On Schinzel-Wójcik problem

by

Mohamed Anwar Mohamed Fouad

A PhD Thesis in Mathematics

Supervisored by

Prof. Francesco Pappalardi

Università degli Studi Roma Tre

Scuola Dottorale in Scienze Matematiche e Fisiche

Sezione Matematica

XXX ciclo

Roma, Italy, 2017

Contents

Abstract

The *Schinzel–Wójcik* problem consists in determming if
Given $a_1, \cdots, a_r \in \mathbb{Q}^* \setminus \{\pm 1\}$, there exist infinitely many primes p such that they have the same multiplicative order modulo p.

In this thesis, we prove, under the assumption of Hypothesis H of Schinzel, necessary and sufficient conditions for the existence of infinitely many primes modulo which all the given numbers are simultaneously primitive roots and we introduce a possible complete characterization, under *Hypothesis H* of the r–touples of rational numbers supported at odd primes for which the *Schinzel-Wójcik problem* has affimative answer. Consequently, we study the *Schinzel–Wójcik* problem on average.

Acknowledgements

IN THE NAME OF ALLAH MOST GRACEFUL MOST MERCIFUL,

All my profound gratitude is expressed to **Prof. Francesco Pappalardi**, professor of Algebra in the department of Mathematics and Physics at Roma Tre University; not only for suggesting this problem to me but also for his encouragement and moral support to pursue, exhibit and extract new ideas.

I'm also very grateful to all my family members for their patience, understanding and encouragement. Many thanks also go to all my colleagues - in Roma and in the departments of Mathematics at Ain Shams University.

Mohamed Anwar

Notations and Terminology

- $\mathbb{N}$ - $\{1, 2, ...\}$.
- $\mathbb{Z}$ - The ring of integers.
- $\mathbb{Q}$ - The field of rationals.
- $\mathbb{Z}/p\mathbb{Z}$ - The ring of integers modulo prime number p
- $(\mathbb{Z}/p\mathbb{Z})^*$ - Multiplicative group of the field of p elements
- $\langle a \rangle$ - Subgroup of $(\mathbb{Z}/p\mathbb{Z})^*$ generated by a
- (a, b) - Greatest common divisor of the integers $a, b \in \mathbb{Z}$
- $[a, b]$ - Least common multiple of the integers $a, b \in \mathbb{Z}$
- $\mathrm{ord}_p\, a$ - Order of an element $a \in (\mathbb{Z}/p\mathbb{Z})^*$
- $\tau(n)$ - The divisor function
- $\sigma(n)$ - The sum of prime factors of n
- $\omega(n)$ - The number of distinct prime factors of n
- $\Omega(n)$ - The number of prime factors of n counted with multiplicity
- $\varphi(n)$ - Euler totient function
- $\mu(n)$ - Möbius function

- $\prod\limits_{p}, \prod\limits_{q}, \prod\limits_{\ell}$ - Denotes the product taken over prime numbers
- LCM$(d;r)$- The number of r-tuples of positive integers such that their least common multiple is d
- ord χ - The order of the character χ in group of the characters
- $f(x) = O(g(x))$ or $f(x) \ll g(x)$ - There exists a positive real number C and a real number t such that $|f(x)| \leq C|g(x)|$ for all $x > t$
- $f(x) = \underline{o}(g(x))$ - For every positive constant ϵ there exists a constant N such that $|f(x)| \leq \epsilon|g(x)|$ for all $x > N$
- $f(x) \sim g(x)$ - $\lim\limits_{x\to\infty} \frac{f(x)}{g(x)} = 1$
- $\pi(x)$ - the number of primes up to a number x
- $\pi(x, a; m)$ - the number of primes up to a number x which is congurent to a modulo m
- $\mathrm{Li}(x) = \int_2^x \frac{dt}{\log t}$
- L/K - L is a field extension of K
- $\mathcal{O}_K$ - The ring of integers of the field K
- $\mathfrak{p}, \mathfrak{q}$ - Prime ideals of $\mathcal{O}_K$
- $D(\mathfrak{q}|\mathfrak{p})$ - The *decomposition group* of $\mathfrak{q}$ over $\mathfrak{p}$
- $I(\mathfrak{q}|\mathfrak{p})$ - The *inertia group* of $\mathfrak{q}$ over $\mathfrak{p}$
- $\left[\dfrac{L/K}{\mathfrak{p}}\right]$ - *Artin symbol* of $\mathfrak{p}$
- $N\mathfrak{p}$ - The norm of the ideal $\mathfrak{p}$
- $\mathrm{Gal}(L/K)$ - The Galois group of the field extension L/K

- $\left[\dfrac{\alpha}{\mathfrak{p}}\right]_n$ - The n-th power residue of α in $\mathcal{O}_K$ over $\mathfrak{p}$
- $\left(\dfrac{\alpha}{p}\right)$ - *Legendre* symbol

Chapter 1

Introduction

One of the famous problems in Number theory is *Artin*'s Conjecture on primitive roots. On September 27, 1927 *Emil Artin* introduced a conjecture on primitive roots to *Helmut Hasse*. It states that a square free integer $a \notin \{0, \pm 1\}$ is a primitive root modulo infinitely many primes p. Moreover, if $N_a(x) := \{p \leq x : a \text{ is a primitive root modulo } p\}$, he conjectured that

$$N_a(x) \sim A(a)\frac{x}{\log x} \qquad \text{as} \qquad x \longrightarrow \infty,$$

where $A(a)$, *Artin's* constant, is a positive constant depending on a.
The concept of primitive roots has been introduced by *Gauss* in articles $315 - 317$ of his Disquisitiones Arithmeticae (1801) during his study of the decimal expansion of the fractions to answer why $\frac{1}{7} = \overline{0.142857}$ has period length 6 and $\frac{1}{11} = \overline{0.09}$ has period length 2. Additionally, he tackled that how often prime p such that 10 is a primitive root modulo p but he did not make a conjecture about it. *Gauss* gave many examples of primes p where 10 is a primitive root modulo p in his tables. Therefore, the following conjecture had ascribed to *Gauss* by many authors
"There exist infinitely many primes p such that 10 is a primitive root modulo p".

In 1967, under the assumption of *GRH* for the kummer field $\mathbb{Q}\left(a^{\frac{1}{k}},\zeta_k\right)$, *Hooley* [6] proved that:

$$N_a(x) = A(a)\frac{x}{\log x} + O\left(\frac{x\log\log x}{\log^2 x}\right) \quad , \quad \text{where} \quad A(a) = \sum_{n\geq 1}\frac{\mu(n)}{[\mathbb{Q}(a^{\frac{1}{k}},\zeta_k):\mathbb{Q}]}.$$

In 1968, free of any hypothesis, *Goldfeld* [5] proved the following:

Theorem 1. *[5] for each $D > 1$,*

$$N_a(x) = A\operatorname{li} x + O\left(\frac{x}{(\log x)^D}\right)$$

holds for all integers $a \leq T$ with at most $c_1 T^{\frac{9}{10}}(5\log x + 1)^{g+D+2}$ exceptions, $g = \frac{x}{\log T}$, where $A = \prod_p \left(1 - \frac{1}{p(p-1)}\right) = 0.3739558\ldots$ is Artin's constant and c_1 and the constant of O-term are positive and depend only on D.

In 1969, *P.J. Stephens* [21] studied *Artin's* conjecture on average. He proved, free of any hypothesis, that the asymptotic formula holds on average with condition on T. More preciesly,

Theorem 2. *[21] If $T > \exp(4(\log x\log\log x)^{\frac{1}{2}})$, then*

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

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

Also, he proved the following:

Theorem 3. *[21] Let A be Artin's constant, and $E > 2$ be an arbitrary real number. Then, for $T > \exp(6(\log x\log\log x)^{\frac{1}{2}})$, we have*

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

Moreover, by using the normal order method of Turan, he proved that the number of exceptions is bounded by $O(T)$ when $T > \exp(6(\log x\log\log x)^{\frac{1}{2}})$ and as x tend to infinity.

Let $\Gamma \subset \mathbb{Q}^*$ be a multiplicative subgroup of finite rank r. For all primes, except those primes with $v_p(g) = 0$ for some $g \in \Gamma$, consider the reduction group $\Gamma_p = \{g \pmod p : g \in \Gamma\}$ which is well-defined subgroup of the multiplicative group $\mathbb{F}_p^*$. Define $N_{\Gamma,m}(x) := \{p \leq x : p \equiv 1 \,(\mathrm{mod}\, m) \text{ and } [\mathbb{F}_{p^*} : \Gamma_p] = m\}$. *L. Cangelmi, F. Pappalardi* and *A. Susa* in [14], [4] and [15] proved, under the assumption of GRH for the kummer field $\mathbb{Q}(\zeta_k, \Gamma^{1/k})$ for $k \in \mathbb{N}$, that for any $\varepsilon > 0$, if $m \leq x^{\frac{r-1}{(r+1)(4r+2)} - \varepsilon}$, then

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

where δ_Γ^m is a rational multiple of $C_r = \sum_{n \geq 1} \frac{\mu(n)}{n^r \varphi(n)} = \prod_p \left(1 - \frac{1}{p^r(p-1)}\right)$.

