18663	0.15941	0.15941
2/5	0.33325	0.20837	0.20837	0.17037	0.17037	0.14557	0.14557
	0.33333	0.20833	0.20833	0.17035	0.17035	0.14551	0.14551
-2/5	0.33342	0.20835	0.20835	0.17036	0.17036	0.14554	0.14554
	0.33333	0.20833	0.20833	0.17035	0.17035	0.14551	0.14551
3/5	0.33326	0.20831	0.20831	0.15190	0.15190	0.12970	0.12970
	0.33333	0.20833	0.20833	0.15190	0.15190	0.12975	0.12975
-3/5	0.33344	0.20836	0.20836	0.19099	0.19099	0.16324	0.16324
	0.33333	0.20833	0.20833	0.19097	0.19097	0.16312	0.16312

$\mathcal{N}_{a,a^2\ldots,a^r}(10^8)/\pi(10^8) \qquad \delta_{a,a^2,\ldots,a^r}$,							
$a \setminus r$	2	3	4	5	6	7	8
4/5	0.33337	0.20837	0.20837	0.12163	0.12163	0.10392	0.10392
	0.33333	0.20833	0.20833	0.12152	0.12152	0.10380	0.10380
-4/5	0.33331	0.20823	0.20823	0.18654	0.18654	0.15936	0.15936
	0.33333	0.20833	0.20833	0.18663	0.18663	0.15941	0.15941
6	0.33330	0.22398	0.22398	0.17721	0.17721	0.15135	0.15135
	0.33333	0.22395	0.22395	0.17730	0.17730	0.15144	0.15144
-6	0.33335	0.22399	0.22399	0.17733	0.17733	0.15156	0.15156
	0.33333	0.22395	0.22395	0.17730	0.17730	0.15144	0.15144
5/6	0.33328	0.20840	0.20840	0.16172	0.16172	0.13813	0.13813
	0.33333	0.20833	0.20833	0.16167	0.16167	0.13809	0.13809
-5/6	0.33322	0.20823	0.20823	0.16157	0.16157	0.13799	0.13799
	0.33333	0.20833	0.20833	0.16167	0.16167	0.13809	0.13809
7	0.33335	0.20842	0.20842	0.16495	0.16495	0.15289	0.15289
	0.33333	0.20833	0.20833	0.16493	0.16493	0.15290	0.15290
-7	0.33327	0.20828	0.20828	0.16483	0.16483	0.11677	0.11677
	0.33333	0.20833	0.20833	0.16493	0.16493	0.11682	0.11682
2/7	0.33332	0.20829	0.20829	0.16483	0.16483	0.14382	0.14382
	0.33333	0.20833	0.20833	0.16493	0.16493	0.14388	0.14388
-2/7	0.33325	0.20830	0.20830	0.16485	0.16485	0.14385	0.14385
	0.33333	0.20833	0.20833	0.16493	0.16493	0.14388	0.14388
3/7	0.33328	0.20829	0.20829	0.16493	0.16493	0.15531	0.15531
	0.33333	0.20833	0.20833	0.16493	0.16493	0.15530	0.15530
-3/7	0.33341	0.20841	0.20841	0.16494	0.16494	0.13377	0.13377
	0.33333	0.20833	0.20833	0.16493	0.16493	0.13366	0.13366
4/7	0.33330	0.20829	0.20829	0.16500	0.16500	0.15296	0.15296
	0.33333	0.20833	0.20833	0.16493	0.16493	0.15290	0.15290
-4/7	0.33327	0.20833	0.20833	0.16484	0.16484	0.11680	0.11680
	0.33333	0.20833	0.20833	0.16493	0.16493	0.11682	0.11682
5/7	0.33326	0.20832	0.20832	0.16497	0.16497	0.13778	0.13778
	0.33333	0.20833	0.20833	0.16493	0.16493	0.13771	0.13771
-5/7	0.33343	0.20836	0.20836	0.16496	0.16496	0.14729	0.14729
	0.33333	0.20833	0.20833	0.16493	0.16493	0.14720	0.14720

$\mathcal{N}_{a,a^2\ldots,a^r}(10^8)/\pi(10^8)$ $\delta_{a,a^2,\ldots,a^r}$,							
$a \setminus r$	2	3	4	5	6	7	8
6/7	0.33333	0.20841	0.20841	0.16496	0.16496	0.13915	0.13915
	0.33333	0.20833	0.20833	0.16493	0.16493	0.13907	0.13907
-6/7	0.33329	0.20823	0.20823	0.16491	0.16491	0.13907	0.13907
	0.33333	0.20833	0.20833	0.16493	0.16493	0.13907	0.13907
8	0.29165	0.25523	0.25523	0.20206	0.20206	0.17264	0.17264
	0.29166	0.25520	0.25520	0.20203	0.20203	0.17257	0.17257
-8	0.29164	0.25519	0.25519	0.20201	0.20201	0.17253	0.17253
	0.29166	0.25520	0.25520	0.20203	0.20203	0.17257	0.17257
3/8	0.33327	0.22399	0.22399	0.17724	0.17724	0.15141	0.15141
	0.33333	0.22395	0.22395	0.17730	0.17730	0.15144	0.15144
-3/8	0.33338	0.22401	0.22401	0.17733	0.17733	0.15149	0.15149
	0.33333	0.22395	0.22395	0.17730	0.17730	0.15144	0.15144
5/8	0.33341	0.20836	0.20836	0.17036	0.17036	0.14552	0.14552
	0.33333	0.20833	0.20833	0.17035	0.17035	0.14551	0.14551
-5/8	0.33326	0.20826	0.20826	0.17034	0.17034	0.14551	0.14551
	0.33333	0.20833	0.20833	0.17035	0.17035	0.14551	0.14551
7/8	0.33334	0.20827	0.20827	0.16490	0.16490	0.14391	0.14391
	0.33333	0.20833	0.20833	0.16493	0.16493	0.14388	0.14388
-7/8	0.33327	0.20823	0.20823	0.16481	0.16481	0.14379	0.14379
	0.33333	0.20833	0.20833	0.16493	0.16493	0.14388	0.14388

It is easy to see that if r is not prime, then

$$\delta_{a,a^2,\ldots,a^r} = \delta_{a,a^2,\ldots,a^{r-1}}.$$

Indeed the formula for $\delta_{a,a^2,\ldots,a^r}$ in Theorem 2 depends only on the squarefree kernel of $1\cdot 2\cdots r$. Note that the squarefree kernel of $1\cdot 2\cdots r$ equals the squarefree kernel of $1\cdot 2\cdots(r-1)$ if and only if r is not prime.

Similarly if r is not prime, for every $x > 1$,

$$\mathcal{N}_{a,a^2,\ldots,a^r}(x) = \mathcal{N}_{a,a^2,\ldots,a^{r-1}}(x).$$

Indeed if $r = st$, then $\operatorname{ord}_p a^s = \operatorname{ord}_p a^t = \operatorname{ord}_p a$ if and only if

$$(\operatorname{ord}_p a, s) = (\operatorname{ord}_p a, t) = 1$$

and this is equivalent to $(\mathrm{ord}_p\, a, st) = 1$.

This explains why the third column in the tables equals the second, the fifth equals the fourth and the seventh equals the sixth.

1.6 Conclusion.

It would be interesting to determine (even conjecturally) a characterization of those finite sets of rational numbers for which the SW problem has an affirmative answer. We are unable to do that at present time but it is reasonable to expect that the SW problem has an affirmative answer for $\{a_1, \ldots, a_r\}$ if and only if

$$\delta_{a_1,\ldots,a_r} \neq 0.$$

Indeed in many variations of Artin's primitive root conjecture it is seen that if a set of primes satisfying certain order conditions had density zero, then the set is finite. In Lenstra's paper [9] there are some results to this effect.

We are also unable to characterize the finite sets for which $\delta_{a_1,\ldots,a_r} \neq 0$ (which in virtue of Theorem 1 provides on GRH a sufficient condition for the SW problem to have affirmative answer). We will address this problem in a future paper.

We conclude with the following elementary result:

Proposition 13. *If $S = \{a_1, \ldots, a_r\} \subset \mathbb{Q}^* \setminus \{0, \pm 1\}$ is such that:*

i. $-1 \in \langle S \rangle$*;*

ii. $S \cap \langle S \rangle^2 \neq \emptyset$*.*

Then the SW problem for S has a negative answer.

Proof. Assume that $\delta = \mathrm{ord}_p\, a_1 = \ldots = \mathrm{ord}_p\, a_r$ for some prime $p > 2$. Since $-1 = a_1^{\omega_1} \cdots a_r^{\omega_r}$ for suitable $\omega_1, \ldots, \omega_r \in \mathbb{Z}$, we have

$$(-1)^\delta \equiv a_1^{\delta\omega_1} \cdots a_r^{\delta\omega_r} \equiv 1 \pmod{p}.$$

This implies that $2 \mid \delta$.

If $a_{i_0} \in S \cap \langle S \rangle^2$, then $a_{i_0} = a_1^{2\tau_1} \cdots a_r^{2\tau_r}$ for suitable $\tau_1, \ldots, \tau_r \in \mathbb{Z}$. Hence

$$a_{i_0}^{\delta/2} = a_1^{\delta\tau_1} \cdots a_r^{\delta\tau_r} \equiv 1 \pmod{p}$$

which contradicts the hypothesis $\operatorname{ind}_p a_{i_0} = \delta$. □

We conclude with a series of remarks:

1. The two conditions of Proposition 13 can be both satisfied only if $r \geq 3$.

2. The second condition in Proposition 13 implies in particular that a_{i_0} is a square and therefore the Matthews constant $C(a_1, \ldots, a_r)$ (defined as in Matthews' Theorem in the introduction) is zero.

3. While the condition $-1 \in \langle S \rangle$ in the previous proposition seems to be necessary in order the have a negative answer to the SW problem (See Wójcik's Theorem in the introduction), we are unable to guess whether the second one is necessary.

4. The only case which is not covered neither by Theorem 1 or by Theorem 2 is $r(a_1, \ldots, a_r) = 1$ and $-1 \in \langle a_1, \ldots, a_r \rangle$. From Proposition 13 we deduce that this case includes some sets for which the SW problem has negative answer.

5. A weaker analogue of the SW problem is the question of whether there exist infinitely many primes p such that $\operatorname{ord}_p a_1 \mid \operatorname{ord}_p a_2 \mid \cdots \mid \operatorname{ord}_p a_r$. Maybe there are examples where this problem has affirmative answer, whereas the SW problem has negative answer. For $r = 2$ this problem has been considered by Moree and Stevenhagen [13]. They prove that if $a = a_1/a_2$ and $b = b_1/b_2$, ($(a_1, a_2) = (b_1, b_2) = 1$) are multiplicatively independent rationals, then the set of primes such that $\operatorname{ord}_p a \mid \operatorname{ord}_p b$ is infinite and is equal to the set of primes dividing at least one term of the sequence $b_2\, a_1^n - b_1\, a_2^n$, $n \geq 1$. This is a special case of a theorem due to Polya. Under GRH this set has a positive density.

2. EXPLICIT COMPUTATION OF $\delta_{A,B}$

In this chapter we want to find an explicit formula for $\delta_{a,b}$, with a, b multiplicatively independent rational numbers. Before doing it, we need to introduce some notations.

Let $a = \prod_{i=1}^{t} p_i^{\alpha_i}$ and $b = \prod_{i=1}^{t} p_i^{\beta_i}$, with $\alpha_i, \beta_i \in \mathbb{Z}$ and $p_1 < p_2 < \ldots < p_t$ (this convention holds for this whole chapter). We denote by $\alpha = (\alpha_1, \ldots, \alpha_t)$ and $\beta = (\beta_1, \ldots, \beta_t)$) the vectors of the powers of a and b. Let $k_1, k_2 \in \mathbb{N}$. We set $k = [k_1, k_2]$, $\widetilde{k_i} = \frac{k}{k_i}$, $M = mk$ and $\Gamma = \langle a^{\widetilde{k_1}}, b^{\widetilde{k_2}} \rangle$ as subgroup of $\mathbb{Q}^*$. As in the previous chapter let $\mathcal{S}_\Gamma$ be the support of Γ.

For any matrix $A \in M_{n\times m}(\mathbb{Z})$ with $\mathrm{rank}(A) = s$, we define the invariant $\Delta_i(A)$ as the greatest common divisor of all the minors of size i of A, with the following conventions: $\Delta_0 = 1$ and $\Delta_i = 0$ for any $i > s$. Further we set $h_1 = \Delta_1(\alpha)$, $h_2 = \Delta_1(\beta)$ and $D = \frac{\Delta_2(\alpha,\beta)}{h_1 h_2}$. We also define, for all prime p fixed, $d_1 = \min(v_p(h_1), v_p(h_2))$, $\overline{d}_1 = \max(v_p(h_1), v_p(h_2))$ and $d_2 = v_p(\Delta_2(\alpha, \beta))$.

Let $\{e_i\}_{i=1,\ldots,t}$ be the canonical basis of $\mathbb{F}_2^t$ as vectorial space over $\mathbb{F}_2$. For any $(n_1, n_2) \in \mathbb{F}_2^2$ and for any p fixed, we define

$$\begin{aligned}
&\underline{n} = \min(n_1, n_2),\ \overline{n} = \max(n_1, n_2),\\
&\delta_1 = \min(v_p(h_1) + n_2, v_p(h_2) + n_1) - \underline{n},\\
&\delta_2 = d_2 + n_1 + n_2 - \underline{n}.
\end{aligned}$$

Let $\varepsilon \in \mathbb{F}_2^t$ be a column vector. For all p fixed, we set:

$$\begin{aligned}
d_2^\varepsilon &= \min(v_p(\Delta_2(\alpha, \varepsilon)), v_p(\Delta_2(\beta, \varepsilon))),\\
\delta_2^\varepsilon &= \min(v_p(\Delta_2(\alpha, \varepsilon)) + n_2, v_p(\Delta_2(\beta, \varepsilon)) + n_1) - \underline{n},\\
d_3^\varepsilon &= v_p(\Delta_3(\alpha, \beta, \varepsilon)),\\
\delta_3^\varepsilon &= n_1 + n_2 - 2\underline{n} + d_3^\varepsilon.
\end{aligned}$$

The main results are the following.

Theorem 14. *Let $a, b \in \mathbb{Q}^+$ be multiplicatively independents, with a and b as above. If $p_1 \neq 2$, then:*

$$\delta_{a,b} = \prod_{p \text{ primes}} \Lambda_p \left\{ 1 + \frac{1}{\Lambda_2} \left[\sum_{\substack{\varepsilon \in \mathbb{F}_2^t \\ \varepsilon \neq \underline{0}}} \prod_{i=1}^{t} \left(1 - \frac{\varepsilon_i}{\Lambda_{p_i}} \right) \mathcal{T}(\varepsilon) \right] \right\} \tag{2.1}$$

otherwise

$$\delta_{a,b} = \prod_{p \text{ primes}} \Lambda_p \left\{ 1 + \frac{1}{\Lambda_2} \left[\mathcal{W}(e_1) + \sum_{\substack{\varepsilon \in \mathbb{F}_2^t \\ \varepsilon \neq \underline{0}, e_1}} \prod_{i=2}^{t} \left(1 - \frac{\varepsilon_i}{\Lambda_p} \right) (\mathcal{T}(\varepsilon) + \mathcal{W}(\varepsilon)) \right] \right\} \tag{2.2}$$

where

$$\Lambda_p = \begin{cases} 1 - \frac{2p^{3d_1 - 2d_2 + 1}}{p^3 - 1} & \text{if } d_1 = \overline{d}_1 \\ 1 - \frac{p^{1-d_1}}{p^2-1} + p^{3d_1 - 2d_2 + 1} \left(\frac{(p^2-p-1)(p-1)}{(p^3-1)(p^2-1)} \right) & \text{otherwise} \end{cases} \tag{2.3}$$

$$\mathcal{T}(\varepsilon) = \begin{cases} \sum_{n_1, n_2 \in \{0,1\}} \left(\frac{-1}{4} \right)^{n_1 + n_2} \sum_n^* \frac{f(n, n_1, n_2)}{\varphi(2^{3n + \overline{n}})}, & \text{if } v_2(P_0(\varepsilon)) = 0, \\ 0, & \text{otherwise} \end{cases}$$

$$\mathcal{W}(\varepsilon) = \begin{cases} \sum_{n_1, n_2 \in \{0,1\}} \left(\frac{-1}{4} \right)^{n_1 + n_2} \sum_n^* \frac{f(n, n_1, n_2)}{\varphi(2^{3n + \overline{n}})}, & \text{if } v_2(P_0(\varepsilon)) > 0, \\ 0, & \text{otherwise} \end{cases}$$

where

$$f(n, n_1, n_2) = 2^{\min(n + n_1 + n_2 + \delta_1 + \underline{n}, \delta_2 + 2\underline{n})},$$

$P_0(\varepsilon) = \prod_{i=1}^{t} p_i^{\varepsilon_i}$, $\sigma(\varepsilon) = v_2(\mathrm{disc}(P_0(\varepsilon)))$,

$$\kappa(n_1, n_2, \varepsilon) = \begin{cases} \delta_2 - \delta_2^{\varepsilon} + 1, & \text{if } \delta_2^{\varepsilon} = \delta_1 \\ \delta_1 + 1, & \text{otherwise} \end{cases}$$

and $\sum_n^*$ is the sum over all $n \in \mathbb{N}$ such that the following conditions hold with respect to ε:

C1: $n \geq K = \max(\sigma(\epsilon), k(n_1, n_2, \underline{\varepsilon})) - \overline{n}$;

C2: $\delta_3^{\epsilon} \geq \min\{\delta_2 + 1, n + \overline{n} + \delta_2^{\epsilon}\}$.

In this case it is possible to improve the formulas for $\mathcal{T}$ and $\mathcal{W}$.

Corollary 15. *With the same notations of above Theorem, we have:*

a) if $d_3^\epsilon \neq d_2$*:*

$$\mathcal{T}(\varepsilon) = \left\{ \sum_{n_1,n_2=0}^{1} (-1)^{n_1+n_2} \left[\frac{2^{\delta_2+4-3s_1}}{7} + \frac{2}{3}\left(2^{2-2s_2+\delta_1} - 2^{3\delta_1-2\delta_2}\right)\chi_0 \right] \right\} \chi_1$$

$$\mathcal{W}(\varepsilon) = \left\{ \sum_{n_1,n_2=0}^{1} (-1)^{n_1+n_2} \left[\frac{2^{\delta_2+4-3s_1}}{7} + \frac{2}{3}\left(2^{2-2s_2+\delta_1} - 2^{3\delta_1-2\delta_2}\right)\chi_0 \right] \right\} \chi_2$$

where χ *is the usual characteristic function,*

$$\chi_0 = \chi(\delta_2^\varepsilon > \delta_1), \quad \chi_1 = \chi(v_2(P_0(\varepsilon)) = 0), \quad \chi_2 = \chi(v_2(P_0(\varepsilon)) > 0)$$

and $s_1 = \max(\delta_2 - \delta_1 + 1, \sigma(\varepsilon))$*,* $s_2 = \max(\delta_1 + 1, \sigma(\varepsilon))$*.*

b) If $d_3^\epsilon = d_2$*:*

$$\mathcal{T}(\varepsilon) = \left\{ \sum_{n_1,n_2=0}^{1} \frac{2}{3}(-1)^{n_1+n_2}\left(2^{2-2s_2+\delta_1} - 2^{2(\delta_2^\varepsilon-\delta_2)+\delta_1}\right)\chi_0 \right\} \chi_1,$$

$$\mathcal{W}(\varepsilon) = \left\{ \sum_{n_1,n_2=0}^{1} \frac{2}{3}(-1)^{n_1+n_2}\left(2^{2-2s_2+\delta_1} - 2^{2(\delta_2^\varepsilon-\delta_2)+\delta_1}\right)\chi_0 \right\} \chi_2.$$

Theorem 16. *Let* $a, b \in \mathbb{Q}^*$ *multiplicatively independents, with at least one between* a *and* b *less than* 0*. If* $p \neq 2$ *and* $a < 0$*, with the same notations above, we have:*

$$\delta_{a,b} = \prod_{p \text{ primes}} \Lambda_p \left\{ 1 + \frac{1}{\Lambda_2} \left[\sum_{\substack{\varepsilon \in \mathbb{F}_2^t \\ \varepsilon \neq \underline{0}}} \prod_{i=1}^{t} \left(1 - \frac{\varepsilon_i}{\Lambda_{p_i}}\right) (\mathcal{T}^*(\varepsilon) + \sum_{z=0,1} \mathcal{Z}^*((z,\varepsilon))) \right] \right\} \tag{2.4}$$

otherwise

$$\delta_{a,b} = \prod_{p \text{ primes}} \Lambda_p \left\{ 1 + \frac{1}{\Lambda_2} \left[\mathcal{W}^*(e_1) + \sum_{\substack{\varepsilon \in \mathbb{F}_2^t \\ \varepsilon \neq \underline{0}, e_1}} \prod_{i=2}^{t} \left(1 - \frac{\varepsilon_i}{\Lambda_p}\right) \left(\mathcal{T}^*(\varepsilon) + \mathcal{W}^*(\varepsilon) + \sum_{z=0,1} \mathcal{Z}^*((z,\varepsilon)) \right) \right] \right\} \tag{2.5}$$

where

$$\mathcal{T}^*(\varepsilon) = \begin{cases} 0, & \text{if } v_2(P_0(\varepsilon)) = 0, \\ \sum_{n_1,n_2 \in \{0,1\}} \left(\frac{-1}{4}\right)^{n_1+n_2} \sum_n^{**} \frac{f(n,n_1,n_2)}{\varphi(2^{3n+\overline{n}})}, & \text{otherwise} \end{cases}$$

$$\mathcal{W}^*(\varepsilon) = \begin{cases} \sum_{n_1,n_2 \in \{0,1\}} \left(\frac{-1}{4}\right)^{n_1+n_2} \sum_n^{**} \frac{f(n,n_1,n_2)}{\varphi(2^{3n+\overline{n}})}, & \text{if } v_2(P_0(\varepsilon)) > 0, \\ 0, & \text{otherwise} \end{cases}$$

where

$$f(n,n_1,n_2) = 2^{\min(n+n_1+n_2+\delta_1+\underline{n}, \delta_2+2\underline{n})},$$

$\sum_n^{**}$ *is the sum over all* $n \in \mathbb{N}$ *such that the following conditions hold with respect to* ε*:*

C1***:** $n \geq \max(\max(\sigma(\epsilon), k(n_1,n_2,\underline{\varepsilon})) - \overline{n}, 2)$

C2***:** $\delta_3^\epsilon \geq \min\{\delta_2 + 1, n + \overline{n} + \delta_2^\epsilon\}$

and $(z,\varepsilon) \in F_2^{t+1}$

$$\mathcal{Z}^*((z,\varepsilon)) = \sum_{n_1,n_2 \in \{0,1\}} \left(\frac{-1}{4}\right)^{n_1+n_2} \sum_n^{***} \frac{f(n,n_1,n_2)}{\varphi(2^{3n+\overline{n}})}$$

where $\sum_n^{***}$ *is the sum over all* $n \in \mathbb{N}$ *such that the following conditions hold with respect to* (z,ε)*:*

C3***:** $n = 1 - \overline{n}$*,* $\delta_1 = 0$*,* $\delta_2 = \delta_2^{(z,\varepsilon)}$ *and* $\delta_3^{(z,\varepsilon)} \geq 1 + \delta_2$*.*

We are aware that the above expressions for $\mathcal{T}(\varepsilon)$, $\mathcal{W}(\varepsilon)$ and $\mathcal{Z}(\varepsilon)$ need to be simplified. This will be the topic of future work.

By Theorem 1, we have that:

$$\delta_{a,b} = \sum_{m,k_1,k_2 \in \mathbb{N}} \frac{\mu(k_1)\mu(k_2)}{\varphi(mk)} \frac{\#\mathcal{B}(mk)}{\#\mathcal{A}(mk)}$$

where

$$\mathcal{A}(mk) = \Gamma \cdot \mathbb{Q}^{*mk}/\mathbb{Q}^{*mk},$$

and if $N = 2^{v_2(mk)}$, then

$$\mathcal{B}(mk) = \left\{ \xi\mathbb{Q}^{*N} \in \Gamma\mathbb{Q}^{*N}/\mathbb{Q}^{*N} : \ [\mathbb{Q}(\sqrt[N]{\xi}) : \mathbb{Q}] \leq 2 \text{ and } \operatorname{disc}(\mathbb{Q}(\sqrt[N]{\xi})) \mid mk \right\}.$$

To show the Theorems we need to compute explicitly $\#\mathcal{A}$ and $\#\mathcal{B}$.

2.1 Preliminary results

Let $\Gamma \subseteq \mathbb{Q}^*$ be a finitely generated multiplicative subgroup of $\operatorname{rank} = s$, with $\mathbb{Z}$–basis $\{b_1, \ldots, b_s\}$, $\operatorname{supp}(\Gamma) = S_\Gamma$ and $M \in \mathbb{N}$. We fix an ordering for the basis and the support (i.e. $S_\Gamma = \{p_1 < p_2 < \ldots p_t\}$).

If $\Gamma \subseteq \mathbb{Q}^+$, we define the *relation matrix* of Γ with respect to basis $\{b_1, \ldots, b_s\}$ and support $\mathcal{S}_\Gamma$ as follows:

$$A(\Gamma, \{b_1, \ldots, b_s\}, \mathcal{S}_\Gamma) = \begin{pmatrix} \alpha_{1,1} & \ldots & \alpha_{1,s} \\ \ldots & \ldots & \ldots \\ \alpha_{t,1} & \ldots & \alpha_{t,s} \end{pmatrix}$$

where $b_i = \prod_{j=1}^{t} p_j^{\alpha_{j,i}}$. If $\{c_1, \ldots, c_s\}$ is another ordered $\mathbb{Z}$-basis of Γ then there exists a matrix $U \in \mathrm{SL_s}(\mathbb{Z})$ such that

$$A(\Gamma, \{b_1, \ldots, b_s\}, \mathcal{S}_\Gamma) = A(\Gamma, \{c_1, \ldots, c_s\}, \mathcal{S}_\Gamma) \cdot U.$$

Because we have fixed the basis and the support, we replace $A(\Gamma, \{b_1, \ldots, b_s\}, \mathcal{S}_\Gamma)$ with $A(\Gamma)$.

The invariant $\Delta_i(\Gamma)$ is defined as Δ_i of the relation matrix of Γ. We note that $\Delta_i(\Gamma)$ is well defined and does not depend on the ordering of the basis or of the support.

More in general, if $\Gamma \in \mathbb{Q}^*$, we can define the subgroup of the absolute values of Γ as follows:

$$||\Gamma|| = \{|a| : \ a \in \Gamma\}.$$

We define as the relation matrix of absolute values of Γ with respect to basis $\{b_1, \ldots, b_s\}$ and support $\mathcal{S}_\Gamma$:

$$A(||\Gamma||) = \begin{pmatrix} \alpha_{1,1} & \ldots & \alpha_{1,s} \\ \ldots & \ldots & \ldots \\ \alpha_{t,1} & \ldots & \alpha_{t,s} \end{pmatrix}$$

while the relation matrix of Γ with respect to basis $\{b_1, \ldots, b_s\}$ and support S_Γ is the matrix

$$\widetilde{A}(\Gamma) = \begin{pmatrix} \alpha_{0,1} & \ldots & \alpha_{0,s} \\ \alpha_{1,1} & \ldots & \alpha_{1,s} \\ \ldots & \ldots & \ldots \\ \alpha_{t,1} & \ldots & \alpha_{t,s} \end{pmatrix}$$

where $b_i = (-1)^{\alpha_{0,i}} \prod_{j=1}^{t} p_j^{\alpha_{j,i}}$ with $\alpha_{0,i} \in \{0, 1\}$. We note that the relation matrix associated at $||\Gamma||$ equals $\widetilde{A}(\Gamma)$ with the first row removed.

The following lemma give us a formula to compute explicitly $\#\mathcal{A}(M)$ in terms of invariants of the subgroup.

Lemma 17. *With the notations above, we have:*

$$\#\mathcal{A}(M) = \frac{M^s}{(M^s, \Delta_1(\Gamma)M^{s-1}, \ldots, \Delta_s(\Gamma))}. \quad \square$$

The proof of this lemma can be found in [3], Sec 3.1.

Lemma 18. *With the same notations of Theorems 14 and 16, let*

$$\delta' = \sum_{m,k_1,k_2 \in \mathbb{N}} \mu(k_1)\mu(k_2) \frac{1}{\#A(mk)\varphi(mk)}.$$

Then δ' is multiplicative and

$$\delta' = \prod_{p \text{ primes}} \Lambda_p$$

where

$$\Lambda_p = \begin{cases} 1 - \frac{2p^{3d_1-2d_2+1}}{p^3-1} & \text{if } d_1 = \overline{d}_1 \\ 1 - \frac{p^{1-d_1}}{p^2-1} + p^{3d_1-2d_2+1}\left(\frac{(p^2-p-1)(p-1)}{(p^3-1)(p^2-1)}\right) & \text{otherwise.} \end{cases} \tag{2.6}$$

Proof. Since

$$\#\mathcal{A}(M) = \prod_{p|M} |\Gamma\mathbb{Q}^{*p^{v_p(M)}}/\mathbb{Q}^{*p^{v_p(M)}}|$$

(see , e.g., [[8], Chapter VIII, Section 8]) then the following expression is multiplicative:

$$\begin{aligned}
\delta' &= \sum_{m,k_1,k_2\in\mathbb{N}} \mu(k_1)\mu(k_2)\frac{(M^2, M\Delta_1(\alpha\widetilde{k}_1, \beta\widetilde{k}_2), \Delta_2(\alpha\widetilde{k}_1, \beta\widetilde{k}_2))}{M^2\varphi(M)} = \\
&= \sum_{m,k_1,k_2\in\mathbb{N}} \mu(k_1)\mu(k_2)\frac{(m^2k_1k_2, m\Delta_1(\alpha)k_2, m\Delta_1(\beta)k_1, \Delta_2(\alpha,\beta))}{m^2k_1k_2\varphi(m[k_1,k_2])} = \\
&= \prod_{p \text{ primes}} \left(\sum_{n=0}^{\infty} \sum_{\substack{n_1=0,1 \\ n_2=0,1}} \left(\frac{-1}{p}\right)^{n_1+n_2} \frac{(p^{2n+n_1+n_2}, p^{n+n_2}h_1, p^{n+n_1}h_2, h_1h_2D)}{\varphi(p^{n+\max\{n_1,n_2\}})p^{2n}} \right) = \\
&= \prod_{p \text{ primes}} \left(1 - \frac{p}{p^2-1}\left[\frac{p^{\min\{\overline{d}_1-d_1,1\}}-1}{p^{d_1}(p-1)} + \frac{p^{3d_1}}{p^{2d_2}}\left(\frac{3p^2+p-1}{(p^3-1)} - \frac{p^{\min\{1,\overline{d}_1-d_1\}}}{(p-1)} \right) \right] \right) = \\
&= \prod_{p \text{ primes}} \Lambda_p
\end{aligned}$$

where

$$\Lambda_p = \begin{cases} 1 - \frac{2p^{3d_1-2d_2+1}}{p^3-1} & \text{if } d_1 = \overline{d}_1 \\ 1 - \frac{p^{1-d_1}}{p^2-1} + p^{3d_1-2d_2+1}\left(\frac{(p^2-p-1)(p-1)}{(p^3-1)(p^2-1)}\right) & \text{otherwise.} \end{cases}$$

We note that $\Lambda_p \neq 0$ for all p, and so $\delta' \neq 0$. □

2.2 Computation of $\mathcal{B}(M)$

It is hard to compute explicitly $\#\mathcal{B}(M)$. We bypass this problem introducing a new set with the same cardinality of $\mathcal{B}(M)$. Now we need distinguish two cases: $\Gamma \subseteq \mathbb{Q}^+$ and $\Gamma \subseteq \mathbb{Q}^*$.

Case 1: $\Gamma \subseteq \mathbb{Q}^+$

Let $\xi\mathbb{Q}^{*N} \in \Gamma\mathbb{Q}^{*N}/\mathbb{Q}^{*N}$ with $\Gamma \subseteq \mathbb{Q}^+$ and $A(\Gamma)$ as above. We define $\mathbf{v}(\xi) = (v_{p_1}(\xi), \ldots, v_{p_t}(\xi)) \pmod N$ (i.e. the vector of p–adic valuations of $\xi \pmod N$) and $\mathbf{z}(\xi) = (z_1, \ldots, z_s)$ where z_i is the power of b_i that occurs in ξ (i.e $\xi = b_1^{z_1} \cdots b_s^{z_s}$).

We can associate ξ to the following linear system of congruences

$$A(\Gamma) \cdot \mathbf{X}^T \equiv \mathbf{v}(\xi)^T \pmod N \tag{2.7}$$

where $\mathbf{X} = (x_1, \ldots, x_s)$ is a vector of unknowns. This system is solvable and a solution is given by $\mathbf{z}(\xi)$ (we note that this depends strongly upon how basis and support are chosen and ordered).

We say that $\mathbf{v}(\xi) \in \mathrm{SLC}(A, N)$ if the linear system of congruences (2.7) can be solved.

If $\xi\mathbb{Q}^{*N} \in \mathcal{B}(M)$, then $[\mathbb{Q}(\sqrt[N]{\xi}) : \mathbb{Q}] \leq 2$. This condition is equivalent to have only two possible values for the components of the vector $\mathbf{v}(\xi)$: $N/2$ or $0 \pmod N$.

Let $\varepsilon \in \mathbb{F}_2^t$, $P(\varepsilon) = \prod_{i=1}^t p_i^{(N\varepsilon_i)/2}$, and $P_0(\varepsilon) = \prod_{i=1}^t p_i^{\varepsilon_i}$. We can construct a bijective application between $\mathcal{B}(M)$ and the set:

$$\mathcal{H}_M = \left\{ \varepsilon \in \mathbb{F}_2^t : \ (N/2)\varepsilon \in \mathrm{SLC}(A, N) \text{ and } \mathrm{disc}(\sqrt{P_0(\varepsilon)}) | M \right\}$$

in the following way: for any $\varepsilon \in \mathcal{H}_M$, we associate $P(\varepsilon)\mathbb{Q}^{*N}$ that lives in $\mathcal{B}(M)$ because $\sqrt[N]{P(\varepsilon)} = \sqrt{P_0(\varepsilon)}$ and $[\mathbb{Q}(\sqrt{P_0(\varepsilon)}) : \mathbb{Q}] \leq 2$. This application is clearly bijective. We have proved the following.

Lemma 19. *Let $\mathcal{B}(M)$ and $\mathcal{H}_M$ as above. Then exists an bijective application between $\mathcal{H}_M$ and $\mathcal{B}(M)$.*

Case 2: $\Gamma \subseteq \mathbb{Q}^*$

Let $\xi\mathbb{Q}^{*N} \in \Gamma\mathbb{Q}^{*N}/\mathbb{Q}^{*N}$ with $\Gamma \subseteq \mathbb{Q}^*$ and $\widetilde{A}(\Gamma)$ as above. We define $\widetilde{\mathbf{v}}(\xi) = (\nu(\xi), \mathbf{v}(||\xi||))$ where

$$\nu(\xi) = \begin{cases} 1, & \text{if } \xi < 0 \\ 0, & \text{otherwise} \end{cases}$$

and $\widetilde{\mathbf{z}}(\xi) = \mathbf{z}(||\xi||)$.

As above, we associate ξ to the linear system of congruences:

$$\widetilde{A}(\Gamma) \cdot \mathbf{X}^T \equiv \widetilde{\mathbf{v}}(\xi)^T \pmod{N} \tag{2.8}$$

and its solution $\widetilde{\mathbf{z}}(\xi)$. In this case the condition $[\mathbb{Q}(\sqrt[N]{\xi}) : \mathbb{Q}] \leq 2$ is equivalent both the following:

1. there are only two possibilities values for the components of the vector $\mathbf{v}(\xi)$: $N/2$ or $0 \pmod{N}$;
2. if $N > 2$, then $\nu(\xi) = 0$.

Let $\widetilde{\varepsilon} = (\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_t) \in \mathbb{F}_2^{t+1}$, $P(\widetilde{\varepsilon}) = (-1)^{\varepsilon_0} \prod_{i=1}^{t} p_i^{(N\varepsilon_i)/2}$ and $P_0(\widetilde{\varepsilon}) = (-1)^{\varepsilon_0} \prod_{i=1}^{t} p_i^{\varepsilon_i}$.