In 2015, *C. Pehlivan* and *L. Menici* [13] studied the average behaviour of $N_{\Gamma,m}(x)$ where $\Gamma = \langle a_1, \cdots, a_r\rangle \subseteq \mathbb{Z}^r$ and they obtained the following results:

Theorem 4. *[13] Let $T_1, \ldots, T_r \in \mathbb{R}$. Assume $T^* := \min\{T_i : i = 1, \ldots, r\} > \exp(4(\log x \log\log x)^{\frac{1}{2}})$ and $m \leq (\log x)^D$ for an arbitrary positive constant D. Then*

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

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

Theorem 5. *[13] if $T^* > \exp(6(\log x \log\log x)^{\frac{1}{2}})$, then*

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

where $M' > 2$ is arbitrarily large.

By using the Euler product expansion and some properties of Euler function, they could write

$$C_{r,m} = \frac{1}{m^{r+1}} \prod_{p|m} \left(1 - \frac{p}{p^{r+1}-1}\right)^{-1} C_r$$

which can be used in the proof of the last last theorem and deduced the following result, For $T_i > \exp(4(\log x \log\log x)^{\frac{1}{2}})$ for all $i = 1, \ldots, r$, $m \le (\log x)^D$ and for any constant $M > 2$,

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

where $J_r(n) = n^r \prod_{\ell | n} (1 - 1/\ell^r)$ is the so called *Jordan's totient function*, which is a generalization of *Moree*'s result in [10].

In this thesis, we will study *Schinzel–Wójcik problem* which is related to Artin's conjecture. In 1992, *Schinzel* and *Wójcik* [20] proved that

> Given any rational $a, b \in \mathbb{Q}^* \setminus \{\pm 1\}$, there exist infinitely many primes p such that $\operatorname{ord}_p a = \operatorname{ord}_p b$.

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 $a, b, c \in \mathbb{Q}^* \setminus \{\pm 1\}$, are there infinitely many primes p with the property that $\operatorname{ord}_p a = \operatorname{ord}_p b = \operatorname{ord}_p c$?

In 1996, *Wójcik* [23] produced an examples of triplets of integers (a, b, c) for which the above property is not satisfied for any odd prime p:

> let $a = e$, $b = e^2$, $c = -e^2$, $e \in \mathbb{Q}^* \setminus \{\pm 1\}$. For any $p \ge 3$ and $\delta = \operatorname{ord}_p e = \operatorname{ord}_p -e^2$, 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 $\operatorname{ord}_p e^2 \mid \frac{\delta}{2}$ contradicting $\operatorname{ord}_p e^2 = \delta$.

However, in 1996, *Wójcik* [23] proved that:

Theorem 6. *Wójcik (1996)[23]. Let $K/\mathbb{Q}$ be a finite extension and $a_1, \cdots, a_r \in K \setminus \{0,1\}$ be such that the multiplicative group $\langle a_1, \ldots, a_r \rangle \subset K$ is torsion free. Then the Schinzel* Hypothesis H *implies that there exist infinitely many primes $\mathfrak{p}$ of degree 1 such that* $\operatorname{ord}_p a_1 = \cdots = \operatorname{ord}_p a_r$.

It is an immediate corollary that if $a, b, c \in \mathbb{Q}^* \setminus \{\pm 1\}$ are such that $-1 \notin \langle a, b, c \rangle$, then *Hypothesis H* implies that the *Schinzel-Wójcik* 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 *Schinzel–Wójcik problem* for $\{2, 3, -6\}$. Theorem 6 does not apply although for $p = 19, 211, 499, 907$ and for many more primes p, one has that $\operatorname{ord}_p 2 = \operatorname{ord}_p 3 = \operatorname{ord}_p -6$. Hence, empirical data suggest that the *Schinzel–Wójcik problem* has an affirmative answer. Observe that *Wójcik* Theorem does not answer the *Schinzel-Wójcik problem* for sets of the form $\{a, b, -ab\} \in \mathbb{Q}^* \setminus \{\pm 1\}$.

The Generalized Riemann Hypothesis (GRH for short) can be applied to the *Schinzel-Wójcik problem.* Indeed, we have the following due to *K. R. Matthews* in 1976:

Theorem 7. *(K. R. Matthews-1976) [9]. Given $a_1, \cdots, a_r \in \mathbb{Z}^*$, there exists a constant $C = C_{(a_1, \cdots, a_r)} \in \mathbb{R}^{\geq 0}$ such that if the Generalized Riemann Hypothesis holds, then*

$$\#\{p \leq x : \operatorname{ord}_p a_i = p - 1, \textit{ for all } i = 1, \cdots, r\} = C \operatorname{li}(x) + O\left(x \frac{(\log \log x)^{2^r - 1}}{(\log x)^2}\right).$$

This result is known as the simultaneous primitive roots Theorem and it has an immadiate consequence which is:

Corollary 8. *With the above notation, if $C = C_{(a_1, \cdots, a_r)} \neq 0$ and the GRH holds, then the Schinzel-Wójcik problem has an affirmative answer for $a_1, \cdots, a_r$.*

Further results in [9] imply that $C = C_{(a_1, \cdots, a_r)} = 0$ if and only if at least one of the following conditions is satisfied:

(α) There exist $1 \le i_1 < \cdots < i_{2s+1} \le r$ such that $a_{i_1} \cdots a_{i_{2s+1}} \in \mathbb{Q}^{*2}$;

(β) There exist $1 \le i_1 < \cdots < i_{2s} \le r$ such that $a_{i_1} \cdots a_{i_{2s}} \in -3\mathbb{Q}^{*2}$, and for all primes $\ell \equiv 1 \bmod 3$ there exists at least one element of S which is a cube modulo ℓ.

Each of the conditions above implies that $a_1, \cdots, a_r$ can not be simultaneously primitive roots for infinitely many primes.

From the above, it follows that so that GRH implies that the *Schinzel-Wójcik problem* has an affirmative answer in this case. So, the *Schinzel–Wójcik problem* is still open both on *Hypothesis H* and on GRH.

Also, *F. Pappalardi* and *A. Susa* [16] proved some results under the GRH with the following notation: Let $\Gamma = \langle a_1, \ldots, a_r \rangle$ be the subgroup of $\mathbb{Q}^*$ generated by $a_1, \ldots, a_r$, and by $r(a_1, \ldots, a_r) = \operatorname{rank}_{\mathbb{Z}} \langle a_1, \ldots, a_r \rangle$ its rank as abelian group. Clearly, $1 \le r(a_1, \ldots, a_r) \le r$. Further, let $\Gamma(N) := \Gamma \cdot \mathbb{Q}^{*N} / \mathbb{Q}^{*N}$,

$$\tilde{\Gamma}(N) = \left\{ \xi \mathbb{Q}^{*N} \in \Gamma(N) \text{ such that } [\mathbb{Q}(\sqrt[N]{\xi}) : \mathbb{Q}] \le 2 \text{ and } \operatorname{disc}(\mathbb{Q}(\sqrt[N]{\xi})) \mid N \right\}$$

and $\Gamma_{\underline{k}} := \langle a_1^{\frac{k}{k_1}}, \ldots, a_r^{\frac{k}{k_r}} \rangle$ if $\underline{k} = (k_1, \ldots, k_r) \in \mathbb{N}^r$, $k = [\underline{k}]$ is the least common multiple of $k_1, \ldots, k_r$ and $\mu(\underline{k}) := \mu(k_1) \cdots \mu(k_r)$.

Theorem 9. *[16] Let $\{a_1, \ldots, a_r\} \subset \mathbb{Q} \setminus \{0, \pm 1\}$ and set $\Gamma = \langle a_1, \ldots, a_r \rangle$. 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 $r(a_1, \ldots, a_r) \ge 2$. Then*

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

where

$$\delta_{a_1,\ldots,a_r} = \sum_{\substack{m \in \mathbb{N} \\ \underline{k} \in \mathbb{N}^r}} \frac{\mu(\underline{k})}{\varphi(mk)} \frac{\#\tilde{\Gamma}_{\underline{k}}(mk)}{\#\Gamma_{\underline{k}}(mk)}$$

and the notation is the same as above.

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

Theorem 10. *[16] 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:*

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

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 $D(b) = \mathrm{disc}(\mathbb{Q}\sqrt{b})$, then

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

where

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

and

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

In this degenerate case, they gave a complete answer to the *Schinzel–Wójcik problem.*

Corollary 11. *[16] 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 Schinzel–Wójcik problem for $\{a^{h_1}, \ldots, a^{h_r}\}$ has an affirmative answer.*

In the case when $a_1, \ldots, a_r$ are all primes they expressed the density in terms of an infinite Euler–product.

Theorem 12. *[16] Let $p_1, \ldots, p_r$ be primes. Set*

$$\Lambda_\ell = -\frac{\ell(\ell^r - (\ell-1)^r - 1)}{(\ell-1)(\ell^{r+1}-1)} \quad \text{and} \quad \delta = \prod_\ell (1 + \Lambda_\ell).$$

Then

$$\delta_{p_1,\ldots,p_r} = \delta \cdot \left(\sum_{d | p_1 \cdots p_r} \left(1 - \frac{2 - 2^{-r}}{3}(1 - \eta_d)\right) \prod_{\substack{\ell | d \\ \ell > 2}} \left(\frac{\Lambda_\ell}{1 + \Lambda_\ell}\right)\right),$$

where $\eta_1 = 1$ and

$$\eta_d = \begin{cases} -1 & \text{if} \quad d \equiv 3 \bmod 4; \\ \mu(d) & \text{if} \quad d \equiv 1 \bmod 4, d \neq 1; \\ -1/2 - 1/2^r & \text{if} \quad d \equiv 2 \bmod 4. \end{cases}$$

In Chapter 2, we recall some topics from Algebraic Number Theory and some Linear Algebra that we will discuss a method to solve a system of congruences in several variables modulo an integer.

In Chapter 3, we state the important hypothesis due to *Schinzel* which is used in Chapter 4 and Chapter 5. Also, it is explained that it implies many well-known other conjecture like the Conjecture of twin primes, Artin's Conjecture and one of Landau's Conjectures which is really due to *Euler*.

In Chapter 4, in collaboration with *F. Papplardi*, we proved that:

Theorem 13. *[2] Assume that* Hypothesis H *holds, let $S = \{a_1, \ldots, a_r\} \subset \mathbb{Q}$ and assume*

1. *For each $1 \le i_1 < \cdots < i_{2s+1} \le r$ one has that $a_{i_1} \cdots a_{i_{2s+1}} \notin \mathbb{Q}^{*2}$;*

2. *If there exist $1 \le i_1 < \cdots < i_{2s} \le r$ such that $a_{i_1} \cdots a_{i_{2s}} \in -3\mathbb{Q}^{*2}$, then there exists a prime $\ell \equiv 1 \bmod 3$ such that none of the elements of S is a cube modulo ℓ.*

Then the set $\mathcal{P}_S = \{p \text{ prime} \mid \forall a \in S, a \text{ is a primitive root modulo } p\}$ is infinite.

In Chapter 5, we introduce a complete characterization, under *Hypothesis H* of the $r-$ touples of rational numbers supported at odd primes for which the *Schinzel-Wójcik problem* has affimative answer. That is,

Theorem 14. *Let* $\{a_1, \dots, a_r\} \subset \mathbb{Q}^* \setminus \{\pm 1\}$, $v_2(a_i) = 0$ *for all* $i = 1, \cdots, r$. *Assume* Hypothesis H. *Then the Schinzel-Wójcik problem has affimative answer for* $\{a_1, \dots, a_r\}$ *if and only if at least one of the following two conditions is satisfied:*

1. $-1 \notin \langle a_1, \dots, a_r \rangle$;
2. *For every* $\nu_1, \dots, \nu_r \in \mathbb{Z}$, *if* $a_1^{\nu_1} \cdots a_r^{\nu_r} = 1$, *then* $\nu_1 + \cdots + \nu_r \equiv 0 \pmod 2$.

In Chapter 6, we prove an average version of the *Schinzel–Wójcik* asymptotic formula free of any hypothesis. More precisely, Assume $T > exp\left(4\left(\log x \log\log x\right)^{\frac{1}{2}}\right)$. Then, for every $k > 1$, we have

$$\frac{1}{T^r}\sum_{\underline{a}\leq T} S_{\underline{a},m}(x) = \delta_m \operatorname{li}(x) + O\left(\frac{x}{(\log x)^k}\right),$$

where $\delta_m = \frac{1}{m^r\varphi(m)}\prod_{\ell}\left(1 + \frac{\varphi((m,\ell))f(\ell)}{\varphi(\ell)(m,\ell)}\right)$, $f(\ell) = (1 - \frac{1}{\ell})^r - 1$.

Chapter 2

Preliminaries

In this chapter, I introduce some basic concepts of Algebraic Number Theory which can be found in many books of algebraic number theory, for example in [18] and [7].

2.1 Artin symbol

Let L/K be a field extension of finite degree n. Let $\mathcal{O}_L$,resp. $\mathcal{O}_K$ be the ring of integers of L (respectively, K). Given $\mathfrak{p}$ a prime ideal of $\mathcal{O}_K$, consider $\mathfrak{p}\mathcal{O}_L$ the extended ideal of $\mathcal{O}_L$. The following property holds $\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1^{e_1}\mathfrak{q}_2^{e_2}\cdots\mathfrak{q}_g^{e_g}$ and $n = \sum_{i=1}^{g} e_i f_i$. The exponent $e_i > 0$ of $\mathfrak{q}_i$ is called the *ramification index* of $\mathfrak{q}_i$ over $\mathcal{O}_K$ and the dimension f_i of $\mathcal{O}_L/\mathfrak{q}_i$ over $\mathcal{O}_K/\mathfrak{p}$ is called the *residual degree* of $\mathfrak{q}_i$ over $\mathcal{O}_K$. Furthrtmore, the prime ideals of L which appear in the factorization of $\mathfrak{p}\mathcal{O}_L$, called the *primes above* $\mathfrak{p}$, are exactly the primes $\mathfrak{q}$ such that $\mathfrak{q} \cap \mathcal{O}_K = \mathfrak{p}$. In the case when L/K is *Galois* extenstion with Galois group $G = \mathrm{Gal}(L/K)$, G acts transitivily on the set of prime ideals above $\mathfrak{p}$. Moreover, they all have the same ramification index e and the same residual degree f. Therefore, we have $\mathfrak{p}\mathcal{O}_L = (\mathfrak{q}_1\mathfrak{q}_2\cdots\mathfrak{q}_g)^e$ and $n = efg$.

Let $\mathfrak{q} \subseteq \mathcal{O}_L$ such that $\mathfrak{q}\cap\mathcal{O}_K = \mathfrak{p}$. The *decomposition group* $D\,(\mathfrak{q}|\mathfrak{p})$ of $\mathfrak{q}$ over $\mathfrak{p}$, is the set of all automorphisms $\sigma \in G$ that fix $\mathfrak{q}$ (i.e., $\sigma(\mathfrak{q}) = \mathfrak{q}$). It is a subgroup of G with cardinality

$\frac{n}{g}$ (as a consequence of the *orbit-stabilizer Theorem*).

Each $\sigma \in D(\mathfrak{q}|\mathfrak{p})$ induces an automrphism $\overline{\sigma}$ of $\mathcal{O}_L/\mathfrak{q}$ such that $\overline{\sigma}(x+\mathfrak{q}) = \sigma(x)+\mathfrak{q}$. Moreover, the map $\sigma \longmapsto \overline{\sigma}$ is a surjective group homomorphism from $D(\mathfrak{q}|\mathfrak{p})$ to $\mathrm{Gal}\left(\frac{\mathcal{O}_L/\mathfrak{q}}{\mathcal{O}_K/\mathfrak{p}}\right)$ with kernel $I(\mathfrak{q}|\mathfrak{p}) = \{\sigma \in D(\mathfrak{q}|\mathfrak{p}) : \sigma(x) - x \in \mathfrak{q}\}$ which called the *inertia group* of $\mathfrak{q}$ over $\mathfrak{p}$. Consequently, the cardinality of $I(\mathfrak{q}|\mathfrak{p})$ is e and $\mathfrak{p}$ is unramified in $\mathcal{O}_{\mathcal{L}}$ *if and only if* for any $\mathfrak{q}$ above $\mathfrak{p}$ the *inertia group* of $\mathfrak{q}$ is trivial. Moreover, the *Decompostion group* and the *inertia group* of $\sigma(\mathfrak{q})$ are conjugated to the *Decompostion group* and the *inertia group* of $\mathfrak{q}$ for each in $\sigma \in G$, i.e. $D(\sigma(\mathfrak{q})|\mathfrak{p}) = \sigma D(\mathfrak{q}|\mathfrak{p})\sigma^{-1}$ and $I(\sigma(\mathfrak{q})|\mathfrak{p}) = \sigma I(\mathfrak{q}|\mathfrak{p})\sigma^{-1}$ for each $\sigma \in G$. In the case of abelian extension, all the groups $D(\sigma(\mathfrak{q})|\mathfrak{p})$ and $I(\sigma(\mathfrak{q})|\mathfrak{p})$ are the same and they depend only on $\mathfrak{p}$, so I shall write it as $D(\mathfrak{p})$.

With the above notation, consider a Galois extention L/K of degree n with Galois group G. Let $\mathfrak{p} \subset \mathcal{O}_K$ be a prime ideal that does not ramify in $\mathcal{O}_L$ and let $\mathfrak{q} \subset \mathcal{O}_L$ be a prime ideal above $\mathfrak{p}$. The *Inertia group* $I(\mathfrak{q})$ of $\mathfrak{q}$ is trivial, so its *Decomposition group* is isomorphic to the Galois group of $\mathrm{Gal}\left(\frac{\mathcal{O}_L/\mathfrak{q}}{\mathcal{O}_K/\mathfrak{p}}\right)$ which is *cyclic* with a generator $\overline{\sigma}$ defined as $x+\mathfrak{q} \longmapsto \sigma(x)+\mathfrak{q}$ where $q = N\mathfrak{q} = |\mathcal{O}_K/\mathfrak{q}|$ and $x \in \mathcal{O}_K$. Therefore, $D(\mathfrak{q}|\mathfrak{p})$ is *cyclic* with a generator σ defined by the relation $\sigma(x) \equiv x^q (\bmod\, \mathfrak{q})$. This generator is called the *Frobenious Automorphism* of $\mathfrak{q}$ which shall be denoted as $(L/K, \mathfrak{q})$. In the case of abelian extention, it depends only on $\mathfrak{p}$ we will call it the *Artin symbol* of $\mathfrak{p}$ and denote it by $\left[\frac{L/K}{\mathfrak{p}}\right]$.

2.2 Power Residues

Let K be a number field with ring of integers $\mathcal{O}_K$ that contains a primitive n-th root of unity ζ_n. Let $\mathfrak{p} \subset \mathcal{O}_K$ be a prime ideal and assume that $n \notin \mathfrak{p}$.