In order to construct our application, we must consider two cases:

a) $N = 2$, we use the set:

$$\mathcal{L}_{M,2} = \left\{ \widetilde{\varepsilon} \in \mathbb{F}_2^{t+1} : \ \widetilde{\varepsilon} \in SLC(A, 2) \text{ and } \operatorname{disc}(\sqrt{P_0(\widetilde{\varepsilon})}) | M \right\};$$

b) $N > 2$, we use:

$$\mathcal{K}_{M,N} = \left\{ \varepsilon \in \mathbb{F}_2^t : \ (N/2) \cdot (0, \varepsilon) \in SLC(A, N) \text{ and } \operatorname{disc}(\sqrt{P_0(\varepsilon)}) | M \right\}.$$

We note that this set is well defined also for $N = 2$.

As above, the application between $\mathcal{B}(M)$ and $\mathcal{K}_{M,N}$ or $\mathcal{L}_{M,2}$ is bijective and we have the following.

Lemma 20. *Let $\mathcal{B}(M)$, $\mathcal{L}_{M,2}$ and $\mathcal{K}_{M,N}$ as above.*

(a) If $v_2(M) = 1$, then there exists an one-to-one application between $\mathcal{L}_{M,2}$ and $\mathcal{B}(M)$.

(b) If $v_2(M) \geq 2$, then there exists an one-to-one application between $\mathcal{K}_{M,N}$ and $\mathcal{B}(M)$.

2.2.1 Computation of $\#\mathcal{H}_M$, $\#\mathcal{L}_{M,2}$ and $\#\mathcal{K}_{M,N}$.

First we need a method to know when a linear system of congruences as (2.7) has solution. The following result, due to Butson and Steward, gives us the answer.

Theorem 21 (Butson–Stewart, 1955,[2])**.** *Let $A \in M_{n\times m}(\mathbb{Z})$, $\mathbf{b} \in \mathbb{Z}^m$ and $\Delta_i = \Delta_i(A)$. The linear system of congruences*

$$A \cdot \mathbf{X}^T \equiv \mathbf{b}^T \qquad (\mathrm{mod}\ N)$$

has solution if and only if one of the following holds:

1. *if $n \leq m$, $(\Delta_i/\Delta_{i-1}, N) = (\overline{\Delta}_i/\overline{\Delta}_{i-1}, N)$ for all $i = 1, \ldots, n$*
2. *if $n > m$, $(\Delta_i/\Delta_{i-1}, N) = (\overline{\Delta}_i/\overline{\Delta}_{i-1}, N)$ for all $i = 1, \ldots, m$ and $(\overline{\Delta}_{m+1}/\overline{\Delta}_m, N) = N$*

where $\overline{\Delta}_i$ is the invariant factor of the augment matrix $(A|\mathbf{b}^T)$. □

The keys are the following lemmas.

Lemma 22. *Let $\Gamma = \langle a^{\widetilde{k}_1}, b^{\widetilde{k}_2}\rangle \subseteq \mathbb{Q}^+$ with k_1, k_2 squarefree. We set $n_1 = v_2(\widetilde{k}_2)$ and $n_2 = v_2(\widetilde{k}_1)$, $\sigma(\varepsilon) = v_2(\mathrm{disc}(P_0(\varepsilon)))$,*

$$\kappa(n_1, n_2, \varepsilon) = \begin{cases} \delta_2 - \delta_2^{\varepsilon} + 1, & \text{if } \delta_2^{\varepsilon} = \delta_1 \\ \\ \delta_1 + 1, & \text{otherwise} \end{cases}$$

and $K = \max(\sigma(\epsilon), k(n_1, n_2, \varepsilon))$. Then $\varepsilon \in \mathcal{H}_{mk}$ if and only if $\mathrm{disc}(P_0(\varepsilon))|mk$ and both the following conditions hold:

C1: $v_2(mk) \geq K = \max(\sigma(\epsilon), k(v_2(\widetilde{k}_1), v_2(\widetilde{k}_2), \varepsilon))$;

C2: $\delta_3^\epsilon \geq \min\{\delta_2 + 1, v_2(mk) + \delta_2^\epsilon\}$.

Proof. The condition that $\mathrm{disc}(P_0(\varepsilon))|mk$ is clear. The others conditions follow from Theorem 21. We set $n = v_2(m)$, so $v_2(mk) = n + \overline{n}$, (we remember that $\overline{n} = \max(n_1, n_2)$).

First of all, we note that it is very easy to show that the condition **C2** is equivalent to $(\overline{\Delta_3}/\overline{\Delta_2}, N) = N$.

Regarding condition **C1**, we have the following:

- $(\Delta_1, N) = (\overline{\Delta}_1, N/2)$ is equivalent to $v_2(mk) - 1 = n + \overline{n} - 1 \geq \delta_1$.
- $(\Delta_2/\Delta_1, N) = (\overline{\Delta}_2/\overline{\Delta}_1, N/2)$ and $\delta_2^\varepsilon = \delta_1$ are equivalent to $n + \overline{n} \geq \delta_2 - \delta_1 + 1$.
- $(\Delta_2/\Delta_1, N) = (\overline{\Delta}_2/\overline{\Delta}_1, N/2)$ and $\delta_2^\varepsilon > \delta_1$ are equivalent to $n + \overline{n} \geq \delta_1 + 1$.

□

Lemma 23. *Let $\Gamma = \langle a^{\widetilde{k}_1}, b^{\widetilde{k}_2} \rangle \subseteq \mathbb{Q}^*$ with k_1, k_2 squarefree. With the same notation as above, we have:*

1. *$\varepsilon \in \mathcal{K}_{mk,N}$ if and only if $\mathrm{disc}(P_0(\varepsilon))|mk$ and both the following conditions hold:*

   C1*: $v_2(mk) \geq \max(\max(\sigma(\epsilon), k(n_1, n_2, \underline{\varepsilon})), 2)$;

   C2*: $\delta_3^\epsilon \geq \min\{\delta_2 + 1, v_2(mk) + \delta_2^\epsilon\}$.

2. *$\widetilde{\varepsilon} \in \mathcal{L}_{mk,2}$ if and only if $\mathrm{disc}(P_0(\widetilde{\varepsilon}))|mk$ and the following condition holds:*

   C3*: $v_2(mk) = 1$, $\delta_1 = 0$, $\delta_2 = \delta_2^\varepsilon$ *and* $\delta_3^\varepsilon \geq 1 + \delta_2$.

Proof. The condition that $\mathrm{disc}(P_0(\widetilde{\varepsilon}))|mk$ is clear. We omit the proof of (1), because it is the same argument of Lemma 22. Let $n = v_2(m)$. Let $\widetilde{\varepsilon} \in \mathcal{L}_{mk,2}$. The condition $v_2(mk) = 1$ is clear.

- $(\Delta_1, N) = (\overline{\Delta}_1, N/2)$ is equivalent to $v_2(mk) - 1 = n + \overline{n} - 1 \geq \delta_1$, but $n + \overline{n} = 1$ so $\delta_1 = 0$.

- $(\Delta_2/\Delta_1, N) = (\overline{\Delta}_2/\overline{\Delta}_1, N/2)$ and $\delta_2^\varepsilon = \delta_1 = 0$ are equivalent to $n + \overline{n} = 1 \geq \delta_2 + 1$, so we have $\delta_2 = \delta_2^\varepsilon = 0$.
- $(\Delta_2/\Delta_1, N) = (\overline{\Delta}_2/\overline{\Delta}_1, N/2)$ and $\delta_2^\varepsilon > 0$ are equivalent to $\delta_2 = \delta_2^\varepsilon$.
- $(\overline{\Delta}_3/\overline{\Delta}_2, N) = N$ is equivalent to $\delta_3^\varepsilon \geq 1 + \delta_2$.

□

2.3 Proof of Theorem 14 and Corollary 15

Let a, b as in Theorem 14. We replace $\delta_{a,b}$ with δ. We set

$$F(m, k_1, k_2) = \mu(k_1)\mu(k_2)\frac{\big(m^2 k_1 k_2, m\Delta_1(\underline{\alpha})k_2, m\Delta_1(\underline{\beta})k_1, \Delta_2(\underline{\alpha}, \underline{\beta})\big)}{m^2 k_1 k_2 \cdot \varphi(m[k_1, k_2])},$$

so we have, by Lemma 19

$$\delta \;=\; \sum_{m,k_1,k_2\geq 1} \frac{\mu(k_1)\mu(k_2)}{\varphi(mk)} \frac{\#\mathcal{B}(mk)}{\#\mathcal{A}(mk)} \;=\; \sum_{m,k_1,k_2\geq 1} F(m, k_1, k_2)\#\mathcal{H}_{mk}$$

where we remember that

$$\#\mathcal{H}_{mk} \;=\; \left\{\varepsilon \in \mathbb{F}_2^t :\; \frac{N}{2}\varepsilon \in \mathrm{SLC(A, N)} \text{ and } \mathrm{disc}(\sqrt{\mathrm{P}_0(\varepsilon)})|\mathrm{mk}\right\}.$$

We need to distinguish two cases: $\Gamma \subseteq \mathbb{Q}^+$ with $2 \notin S_\Gamma$ and $\Gamma \subseteq \mathbb{Q}^+$ with $2 \in S_\Gamma$.

Case 1: $\Gamma \subseteq \mathbb{Q}^+$ and $2 \notin S_\Gamma$

In this case, we have $\#\mathcal{B}(mk) = \#\mathcal{H}_{mk}$, so we can rewrite

$$\delta = \sum_{m,k_1,k_2\in\mathbb{N}} F(m,k_1,k_2)\#\mathcal{H}_{mk} = \sum_{\varepsilon\in\mathbb{F}_2^t} \sum_{\substack{m,k_1,k_2\in\mathbb{N}\\ \varepsilon\in\mathcal{H}_{mk}}} F(m,k_1,k_2) =$$
$$= \sum_{m,k_1,k_2\in\mathbb{N}} F(m,k_1,k_2) + \sum_{\varepsilon\in\mathbb{F}_2^t\setminus\{0\}} \sum_{\substack{m,k_1,k_2\in\mathbb{N}\\ \varepsilon\in\mathcal{H}_{mk}}} F(m,k_1,k_2).$$

By Lemma 18, we have that:

$$\sum_{m,k_1,k_2\in\mathbb{N}} F(m,k_1,k_2) = \prod_{p \text{ primes}} \Lambda_p$$

and to simplify the notation, we set:

$$\delta' = \prod_{p \text{ primes}} \Lambda_p \,.$$

So

$$\delta = \delta' + \sum_{\varepsilon\in\mathbb{F}_2^t\setminus\{0\}} \sum_{\substack{m,k_1,k_2\in\mathbb{N}\\ \varepsilon\in\mathcal{H}_{mk}}} F(m,k_1,k_2).$$

By Lemma 22, we have that $\varepsilon \in \mathcal{H}_{mk}$ if and only if conditions **C1** and **C2** hold. We fix $\varepsilon \neq \underline{0}$. If $p \notin \mathcal{S}_\Gamma \bigcup \{2\}$ we can obtain from $\sum F(m,k_1,k_2)$ a factor Λ_p. Instead if $p_i \in \mathcal{S}_\Gamma$ we obtain a factor $(\Lambda_{p_i} - \varepsilon_i)$ while the remaining sum over the powers of 2 give us the coefficient

$$\mathcal{T}(\varepsilon) = \sum_{n_1,n_2\in\{0,1\}} \left(\frac{-1}{4}\right)^{n_1+n_2} \sum_n^* \frac{f(n,n_1,n_2)}{\varphi(2^{3n+\overline{n}})}$$

where $f(n,n_1,n_2) = 2^{\min\{n+n_1+n_2+\delta_1+\underline{n},\delta_2+2\underline{n}\}}$ and $\sum^*$ is over all n such that conditions **C1** and **C2** holds with respect to ε.

We can extend the definition of $\mathcal{T}(\varepsilon)$ in the following way:

$$\mathcal{T}(\varepsilon) = \begin{cases} \sum_{n_1,n_2\in\{0,1\}} \left(\frac{-1}{4}\right)^{n_1+n_2} \sum_n^* \frac{f(n,n_1,n_2)}{\varphi(2^{3n+\overline{n}})}, & \text{if } v_2(P_=(\varepsilon)) = 0 \\ 0, & \text{otherwise.} \end{cases}$$

So:

$$\delta = \delta' \left(1 + \frac{1}{\Lambda_2} \sum_{\varepsilon \neq \underline{0}} \prod_{p_i \in S_\Gamma} \left(1 - \frac{\varepsilon_i}{\Lambda_{p_i}} \right) \mathcal{T}(\varepsilon) \right) \tag{2.9}$$

and (2.1) of Theorem is proved.

Before starting the proof for (2.2) we show the formulas of $\mathcal{T}$ in the Corollary 15. We need to distinguish two cases:

i) If $\delta_3^\epsilon \geq \delta_2 + 1$, then the condition **C2** is verified;

ii) if $\delta_3^\epsilon = \delta_2$, then **C2** is equivalent to $n \leq \delta_3^\epsilon - \delta_2^\epsilon - \overline{n}$.

We note that $\delta_3^\epsilon = \delta_2$ if and only if $d_3^\varepsilon = d_2$. We define

$$\begin{aligned} s_1 &= \max(\delta_2 - \delta_1 + 1, \sigma(\varepsilon)), \\ s_2 &= \max(\delta_1 + 1, \sigma(\varepsilon)). \end{aligned}$$

Case i) $d_3^\epsilon \neq d_2$:

We have, if $v_2(P_0(\varepsilon)) = 0$:

$$\begin{aligned} \mathcal{T}(\varepsilon) &= \sum_{n_1,n_2 \in \{0,1\}} \left(\frac{-1}{4} \right)^{n_1+n_2} \sum_n^* \frac{2^{\min\{n+n_1+n_2+\delta_1+\underline{n}, \delta_2+2\underline{n}\}}}{\varphi(2^{3n+\overline{n}})} \\ &= \sum_{n_1,n_2=0}^{1} \left(\frac{-1}{4} \right)^{n_1+n_2} \left[\sum_{n+\overline{n}=s_1}^{\infty} \frac{2^{\delta_2+1+2(\underline{n}+\overline{n})}}{2^{3(n+\overline{n})}} + \sum_{\substack{n+\overline{n}=s_2 \\ \delta_2^\varepsilon > \delta_1}}^{\delta_2-\delta_1} \frac{2^{2(n_1+n_2)+\delta_1+1}}{2^{2(n+\overline{n})}} \right] \\ &= \sum_{n_1,n_2=0}^{1} (-1)^{n_1+n_2} \left[\frac{2^{\delta_2+4-3s_1}}{7} + \frac{2}{3} \left(2^{2-2s_2+\delta_1} - 2^{3\delta_1-2\delta_2} \right) \chi \right]. \end{aligned}$$

where $\chi_0 = \chi(\delta_2^\varepsilon > \delta_1)$ and the first formula of Corollary 15 is proved.

Case ii) $d_3^\epsilon = d_2$: In this case we have:

$$n + \overline{n} \leq \delta_3^\varepsilon - \delta_2^\varepsilon < \delta_2 - \delta_1 + 1$$

and so

$$\begin{cases} \delta_2^{\varepsilon} > \delta_1 \\ n + \overline{n} \geq \delta_1 + 1. \end{cases}$$

Then

$$\begin{aligned} \mathcal{T}(\varepsilon) &= \sum_{n_1,n_2\in\{0,1\}} \left(\frac{-1}{4}\right)^{n_1+n_2} \sum_{n}^{*} \frac{2^{\min\{n+n_1+n_2+\delta_1+\underline{n},\delta_2+2\underline{n}\}}}{\varphi(2^{3n+\overline{n}})} \\ &= \sum_{n_1,n_2=0}^{1} \left(\frac{-1}{4}\right)^{n_1+n_2} \sum_{\substack{n+\overline{n}=s_2 \\ \delta_2^{\varepsilon}>\delta_1}}^{\delta_2-\delta_2^{\varepsilon}} \frac{2^{2(n_1+n_2)+\delta_1+1}}{2^{2(n+\overline{n})}} \\ &= \sum_{n_1,n_2=0}^{1} \frac{2}{3}\left(-1\right)^{n_1+n_2} \left(2^{2-2s_2+\delta_1} - 2^{2(\delta_2^{\varepsilon}-\delta_2)+\delta_1}\right)\chi_0 \end{aligned}$$

and the second formula of Corollary 15 is proved.

Case 2: $\Gamma \subseteq \mathbb{Q}^+$ and $2 \in S_\Gamma$.

Because S_Γ is ordered, $p_1 = 2$. It is clear that, as in **Case 1**, we can write

$$\begin{aligned} \delta &= \delta' + \sum_{\varepsilon\in\mathbb{F}_2^t\setminus\{0\}} \sum_{\substack{m,k_1,k_2\in\mathbb{N} \\ \varepsilon\in\mathcal{H}_{mk}}} F(m,k_1,k_2) \\ &= \delta' + \sum_{\substack{m,k_1,k_2\in\mathbb{N} \\ e_1\in\mathcal{H}_{mk}}} F(m,k_1,k_2) + \sum_{\varepsilon\in\mathbb{F}_2^t\setminus\{0,e_1\}} \sum_{\substack{m,k_1,k_2\in\mathbb{N} \\ \varepsilon\in\mathcal{H}_{mk}}} F(m,k_1,k_2). \end{aligned}$$

By the same argument as above, we can rewrite:

$$\delta = \delta' \left\{ 1 + \frac{1}{\Lambda_2} \left[\mathcal{W}(e_1) + \sum_{\varepsilon\in\mathbb{F}_2^t\setminus\{0,e_1\}} \prod_{\substack{p_i\in S_\Gamma \\ i\geq 2}} \left(1 - \frac{\varepsilon_i}{\Lambda_{p_i}}\right) \left(\mathcal{T}(\varepsilon) + \mathcal{W}(\varepsilon)\right) \right] \right\} \tag{2.10}$$

where

$$\mathcal{W}(\varepsilon) = \begin{cases} \sum_{n_1,n_2\in\{0,1\}} \left(\frac{-1}{4}\right)^{n_1+n_2} \sum_{n}^{*} \frac{f(n,n_1,n_2)}{\varphi(2^{3n+\overline{n}})}, & \text{if } v_2(P_{=}(\varepsilon)) > 0 \\ 0, & \text{otherwise} \end{cases}$$

and so we have the Theorem. The proof for the remaining formulas for $\mathcal{W}(\varepsilon)$ is the same as $\mathcal{T}(\varepsilon)$.