An analogue of Fermat's Little Theorem holds in $\mathcal{O}_K$, $\alpha^{N\mathfrak{p}-1} \equiv 1 \,(\bmod\, \mathfrak{p})$ for $\alpha \in \mathcal{O}_K \setminus \mathfrak{p}$. In particular, $\zeta_n^{N\mathfrak{p}-1} \equiv 1 \,(\bmod\, \mathfrak{p})$. By the following Lemma, $N\mathfrak{p} \equiv 1 (\bmod\, n)$.

Lemma 15. $\zeta_n^a \equiv \zeta_n^b \,(\bmod\, \mathfrak{p})$ *if and only if* $\zeta_n^a \equiv \zeta_n^b$.

Proof. Suppose that $\zeta_n^a \equiv \zeta_n^b \,(\bmod\, \mathfrak{p})$, hence $\zeta_n^{a-b} \equiv 1 \,(\bmod\, \mathfrak{p})$ since ζ_n^b is unit. Therefore

$\zeta_n^a = \zeta_n^b$, otherwise $n = \prod_{i=1}^{n-1}(1-\zeta_n^i) \in \mathfrak{p}$ which contadicts the assumption. The converse is immediate. $\square$

As a consequence, the equation $x^n \equiv 1 \,(\mathrm{mod}\,\mathfrak{p})$ has exactly n solutions, namely, $1, \zeta_n, \ldots, \zeta_n^{n-1}$. Since $\left(\alpha^{\frac{N\mathfrak{p}-1}{n}}\right)^n \equiv 1 \,(\mathrm{mod}\,\mathfrak{p})$, there exist a unique $s \in \{0, 1, \cdots, n-1\} : \alpha^{N\mathfrak{p}-1/n} \equiv \zeta_n^s \,(\mathrm{mod}\,\mathfrak{p})$. This root of unity is defined to be the n-th power residue of α in $\mathcal{O}_K$ over $\mathfrak{p}$, denoted by $\left[\dfrac{\alpha}{\mathfrak{p}}\right]_n$. We will conclude by the following properties:

(i) $\left[\dfrac{\alpha}{\mathfrak{p}}\right]_n = 1$ *if and only if* $x^n \equiv \alpha(\mathrm{mod}\,\mathfrak{p})$ has a solution $x \in \mathcal{O}_K$;

(ii) $\left[\dfrac{\alpha}{\mathfrak{p}}\right]_n \equiv \alpha^{(N\mathfrak{p}-1)/n} \,(\mathrm{mod}\,\mathfrak{p})$;

(iii) $\left[\dfrac{\alpha}{\mathfrak{p}}\right]_n \left[\dfrac{\beta}{\mathfrak{p}}\right]_n = \left[\dfrac{\alpha\beta}{\mathfrak{p}}\right]_n$.

(iv) If $\alpha \equiv \beta \;(\mathrm{mod}\,\mathfrak{p})$, then $\left[\dfrac{\alpha}{\mathfrak{p}}\right]_n = \left[\dfrac{\beta}{\mathfrak{p}}\right]_n$.

2.2.1 Legendre Symbol

Consider $K = \mathbb{Q}$ and $n = 2$. For a prime p, odd, and for $\alpha \in \mathbb{Z}$, the *Legendre symbol*, denoted by $\left(\dfrac{\alpha}{p}\right)$, is defined to be $\alpha^{p-1/2}$ in $\mathbb{Z}/p\mathbb{Z}$. Since $p |\, (\alpha^{p-1} - 1) = \left(\alpha^{\frac{p-1}{2}} - 1\right)\left(\alpha^{\frac{p-1}{2}} + 1\right)$, therefore $\left(\dfrac{\alpha}{p}\right) = \alpha^{\frac{p-1}{2}} = 1$ or -1 according as α is square mod p or not. We have the following properties:

(i) $\left(\dfrac{-1}{p}\right) = (-1)^{p-1/2}$;

(ii) $\left(\dfrac{\alpha}{p}\right) \equiv \alpha^{p-1/2} \,(\mathrm{mod}\,p)$;

(iii) $\left(\dfrac{\alpha}{p}\right)\left(\dfrac{\beta}{p}\right) = \left(\dfrac{\alpha\beta}{p}\right)$;

(iv) If $\alpha \equiv \beta \;(\mathrm{mod}\,p)$, then $\left(\dfrac{\alpha}{p}\right) = \left(\dfrac{\beta}{p}\right)$;

(v) (*Law of Quadratic Reciprocity*) Let p, q are two distinct odd primes,

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{p-1}{2}}.$$

2.2.2 Cubic Residue Symbol

Consider $K = \mathbb{Q}(\omega)$, where ω is a primitive cubic root of unity and $n = 3$. We have that $\mathcal{O}_K = \mathbb{Z}[\omega]$ is a principle ideal domain. Given a prime ideal $\langle \pi \rangle$ such that $N(\pi) \neq 3$. For $\alpha \in \mathcal{O}_K$, the *Cubic Residue Symbol*, denoted by $\left[\frac{\alpha}{\pi}\right]_3$, is defined to be $\alpha^{N(\pi)-1/3}$ in $\mathbb{Z}[\omega]/\langle \pi \rangle$ which equals exactly one of the cubic roots of unity 1 or ω or ω^2. In paricular, it equals 1 *if and only if* α is a cubic residue(,i.e. $x^3 \equiv \alpha \pmod{\pi}$ has a solution). We have the following properties:

(i) $\left[\frac{\alpha}{\pi}\right]_3 \equiv \alpha^{(N(\pi)-1)/3} \pmod{\pi}$;

(ii) $\left[\frac{\alpha}{\pi}\right]_3 \left[\frac{\beta}{\pi}\right]_3 = \left[\frac{\alpha\beta}{\pi}\right]_3$;

(iii) If $\alpha \equiv \beta \pmod{\pi}$, then $\left[\frac{\alpha}{\pi}\right]_3 = \left[\frac{\beta}{\pi}\right]_3$;

(iv) $\overline{\left[\frac{\alpha}{\pi}\right]_3} = \left[\frac{\alpha}{\pi}\right]_3^2 = \left[\frac{\alpha^2}{\pi}\right]_3$;

(v) $\overline{\left[\frac{\alpha}{\pi}\right]_3} = \left[\frac{\overline{\alpha}}{\pi}\right]_3$;

(vi) $\left[\frac{\overline{\alpha}}{\pi}\right]_3 = \left[\frac{\alpha^2}{\pi}\right]_3$ and $\left[\frac{n}{q}\right]_3 = 1$ if n is a rational integer relatively prime to a rational prime $q \equiv 2 \pmod{3}$.

The following definition is essential in stating the *Law of Cubic Reciprocity*.

Definition 16. *A prime element $\pi \in \mathbb{Z}[\omega]$ is said to be primary if $\pi \equiv 2 \pmod{3}$, equivelantly, $a \equiv 2 \pmod{3}$ and $b \equiv 0 \pmod{3}$ whenever $\pi = a + b\omega$.*

(vii) If $N(\pi) = p \equiv 1 \pmod 3$, then among the associates of π exactly one is *primary*.

(viii) (*Law of Cubic Reciprocity*) Let π_1, π_2 be primary, $N(\pi_1), N(\pi_2) \neq 3$ and $N(\pi_1) \neq N(\pi_2)$. Then

$$\left[\frac{\pi_1}{\pi_2}\right]_3 = \left[\frac{\pi_2}{\pi_1}\right]_3$$

(viii) (*Supplement to the Cubic Reciprocity Law*) Suppose that $N(\pi) \neq 3$. If $\pi = q$ is rational, write $q = 3m - 1$. If $\pi = a + b\omega$ is a primary complex prime, write $a = 3m - 1$. Then

$$\left[\frac{1-\omega}{\pi}\right]_3 = \omega^{2m}.$$

2.3 Chebotarev Density Theorem

Chebotarev Density Theorem is a wonderful important theorem in Algebraic Number Theory. Chebotarev Density Theorem can be considered as a generalisation of Dirichlet's Theorem on Arithmetic Progressions and Frobenious Theorem. It is used in the study of Artin's conjecture on primitive roots. Informally, in a Galois extension of a number field, the density of prime ideals such that the *Artin symbol* of these prime ideals equal to a certain conjuagacy class of the Galois group of the field extension equals the portion of the elements of the Galois group which are in the conjuagacy class . There are many versions; however, in this research the following is applied.

Theorem 17. *(Chebotarev). Let L/K be a Galois extention of a number field and C be a conguagcy class(or union of conjuagacy classes) of the Galois group* $\mathrm{Gal}\,(L/K)$*. Define*

$$P_C := \left\{ \mathfrak{p} \subseteq \mathcal{O}_K : \mathfrak{p} \textit{ is unramified in } L \textit{ and } \left[\frac{L/K}{\mathfrak{p}}\right] \subseteq C \right\},$$

then the natural density of P_C exists and equals to $\dfrac{|C|}{|\,\mathrm{Gal}\,(L/K)\,|}$.

Corollary 18. *With the above notation assume further that* $\mathrm{Gal}(L/K)$ *is abelian. Given any* $\sigma \in \mathrm{Gal}(L/K)$*, there are infinitley many unramified prime ideals of* $\mathcal{O}_K$ *such that the Artin symbol of* $\mathfrak{p}$ *equals* σ*.*

Corollary 19. *With the same notation. Let* $\mathfrak{p} \subseteq \mathcal{O}_K$ *be an unramified prime ideal in* $\mathcal{O}_K$*.* $\mathfrak{p}$ *splits completely in* $\mathcal{O}_L$ *if and only if the Artin symbol of* $\mathfrak{p}$ *equals the identity.*

Proof. It is a direct consequence of the fundamental relation $n = \sum_{i=1}^{g} e_i f_i$ and the result $D(\mathfrak{q}|\mathfrak{p})$ is isomorphic to $\mathrm{Gal}\left(\dfrac{\mathcal{O}_L/\mathfrak{q}}{\mathcal{O}_K/\mathfrak{p}}\right)$. □

2.4 Smith Normal Form

Let A be a matrix with entries in $\mathbb{Z}$ (or in any principal ideal domain R), By using row and coulmn operations, we can get a daigonal matrix with certain properties. The row (respectively, column) operations are

1. interchange two rows (respectively, columns);
2. multiply a row (respectively, column) by a unit;
3. add an integer multiple of row (respectively, coulmn) to another row (respectively, coulmn).

Theorem 20. *Let* $A \in M_{m\times n}(\mathbb{Z})$*. There exist* $L \in SL_m(\mathbb{Z})$ *and* $R \in SL_n(\mathbb{Z})$ *such that*

$$LAR = D = diag(d_1, d_2, \ldots, d_s, 0, \ldots, 0),$$

where $d_i > 0, i = 1, \ldots, s$ *and* $d_i | d_{i+1}, i = 1, \ldots, s-1$*.*

Proof. By using Euclidean algorithm, by using the row operations, we get a row whose first element is the GCD of the elements in the first column. Then by using the row operations, we matrix with the GCD in $(1,1)$ position and zeros in the rest of the first column. By repeating the same thing for the first row, using coulmn operations, we get the GCD of the elements in the first row in $(1,1)$ position and zeros in the rest of the first row.

The zeros in the first coulmn most likely are not zeros anymore. By repeating this procedure for the first row and the first coulmn, we get that all elements in the first row and the first column are zeros except for the element in the position $(1,1)$. This process is guaranteed to terminate because the GCD gets smaller each time.

If we continue in the same manner for the second row and the second coulmn and then for the rest rows and coulmns, one by one, we get a diagonal form of A which is $diag(e_1,\ldots,e_s,0,\ldots,0)$.

Since each row(resp. coulmn) operation can be represented as a left(resp. right) mulipli-cation of an elementry(unimodular) matrix by A, we can write

$$L^{'}AR^{'} = diag(e_1,\ldots,e_s,0,\ldots,0),$$

where $L^{'} \in SL_m(\mathbb{Z})$ and $R^{'} \in SL_n(\mathbb{Z})$.

It remains for us to transform $L^{'}AR^{'} = diag(e_1,\ldots,e_s,0,\ldots,0)$ to a diagonal form satisfying the divisiblity condition. Let us look on the submatrix $diag(e_1,e_2)$. Let $d = gcd(e_1,e_2)$. We may write $d = e_1x + e_2y$ for some $x,y \in \mathbb{Z}$ and $e_1 = d\alpha$ and $e_2 = d\beta$ for some $\alpha,\beta \in \mathbb{Z}$. By performing the following row and column operations

1. $xR_1 + R_2 \to R_2$;

2. $yC_2 + C_1 \to C_1$;

3. $-\alpha R_2 + R_1 \to R_1$;

4. $\beta C_1 + C_2 \to C_2$;

5. Interchange R_1 and R_2.

We get $diag(d, -e_2\alpha$ which satisfies the divisiblity condition. Then by applying the same manner for the rest of the digonal elements, we get

$$LAR = D = diag(d_1, d_2, \ldots, d_s, 0, \ldots, 0),$$

where $L \in SL_m(\mathbb{Z})$ and $R \in SL_n(\mathbb{Z})$, $d_i > 0, i = 1, \ldots, s$ and $d_i | d_{i+1}, i = 1, \ldots, s-1$. $\square$

2.5 Solving a system of linear congruences

Let A is a nonzero $m \times n$ matrix with integer entries, B is $m \times 1$, X is $n \times 1$ and $\ell \in \mathbb{N}$. Consider the system of linear congruences

$$\begin{aligned} & a_{11}x_1 + \cdots + a_{1n}x_n \equiv b_1 \pmod{\ell} \\ & \vdots \\ & a_{m1}x_1 + \cdots + a_{mn}x_n \equiv b_m \pmod{\ell} \end{aligned}$$

which can be written shortly as $AX \equiv B \pmod{\ell}$. We are going to introduce a criteria to solve the system of linear congruences. By Theorem 1, there exist $L \in SL_m(\mathbb{Z})$ and $R \in SL_n(\mathbb{Z})$ such that

$$LAR = D = diag(d_1, d_2, \ldots, d_s, 0, \ldots, 0),$$

where $d_i > 0$, $i = 1, \ldots, s$ and $d_i | d_{i+1}$, $i = 1, \ldots, s-1$. Therefore, we get a comparable system(since L and R are invertable) $DY \equiv K \pmod{\ell}$, where $X = RY$ and $K = LB$, that is,

$$
\begin{aligned}
&d_1x_1 \equiv k_1 \pmod{\ell}\\
&\vdots\\
&d_sx_1 \equiv k_s \pmod{\ell}\\
&0 \equiv k_{s+1} \pmod{\ell}\\
&\vdots\\
&0 \equiv k_m \pmod{\ell},
\end{aligned}
$$

which is solvable *if and only if* $\ell | k_i$ for $i = s+1, \ldots, m$ and $gcd(d_i, \ell) | k_i$ for $i = 1, \ldots, s$.

Chapter 3

Hypothesis H And Its Applications

3.1 Hypothesis H

Hypothesis H has been introduced by *A. Schinzel*. Informally, let $f_1, f_2, \cdots, f_k$ be integer valued irriducible polynomials, (under some conditions) *A. Schinzel* conjecured that there are infinitely many integers n such that $f_1(n), f_2(n), \cdots, f_k(n)$ are primes similtineously. It covers many famous conjectures as one of *Landau's conjectures* and *Twin prime conjecture* as shown herewith. Actually, it bulids on the *Bunyakovsky conjecture* for a single polynomial and on the *Hardy-Littlewood conjectures* for multiple linear polynomials.

To figure out which condition we need to add, let us study these two polynomials $x + 2, x + 3$. It is easy to see that they can not generate primes simltineously because one of them is even > 2 and the other is odd. Therefore, we need to add a condition to pin all the fixed divisors down, that is, for any prime p, there exist an integer n such that $p \nmid f_i(n)$ for $i = 1, \cdots, k$. Now, we can formulate Hypothesis H as in [19]:

> **Hypothesis H (Schinzel, 1959)** *Let $f_1, \ldots, f_k \in \mathbb{Z}[x]$ be irreducible polynomials with positive leading 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 $f_1(t), \ldots, f_k(t)$ are all primes.*

3.2 Applications of Hypothesis H

Let us see how Hypothesis H cover some famous conjectures.

- Twin primes conjecture:

  Consider the polynomials x, $x+2$. It is easy to see that they do not have any fixed divisor, so Hypothesis H implies that there are infinitly many n such that n, $n+2$ are primes similtiniously. Therefore, Hypothesis H implies the Twin primes conjecture.

- One of *Landau*'s conjectures:

  Actually, this conjecture goes back to *Euler* and is still unproven. In 1725, *Euler* mentioned in a letter to *Goldbach* that n^2+1 is often prime for $n \leq 1500$. Hypothesis H implies this conjecture just by considering this polynomial x^2+1.

- *Artin*'s conjecture on primitive roots:

  In 1958, *A. Schinzel* and *W. Sierpiński* [19] proved the following theorem:

Theorem 21. *[19] Hypothesis H implies Artin's conjecture.*

Proof. Let $g = a^2b : a \in \mathbb{N}, b \in \mathbb{Z}, b \neq 1$ be square free. Let b_1 be the greatest odd divisor of b. Firstly, we will prove that there exist two polynomials $f_1(x)$ and $f_2(x)$ satisfying

- Condition S: There is no integer > 1 divides the product $f_1(x)f_2(x)$ for every $x \in \mathbb{Z}$;

- Condition 1: For every $x \in \mathbb{N}$, b is non-quadratic residue modulo $f_1(x)$;

- Condition 2: $f_1(x) - 1 = 2f_2(x)$ if $b \neq 3$ and $f_1(x) - 1 = 2f_2(x)$ if $b = 3$.

Consider the case that $b < 0$. Let $f_1(x) = -4bx - 1$ and $f_2(x) = -2bx - 1$. It is clear that Condition 2 holds and Condition S is satisfied because $f_1(0)f_2(0) = 1$. Now, we are going to study Condition 1. If b is even, we have $f_1(x) \equiv -1 \pmod 8$ and the *Jacobi symbol* $\left(\dfrac{2}{f_1(x)}\right) = 1$, consequently

$$\left(\frac{b}{f_1(x)}\right) = \left(\frac{2}{f_1(x)}\right)\left(\frac{-b_1}{f_1(x)}\right) = -\left(\frac{b_1}{f_1(x)}\right) = -(-1)^{\frac{b_1-1}{2}}(-1)^{\frac{b_1-1}{2}} = -1$$

which proves that b is non-quadratic residue modulo $f_1(x)$, i.e., Condition 1 holds. If b is odd, $b = -b_1$. Thus, b is non-quadratic residue modulo $f_1(x)$.