2.4 Proof of Theorem 16

Let a, b as in Theorem 14. We use the same notations as the above section. We prove only formula (2.4) (the proof of other formula is analogous). We have, by Lemma 20:

$$\delta = \sum_{m,k_1,k_2\in\mathbb{N}} F(m,k_1,k_2)\#\mathcal{B}_{mk} = \sum_{\varepsilon\in\mathbb{F}_2^t}\sum_{\substack{m,k_1,k_2\in\mathbb{N}\\ \varepsilon\in\mathcal{B}_{mk}}} F(m,k_1,k_2) =$$

$$= \sum_{m,k_1,k_2\in\mathbb{N}} F(m,k_1,k_2) + \sum_{\varepsilon\in\mathbb{F}_2^t\setminus\{0\}} \left[\sum_{\substack{m,k_1,k_2\in\mathbb{N}\\ \varepsilon\in\mathcal{L}_{mk,2}}} F(m,k_1,k_2) + \right.$$

$$\left. \sum_{\substack{m,k_1,k_2\in\mathbb{N}\\ \varepsilon\in\mathcal{K}_{mk,N}}} F(m,k_1,k_2) \right].$$

By Lemma 23, and using the same argument of previous proof, we have:

$$\delta = \delta' \left(1 + \frac{1}{\Lambda_2} \sum_{\varepsilon\neq\underline{0}} \prod_{p_i\in S_\Gamma} \left(1 - \frac{\varepsilon_i}{\Lambda_{p_i}}\right) \left(\mathcal{T}^*(\varepsilon) + \sum_{z=0,1} \mathcal{Z}^*((z,\varepsilon)) \right) \right)$$

where

$$\mathcal{T}^*(\varepsilon) = \sum_{n_1,n_2\in\{0,1\}} \left(\frac{-1}{4}\right)^{n_1+n_2} \sum_{n}^{**} \frac{2^{\min(n+n_1+n_2+\delta_1+\underline{n},\delta_2+2\underline{n})}}{\varphi(2^{3n+\overline{n}})},$$

where $\sum_n^{**}$ is the sum over all $n \in \mathbb{N}$ such that the following conditions hold with respect to ε:

C1***:** $n \geq \max(\max(\sigma(\epsilon), k(n_1, n_2, \underline{\varepsilon})) - \overline{n}, 2)$

C2***:** $\delta_3^\epsilon \geq \min\{\delta_2 + 1, n + \overline{n} + \delta_2^\epsilon\}$

and

$$\mathcal{Z}^*((z,\varepsilon)) = \sum_{n_1,n_2\in\{0,1\}} \left(\frac{-1}{4}\right)^{n_1+n_2} \sum_n^{***} \frac{2^{\min(n+n_1+n_2+\delta_1+\underline{n},\delta_2+2\underline{n})}}{\varphi(2^{3n+\overline{n}})}$$

where $\sum_n^{***}$ is the sum over all $n \in \mathbb{N}$ such that the following conditions hold with respect to (z, ε):

C3***:** $n = 1 - \overline{n}$, $\delta_1 = 0$, $\delta_2 = \delta_2^{(z,\varepsilon)}$ and $\delta_3^{(z,\varepsilon)} \geq 1 + \delta_2$.

2.5 Simplest case: $\delta_{p^\alpha,q^\beta}$

In this section we analyze the case of $a = p^\alpha$ and $b = q^\beta$. Our analysis requires a subdivision into two cases: $(\alpha, \beta) = (1, 1)$ and $(\alpha, \beta) \neq (1, 1)$. All following tables compare the densities $\delta_{a,b}$ with the quantities $\mathcal{N}_{a,b}(10^7)/\pi(10^7)$ with natural height up to 7. Both quantities have been truncated at the fifth decimal digit. We set $N_{a,b}(10^7) = \mathcal{N}_{a,b}(10^7)/\pi(10^7)$ and

$$A(x) = \frac{x}{x^3 - 2x - 1} \, .$$

Computation of $\delta_{p,q}$

Let p, q be primes with $p \neq q$. We have

$$\delta' \;=\; \prod_{l\ primes} \Lambda_l \;=\; \prod_{l\ primes} \left(1 - \frac{2l}{l^3 - 1}\right) = 0.273273\ldots$$

We have only three possibilities for p, q:

I. $p = 2$, $q \equiv 1, 3 \pmod 4$;

II. $p, q \equiv 1$ or $p, q \equiv 3 \pmod 4$;

III. $p \equiv 3$ or $q \equiv 1 \pmod 4$.

I. $p = 2$ and $q \equiv 1, 3 \pmod 4$.

Using (2.2), we obtain:

$$\delta_{2,q} = \delta' \cdot \left(\frac{47}{48} + \frac{3q}{8(q^3 - 2q - 1)} \right).$$

Computation of $\delta_{2,p}$, with $p \leq 100$, $p \equiv 1, 3 \pmod 4$							
2	p	$N_{2,p}(10^7)$	$\delta_{2,p}$	2	p	$N_{2,p}(10^7)$	$\delta_{2,p}$
2	3	0,28280	0,28295	2	43	0,26819	0,26763
2	5	0,27230	0,27207	2	47	0,26821	0,26762
2	7	0,27006	0,26976	2	53	0,26770	0,26761
2	11	0,26851	0,26844	2	59	0,26755	0,26760
2	13	0,26823	0,26819	2	61	0,26784	0,26760
2	17	0,26749	0,26793	2	67	0,26771	0,26760
2	19	0,26834	0,26786	2	71	0,26734	0,26760
2	23	0,26727	0,26777	2	73	0,26761	0,26759
2	29	0,26779	0,26770	2	79	0,26736	0,26759
2	31	0,26799	0,26768	2	83	0,26799	0,26759
2	37	0,26806	0,26765	2	89	0,26733	0,26759
2	41	0,26787	0,26764	2	97	0,26736	0,26759

II. $p, q \equiv 1 \pmod 4$ or $p, q \equiv 3 \pmod 4$.

In this case, the formula (2.1) yields:

$$\delta_{p,q} = \delta' \cdot \left[1 + \frac{1}{3} \left(A(p) + A(q) \right) + 4A(p)A(q) \right].$$

(a) $p, q \leq 50$ with $p, q \equiv 3 \pmod 4$.

Computation of $\delta_{p,q}$, with $p, q \equiv 3 \pmod 4$							
p	q	$N_{p,q}(10^7)$	$\delta_{p,q}$	p	q	$N_{p,q}(10^7)$	$\delta_{p,q}$
3	7	0,29217	0,29237	11	23	0,27428	0,27422
3	11	0,28912	0,28908	11	31	0,27405	0,27414
3	19	0,28795	0,28764	11	43	0,27446	0,27409
3	23	0,28766	0,28742	11	47	0,27386	0,27408
3	31	0,28699	0,28720	19	23	0,27338	0,27370
3	43	0,28746	0,28707	19	31	0,27359	0,27362
3	47	0,28709	0,28705	19	43	0,27380	0,27357
7	11	0,27635	0,27617	19	47	0,27407	0,27356
7	19	0,27588	0,27553	23	31	0,27357	0,27354
7	23	0,27555	0,27543	23	43	0,27420	0,27349
7	31	0,27571	0,27533	23	47	0,27344	0,27348
7	43	0,27546	0,27527	31	43	0,27340	0,27341
7	47	0,27507	0,27526	31	47	0,27378	0,27340
11	19	0,27476	0,27431	43	47	0,27318	0,27336

(b) $p, q \leq 50$ with $p, q \equiv 1 \pmod 4$.

Computation of $\delta_{p,q}$, with $p, q \equiv 1 \pmod 4$							
p	q	$N_{p,q}(10^7)$	$\delta_{p,q}$	p	q	$N_{p,q}(10^7)$	$\delta_{p,q}$
5	13	0,27814	0,27810	13	41	0,27387	0,27387
5	17	0,27771	0,27775	17	29	0,27394	0,27370
5	29	0,27816	0,2	17	37	0,27457	0,27365
5	37	0,27786	0,27736	17	41	0,27313	0,27364
5	41	0,27786	0,27735	29	37	0,27343	0,27344
13	17	0,27433	0,27415	29	41	0,27398	0,27343
13	29	0,27357	0,27393	37	41	0,27331	0,27339
13	37	0,27372	0,27389				

III. $p \equiv 3$ and $q \equiv 1 \pmod 4$.

Holds the following formula:

$$\delta_{p,q} = \delta' \cdot \left[1 + \frac{1}{3}\left(A(p) + A(q)\right) - \frac{2}{3}A(p)A(q)\right].$$

For all $p, q \leq 50$, we have:

Computation of $\delta_{p,q}$, with $p \equiv 3$ and $q \equiv 1 \pmod 4$							
p	q	$N_{p,q}(10^7)$	$\delta_{p,q}$	p	q	$N_{p,q}(10^7)$	$\delta_{p,q}$
3	5	0,28992	0,28973	23	5	0,27728	0,27742
3	13	0,28717	0,28731	23	13	0,27467	0,27398
3	17	0,28759	0,28715	23	17	0,27426	0,27376
3	29	0,28677	0,28701	23	29	0,27357	0,27355
3	37	0,28763	0,28698	23	37	0,27357	0,27351
3	41	0,28676	0,28697	23	41	0,27329	0,27349
7	5	0,27922	0,27904	31	5	0,27767	0,27735
7	13	0,27566	0,27573	31	13	0,27454	0,27391
7	17	0,27518	0,27552	31	17	0,27346	0,27368
7	29	0,27602	0,27532	31	29	0,27397	0,27347
7	37	0,27543	0,27528	31	37	0,27313	0,27343
7	41	0,27580	0,27526	31	41	0,27349	0,27342
11	5	0,27786	0,27796	43	5	0,27741	0,27731
11	13	0,27440	0,27457	43	13	0,27450	0,27386
11	17	0,27494	0,27435	43	17	0,27381	0,27363
11	29	0,27388	0,27414	43	29	0,27383	0,27343
11	37	0,27378	0,27410	43	37	0,27371	0,27338
11	41	0,27422	0,27409	43	41	0,27350	0,27337
19	5	0,27773	0,27749	47	5	0,27788	0,27730
19	13	0,27450	0,27406	47	13	0,27438	0,27385
19	17	0,27397	0,27384	47	17	0,27369	0,27363
19	29	0,27391	0,27363	47	29	0,27353	0,27342
19	37	0,27410	0,27359	47	37	0,27359	0,27338
19	41	0,27370	0,27358	47	41	0,27316	0,27336

Computation of $\delta_{p^\alpha,q^\beta}$

We show the following case, only with $p, q \equiv 1 \pmod 4$:

I. $a = p^\alpha$, $b = q^\beta$ with $v_2(\alpha) = v_2(\beta)$

II. $a = p^\alpha$, $b = q^\beta$ with $v_2(\alpha) = v_2(\beta) + 1$

III. $a = p^\alpha$, $b = q^\beta$ with $v_2(\alpha) > v_2(\beta) + 1$.

I. $a = p^\alpha$, $b = q^\beta$ with $v_2(\alpha) = v_2(\beta)$.

We pick $v_2(\alpha) = h$. The following expression for $\delta_{a,b}$ holds:

$$\begin{aligned}\delta_{a,b} =& \delta' \left\{ 1 + \frac{1}{\Lambda_2} \left[\lambda_p \left(\frac{3 \cdot 2^{-h}}{7} - \frac{2}{3} \left(2^{-h} - 2^{-h-2} \right) \right) \right.\right. \\ & \left.\left. + \lambda_q \left(\frac{3 \cdot 2^{-h}}{7} - \frac{2}{3} \left(2^{-h} - 2^{-h-2} \right) \right) + \lambda_p \lambda_q \frac{3 \cdot 2^{-h}}{7} \right] \right\}\end{aligned}$$

where

$$\delta' = \prod_{p\, prime} \Lambda_p$$

with

$$\Lambda_p = \begin{cases} \left(1 - \frac{2p^{1-v_p(\alpha)}}{p^3-1} \right), & \text{if } v_p(\alpha) = v_p(\beta) \\ \left(1 - \frac{p^{1-d_1}}{p^2-1} + p^{3d_1-2d_2+1} \frac{(p^2-p-1)(p-1)}{(p^3-1)(p^2-1)} \right), & \text{otherwise} \end{cases}$$

and

$$\lambda_p = \left(1 - \frac{1}{\Lambda_p} \right).$$

(a) $a = p^2$, $b = q^2$, $h = 1$.
In this case

$$\delta' = \frac{5}{7} \prod_{l>2\ primes} \left(1 - \frac{2l}{l^3 - 1} \right) = 0.455455\ldots$$

The formula for δ_{p^2,q^2} is:

$$\delta' \left[1 + \frac{1}{10}\left(A(p) + A(q)\right) + \frac{6}{5}A(p)A(q)\right]$$

Computation of δ_{p^2,q^2}, with $p, q \equiv 1 \pmod 4$							
p	q	$N_{p^2,q^2}(10^7)$	δ_{p^2,q^2}	p	q	$N_{p^2,q^2}(10^7)$	δ_{p^2,q^2}
5	13	0,45824	0,45786	13	41	045613	0,45575
5	17	0,45798	0,45769	17	29	0,45592	0,45567
5	29	0,45811	0,45753	17	37	0,45637	0,45564
5	37	0,45833	0,45750	17	41	0,45473	0,45564
5	41	0,45815	0,45749	29	37	0,45577	0,455544
13	17	0,45557	0,45589	29	41	0,45544	0,45553
13	29	0,45608	0,45578	37	41	0,45555	0,45551
13	37	0,45575	0,45576				

(b) $a = p^2$, $b = q^6$ with $h = 1$.

We have:

$$\delta'_{p^2,q^6} \;=\; \frac{5}{7} \times \frac{25}{39} \prod_{l>3\ primes} \left(1 - \frac{2l}{l^3 - 1}\right) = 0.379545\ldots$$

The formula is the following:

$$\delta_{p^2,q^6} \;=\; \delta'_{p^2,q^6} \left[1 + \frac{1}{10}\left(A(p) + A(q)\right) + \frac{6}{5}A(p)A(q)\right].$$

Computation of δ_{p^2,q^6}, with $p, q \equiv 1 \pmod 4$							
p	q	$N_{p^2,q^6}(10^7)$	δ_{p^2,q^6}	p	q	$N_{p^2,q^6}(10^7)$	δ_{p^2,q^6}
5	13	0,38209	0,38151	13	5	0,38188	0,38155
5	17	0,38134	0,38141	17	5	0,38138	0,38141
5	29	0,38182	0,38127	29	5	0,38180	0,38127
5	37	0,38155	0,38125	37	5	0,38167	0,38125
5	41	0,38142	0,38124	41	5	0,38145	0,38124
13	17	0,37977	0,37991	17	13	0,37952	0,37991
13	29	0,37986	0,37982	29	13	0,37953	0,37991
13	37	0,38017	0,37980	37	13	0,38016	0,37980
13	41	0,38072	0,37979	41	13	0,38039	0,37979
17	29	0,38012	0,37972	29	17	0,37984	0,37972
17	37	0,38006	0,37970	37	17	0,38014	0,37970
17	41	0,37938	0,37970	41	17	0,37937	0,37970

(c) $a = p^2$, $b_2 = q^{10}$ $h = 1$.

We have:

$$\delta'_{p^2,q^{10}} \;=\; \frac{5}{7} \;\times\; \frac{247}{310} \prod_{\substack{l \; primes \\ l \neq 2,5}} \left(1 - \frac{2l}{l^3 - 1}\right) = 0.394727\ldots$$

The formula is the following:

$$\delta_{p^2,q^{10}} \;=\; \delta'_{p^2,q^{10}} \left[1 + \frac{1}{20}\left(-\lambda_p - \lambda_q + 6\lambda_p\lambda_q\right)\right]$$

where

$$\Lambda_l \;=\; \begin{cases} \frac{247}{310}, & \text{if } l = 5, \\ 1 - \frac{2l}{l^3-1}, & \text{otherwise.} \end{cases}$$

Computation of $\delta_{p^2,q^{10}}$, with $p, q \equiv 1 \pmod 4$							
p	q	$N_{p^2,q^{10}}(10^7)$	$\delta_{p^2,q^{10}}$	p	q	$N_{p^2,q^{10}}(10^7)$	$\delta_{p^2,q^{10}}$
5	13	0.40042	0.40036	13	5	0.40046	0.40036
5	17	0.39976	0.40010	17	5	0.39979	0.40010
5	29	0.39968	0.39988	29	5	0.39969	0.39988
5	37	0.40028	0.39983	37	5	0.40016	0.39983
5	41	0.40050	0.39982	41	5	0.40037	0.39982
13	17	0.39482	0.39486	17	13	0.39484	0.39496
13	29	0.39548	0.39477	29	13	0.39542	0.39496
13	37	0.39506	0.39475	37	13	0.39468	0.39496
13	41	0.39506	0.39475	41	13	0.39461	0.39496
17	29	0.39472	0.39477	29	17	0.394508	0.39486
17	37	0.39537	0.39475	37	17	0.39514	0.39486
17	41	0.39422	0.39475	41	17	0.39411	0.39486

II. $a = p^\alpha$, $b = q^\beta$ with $v_2(\alpha) = v_2(\beta) + 1$.

We set $v_2(\beta) = h$. The following expression for $\delta_{a,b}$ holds:

$$\delta_{a,b} = \delta' \left\{ 1 + \frac{1}{\Lambda_2} \left[\lambda_p \left(-\frac{2^{-h-3}}{7} \right) + \lambda_q \left(-\frac{2^{-h-3}}{7} + \frac{2}{3} \left(2^{-h} - \frac{7}{16} 2^{-h} \right) \right) + \lambda_p \lambda_q \left(-\frac{2^{-h-3}}{7} \right) \right] \right\}$$

with δ' and Λ_p defined as in **I.**

(a) $a = p^4$ and $b = q^2$ with $p, q \leq 50$ and $p, q \equiv 1 \pmod 4$.

We have:

$$\delta'_{p^4,q^2} = \frac{19}{28} \prod_{l>2} \left(1 - \frac{2l}{l^3 - 1} \right) = 0.432682\ldots$$

Computation of δ_{p^4,q^2}, with $p, q \equiv 1 \pmod 4$							
p	q	$N_{p^4,q^2}(10^7)$	δ_{p^4,q^2}	p	q	$N_{p^4,q^2}(10^7)$	δ_{p^4,q^2}
5	13	0.43231	0.43181	13	5	0.42334	0.42275
5	17	0.43306	0.43238	17	5	0.42302	0.42273
5	29	0.43342	0.4329	29	5	0.42339	0.4227
5	37	0.43306	0.43301	37	5	0.42313	0.4227
5	41	0.43323	0.43304	41	5	0.42271	0.4227
13	17	0.4319	0.43195	17	13	0.43139	0.43135
13	29	0.43312	0.43247	29	13	0.43165	0.43133
13	37	0.43258	0.43258	37	13	0.43136	0.43132
13	41	0.43272	0.43261	41	13	0.43141	0.43132
17	29	0.43263	0.43245	29	17	0.43202	0.4319
17	37	0.43278	0.43255	37	17	0.43219	0.43189
17	41	0.4318	0.43258	41	17	0.43126	0.43189
29	37	0.43287	0.43252	37	29	0.4325	0.43241
29	41	0.43265	0.43256	41	29	0.43242	0.43241
37	41	0.43229	0.43255	41	37	0.43238	0.43252

(b) $a = p^4$ and $b = q^6$ with $p, q \leq 50$ and $p, q \equiv 1 \pmod 4$.
We have:

$$\delta'_{p^4,q^6} = \frac{19}{28} \times \frac{25}{39} \prod_{l>3} \left(1 - \frac{2l}{l^3 - 1}\right) = 0.360568\ldots$$

Computation of δ_{p^4,q^6}, with $p, q \equiv 1 \pmod 4$							
p	q	$N_{p^4,q^6}(10^7)$	δ_{p^4,q^6}	p	q	$N_{p^4,q^6}(10^7)$	δ_{p^4,q^6}
5	13	0.36022	0.35984	13	5	0.35275	0.35229
5	17	0.36038	0.36032	17	5	0.35226	0.35227
5	29	0.36108	0.36075	29	5	0.35291	0.35225
5	37	0.36081	0.36084	37	5	0.35243	0.35225
5	41	0.36082	0.36087	41	5	0.35231	0.35225

Computation of δ_{p^4,q^6}, with $p,q \equiv 1 \pmod 4$							
p	q	$N_{p^4,q^6}(10^7)$	δ_{p^4,q^6}	p	q	$N_{p^4,q^6}(10^7)$	δ_{p^4,q^6}
13	17	0.36022	0.35996	17	13	0.35949	0.35946
13	29	0.36096	0.36039	29	13	0.35941	0.35944
13	37	0.36106	0.36048	37	13	0.35989	0.35943
13	41	0.36099	0.36051	41	13	0.35953	0.35943
17	29	0.36016	0.36037	29	17	0.35996	0.35991
17	37	0.36031	0.36046	37	17	0.35988	0.35991
17	41	0.36045	0.36048	41	17	0.35986	0.35991
29	37	0.3605	0.36044	37	29	0.36003	0.36034
29	41	0.3605	0.36046	41	29	0.36037	0.36034
37	41	0.36059	0.36046	41	37	0.36061	0.36043

III. $a = p^\alpha$, $b = q^\beta$ with $v_2(\alpha) > v_2(\beta) + 1$.

We pick $v_2(\beta) = h$. The following expression for $\delta_{a,b}$ holds:

$$\delta_{a,b} = \delta' \left\{ 1 + \frac{1}{\Lambda_2} \left[\lambda_p \left(-\frac{2^{-h-3}}{7} \right) + \lambda_q \left(-\frac{2^{-2d_2-1+3h}}{7} + \frac{2^{-h}}{3} + \frac{2^{3h-2d_2-1}}{3} \right) + \lambda_p \lambda_q \left(-\frac{2^{-h-3}}{7} \right) \right] \right\}.$$

(a) $a = p^4$ and $b = q$ with $p, q \leq 50$ and $p, q \equiv 1 \pmod 4$.

We have:

$$\delta' = \frac{19}{56} \prod_{\substack{l \text{ primes} \\ l>2}} \left(\frac{2l}{l^3 - 1} \right) = 0.216341\ldots$$

Computation of $\delta_{p^4,q}$, with $p,q \equiv 1 \pmod 4$							
p	q	$N_{p^4,q}(10^7)$	$\delta_{p^4,q}$	p	q	$N_{p^4,q}(10^7)$	$\delta_{p^4,q}$
5	13	0.21402	0.21473	13	5	0.198	0.19748
5	17	0.21516	0.21582	17	5	0.1977	0.19743
5	29	0.21656	0.21682	29	5	0.19795	0.19738
5	37	0.21618	0.21702	37	5	0.19761	0.19737
5	41	0.2163	0.21708	41	5	0.19777	0.19737

Computation of $\delta_{p^4,q}$, with $p, q \equiv 1 \pmod 4$							
p	q	$N_{p^4,q}(10^7)$	$\delta_{p^4,q}$	p	q	$N_{p^4,q}(10^7)$	$\delta_{p^4,q}$
13	17	0.21475	0.21496	17	13	0.21347	0.21382
13	29	0.2162	0.21596	29	13	0.21371	0.21377
13	37	0.21591	0.21616	37	13	0.21374	0.21376
13	41	0.21601	0.21621	41	13	0.2135	0.21376
17	29	0.21598	0.2159	29	17	0.21501	0.21486
17	37	0.21582	0.2161	37	17	0.21461	0.21484
17	41	0.21556	0.21616	41	17	0.21436	0.21484
29	37	0.21589	0.21605	37	29	0.21584	0.21584
29	41	0.21575	0.21611	41	29	0.21555	0.21583
37	41	0.21535	0.2161	41	37	0.21569	0.21603

(b) $a = p^4$ and $b = q^3$ with $p, q \leq 50$ and $p, q \equiv 1 \pmod 4$.
We have:

$$\delta' \;=\; \frac{19}{56}\,\frac{25}{36}\prod_{\substack{l \text{ primes}\\ l>2}}\left(\frac{2l}{l^3-1}\right) \;=\; 0.180284\ldots$$

Computation of δ_{p^4,q^3}, with $p, q \equiv 1 \pmod 4$							
p	q	$N_{p^4,q^3}(10^7)$	δ_{p^4,q^3}	p	q	$N_{p^4,q^3}(10^7)$	δ_{p^4,q^3}
5	17	0.17913	0.17985	17	5	0.16452	0.16453
5	29	0.18063	0.18068	29	5	0.16466	0.16449
5	37	0.18016	0.18085	37	5	0.16451	0.16448
5	41	0.18004	0.1809	41	5	0.16479	0.16448
13	17	0.17895	0.17914	17	13	0.17783	0.17818
13	29	0.18015	0.17996	29	13	0.17786	0.17814
13	37	0.18006	0.18013	37	13	0.17842	0.17813
13	41	0.18025	0.18018	41	13	0.17763	0.17813
17	29	0.17975	0.17992	29	17	0.17903	0.17905
17	37	0.17988	0.18008	37	17	0.17881	0.17904
17	41	0.17999	0.18013	41	17	0.17895	0.17903
29	37	0.17998	0.18004	37	29	0.18026	0.17986
29	41	0.17978	0.18009	41	29	0.17963	0.17986
37	41	0.18006	0.18008	41	37	0.17981	0.18003

3. ON DISTRIBUTION OF SUBGROUPS WITH FIXED INDEX.

3.1 Introduction

Let $\Gamma \subseteq \mathbb{Q}^*$ be a finitely generated subgroup such that Γ be torsion free with support $\mathcal{S}_\Gamma$ and $m \in \mathbb{N}^+$. We are interested in the density of primes p for which the index of the group generated by the reduction of $\Gamma \pmod p$ is m. In other words, we want to study the following function:

$$\mathcal{N}_\Gamma(x;m) = \#\{p \leq x : \ p \notin \mathcal{S}_\Gamma, \text{ and } [\mathbb{F}_p^* : \Gamma_p] = m\}$$

and its natural density:

$$\lim_{x\to\infty} \frac{\mathcal{N}_\Gamma(x;m)}{\pi(x)} = \rho(\Gamma, m).$$

This problem is a generalization of some earlier works by Lenstra [9], Murata [14], Wagstaff [21], Pappalardi [17] and Cangelmi & Pappalardi [3].

- Murata studied

  $$\mathcal{N}_a(x;m) \ = \ \#\{p \leq x \ : \ p \not| a \text{ and } \mathrm{ind_p(a) = m}\}$$

  for any $a \geq 2$ integer squarefree. His result is the following.

  Theorem (Murata, 1991, [14])**.** *Let $a \geq 2$ be a squarefree natural number and assume that the GRH holds. Then we have, for any $\epsilon > 0$*

  $$\mathcal{N}_a(x;m) \ = \ \left(c_{a,m} + O\left(\frac{m^\epsilon \log\log x + \log a}{\log x}\right)\right) \mathrm{li}(x)$$

  where $c_{a,m}$ is a suitable non negative constant, and the constant implied in the O–symbol may depend on ϵ.

The problem of determining when $c_{a,m}$ is equal to zero has been addressed by H. Lenstra [9]. A general expression for the constant $c_{a,m}$ has been obtained by S. Wagstaff [21].

In Chapter 1 we obtained, as a side-product of our Theorem 1, the following analogue of Murata's Theorem:

Theorem. *Let $\{a_1, \dots, a_r\} \subset \mathbb{Q} \setminus \{0, \pm 1\}$, $m \in \mathbb{N}$, assume that the GRH holds and that $r(a_1, \dots, a_r) \geq 2$. Then*

$$\mathcal{N}_{a_1,\dots,a_r}(x,m) = \left(c_{a_1,\dots,a_r,m} + O_{a_1,\dots,a_r,m}\left(\frac{(\log\log x)^{2^r-2}}{\log x} \right) \right) \mathrm{li}(x)$$

where

$$c_{a_1,\dots,a_r,m} = \sum_{k_1,\dots,k_r \in \mathbb{N}} \frac{\mu(k_1)\cdots\mu(k_r)}{\varphi(mk)} \frac{\#\mathcal{B}}{\#\mathcal{A}} \tag{3.1}$$

and the notations are the same as in the statement of Theorem 1. □

- Pappalardi in [16], has determined on GRH an asymptotic formula for the number of primes for which $\mathbb{F}_p^*$ can be generated by r given multiplicatively independent rational numbers. In particular, if Γ is generated by a single element, then this problem coincides with Artin's Conjecture. His result:

Theorem (Pappalardi, 1997, [17])**.** *Let $\Gamma = \langle a_1, \dots a_r \rangle \subset \mathbb{Q}^*$, be a finitely generated subgroup with $\mathrm{rank}(\Gamma) = r > 1$. Assume that the GRH holds. Then*

$$\{p \leq x : \ p \notin \mathcal{S}_\Gamma, \ [\mathbb{F}_p^* : \Gamma_p] = 1\} = \delta_\Gamma \, \mathrm{li}(x) + O\left(\frac{x \log(a_1 \cdots a_r)}{\log^2 x} \right)$$

where

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

and the error term is uniform with respect to $r \leq \frac{1}{3\log 2}\log x$ and $a_1, \dots, a_r$.

In particular, if $a_1, \dots, a_r$ are primes, then

$$\{p \leq x : \ p \notin \mathcal{S}_\Gamma, \ [\mathbb{F}_p^* : \Gamma_p] = 1\} = \delta_\Gamma \, \mathrm{li}(x) + O\left(\frac{x 4^r \log(x a_1 \cdots a_r)}{\log^{r+2} x} \right)$$

uniformly with respect to $r \leq \frac{1}{4}\log x / \log\log x$ and $a_1, \dots, a_r$.

□

The value of density can be expressed as an Euler product and Pappalardi has computed this in the last case.

- Cangelmi & Pappalardi in [3], have determined the number of primes p such that the image of $\Gamma \pmod p$ contains a promitive root, and so $[\mathbb{F}_p^* : \Gamma_p] = 1$. Their results:

  Theorem (Cangelmi & Pappalardi, 1999, [3])**.** *Let $\Gamma \subset \mathbb{Q}^*$, be a finitely generated subgroup with $\operatorname{rank}(\Gamma) = s > 1$. Assume that the GRH holds. Then*

  $$\{p \leq x \mid p \notin \mathcal{S}_\Gamma \text{ and } [\mathbb{F}_p^* : \Gamma_p] = 1\} = \left(\delta_\Gamma + O\left(\frac{1}{\log^s(x)(\log\log x)^s}\right)\right)\operatorname{li}(x)$$

  where δ_Γ is a suitable non negative constant, and the constant implied in the O–symbol depends only on Γ.

The main goal of this chapter is to prove a result that generalizes the above formulas, in particular the first and the third. The main results are the following.

Theorem 24. *Let Γ as above and $m = o(x^{1/6})$. Assume that the GRH holds for the fields of the form $\mathbb{Q}(\zeta_M, \Gamma^{1/M})$ with $M \in \mathbb{N}^+$. Then*

$$\mathcal{N}_\Gamma(x; m) = \left(\rho(\Gamma, m) + O\left(\frac{\log x}{m\log^2(x/m)}\right)\right)\operatorname{li}(x)$$

where if $M = mk$, then

$$\rho(\Gamma, m) = \sum_{k\geq 1} \frac{\mu(k)}{\varphi(M)} \frac{1}{|\Gamma \cdot \mathbb{Q}_M^{*M}/\mathbb{Q}_M^{*M}|}. \tag{3.2}$$

We can compute exactly the value of $\rho(\Gamma, m)$. For any $M \in \mathbb{N}^+$, we define $N = 2^{v_2(M)}$ and $s(\xi) = \operatorname{disc}(\mathbb{Q}(\sqrt{\xi}))$

$$\begin{aligned}
\mathcal{A}(M) &= \Gamma\mathbb{Q}^{*M}/\mathbb{Q}^{*M},\\
\mathcal{C}(M) &= \left\{\xi\mathbb{Q}^{*N} \in \Gamma\mathbb{Q}^{*N}/\mathbb{Q}^{*N} :\ [\mathbb{Q}(\sqrt[N]{\xi}) : \mathbb{Q}] \leq 2\right\},\\
\mathcal{B}(M) &= \left\{\xi\mathbb{Q}^{*N} \in \mathcal{C}(M) :\ s(\xi) \mid M\right\}.
\end{aligned}$$

Theorem 25. *With the same notation as above*

$$\rho(\Gamma,m)=\mathfrak{A}_{\Gamma}^{(m)}\left(\sum_{\substack{\xi\in\mathcal{C}(2^{v_2(m)})\\ \frac{s(\xi)}{(m,s(\xi))}\ odd}}\prod_{\substack{l\mid s(\xi)\\ l\nmid m}}\left(\frac{-1}{(l-1)\#\mathcal{A}(l)-1}\right)-\right. \tag{3.3}$$

$$\left.\frac{\#\mathcal{A}(2^{v_2(m)})}{(2,m)\#\mathcal{A}(2^{1+v_2(m)})|}\sum_{\substack{\xi\in\mathcal{C}(2^{1+v_2(m)})\\ \frac{s(\xi)}{(2m,s(\xi))}\ odd}}\prod_{\substack{l\mid s(\xi)\\ l\nmid 2m}}\left(\frac{-1}{(l-1)\#\mathcal{A}(l)-1}\right)\right) \tag{3.4}$$

where

$$\mathfrak{A}_{\Gamma}^{(m)}=\frac{1}{\varphi(m)\#\mathcal{A}(m)}\prod_{\substack{l>2\\ l\nmid m}}\left(1-\frac{1}{(l-1)\#\mathcal{A}(l)}\right)\times\prod_{\substack{l>2\\ l\mid m}}\left(1-\frac{\#\mathcal{A}(l^{v_l(m)})}{l\#\mathcal{A}(l^{1+v_l(m)})}\right).$$

In the last section of this chapter we will prove that we can derive the results of Murata and Cangelmi & Pappalardi from our formula (3.3).

3.2 Proof of Theorem 24

Let Γ and m as in the Theorem 24. We denote by $s=rank_{\mathbb{Z}}(\Gamma)$ and $\mathcal{S}_{\Gamma}$ the support of Γ. We can suppose that $s\geq 2$ (otherwise we can use Murata's Theorem). We start the proof using the Inclusion/Exclusion Principle:

$$\mathcal{N}_{\Gamma}(x;m)=\sum_{k\geq 1}\mu(k)\#\left\{p\leq x:\ p\notin\mathcal{S}_{\Gamma},\ mk\mid[\mathbb{F}_P^*:\Gamma_p]\right\}.$$

So, for each $t\in[1,x]$, we have

$$\mathcal{N}_\Gamma(x;m) \leq \sum_{k \mid P(t)} \mu(k) \#\left\{p \leq x:\ p \notin \mathcal{S}_\Gamma,\ mk | [\mathbb{F}_P^* : \Gamma_p]\ \right\} = \mathcal{U}(x;m,t)$$

and

$$\begin{aligned}\mathcal{N}_\Gamma(x;m) &= \sum_{k \mid P(t)} \mu(k) \#\left\{p \leq x:\ p \notin \mathcal{S}_\Gamma,\ mk \mid [\mathbb{F}_P^* : \Gamma_p]\right\} \\ &\quad + O\left(\#\{p \leq x:\ p \notin \mathcal{S}_\Gamma,\ \exists l > t,\ lm \mid [\mathbb{F}_P^* : \Gamma_p]\}\right) \\ &= \mathcal{U}(x;m,t) + O\left(\mathcal{E}(x,m,t)\right).\end{aligned}$$

Before we estime $\mathcal{U}(x;m,t)$, we need the following result.

Lemma 26. *Let Γ and m as above. If $M = mk$, then we have the following identity:*

$$\sum_{k|P(t)} \frac{\mu(k)}{[\mathbb{Q}(\zeta_M, \Gamma^{1/M}) : \mathbb{Q}]} \ = \ \rho(\Gamma, m) + O\left(\frac{1}{m^s \varphi(m) t}\right). \tag{3.5}$$

Proof. First, we note that

$$\sum_{k \geq 1} \frac{\mu(k)}{\varphi(k) k}$$

converges to Artin's constant.