Consider the case that $b > 0$ and even. Hence, $b = 2b_1, b_1$ is odd. Let $f_1(x) = 4bx + 2b - 1$, $f_2(x) = 2bx + b - 1$ and $P(x) = f_1(x)f_2(x)$. Since $P(1) + P(-1) - 2P(0) = 16b^2$, $P(0) = (2b-1)(b-1)$ and b is even, $gcd(P(1) + P(-1) - 2P(0), P(0)) = 1$. Therefore, Condition S holds. Also, it is clear that Condition 2 holds. Since $b = 2b_1 = 2(2k+1)$, $f_1(x) \equiv 3 \pmod 3$, consequently

$$\begin{aligned}\left(\frac{2}{f_1(x)}\right) = -1 \quad \text{and} \quad \left(\frac{b}{f_1(x)}\right) &= \left(\frac{2}{f_1(x)}\right)\left(\frac{b_1}{f_1(x)}\right) \\ &= -\left(\frac{b_1}{f_1(x)}\right) = -(-1)^{\frac{b_1-1}{2}}\left(\frac{f_1(x)}{b_1}\right) \\ &= -(-1)^{\frac{b_1-1}{2}}\left(\frac{-1}{b_1}\right) = -1.\end{aligned}$$

which proves that b is non-quadratic residue modulo $f_1(x)$, i.e., Condition 1 holds.

Consider the case that $b > 0$ and odd integer > 3. So, $b = \ell_1\ell_2\cdots\ell_k$ such that $\ell_1 < \ell_2 < \cdots < \ell_k$ and $\ell_i > 3$ is prime for all $i = 1, \cdots, k$. There are at least two non-quadratic residues modulo ℓ_k and one of them satisfying $n_0 \not\equiv -1 \pmod{\ell_k}$. The following system

$$n \equiv -1 \pmod{4\ell_1\ell_2\cdots\ell_{k-1}}$$

$$n \equiv -n_0 \pmod{\ell_k}$$

has obviously a solution $n = n_1$. Let $f_1(x) = 4bx + n_1$, $f_2(x) = 2bx + \frac{1}{2}(n_1 - 1)$ and $P(x) = f_1(x)f_2(x)$. It is easy to see that $P(1) + P(-1) - 2P(0) = 16b^2$ and $P(0) = \frac{1}{2}n_1(n_1 - 1)$. Since $\frac{1}{2}n_1(n_1 - 1) \equiv -1 \pmod{2\ell_1\ell_2 \cdots \ell_{k-1}}, n_1 \not\equiv 0 \pmod{\ell_k}$ and $\frac{1}{2}(n_1 - 1) \not\equiv 0 \pmod{\ell_k}$, $gcd(4b, n_1) = 1$ and $gcd(2b, \frac{1}{2}(n_1 - 1)) = 1$. Therefore, $gcd(16b^2, \frac{1}{2}n_1(n_1 - 1)) = 1$ which implies that $gcd(P(1) + P(-1) - 2P(0), P(0)) = 1$. Hence, the polynomials $f_1(x)$ and $f_2(x)$ satisfy Condition S. Also, Condition 2 is satisfied. Since $f_1(x) \equiv -1 \pmod{4\ell_1\ell_2 \cdots \ell_{k-1}}$ and $f_1(x) \equiv n_1 \pmod{\ell_k}$, so

$$\begin{aligned}\left(\frac{b}{f_1(x)}\right) &= (-1)^{\frac{b_1-1}{2}}\left(\frac{f_1(x)}{b}\right) = \left(\frac{-f_1(x)}{b}\right)\\ &= \left(\frac{-n_1}{\ell_1\ell_2\cdots\ell_{k-1}}\right)\left(\frac{-n_1}{\ell_k}\right) = \left(\frac{1}{\ell_1\ell_2\cdots\ell_{k-1}}\right)\left(\frac{n_0}{\ell_k}\right)\\ &= -1\end{aligned}$$

which proves than b is non-quadratic residue modulo $f_1(x)$, i.e. Condition 1 holds.

In the case $b = 3$, let $f_1(x) = 12x + 5$ and $f_2(x) = 3x + 1$. It is clear that Condition 1, Condition 2 and Condition S hold.

Let x be one of such numbers such that $f_1(x) > g^4$. Suppose, by contrary, that g is not primitive root modulo $f_1(x)$, i.e., g belong to an exponent modulo $f_1(x)$ which less that $f_1(x) - 1$. So by Condition 2, we have $f_1(x) | g^{\frac{f_1(x)-1}{2}} - 1$ or $f_1(x) | g^4 - 1$. By *Euler*'s criterion for *Legendre* symbol and by Condition 1, we get

$$g^{\frac{f_1(x)-1}{2}} \equiv \left(\frac{g}{f_1(x)}\right) \equiv \left(\frac{a}{f_1(x)}\right)^2\left(\frac{b}{f_1(x)}\right) = \left(\frac{b}{f_1(x)}\right) \equiv -1 \pmod{f_1(x)}$$

Which contradicts the fact that $f_1(x) | g^{\frac{f_1(x)-1}{2}} - 1$. Hence, $f_1(x) | g^4 - 1$, which also contradicts with $f_1(x) > g^4 > 1$. Therefore, g is a primitive root modulo $f_1(x)$.

By Hypothesis H, there exist infinitely many $x \in \mathbb{N}$ such that $f_1(x)$ and $f_2(x)$ are both primes. Therefore, g is a primitive root for infinitely many primes. $\square$

3.3 A fake Analouge

Finally, Hypothesis H fails over finite fields. In 1962, *Swan* noted that although $x^8 + \alpha^3$ over the ring $\mathbb{F}_2[\alpha]$ is irreducible and since it has no fixed prime polynomial divisor, all the other values over are composite.

Chapter 4

On Simultaneous Primitive Roots

This work has been done in collaboration with *F. Pappalardi* and published in *Acta Arithmetica* [2] . This paper was inspired by A. Granville at the Centre de Recherches Mathématiques of Montréal in January 2006. The authors would like to thank Denis R. Akhmetov and Sergei Konyagin for some useful comments.

4.1 Introduction

Given a prime p and $a \in \mathbb{Q}^*$, we say that a is a *primitive root modulo* p if p does not divide either the numerator or the denominator of a and the multiplicative order of a mod p equals $p-1$. Let $S = \{a_1, \ldots, a_r\} \subset \mathbb{Q}^* \setminus \{\pm 1\}$ and denote

$$\mathcal{P}_S = \{p \text{ prime } \mid \forall a \in S, a \text{ is a primitive root modulo } p\}.$$

In the case where $S \subset \mathbb{Z}$, assuming the Generalized Riemann Hypothesis for suitable number fields, it was proved by K. Matthews in 1976 [9] that $\mathcal{P}_S$ is finite if and only if at least one of the two following conditions is satisfied:

(α) There exist $1 \le i_1 < \cdots < i_{2s+1} \le r$ such that $a_{i_1} \cdots a_{i_{2s+1}} \in \mathbb{Q}^{*2}$;

(β) There exist $1 \le i_1 < \cdots < i_{2s} \le r$ such that $a_{i_1} \cdots a_{i_{2s}} \in -3\mathbb{Q}^{*2}$, and for all primes

$\ell \equiv 1 \bmod 3$ there exists at least one element of S which is a cube modulo ℓ.

Note that it is easy to verify without appealing to the GRH (see Proposition 23 below) that if either (α) or (β) are satisfied, then $\mathcal{P}_S$ is finite. In all other cases, not only $\mathcal{P}_S$ is infinite but it has non zero density (under GRH). The hypothesis that all the elements of S are integers does not seem crucial in Matthews work.

The goal of this note is to prove the conclusion of Matthews Theorem assuming the Schinzel's Hypothesis H as in [19]:

Hypothesis H (Schinzel, 1959) *Let $f_1, \dots, f_k \in \mathbb{Z}[x]$ be irreducible polynomials with positive leading 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 primes.*

We will prove the following

Theorem 22. *[2] Assume that Hypothesis H holds, let $S = \{a_1, \dots, a_r\} \subset \mathbb{Q}$ and assume*

1. *For each $1 \leq i_1 < \cdots < i_{2s+1} \leq r$ one has that $a_{i_1} \cdots a_{i_{2s+1}} \notin \mathbb{Q}^{*2}$;*

2. *If there exist $1 \leq i_1 < \cdots < i_{2s} \leq r$ such that $a_{i_1} \cdots a_{i_{2s}} \in -3\mathbb{Q}^{*2}$, then there exists a prime $\ell \equiv 1 \bmod 3$ such that none of the elements of S is a cube modulo ℓ.*

Then the set $\mathcal{P}_S$ is infinite.

When $r = 1$, the statement that $\mathcal{P}_{\{a_1\}}$ is infinite is the *Artin Conjecture for primitive roots*. It was proven to hold under the assumption of the Generalized Riemann Hypothesis by C. Hooley in 1967 [6]. It was also considered by Schinzel and Sierpinski in [19, page 199] as an example of application of Hypothesis H that they proved to imply Artin Conjecture.

Remark. Suppose that $S = \{q_1 b_1^3, q_2 b_2^3, q_1 q_2 b_3^3, q_1^2 q_2 b_4^3\}$ where q_1 and q_2 are distinct primes different from 3 and $b_1, b_2, b_3, b_4 \in \mathbb{Q}^*$. Then, for all primes $p \equiv 1 \bmod 3$, at least one element of S is congruent to a cube modulo p.