Following the proof of Lemma 9, we have that:

$$\frac{1}{[\mathbb{Q}(\zeta_{mk}, \Gamma^{1/km}) : \mathbb{Q}]} \leq \frac{1}{\varphi(m) m^s} \times \frac{2^s \Delta_s(\Gamma)}{\varphi(k) k^s} \ll \frac{1}{\varphi(m) m^s} \times \frac{1}{\varphi(k) \cdot k}.$$

Hence

$$\begin{aligned}\sum_{k|P(t)} \frac{\mu(k)}{[\mathbb{Q}(\zeta_M, \Gamma^{1/M}) : \mathbb{Q}]} \ &\ll \ \frac{1}{\varphi(m) m^s} \sum_{k|P(t)} \frac{\mu(k)}{\varphi(k) k} \\ &= O\left(\frac{1}{\varphi(m) m^s t}\right).\end{aligned}$$

□

Now, by Chebotarev Density Theorem 5 and Lemma 26, we have:

$$\begin{aligned}\mathcal{U}(x;m,t) &= \sum_{k\,|\,P(t)} \mu(k)\#\left(\frac{\mathrm{li}(x)}{[\mathbb{Q}(\zeta_M,\Gamma^{1/M}):\mathbb{Q}]} + O\left(\sqrt{x}\log(xM\#S_\Gamma)\right)\right)\\ &= \mathrm{li}(x)\left(\rho(\Gamma,m) + O\left(\frac{1}{m^s\varphi(m)t}\right)\right) + O\left(\sqrt{x}P(t)\log(xmP(t))\right).\end{aligned}$$

In order to estimate $\mathcal{E}(x;m,t)$, we define, for any $t \le \eta < \theta \le x$,

$$\mathcal{E}(x;m,\eta,\theta) = \#\{p \le x :\ p \notin \mathcal{S}_\Gamma,\ \exists l \in (\theta,\eta],\ lm \mid [\mathbb{F}_P^* : \Gamma_p]\}$$

so

$$\mathcal{E}(x;m,t) \le \mathcal{E}(x,m,\eta,t) + \mathcal{E}(x,m,x,\eta).$$

Applying Lemma 7, we obtain

$$\mathcal{E}(x,m,x,\eta) \ll \left(\frac{x}{m\eta}\right)^{(s+1)/s} \frac{1}{\log(x/(m\eta))} \ll \frac{x}{m\log^2(x/m)},$$

if we choose $\eta = (\frac{x}{m}\log^s(x))^{1/(s+1)}$.

Using Chebotarev Density Theorem 1.3, Brun–Tithsmarch Theorem and Merten's formula, we deduce:

$$\begin{aligned}\mathcal{E}(x,m,\eta,t) &\le \sum_{l=\in(t,\eta]}\left(\frac{\mathrm{li}(x)}{[\mathbb{Q}_M(\Gamma)^{1/M}:\mathbb{Q}]} + O(\sqrt{x}\log(xml))\right)\\ &= O\left(\mathrm{li}(x)\sum_{l>t}\frac{1}{\varphi(m)m^s}\frac{1}{l^2-l} + \sum_{l<\eta}\sqrt{x}\log(xml)\right)\\ &= O\left(\frac{\mathrm{li}(x)}{\varphi(m)m^s t} + \eta\sqrt{x}\log(xm\eta)\right).\end{aligned}$$

Because $m = o(x^{1/6})$, if we choose $t = \frac{1}{6}\log x - \frac{1}{2}\log m$, we deduce the thesis.

3.2.1 An unconditionally estimate for the upperbound

It is possible to obtain an unconditionally estimate for the upperbound using Chebotarev Density Theorem without GRH (see for example [20] Theorem 2 and [16], Lemma 2.1).

Lemma 27 (Chebotarev Density Theorem)**.** *Let $\Gamma \subseteq \mathbb{Q}^*$ finitely generated. There exist two absolute constants A and B such that if $M \leq B \log^{1/8} x$, then*

$$\#\left\{p \leq x : \ M \mid [\mathbb{F}_p^* : \Gamma_p]\right\} = \frac{\mathrm{li}(x)}{[\mathbb{Q}_M(\Gamma^{1/M}) : \mathbb{Q}]} + O\Big(x \exp(-A\sqrt{\log x}/M)\Big). \qquad \square \tag{3.6}$$

By this result, if we replace the hypothesis $m = \underline{o}(x^{1/6})$ of Theorem with $m = \underline{o}(\log^{1/8} x)$ and we suppose that $mP(t) \leq B \log^{1/8} x$, then

$$\mathcal{U}(x; m, t) = \mathrm{li}(x)\left(\rho(\Gamma, m) + O\left(\frac{1}{\varphi(m) m^s t}\right)\right) + O\left(\frac{xP(t)}{m \exp(A\sqrt{\log x} m P(t)}\right).$$

If we choose $t = \log\log x - \log m - \log\log\log x$, then

$$\mathcal{U}(x; m, t) = \mathrm{li}(x)\left(\rho(\Gamma, m) + O\left(\frac{\log^{9/8} x}{m \exp(C \log^{3/8} x)}\right)\right).$$

3.3 Proof of Theorem 25

We set $\rho = \rho(\Gamma, m)$, $\mathcal{A}(M) = \Gamma\mathbb{Q}^{*M}/\mathbb{Q}^{*M}$, $N = 2^{v_2(M)}$,

$$\mathcal{C}(M) = \left\{\xi\mathbb{Q}^{*N} \in \Gamma\mathbb{Q}^{*N}/\mathbb{Q}^{*N} : \ [\mathbb{Q}(\sqrt[N]{\xi}) : \mathbb{Q}] \leq 2\right\}.$$

Moreover if $\xi\mathbb{Q}^{*N} \in \mathcal{C}(M)$ we denote by $s(\xi) = \mathrm{disc}(\mathbb{Q}(\sqrt{\xi}))$ and define

$$\mathcal{B}(M) = \left\{\xi\mathbb{Q}^{*N} \in \mathcal{C}(M) : \ s(\xi) \mid M\right\}.$$

Let us start from:

$$\begin{aligned}\rho &= \sum_{n\geq 1} \frac{\mu(n)}{\varphi(mn)} \frac{\#\mathcal{B}(mn)}{\#\mathcal{A}(mn)} \\ &= \sum_{\substack{n\geq 1 \\ (n,2)=1}} \frac{\mu(n)}{\varphi(mn)} \frac{\#\mathcal{B}(mn)}{\#\mathcal{A}(mn)} + \sum_{\substack{n\geq 1 \\ (n,2)=1}} \frac{\mu(2n)}{\varphi(2mn)} \frac{\#\mathcal{B}(2mn)}{\#\mathcal{A}(2mn)} \\ &= \rho_o - \rho_e.\end{aligned}$$

First we compute ρ_o.

$$\rho_o = \sum_{\substack{n\geq 1 \\ (n,2)=1}} \frac{\mu(n)}{\varphi(mn)} \frac{\#\mathcal{B}(mn)}{\#\mathcal{A}(mn)} = \sum_{\xi\in\mathcal{C}(2^{v_2(m)})} \sum_{\substack{(n,2)=1 \\ s(\xi)\mid mn}} \frac{\mu(n)}{\varphi(mn)\#\mathcal{A}(mn)}.$$

Let $g = s(\xi)/\gcd(s(\xi), m)$ and note that the condition $s(\xi) \mid nm$ above is equivalent to $n = kg$ where $\gcd(2g, k) = 1$. Therefore

$$\begin{aligned}\rho_o &= \sum_{\substack{\xi\in\mathcal{C}(2^{v_2(m)}) \\ g \text{ odd}}} \mu(g) \sum_{\substack{k\in\mathbb{N} \\ (k,2g)=1}} \frac{\mu(k)}{\varphi(kgm)\#\mathcal{A}(kgm)} \\ &= \frac{1}{\varphi(m)\#\mathcal{A}(m)} \sum_{\substack{\xi\in\mathcal{C}(v_2(m)) \\ g \text{ odd}}} \frac{\mu(g)}{\varphi(g)\#\mathcal{A}(g)} \sum_{\substack{k\in\mathbb{N} \\ (k,2g)=1}} \mu(k) \frac{\varphi((k,mg))\#\mathcal{A}(gm)}{\varphi(k)(k,mg)\#\mathcal{A}(kgm)}\end{aligned}$$

where we used the following identity:

$$\varphi(kgm)\#\mathcal{A}(kgm) = (\varphi(m)\#\mathcal{A}(m) \times \varphi(g)\#\mathcal{A}(g)) \times \left(\varphi(k)\frac{(k,gm)}{\varphi((k,gm))}\frac{\#\mathcal{A}(kgm)}{\#\mathcal{A}(gm)}\right).$$

For gm fixed, the function

$$\left(\varphi(k)\frac{(k,gm)}{\varphi((k,gm))}\frac{\#\mathcal{A}(kgm)}{\#\mathcal{A}(gm)}\right)$$

is multiplicative in k. Hence

$$\rho_o = \frac{1}{\varphi(m)\#\mathcal{A}(m)} \sum_{\substack{\xi\in\mathcal{C}(2^{v_2(m)}) \\ g \text{ odd}}} \frac{\mu(g)}{\varphi(g)\#\mathcal{A}(g)} \prod_{\substack{l>2 \\ l\nmid g}} \left(1 - \frac{\varphi((l,m))\#\mathcal{A}(l^{v_l(m)})}{(l-1)(l,m)\#\mathcal{A}(l^{1+v_l(m)})}\right)$$

$$= \frac{1}{\varphi(m)\#\mathcal{A}(m)} \prod_{\substack{l>2 \\ l\nmid m}} \left(1 - \frac{1}{(l-1)\#\mathcal{A}(l)}\right) \times \prod_{\substack{l>2 \\ l\mid m}} \left(1 - \frac{\#\mathcal{A}(l^{v_l(m)})}{l\#\mathcal{A}(l^{1+v_l(m)})}\right) \times$$

$$\times \sum_{\substack{\xi\in\mathcal{C}(2^{v_2(m)}) \\ g \text{ odd}}} \frac{\mu(g)}{\varphi(g)\#\mathcal{A}(l^g)} \prod_{l\mid g} \left(1 - \frac{\varphi((l,m))\#\mathcal{A}(l^{v_l(m)})}{(l-1)(l,m)\#\mathcal{A}(l^{1+v_l(m)})}\right)^{-1}.$$

Because $g = s(\xi)/\gcd(s(\xi), m)$, we have the identity

$$\frac{\mu(g)}{\varphi(g)\#\mathcal{A}(g)} \prod_{l\mid g} \left(1 - \frac{\varphi((l,m))\#\mathcal{A}(l^{v_l(m)})}{(l-1)(l,m)\#\mathcal{A}(l^{1+v_l(m)})}\right)^{-1} = \prod_{\substack{l\mid s(\xi) \\ l\nmid m}} \frac{-1}{(l-1)\#\mathcal{A}(l)-1}.$$

If we set

$$\mathfrak{A}_\Gamma^{(m)} = \frac{1}{\varphi(m)\#\mathcal{A}(m)} \prod_{\substack{l>2 \\ l\nmid m}} \left(1 - \frac{1}{(l-1)\#\mathcal{A}(l)}\right) \times \prod_{\substack{l>2 \\ l\mid m}} \left(1 - \frac{\#\mathcal{A}(l^{v_l(m)})}{l\#\mathcal{A}(l^{1+v_l(m)})}\right),$$

then

$$\rho_o = \mathfrak{A}_\Gamma^{(m)} \times \sum_{\substack{\xi\in\mathcal{C}(2^{v_2(m)}) \\ \frac{s(\xi)}{(m,s(\xi))} \text{ odd}}} \prod_{\substack{l\mid s(\xi) \\ l\nmid m}} \left(\frac{-1}{(l-1)\#\mathcal{A}(l)-1}\right).$$

A similar calculation shows that

$$\rho_e = \mathfrak{A}_\Gamma^{(2m)} \times \sum_{\substack{\xi\in\mathcal{C}(2^{1+v_2(m)}) \\ \frac{s(\xi)}{(m,s(\xi))} \text{ odd}}} \prod_{\substack{l\mid s(\xi) \\ l\nmid 2m}} \left(\frac{-1}{(l-1)\#\mathcal{A}(l)-1}\right).$$

We note that

$$\frac{\mathfrak{A}_\Gamma^{(2m)}}{\mathfrak{A}_\Gamma^{(m)}} = \frac{\#\mathcal{A}(2^{v_2(m)})}{(2,m)\#\mathcal{A}(2^{1+v_2(m)})}.$$

Therefore, subtracting the two expressions for ρ_o and for ρ_e, we obtain

$$\rho = \mathfrak{A}_\Gamma^{(m)} \left(\sum_{\substack{\xi \in \mathcal{C}(2^{v_2(m)}) \\ \frac{s(\xi)}{(m,s(\xi))} \text{ odd}}} \prod_{\substack{l \mid s(\xi) \\ l \nmid m}} \left(\frac{-1}{(l-1)\#\mathcal{A}(l) - 1} \right) - \right.$$

$$\left. \frac{\#\mathcal{A}(2^{v_2(m)})}{(2,m)\#\mathcal{A}(2^{1+v_2(m)})|} \sum_{\substack{\xi \in \mathcal{C}(2^{1+v_2(m)}) \\ \frac{s(\xi)}{(2m,s(\xi))} \text{ odd}}} \prod_{\substack{l \mid s(\xi) \\ l \nmid 2m}} \left(\frac{-1}{(l-1)\#\mathcal{A}(l) - 1} \right) \right). \tag{3.7}$$

3.4 Recovering results of Murata and Cangelmi & Pappalardi

In this section, we show how our formula is a generalization of the formulas of Murata and Cangelmi & Pappalardi.

3.4.1 Recovering Murata's result

If $a \in \mathbb{N}^+$ squarefree, then from a work of Murata [14] we have

$$c_{a,m} = d_{a,m} \left(1 + \epsilon_{a,m} \prod_{\substack{l \mid a \\ l \nmid m}} \frac{-1}{l^2 - l - 1} \right)$$

where

$$d_{a,m} = \frac{1}{m\varphi(m)} \prod_l \left(1 - \frac{\varphi((l,m))}{l(l-1) \cdot (l,m)} \right)$$

and

$$\epsilon_{a,m} = \begin{cases} 1 & \text{if } a \equiv 1 \bmod 4, 2 \mid m \\ & \text{if } a \equiv 3 \bmod 4, 4 \mid m \\ & \text{if } a \equiv 2 \bmod 4, 8 \mid m \\ -1 & \text{if } a \equiv 1 \bmod 4, 2 \nmid m \\ -1/3 & \text{if } a \equiv 2 \bmod 4, 4 \| m \\ & \text{if } a \equiv 3 \bmod 4, 2 \| m \\ 0 & \text{if } a \equiv 2 \bmod 4, 4 \nmid m \\ & \text{if } a \equiv 3 \bmod 4, 2 \nmid m \end{cases}$$

In order to compute ρ, we set $\Gamma = \langle a \rangle$, with $a \in \mathbb{N}^+$ squarefree. Then $\#A(m) = \#(\Gamma\mathbb{Q}^{*m}/\mathbb{Q}^{*m}) = m$. So

$$\begin{aligned} \mathfrak{A}_\Gamma^{(m)} &= \frac{1}{m\varphi(m)} \prod_{\substack{l>2 \\ l \nmid m}} \left(1 - \frac{1}{l(l-1)}\right) \times \prod_{\substack{l>2 \\ l \mid m}} \left(1 - \frac{l^{v_l(m)}}{l^{2+v_l(m)}}\right) \\ &= \frac{1}{m\varphi(m)} \prod_{\substack{l>2 \\ l \nmid m}} \left(1 - \frac{1}{l(l-1)}\right) \times \prod_{\substack{l>2 \\ l \mid m}} \left(1 - \frac{1}{l^2}\right) \end{aligned}$$

and

$$\frac{\#\mathcal{A}(2^{v_2(m)})}{(2,m)\#\mathcal{A}(2^{1+v_2(m)})|} = \frac{2^{v_2(m)}}{(2,m)2^{1+v_2(m)}} = \frac{1}{2(2,m)}.$$

It is obvious that

$$\left(1 - \frac{1}{2(2,m)}\right) \mathfrak{A}_\Gamma^{(m)} = d_{a,m}.$$

Let

$$\mathcal{D}_1 = \left\{ \xi \in \mathcal{C}(2^{v_2(m)}) : \frac{s(\xi)}{(m, s(\xi))} \text{ odd} \right\}$$

and

$$\mathcal{D}_2 = \left\{ \xi \in \mathcal{C}(2^{1+v_2(m)}) : \frac{s(\xi)}{(2m, s(\xi))} \text{ odd} \right\}.$$

Then

$$\mathcal{D}_1 = \begin{cases} \left\{\mathbb{Q}^{2^{v_2(m)}}, a^{2^{v_2(m)-1}}\mathbb{Q}^{2^{v_2(m)}}\right\} & \text{if } 2 \mid m, a \equiv 1 \bmod 4 \\ & \text{if } 4 \mid m, a \equiv 3 \bmod 4 \\ & \text{if } 8 \mid m, a \equiv 2 \bmod 4 \\ \{\mathbb{Q}^{2^{v_2(m)}}\} & \text{otherwise} \end{cases}$$

while

$$\mathcal{D}_2 = \begin{cases} \left\{\mathbb{Q}^{2^{v_2(m)+1}}, a^{2^{v_2(m)}}\mathbb{Q}^{2^{v_2(m)+1}}\right\} & \text{if } a \equiv 1 \bmod 4 \\ & \text{if } 2 \mid m, a \equiv 3 \bmod 4 \\ & \text{if } 4 \mid m, a \equiv 2 \bmod 4 \\ \left\{\mathbb{Q}^{2^{v_2(m)+1}}\right\} & \text{otherwise.} \end{cases}$$

We note that if a and m satisfy the conditions such that $\#\mathcal{D}_1 = 2$, then $\#\mathcal{D}_2 = 2$.