Proposition 23. *[16] Let $S = \{a_1, \ldots, a_r\} \subset \mathbb{Q}^* \setminus \{\pm 1\}$ such that if either (α) or (β) are satisfied. Then, $\mathcal{P}_S$ is finite.*

Proof. If $p \in \mathcal{P}_S$, then $a_i^{\frac{p-1}{2}} \equiv -1(\bmod p)$ for all $i = 1, \ldots, r$. If (α) holds, then there exists $b \in \mathbb{Q}^*$ such that $a_{i_1} = b^2 a_{i_2} \cdots a_{i_{2s+1}}$. Hence

$$-1 \equiv a_{i_1}^{\frac{p-1}{2}} \equiv \left(b^2 a_{i_2} \cdots a_{i_{2s+1}}\right)^{\frac{p-1}{2}} \equiv 1 \bmod p$$

so that $p \mid 2$. If (β) holds and if $a_{i_1} \cdots a_{i_{2s}} = -3b^2$ for some $b \in \mathbb{Q}^*$, then

$$1 \equiv (a_{i_1} \cdots a_{i_{2s}})^{\frac{p-1}{2}} \equiv \left(\frac{-3}{p}\right) \bmod p$$

which implies that $p \equiv 1 \bmod 3$. From the second part of (β), there exists i_k such that $a_{i_k} \equiv c^3 \bmod p$ which contradicts the fact that a_{i_k} is a primitive root modulo p. $\square$

4.2 Lemmata

Given $S = \{a_1, \ldots, a_r\} \subset \mathbb{Q}^* \setminus \{\pm 1\}$, we set

$$\mathcal{L} = \{\ell \text{ prime} \mid v_\ell(a) \neq 0 \text{ for some } a \in S\}.$$

Then $\mathcal{L}$ is clearly finite. Furthermore, we set

$$\mathcal{L}' = \begin{cases} \mathcal{L} \cup \{-1\} & \text{if } S \not\subseteq \mathbb{Q}^{>0}; \\ \mathcal{L} & \text{otherwise.} \end{cases}$$

We write $\mathcal{L}' = \{\ell_1, \ldots, \ell_s\}$ and when $\mathcal{L}' \not\subseteq \mathbb{Q}^{>0}$ we assume that $\ell_1 = -1$. Further, we set $L = 4|\ell_1 \cdots \ell_s|$.

For each $j = 1, \ldots, r$, write $a_j = \ell_1^{e_{1j}} \cdot \ell_2^{e_{2j}} \cdots \ell_s^{e_{sj}}$. Then, the matrix

$$\mathcal{E} = \begin{pmatrix} e_{11} & \cdots & e_{s1} \\ \vdots & & \vdots \\ e_{1r} & \cdots & e_{sr} \end{pmatrix}$$

has coefficients in $\mathbb{Z}$ and the first condition in the statement of the Theorem implies that the sum of any odd number of rows of $\mathcal{E}$ is not the zero vector modulo 2. We claim that this implies that the linear system

$$\mathcal{E} \cdot \begin{pmatrix} X_1 \\ \vdots \\ X_s \end{pmatrix} = \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} \tag{4.1}$$

admits a solution in $(\mathbb{Z}/2\mathbb{Z})^s$. Indeed perform a Gauss elimination on the rows of the enlarged matrix obtained attaching to $\mathcal{E}$ the column of 1's. We obtain a row echelon form. The last column has a "1" in the rows that were obtained adding together an odd number of the original rows and has a "0" in the rows that were obtained adding together an even number of rows. The first condition in the statement implies that whenever there is a "1" in the last entry of a row, that row contains at least one more entry with a "1". Therefore, the original system can be solved recursively.

We need the following

Lemma 24. *Assume that* $(x_1, \ldots, x_s) \in (\mathbb{Z}/2\mathbb{Z})^s$ *is a solution of the linear system* (4.1)*. Then, there exists an invertible integer* m *modulo* L *(i.e.* $\gcd(m, L) = 1$*) such that*

(i) *if* p *is prime with* $p \equiv m(\bmod L)$*, then* $\left(\frac{\ell_i}{p}\right) = (-1)^{x_i}$ *for all* $i = 1, \ldots, s$*;*

(ii) $m \not\equiv 1(\bmod \ell_i)$ *for all* $i = 1, \ldots, s$ *such that* $\ell_i > 3$.

Furthermore conclusion (ii)*. above also holds for* $\ell_i = 3$ *when* $\{-1, 3\} \nsubseteq \mathcal{L}'$ *and also when* $\{-1, 3\} \subseteq \mathcal{L}'$ *but* $x_i \neq x_1$*.*

Proof. We will first determine a congruence class m_4 for m modulo 4 and then its congruence class m_{ℓ_i} of m modulo each ℓ_i such that $\ell_i > 2$. If $2 \in \mathcal{L}$ we will also determine the congruence class m_8 of m modulo 8. Next, we will apply the Chinese Reminder Theorem and deduce the existence of a congruence class modulo L with the required properties.

The congruence class m_4 for m modulo 4 is defined by the following:

$$m_4 = \begin{cases} (-1)^{x_1} & \text{if } -1 \in \mathcal{L}'; \\ \\ -1 & \text{if } \{-1, 3\} \cap \mathcal{L}' = \emptyset; \\ \\ (-1)^{x_i+1} & \text{if } 3 \in \mathcal{L}', -1 \notin \mathcal{L}' \text{ and } \ell_i = 3. \end{cases}$$

In the event that $2 \in \mathcal{L}$ and that $\ell_j = 2$, then let m_8 be the unique invertible congruence class modulo 8 with the properties that $m_8 \equiv m_4(\bmod 4)$ and that

$$(m_8^2 - 1)/8 \equiv x_j(\bmod 2).$$

Note that if $p \equiv m_8(\bmod 8)$ then

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = (-1)^{x_j}.$$

For all other odd primes $\ell_i \in \mathcal{L}$, let m_{ℓ_i} be any of the $(\ell_i - 1)/2$ integers such that

$$\left(\frac{m_{\ell_i}}{\ell_i}\right) = (-1)^{x_i + (m_4-1)(\ell_i-1)/4}.$$

Note that: if p is a prime with $p \equiv m_{\ell_i}(\bmod \ell_i)$ and $p \equiv m_4(\bmod 4)$, by the quadratic reciprocity law, we have:

$$\begin{aligned} \left(\frac{\ell_i}{p}\right) &= (-1)^{(p-1)(\ell_i-1)/4} \left(\frac{p}{\ell_i}\right) \\ &= (-1)^{(m_4-1)(\ell_i-1)/4} \left(\frac{m_{\ell_i}}{\ell_i}\right) = (-1)^{x_i}. \end{aligned}$$

If $\ell_i > 3$, then $(\ell_i - 1)/2 > 1$. Therefore, there is always a choice for a class m_{ℓ_i} modulo ℓ_i with $m_{\ell_i} \not\equiv 1(\bmod \ell_i)$.

If $\ell_i = 3$ and $-1 \notin \mathcal{L}'$, then we have $m_3 \equiv 2(\bmod 3)$ since

$$\left(\frac{m_3}{3}\right) = (-1)^{x_i + (m_4-1)/2} = -1 = \left(\frac{2}{3}\right).$$

If $\ell_i = 3$ and $-1 = \ell_1 \in \mathcal{L}'$, then $m_3 \equiv 2(\mod 3)$ is verified if and only if

$$\left(\frac{m_3}{3}\right) = (-1)^{x_i+(m_4-1)/2} = (-1)^{x_i+x_1} = -1.$$

The latter is equivalent to $x_1 \neq x_i$ and this ends the proof of the Lemma. □

4.3 Proof of Theorem 22

A consequence of Lemma 24 is that if $L = 4|\ell_1 \cdots \ell_s|$ and m is the integer modulo L postulated in the statement of Lemma 24, then for any prime $p \equiv m \bmod L$,

$$\left(\frac{a_j}{p}\right) = \prod_{i=1}^{s} \left(\frac{\ell_i}{p}\right)^{e_{ij}} = (-1)^{e_{1j}x_1+\ldots+e_{sj}x_s} = -1. \tag{4.2}$$

Consequently, each a_i is a quadratic non residue modulo p.

Let us now prove the statement of the Theorem in the case when $\{-1, 3\} \nsubseteq \mathcal{L}'$ and also in the case when $\{-1, 3\} \subseteq \mathcal{L}'$ and it exists a solution $(x_1, \ldots, x_s) \in (\mathbb{Z}/2\mathbb{Z})^s$ of the linear system (4.1) where the components relative to -1 and to 3 are distinct.

Let $f_1(X) = m + LX$ and

$$f_2(X) = \begin{cases} (m-1)/2 + (L/2)X & \text{if } m \equiv 3 \bmod 4; \\ (m-1)/4 + (L/4)X & \text{if } m \equiv 5 \bmod 8; \\ (m-1)/8 + (L/8)X & \text{if } m \equiv 1 \bmod 8. \end{cases}$$

If $2 \notin \mathcal{L}$, we can assume that $m \not\equiv 1(\mod 8)$. So the condition $m \equiv 1 \bmod 8$ arises only on the case when $2 \in \mathcal{L}$ (i.e. $8 \mid L$) and the polynomial $f_2(X)$ has always integer coefficients.

Lemma 25. *Let f_1 and f_2 as above. Then the three integers*

$$f_1(0)f_2(0), \quad f_1(1)f_2(1), \quad f_1(2)f_2(2)$$

are coprime.