Case 1: $\mathcal{D}_1 = \left\{\mathbb{Q}^{2^{v_2(m)}}\right\}$ and $\mathcal{D}_2 = \left\{\mathbb{Q}^{2^{v_2(m)+1}}\right\}$. So

$$\rho = \frac{1}{m\varphi(m)} \prod_{\substack{l>3 \\ l\nmid m}} \left(1 - \frac{1}{l(l-1)}\right) \prod_{\substack{l>3 \\ l\mid m}} \left(1 - \frac{1}{l^2}\right) \left(1 - \frac{1}{(2,m)2}\right).$$

This case includes:

- m odd and $a \equiv 3 \pmod 4$;
- $4 \nmid m$ and $a \equiv 2 \pmod 4$.

Case 2: $\mathcal{D}_1 = \left\{\mathbb{Q}^{2^{v_2(m)}}\right\}$ and $\mathcal{D}_2 = \left\{\mathbb{Q}^{2^{v_2(m)+1}}, a^{2^{v_2(m)}}\mathbb{Q}^{2^{v_2(m)+1}}\right\}$.

- If m odd and $a \equiv 1 \pmod 4$, then

$$\rho = \frac{1}{m\varphi(m)} \prod_{\substack{l>3 \\ l\nmid m}} \left(1 - \frac{1}{l(l-1)}\right) \prod_{\substack{l>3 \\ l\mid m}} \left(1 - \frac{1}{l^2}\right) \left(\frac{1}{2} - \frac{1}{2} \prod_{\substack{l\mid a \\ l\nmid m}} \frac{-1}{l(l-1)-1}\right).$$

- If $4\|m$ and $a \equiv 2 \pmod 4$ or $2\|m$ and $a \equiv 3 \pmod 4$

$$\rho = \frac{1}{m\varphi(m)}\, T(3,m) \left(1 - \frac{1}{3} \prod_{\substack{l|a \\ l\nmid m}} \frac{-1}{l(l-1)-1} \right)$$

where

$$T(p,m) = \left(\frac{3}{4}\right) \prod_{\substack{l>p \\ l\nmid m}} \left(1 - \frac{1}{l(l-1)}\right) \prod_{\substack{l>p \\ l|m}} \left(1 - \frac{1}{l^2}\right).$$

Case 3: $\mathcal{D}_1 = \left\{ \mathbb{Q}^{2^{v_2(m)}}, a^{2^{v_2(m)-1}} \mathbb{Q}^{2^{v_2(m)}} \right\}$ and $\mathcal{D}_2 = \left\{ \mathbb{Q}^{2^{v_2(m)+1}} \right\}$. Then

$$\begin{aligned} \rho &= \frac{1}{m\varphi(m)}\, T(3,m) \left(1 + \frac{1-\frac{1}{4}}{1-\frac{1}{4}} \prod_{\substack{l|a \\ l\nmid m}} \frac{-1}{l(l-1)-1} \right) \\ &= \frac{1}{m\varphi(m)}\, T(3,m) \left(1 + \prod_{\substack{l|a \\ l\nmid m}} \frac{-1}{l(l-1)-1} \right). \end{aligned}$$

This case include:

- $8|m$ and $a \equiv 2 \pmod 4$;
- $4|m$ and $a \equiv 3 \pmod 4$;
- $2\|m$ and $a \equiv 3 \pmod 4$.

Therefore, the formulas always agree.

3.4.2 Recovering result of Cangelmi & Pappalardi

The value of the costant δ_Γ is

$$A_\Gamma \left(1 - \frac{1}{\#\mathcal{A}(2)} \sum_{\xi \in \mathcal{F}(2)} \mu(|s(\xi)|) \prod_{l | s(\xi)} \frac{1}{(l-1)\#\mathcal{A}(l) - 1} \right)$$

where

$$A_\Gamma = \prod_{l>2} \left(1 - \frac{1}{\#\mathcal{A}(l)(l-1)} \right),$$

and

$$\mathcal{F}(2) = \{ \xi \in \mathcal{A}(2) : \ s(\xi) \equiv 1 \pmod 4 \}.$$

Since $m = 1$, we have that $\#A(2^{v_2(m)}) = \#C(2^{v_2(m)}) = 1$ and the condition $s(\xi)/(2m, s(\xi))$ odd is equivalent to $s(\xi) \equiv 1 \pmod 4$. Then

$$\{ \xi \in \mathcal{C}(2) : \ s(\xi) \text{ odd} \} = \mathcal{F}(2).$$

Therefore

$$\begin{aligned} \rho(\Gamma, 1) &= \mathfrak{A}_\Gamma^{(1)} \left(1 - \frac{1}{\#\mathcal{A}(2)} \sum_{\xi \in \mathcal{F}(2)} \prod_{\substack{l | s(\xi) \\ l>2}} \left(\frac{-1}{(l-1)\#\mathcal{A}(l) - 1} \right) \right) \\ &= \mathfrak{A}_\Gamma^{(1)} \left(1 - \frac{1}{\#\mathcal{A}(2)} \sum_{\xi \in \mathcal{F}(2)} \mu(|s(\xi)|) \prod_{l | s(\xi)} \frac{1}{(l-1)\#\mathcal{A}(l) - 1} \right) \end{aligned}$$

where

$$\mathfrak{A}_\Gamma^{(1)} = \prod_{l>2} \left(1 - \frac{1}{(l-1)\#\mathcal{A}(l)} \right).$$

4. SOME COMPUTATIONS OF $\rho(\Gamma, M)$

Let $\Gamma \subseteq \mathbb{Q}^+$ as in Theorem 24 with $s = \operatorname{rank}(\Gamma)$, support $\mathcal{S}_\Gamma$ and $\#\mathcal{S}_\Gamma = r$. In this chapter we give an explicit computation of $\rho(\Gamma, m)$ in the simple case of $\Gamma = \langle q_1, q_2 \rangle$ and $m = p^\alpha$ prime. We have:

$$\rho(\Gamma, m) = \mathfrak{A}_\Gamma^{(m)} \left(\sum_{\substack{\xi \in \mathcal{C}(2^{v_2(m)}) \\ \frac{s(\xi)}{(m, s(\xi))} \text{ odd}}} \prod_{\substack{l \mid s(\xi) \\ l \nmid m}} \left(\frac{-1}{(l-1)\#\mathcal{A}(l) - 1} \right) - \right.$$

$$\left. \frac{\#\mathcal{A}(2^{v_2(m)})}{(2, m)\#\mathcal{A}(2^{1+v_2(m)})|} \sum_{\substack{\xi \in \mathcal{C}(2^{1+v_2(m)}) \\ \frac{s(\xi)}{(2m, s(\xi))} \text{ odd}}} \prod_{\substack{l \mid s(\xi) \\ l \nmid 2m}} \left(\frac{-1}{(l-1)\#\mathcal{A}(l) - 1} \right) \right)$$

where

$$\mathfrak{A}_\Gamma^{(m)} = \frac{1}{\varphi(m)\#\mathcal{A}(m)} \prod_{\substack{l > 2 \\ l \nmid m}} \left(1 - \frac{1}{(l-1)\#\mathcal{A}(l)} \right) \times \prod_{\substack{l > 2 \\ l \mid m}} \left(1 - \frac{\#\mathcal{A}(l^{v_l(m)})}{l\#\mathcal{A}(l^{1+v_l(m)})} \right).$$

By Lemma 17, we have:

$$\#\mathcal{A}(M) \ = \ \frac{M^s}{(M^s, \Delta_1(\Gamma) M^{s-1}, \ldots, \Delta_s(\Gamma))}$$

where $\Delta_i(\Gamma)$ are the invariants defined in Section 2.1. We put $\Delta_i = \Delta_i(\Gamma)$. So, we have:

$$\#\mathcal{A}(p^\alpha) \ = \ \begin{cases} p^{\alpha s}, & \text{if } p \not\mid \Delta_i(\Gamma) \ \forall\, i = 1, \ldots, s \\ p^{\alpha i_0 + t_{p^\alpha}}, & \text{otherwise} \end{cases} \tag{4.1}$$

where $i_0 = \min\{i = 1, \dots, s : \ p|\Delta_i\}$, $t_{p^\alpha} = \min(v_p(\Delta_{i_0}), \alpha)$. We need to distinguish two cases: $p = 2$ and $p > 3$.

4.1 Computation of $\rho(\Gamma, p^\alpha)$

In this case, we have that $\#A(2^{v_2(m)}) = \#C(2^{v_2(m)}) = 1$ and the condition $s(\xi)/(2m, s(\xi))$ odd is equivalent to $s(\xi) \equiv 1 \pmod 4$. We define

$$\mathcal{F}(2) = \{\xi \in \mathcal{C}(2) : \ s(\xi) \equiv 1 \pmod 4\}.$$

Then:

$$\begin{aligned}\rho(\Gamma, p^\alpha) &= \mathfrak{A}_\Gamma^{(p^\alpha)} \left(1 - \frac{1}{\#\mathcal{A}(2)} \sum_{\xi \in \mathcal{F}(2)} \prod_{\substack{l | s(\xi) \\ l \neq p}} \left(\frac{-1}{(l-1)\#\mathcal{A}(l) - 1}\right)\right) \\ &= \mathfrak{A}_\Gamma^{(p^\alpha)} \left(1 - \frac{1}{\#\mathcal{A}(2)} \sum_{\xi \in \mathcal{F}(2)} \mu(|s(\xi)|) \prod_{\substack{l | s(\xi) \\ l \neq p}} \left(\frac{1}{(l-1)\#\mathcal{A}(l) - 1}\right)\right)\end{aligned}$$

where

$$\mathfrak{A}_\Gamma^{(p^\alpha)} = \frac{1}{p^{\alpha-1}(p-1)\#\mathcal{A}(p^\alpha)} \times \left(1 - \frac{\#\mathcal{A}(p^\alpha)}{p\#\mathcal{A}(p^{\alpha+1})}\right) \prod_{l \neq 2,p} \left(1 - \frac{1}{(l-1)\#\mathcal{A}(l)}\right).$$

In particular, by (4.1) we have:

$$\mathfrak{A}_\Gamma^{(p^\alpha)} = \mathfrak{B}_\Gamma^{(p^\alpha)} \prod_{\substack{l \neq 2,p \\ l \not| \Delta_i \ i=1,\dots,s}} \left(1 - \frac{1}{(l-1)l^s}\right) \prod_{\substack{l \neq 2,p \\ l | \Delta_i}} \left(1 - \frac{1}{(l-1)l^{i_0 + t_l}}\right)$$

where

$$\mathfrak{B}_\Gamma^{(p^\alpha)} = \begin{cases} \frac{1}{p^{\alpha(s+1)-1}(p-1)} \times \left(1 - \frac{1}{p^{s+1}}\right) & \text{if } p \not| \Delta_i(\Gamma) \ \forall\, i = 1, \dots, s \\ \frac{1}{p^{\alpha(s+1)-1}(p-1)} \times \left(1 - \frac{1}{p^{1+i_0+(t_{p^{(\alpha+1)}} - t_{p^\alpha})}}\right) & \text{otherwise.} \end{cases}$$

Now we must compute $\mathcal{F}(2)$. As in Section 2.2, we introduce a new set with the same cardinality of $\mathcal{F}(2)$. With the same notation of Section 2.2 let

$$\mathcal{H}_2 \;=\; \{\varepsilon \in \mathbb{F}_2^r :\; \varepsilon \in SLC(A(\Gamma), 2) \text{ and } s(P_0(\varepsilon)) \equiv 1 \pmod 4\}.$$

It is clear that $\#\mathcal{H}_2 = \#\mathcal{F}_2$ (the argument is the same of Lemma 19).

Examples

Let $\Gamma = \langle q_1, q_2\rangle \subseteq \mathbb{Q}^+$ with q_i primes and $\operatorname{rank}(\Gamma) = 2$. We want to compute $\rho(\Gamma, p)$.

It is clear the following.

Claim. *With the same notation of Section 2.2, if $\varepsilon \in \mathcal{H}_2$ then holds all the following conditions:*

A1 $d_1 = 0$*;*

A2 $d_2 = d_2^{\varepsilon}$*;*

A3 $d_3^{\varepsilon} \geq 1 + d_2$*;*

1. $\Gamma = \langle 2, q\rangle$, with $q \equiv 3 \pmod 4$.

   In this case, we have that $A(\Gamma)$ is the identity matrix and all conditions of the Claim are satisfied, but $q \equiv 3 \pmod 4$ and so $\#\mathcal{H}_2 = 1$. Then:

   $$\rho(\Gamma, p) \;=\; \frac{p^3 - 1}{p^5(p-1)} \times \left(1 - \frac{1}{\#\mathcal{A}(2)}\right) \prod_{l \neq 2,p} \left(1 - \frac{1}{l^2(l-1)}\right).$$

   We show the case of $\Gamma = \langle 2, q\rangle$ with $q \leq 100$, $q \equiv 3 \pmod 4$ and $p = 3, 5$.

   (a) $\Gamma = \langle 2, q\rangle$, with $q \leq 100$, $q \equiv 3 \pmod 4$ and $p = 3$. In this case the value of $\rho(\Gamma, 3)$ is constant for all q as above:

   $$\rho(\Gamma, 3) \;=\; 0.039501\ldots$$

Computation of $\rho(\Gamma, 3)$, with $\Gamma = \langle 2, q\rangle$					
q	$N_\Gamma(10^7, 3)$	$\rho(\langle 2, q\rangle, 3)$	q	$N_\Gamma(10^7, 3)$	$\rho(\langle 2, q\rangle, 3)$
3	0.03958	0.03950	47	0.03944	0.03950
7	0.03957	0.03950	59	0.03942	0.03950
11	0,28912	0.03950	67	0.03930	0.03950
19	0.03947	0.03950	71	0.03967	0.03950
23	0.03961	0.03950	79	0.03965	0.03950
31	0.03943	0.03950	83	0.03954	0.03950
43	0.03926	0.03950			

(b) $\Gamma = \langle 2, q\rangle$, with $q \leq 100$, $q \equiv 3 \pmod 4$ and $p = 5$. Also in this case the value of $\rho(\Gamma, 5)$ is constant for all q as above:

$$\rho(\Gamma, 5) \;=\; 0.006989\ldots$$

Computation of $\rho(\Gamma, 5)$, with $\Gamma = \langle 2, q\rangle$					
q	$N_\Gamma(10^7, 5)$	$\rho(\langle 2, q\rangle, 5)$	q	$N_\Gamma(10^7, 5)$	$\rho(\langle 2, q\rangle, 5)$
3	0.00704	0.00698	47	0.00678	0.00698
7	0.00693	0.00698	59	0.00689	0.00698
11	0.00706	0.00698	67	0.00696	0.00698
19	0.00707	0.00698	71	0.00697	0.00698
23	0.00696	0.00698	79	0.00700	0.00698
31	0.00687	0.00698	83	0.00693	0.00698
43	0.00708	0.00698			

2. $\Gamma = \langle q_1, q_2\rangle$, with $q_1 \equiv 1$, $q_2 \equiv 2, 3 \pmod 4$.

In this case, we have that $A(\Gamma)$ is the identity matrix and all conditions of the Claim are satisfied but only $q_1 \equiv 1 \pmod 4$ and so $\#\mathcal{H}_2 = 2$. Then:

$$\rho(\Gamma, p) \;=\; \frac{p^3 - 1}{p^5(p-1)} \times \prod_{l \neq 2, p} \left(1 - \frac{1}{l^2(l-1)}\right) \times \left(1 - \frac{1}{\#\mathcal{A}(2)} + \frac{A(q_1)}{\#\mathcal{A}(2)}\right)$$

where

$$A(q) = \frac{1}{q^2(q-1) - 1}\,.$$

(a) $\Gamma = \langle 5, q\rangle$ with $q \leq 100$, $q \equiv 3 \pmod 4$ and $p = 3$. In this case the value of $\rho(\Gamma, 3)$ is constant for all q as above:

$$\rho(\Gamma, 3) \;=\; 0.03964\ldots$$

Computation of $\rho(\Gamma, 3)$, with $\Gamma = \langle 5, q\rangle$ and $q \equiv 3 \pmod 4$					
q	$N_\Gamma(10^7, 3)$	$\rho(\langle 5, q\rangle, 3)$	q	$N_\Gamma(10^7, 3)$	$\rho(\langle 5, q\rangle, 3)$
3	0.03957	0.03964	47	0.03946	0.03964
7	0.03967	0.03964	59	0.03964	0.03964
11	0.03952	0.03964	67	0.03950	0.03964
19	0.03949	0.03964	71	0.03949	0.03964
23	0.03954	0.03964	79	0.03981	0.03964
31	0.03948	0.03964	83	0.03985	0.03964
43	0.03947	0.03964			

(b) $\Gamma = \langle l, q\rangle$ with $l = 2, 3$, $q \leq 50$, $q \equiv 1 \pmod 4$ and $p = 3$. In this case the value of $\rho(\Gamma, 3)$ is not a constant:

$$\rho(\Gamma, 3) \;=\; \frac{13}{243} \times \left[1 - \frac{1}{4}\left(1 - A(q)\right)\right] \times 0.984707\ldots$$

Computation of $\rho(\Gamma, 3)$, with $\Gamma = \langle l, q\rangle$, $l = 2, 3$ and $q \equiv 1 \pmod 4$					
q	$N_\Gamma(10^7, 3)$	$\rho(\langle 2, q\rangle, 3)$	q	$N_\Gamma(10^7, 3)$	$\rho(\langle 3, q\rangle, 3)$
5	0.03968	0.03964	5	0.03957	0.03964
13	0.03979	0.03951	13	0.03953	0.03951
17	0.03954	0.03951	17	0.03967	0.03951
29	0.03966	0.03951	29	0.03950	0.03951
37	0.03959	0.03951	37	0.03981	0.03951
41	0.03954	0.03951	41	0.03985	0.03951

3. $\Gamma = \langle q_1, q_2\rangle$, with $q_i \equiv 1 \pmod 4$.

In this case, we have that $A(\Gamma)$ is the identity matrix and all conditions of the Claim are satisfied and $q_i \equiv 1 \pmod 4$ and so $\#\mathcal{H}_2 = 4$. Then:

$$\rho(\Gamma, p) \;=\; \frac{p^3 - 1}{p^5(p-1)} \times \prod_{l \neq 2, p} \left(1 - \frac{1}{l^2(l-1)}\right) \times \left(1 - \frac{1}{\#\mathcal{A}(2)} + \frac{1}{\#\mathcal{A}(2)}\left(A(q_1) + A(q_2) - A(q_1)A(q_2)\right)\right).$$

$\Gamma = \langle q_1, q_2 \rangle$, $q_i \leq 50$, $q_i \equiv 1 \pmod 4$ and $p = 3$. We have:

$$\rho(\Gamma, 3) \;=\; \frac{13}{243}\left[1 - \frac{1}{4}\left(1 - A(q_1) - A(q_2) + A(q_1)A(q_2)\right)\right] \times 0.984707\ldots$$

Computation of $\rho(\Gamma, 3)$, with $\Gamma = \langle q_1, q_2 \rangle$ and $q_i \equiv 1 \pmod 4$							
q_1	q_2	$N_\Gamma(10^7, 3)$	$\rho(\langle q_1, q_2 \rangle, 3)$	q_1	q_2	$N_\Gamma(10^7, 3)$	$\rho(\langle q_1, q_2 \rangle, 3)$
5	13	0.03968	0.03964	13	41	0.03955	0.03951
5	17	0.03956	0.03964	17	29	0.03979	0.03951
5	29	0.03948	0.03964	17	37	0.03948	0.03951
5	37	0.03959	0.03964	17	41	0.03925	0.03951
5	41	0.03959	0.03964	29	37	0.03950	0.03951
13	17	0.03964	0.03951	29	41	0.03934	0.03951
13	29	0.03975	0.03951	37	41	0.03955	0.03951
13	37	0.03925	0.03951				

4. $\Gamma = \langle q_1, q_2 \rangle$, with $q_i \equiv 3 \pmod 4$.

In this case, we have that $A(\Gamma)$ is the identity matrix and all conditions of the Claim are satisfied and $q_1 q_2 \equiv 1 \pmod 4$ and so $\#\mathcal{H}_2 = 2$. Then:

$$\rho(\Gamma, p) \;=\; \frac{p^3 - 1}{p^5(p-1)} \times \prod_{l \neq 2, p} \left(1 - \frac{1}{l^2(l-1)}\right) \times \left(1 - \frac{1}{\#\mathcal{A}(2)} + \frac{1}{\#\mathcal{A}(2)} A(q_1)A(q_2)\right).$$

$\Gamma = \langle q_1, q_2 \rangle$, $q_i \leq 50$, $q_i \equiv 3 \pmod 4$ and $p = 3$. We have:

$$\rho(\Gamma, 3) \;=\; \frac{13}{243}\left[1 - \frac{1}{4}\left(1 - A(q_1)A(q_2)\right)\right] \times 0.984707\ldots$$

Computation of $\rho(\Gamma, 3)$, with $\Gamma = \langle q_1, q_2 \rangle$ and $q_i \equiv 3 \pmod 4$							
q_1	q_2	$N_\Gamma(10^7, 3)$	$\rho(\langle q_1, q_2 \rangle, 3)$	q_1	q_2	$N_\Gamma(10^7, 3)$	$\rho(\langle q_1, q_2 \rangle, 3)$
3	7	0.03961	0.03951	3	43	0.03964	0.03950
3	11	0.03945	0.03951	3	47	0.03957	0.03950
3	19	0.03972	0.03951	7	11	0.03963	0.03950
3	23	0.03954	0.03950	7	19	0.03956	0.03950
3	31	0.03947	0.03950	7	23	0.03947	0.03950

Computation of $\rho(\Gamma, 3)$, with $\Gamma = \langle q_1, q_2 \rangle$ and $q_i \equiv 3 \pmod 4$							
q_1	q_2	$N_\Gamma(10^7, 3)$	$\rho(\langle q_1, q_2 \rangle, 3)$	q_1	q_2	$N_\Gamma(10^7, 3)$	$\rho(\langle q_1, q_2 \rangle, 3)$
7	31	0.039650	0.0395	19	31	0.03924	0.03950
7	43	0.03935	0.03950	19	43	0.03962	0.03950
7	47	0.03960	0.03950	19	47	0.03948	0.03950
11	19	0.03959	0.03950	23	31	0.03939	0.03950
11	23	0.03943	0.03950	23	43	0.03940	0.03950
11	31	0.03959	0.03950	23	47	0.03927	0.03950
11	43	0.03957	0.03950	31	43	0.03947	0.03950
11	47	0.03932	0.03950	31	47	0.03902	0.03950
19	23	0.03952	0.03950	43	47	0.03920	0.03950

4.2 Computation of $\rho(\Gamma, 2)$

In this case, we have that the condition $s(\xi)/(2, s(\xi))$ odd is equivalent to $s(\xi) \equiv 1 \pmod 4$ and the condition $s(\xi)/(4, s(\xi))$ odd is equivalent to $s(\xi) \equiv 1, 3 \pmod 4$. So we define:

$$\mathcal{F}(2) = \{\xi \in C(2) : \ s(\xi) \equiv 1 \pmod 4\},$$
$$\mathcal{F}(4) = \{\xi \in C(4) : \ s(\xi) \equiv 1, 3 \pmod 4\}.$$

The value of ρ is the following:

$$\rho(\Gamma, 2) = \mathfrak{A}_\Gamma^{(2)} \left(\sum_{\xi \in \mathcal{F}(2)} \prod_{l | s(\xi)} \left(\frac{-1}{(l-1)\#\mathcal{A}(l) - 1} \right) - \frac{\#\mathcal{A}(2)}{2\#\mathcal{A}(4)} \sum_{\xi \in \mathcal{F}(4)} \prod_{l | s(\xi)} \left(\frac{-1}{(l-1)\#\mathcal{A}(l) - 1} \right) \right)$$

where

$$\mathfrak{A}_\Gamma^{(2)} = \frac{1}{\#\mathcal{A}(2)} \prod_{l > 2} \left(1 - \frac{1}{(l-1)\#\mathcal{A}(l)} \right).$$

As above, we have that $\#\mathcal{F}(2^e) = \#\mathcal{H}_{2^e}$ with $e = 1, 2$, so

$$\rho(\Gamma, 2) = \mathfrak{A}_\Gamma^{(2)} \left(\sum_{\varepsilon \in \mathcal{H}_2} \prod_{l | s(P_0(\varepsilon))} \left(\frac{-1}{(l-1)\#\mathcal{A}(l) - 1} \right) - \frac{\#\mathcal{A}(2)}{2\#\mathcal{A}(4)} \sum_{\varepsilon \in \mathcal{H}_4} \prod_{l | s(P_0(\varepsilon))} \left(\frac{-1}{(l-1)\#\mathcal{A}(l) - 1} \right) \right).$$

The following Claim holds

Claim. *If $\varepsilon \in \mathcal{H}_4$ then holds all the following conditions:*

B1 $d_1 \leq 1$*;*

B2 $d_2 = d_2^\varepsilon$*;*

B3 $d_3^\varepsilon - d_2^\varepsilon \geq 2$*;*

Examples

Let $\Gamma = \langle q_1, q_2 \rangle$ with q_i primes. We want to compute $\rho(\Gamma, 2)$.
In this case, we have that

$$\mathfrak{A}_\Gamma^2 = \frac{1}{4} \prod_{l \neq 2} \left(1 - \frac{1}{l^2(l-1)} \right) = 0.232500\ldots$$

and $\#\mathcal{A}(2)/2\#\mathcal{A}(2) = 1/8$. We set $N_\Gamma(x, 2) = \mathcal{N}_\Gamma(x, 2)/\pi(x)$.

1. $\Gamma = \langle 2, q \rangle$, with $q \equiv 3 \pmod 4$.

   In this case, we have that $A(\Gamma)$ is the identity matrix and all conditions of the Claims are satisfied. In this case we have that $\#\mathcal{H}_2 = 1$ and $\#\mathcal{H}_4 = 2$.

   Then:

   $$\rho(\Gamma, 2) = \left[1 - \frac{1}{8} (1 - A(q)) \right] \times 0.232500\ldots$$

   where

   $$A(q) = \frac{1}{q^2(q-1) - 1}.$$

   We compute $\rho(\Gamma, 2)$ with $\Gamma = \langle 2, q \rangle$, with $q \leq 100$ and $q \equiv 3 \pmod 4$.

Computation of $\rho(\Gamma, 2)$, with $\Gamma = \langle 2, q\rangle$ and $q \equiv 3 \pmod 4$					
q	$N_\Gamma(10^7, 2)$	$\rho(\langle 2, q\rangle, 2)$	q	$N_\Gamma(10^7, 2)$	$\rho(\langle 2, q\rangle, 2)$
3	0.20545	0.20514	59	0.20363	0.20343
7	0.20345	0.20353	67	0.20341	0.20343
11	0.20370	0.20346	71	0.20345	0.20343
19	0.20344	0.20344	79	0.20346	0.20343
23	0.20375	0.20344	83	0.20371	0.20343
31	0.20368	0.20343	89	0.20422	0.20343
43	0.20344	0.20343	97	0.20331	0.20343
47	0.20351	0.20343			

2. $\Gamma = \langle q_1, q_2\rangle$, with $q_1 \equiv 1$, $q_2 \equiv 3 \pmod 4$.

   In this case, we have that $A(\Gamma)$ is the identity matrix and all conditions of the Claim are satisfied. In particular: $\#\mathcal{H}_2 = 2$ and $\#\mathcal{H}_4 = 4$.

$$\begin{aligned}\rho(\Gamma, 2) &= \mathfrak{A}_\Gamma^{(2)}\left[(1 - A(q_1)) - \frac{1}{8}\left(1 - A(q_1) - A(q_2) + A(q_1)A(q_2)\right)\right] \\ &= \frac{1}{8}\mathfrak{A}_\Gamma^{(2)}\left[7 - (7A(q_1) - A(q_2) + A(q_1)A(q_2))\right].\end{aligned}$$

   (a) $\Gamma = \langle 5, q\rangle$ with $q \leq 100$ and $q \equiv 3 \pmod 4$. In this case the value of ρ is the following:

$$\rho(\Gamma, 2) = \left[1 - \frac{1}{99} - \frac{1}{8}\left(1 - \frac{1}{99} - A(q) + \frac{1}{99}A(q)\right)\right] \times 0.2325\ldots$$

Computation of $\rho(\Gamma, 2)$, with $\Gamma = \langle 5, q\rangle$ and $q \equiv 3 \pmod 4$					
q	$N_\Gamma(10^7, 2)$	$\rho(\langle 5, q\rangle, 2)$	q	$N_\Gamma(10^7, 2)$	$\rho(\langle 5, q\rangle, 2)$
3	0.20311	20307	59	0.20121	0.20138
7	0.20156	0.20148	67	0.20141	0.20138
11	0.20167	0.20140	71	0.20149	0.20138
19	0.20117	0.20138	79	0.20139	0.20138
23	0.20141	0.20138	83	0.20144	0.20138
31	0.20146	0.20138	89	0.20166	0.20138
43	0.20113	0.20138	97	0.20135	0.20138
47	0.20098	0.20138			

(b) $\Gamma = \langle 3, q\rangle$ with $q \leq 100$ and $q \equiv 1 \pmod 4$. In this case the value of ρ is the following:

$$\rho(\Gamma, 2) = \left[1 - A(q) - \frac{1}{8}\left(1 - A(q) - \frac{1}{17} + \frac{1}{17}A(q)\right)\right] \times 0.2325\ldots$$

Computation of $\rho(\Gamma, 2)$, with $\Gamma = \langle 3, q\rangle$ and $q \equiv 1 \pmod 4$					
q	$N_\Gamma(10^7, 2)$	$\rho(\langle 3, q\rangle, 2)$	q	$N_\Gamma(10^7, 2)$	$\rho(\langle 3, q\rangle, 2)$
13	0.20495	0.20504	53	0.20547	0.20514
17	0.20535	0.20510	61	0.20329	0.20343
29	0.20540	0.20513	73	0.20531	0.20514
37	0.20519	0.20514	89	0.20534	0.20514
41	0.20519	0.20514	97	0.20550	0.20514

3. $\Gamma = \langle q_1, q_2\rangle$, with $q_i \equiv 1 \pmod 4$.

   In this case: $\#\mathcal{H}_2 = \#\mathcal{H}_4 = 4$.

$$\rho(\Gamma, 2) = \frac{7}{8}\mathfrak{A}_\Gamma^{(2)}\left[1 - (A(q_1) + A(q_2) - A(q_1)A(q_2))\right].$$

Computation of $\rho(\Gamma, 2)$, with $\Gamma = \langle q_1, q_2\rangle$ and $q_i \equiv 1 \pmod 4$							
q_1	q_2	$N_\Gamma(10^7, 2)$	$\rho(\langle q_1, q_2\rangle, 2)$	q_1	q_2	$N_\Gamma(10^7, 2)$	$\rho(\langle q_1, q_2\rangle, 2)$
5	13	0.20122	0.20128	13	41	0.20338	0.20333
5	17	0.20145	0.20133	17	29	0.20356	0.20338
5	29	0.20141	0.20137	17	37	0.20341	0.20338
5	37	0.20141	0.20137	17	41	0.20337	0.20339
5	41	0.20161	0.20137	29	37	0.20345	0.20342
13	17	0.20343	0.20329	29	41	0.20350	0.20342
13	29	0.20357	0.20332	37	41	0.20364	0.20343
13	37	0.20338	0.20333				

4. $\Gamma = \langle q_1, q_2 \rangle$, with $q_i \equiv 3 \pmod 4$.
   In this case: $\#\mathcal{H}_2 = 2$ and $\#\mathcal{H}_4 = 4$.

$$\rho(\Gamma, 2) = \frac{1}{8}\mathfrak{A}_\Gamma^{(2)} \left[(7 + A(q_1) + A(q_2) - 9A(q_1)A(q_2))\right].$$

Computation of $\rho(\Gamma, 2)$, with $\Gamma = \langle q_1, q_2 \rangle$ and $q_i \equiv 3 \pmod 4$							
q_1	q_2	$N_\Gamma(10^7, 2)$	$\rho(\langle q_1, q_2 \rangle, 2)$	q_1	q_2	$N_\Gamma(10^7, 2)$	$\rho(\langle q_1, q_2 \rangle, 2)$
3	7	0.20534	0.20519	11	23	0.20345	0.20346
3	11	0.20543	0.20515	11	31	0.20359	0.20346
3	19	0.20511	0.20514	11	43	0.20370	0.20346
3	23	0.20510	0.20514	11	47	0.20292	0.20346
3	31	0.20525	0.20514	19	23	0.20328	0.20344
3	43	0.20517	0.20514	19	31	0.20331	0.20344
3	47	0.20506	0.20514	19	43	0.20334	0.20344
7	11	0.20390	0.20355	19	47	0.20318	0.20344
7	19	0.20394	0.20354	23	31	0.20338	0.20344
7	23	0.20360	0.20353	23	43	0.20327	0.20344
7	31	0.20361	0.20353	23	47	0.20334	0.20334
7	43	0.20338	0.20353	31	43	0.20381	0.20343
7	47	0.20341	0.20353	31	47	0.20332	0.20343
11	19	0.20369	0.20346	43	47	0.20332	0.20343

BIBLIOGRAPHY

[1] ARTIN, E. , *Collected Papers*. Addison-Wesley, Reading, Mass., (1965).

[2] BUTSON, A.T. AND STEWART, B.M., *Systems of linear congruences*. Canad. J. Math. **7** (1955), 358–368.

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

[4] DELANGE, H., *Généralisation du théorème de Ikehara*. Ann. Sci. Ecole Norm. Sup. (3) **71** (1954), 213–242.

[5] HEATH–BROWN, D. R., *Artin's conjecture for primitive roots.* Quart. J. Math. Oxford **2** 37 (1986), 27–38.

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

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

[8] LANG, S., Algebra. Second edition. *Addison-Wesley Publishing Company, Advanced Book Program, Reading*, MA, 1984. xv+714.

[9] LENSTRA, H. W., JR., *On Artin's conjecture and Euclid's algorithm in global fields*. Invent. Math. **42** (1977), 201–224.

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

[11] MATTHEWS, K. R., *A generalisation of Artin's conjecture for primitive roots*. Acta Arith. **29** (1976), no. 2, 113–146.

[12] MOREE, P. *On primes p for which d divides* $\mathrm{ord}_p(g)$. Funct. Approx. Comment. Math. **33** (2005), 85–95.

[13] MOREE, P. AND STEVENHAGEN, P., *A two-variable Artin conjecture.* J. Number Theory **85** (2000), no. 2, 291–304.

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

[15] MURTY, M. R.. *Artin's conjecture for primitive roots* Math. Intelligencer, **10** (1988), no. 4, 59-67.

[16] PAPPALARDI, F., *Square free values of the order fuction*. New York J. Math **9** (2003), 331–344.

[17] PAPPALARDI, F., *The r-rank Artin Conjecture*. Math. Comp. **66** (1997), 853-868.

[18] SCHINZEL, A. AND SIERPINSKI, W., *Sur certaines hypothéses concernant les nombres premiers.* Acta Arith. **4** (1958), 185–208.

[19] SCHINZEL, A. AND WÒJCIK, J., *On a problem in elementary number theory.* Math. Proc. Cambridge Philos. Soc. **112** (1992), no. 2, 225–232.

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

[21] WAGSTAFF, S. S., JR., *Pseudoprimes and a generalization of Artin's conjecture.* Acta Arith. **41** (1982), no. 2, 141–150.

[22] WIERTELAK, K., *On the density of some sets of primes p, for which* $n|\operatorname{ord}_p a$. Funct. Approx. Comment. Math. **28** (2000), 237–241.

[23] WIERTELAK, K., *On the density of some sets of primes p, for which* $(ord_p b, n) = d$. Funct. Approx. Comment. Math. **21** (1992), 69-73.

[24] WÓJCIK, J., *On a problem in algebraic number theory.* Math. Proc. Cambridge Philos. Soc. **119** (1996), no. 2, 191–200.

ACKNOWLEDGMENTS

There are many people who I would like to thank.

First of all I would like to thank my advisor Francesco Pappalardi for having trusted me and supported me for all these years; without his help and guidance, this work would not exist.

I would also like to thanks my friends Anna S., Flavio P. and Valerio T. for their comments, suggestions and excellent proofreading skills.

I acknowledge the Dipartimento di Matematica di “Roma Tre” for the support given during the preparation of my thesis, in particular Prof. Lucia Caporaso, Prof. Marco Fontana and Prof. Francesca Tartarone.

Finally, I would like to thanks L.L.L. for his continuous encouragement, support and patience.

****

Un grazie particolare anche ad Antonella & Antonella, Andrea e Gaetano: molto più che amici... un pezzo di questo lavoro è anche vostro...