Proof. Let q be a prime dividing the gcd

$$\left(\frac{m(m-1)}{2^t}, \frac{(m+L)(m-1+L)}{2^t}, \frac{(m+2L)(m-1+2L)}{2^t}\right) \tag{4.3}$$

where $t = 1, 2, 3$ according to $m \equiv 3(\mod 4)$, $m \equiv 5(\mod 8)$ or $m \equiv 1(\mod 8)$

If q is odd and $q|m(m-1)$ then either $q \mid m$ or $q \mid m-1$.

In the first instance, $q \nmid m+L$ and $q \nmid m+2L$ since $\gcd(m, L) = 1$. If it happened that $q \mid (m-1+L)$ and $q \mid (m-1+2L)$ then $q \mid L$ which is a contradiction.

In the second instance observe that $q \nmid L$ by (ii) of Lemma 24. Therefore, $q \nmid m-1+L$ and $q \nmid m-1+2L$. If $q \mid (m+L)$ and $q \mid (m+2L)$ then $q \mid L$ which is again a contradiction.

Next note that $\frac{m(m-1)}{2^t}$ is odd unless $m \equiv 1(\mod 8)$. So if $q = 2$, then $16 \mid (m-1)$ and since $m+L$ is odd, this implies that $16 \mid (m-1+L)$ and the contradiction that $16 \mid L$. $\square$

From Lemma 25 we deduce that the conditions for Schinzel's Hypothesis H in [19] are satisfied and so there exists infinitely many x such that $f_1(x)$ and $f_2(x)$ are both primes. Hence, there exist infinitely many primes $p \equiv m \bmod L$ that have the form

$$p = \begin{cases} 1+2q & \text{if } m \equiv 3 \bmod 4; \\ 1+4q & \text{if } m \equiv 5 \bmod 8; \\ 1+8q & \text{if } m \equiv 1 \bmod 8, \end{cases}$$

where q is also prime.

Let p be sufficiently large so that none of the a_i's can have as order a divisor of 8. It will be enough to require that $p > \max\{|b_i^8 - c_i^8|, i = 1, \dots, r\}$ where $a_i = b_i/c_i$. From this position we deduce that

$$a_i^{(p-1)/q} \not\equiv 1 \bmod p.$$

Furthermore, the condition

$$-1 = \left(\frac{a_i}{p}\right) \equiv a_i^{(p-1)/2} \bmod p$$

observed in (4.2) implies that $a_i^{(p-1)/2} \not\equiv 1 \bmod p$. Finally, each a_i is a primitive root modulo p and this concludes the proof of the particular case of the Theorem.

We are now left with the case when $\{-1, 3\} \subseteq \mathcal{L}'$ and the solutions $(x_1, \dots, x_s) \in (\mathbb{Z}/2\mathbb{Z})^s$ of the linear system (4.1) are all such that components relative to -1 and to 3 are equal.

Let us prove the following

Lemma 26. *Let $\mathcal{E}$ be a matrix with s columns, r rows and entries in $\mathbb{Z}/2\mathbb{Z}$. Assume that the first two columns of $\mathcal{E}$ are non zero and that the linear system*

$$\mathcal{E}\cdot\begin{pmatrix}X_1\\ \vdots\\ X_s\end{pmatrix}=\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix}$$

is solvable in $(\mathbb{Z}/2\mathbb{Z})^s$ and such that each solution $(x_1,\ldots,x_s)$ verifies $x_1=x_2$. Then there exists an even number of rows of $\mathcal{E}$ such that their sum is the vector $(0,\ldots,0,1,1)\in(\mathbb{Z}/2\mathbb{Z})^s$.

Proof. After performing a complete Gauss elimination on the extended matrix, we obtain an extended matrix in row echelon form. We can obtain an extended matrix such that there will 1's in the first two entries of the first row. The only possibility for the above equation to produce solutions where the first two components are always equal is that $k=2$ and that $C=0$. The equality $C=0$ implies that the first row of our matrix was produced by the original matrix summing an even number of rows , and this leads to the statement of the lemma. □

From Lemma 26 we deduce that when $\{-1,3\}\subseteq\mathcal{L}'$ and all the solutions $(x_1,\ldots,x_s)\in(\mathbb{Z}/2\mathbb{Z})^s$ of the linear system (4.1) are such that components relative to -1 and to 3 are equal then there exists an even number of indexes $1\le i_1<\cdots<i_{2s}\le r$ such that $a_{i_1}\cdots a_{i_{2s}}\in-3(\mathbb{Q}^*)^2$.

The second condition in the statement of the Theorem implies that there exists a prime $\ell\equiv 1 \bmod 3$ such that none of $a_1,\ldots,a_r$ is a perfect cube modulo ℓ. Now, we need the following:

Lemma 27. *Let $a_1\ldots a_r\in\mathbb{Q}^*\setminus\{\pm1\}$ and suppose that*

(a) *for every* $1 \leq i_1 < \ldots < i_{2t+1} \leq r$, $a_{i_1} \cdots a_{i_{2t+1}} \notin (\mathbb{Q}^*)^2$*;*

(b) *there exists* $1 \leq j_1 < \ldots < j_{2t} \leq r$ *such that* $a_{j_1} \cdots a_{j_{2t}} \in -3(\mathbb{Q}^*)^2$*;*

(c) *there exists a prime* $\ell \equiv 1 \bmod 3$ *such that each of* $a_1, \ldots, a_r$ *is a cubic non residue modulo* ℓ*.*

Then, there exists another prime $q \equiv 1 \bmod 3$ *such that each of* $a_1, \ldots, a_r$ *is both a cubic non residue and a quadratic non residue modulo* q*.*

Proof. Let $K_0 = \mathbb{Q}(\sqrt{-3})$, $\quad K_1 = K_0(a_1^{1/3}, \ldots, a_r^{1/3})$ and $K_2 = \mathbb{Q}(a_1^{1/2}, \ldots, a_r^{1/2})$. We have that $K_0 \subset K_2$ in virtue of hypothesis (b) in the statement. Furthermore, the two field extensions K_1/K_0 and K_2/K_0 are abelian and linearly disjoint by Theorem 8.1 in [8]. Let λ be a prime of K_0 above ℓ and consider the *Artin symbol* $\sigma_\lambda \in \mathrm{Gal}(K_1/K_0)$. By definition $\sigma_\lambda(a_i^{1/3}) \neq a_i^{1/3}$ for all $i = 1, \ldots, r$. Similarly let $p \equiv 1 \bmod 3$ be a prime such that $\left(\frac{a_i}{p}\right) = -1$ for all $i = 1 \ldots, r$. The existence of such a p is guaranteed by Lemma 24. If π is a prime of K_0 above p, then the *Artin symbol* $\sigma_\pi \in \mathrm{Gal}(K_2/K_0)$ verifies $\sigma_\pi(a_i^{1/2}) = -a_i^{1/2}$ for all $i = 1, \ldots, r$. Since

$$\mathrm{Gal}(K_1K_2/K_0) \cong \mathrm{Gal}(K_1/K_0) \times \mathrm{Gal}(K_2/K_0),$$

by the Chebotarev Density Theorem (see for example [17, page 552]), there exists a prime η of K_0 such that $(\sigma_\lambda, \sigma_\pi) = \sigma_\eta$. Finally, the prime $q = N(\eta) \in \mathbb{Z}$ will have the required properties. $\square$

Lemma 28. *Let* $S = \{a_1 \ldots a_r\} \subset \mathbb{Q}^* \setminus \{\pm 1\}$ *for which the hypotheses of Lemma* 27 *are satisfied and let* $q \equiv 1 \bmod 3$ *be a prime such that each of* $a_1, \ldots, a_r$ *is both a cubic non* *residue and a quadratic non residue modulo q. Let η be a primary prime in $\mathbb{Z}[\omega]$ ($\omega = (-1+\sqrt{-3})/2$) with norm q. Then there exists $L' \in \mathbb{Z}$ such that for all primes $\pi \in \mathbb{Z}[\omega]$ such that $\pi \equiv \eta \bmod L'$, one has that, if $p = N(\pi)$, then each of $a_1, \ldots, a_r$ is both a cubic non residue and a quadratic non residue modulo p.*

Proof. Let us show that as L' one can take

$$L' = 12 \cdot \prod_{\substack{\ell \text{ prime:} \\ \exists a \in S, v_\ell(a) \neq 0}} \ell = 3L.$$

We want to show that any π is a primary prime in $\mathbb{Z}[\omega]$ such that $\pi \equiv \eta \bmod L'$ satisfies the required properties.

To this end, set

$$\mathfrak{L} = \{\omega, 1-\omega\} \cup \{\lambda \in \mathbb{Z}[\omega], \lambda \text{ primary prime and } \exists a \in S, v_\lambda(a) \neq 0\}$$

and write $\mathfrak{L} = \{\lambda_1, \lambda_2, \lambda_3, \ldots, \lambda_s\}$, where $\lambda_1 = \omega$, $\lambda_2 = 1 - \omega$. We have

$$a_i = \pm \lambda_1^{e_{1i}} \cdots \lambda_s^{e_{si}}, \quad \left[\frac{a_j}{\eta}\right]_3 = \omega^{t_j} (\text{with } t_j \in \{\pm 1\}).$$

For any $i = 3, \ldots, s$ we have that $\pi \equiv \eta \bmod L'$ implies $\pi \equiv \eta \bmod \lambda_i$. So by cubic reciprocity (see for example [1, 7])

$$\left[\frac{\lambda_i}{\eta}\right]_3 = \left[\frac{\lambda_i}{\pi}\right]_3.$$

While $\pi \equiv \eta \bmod 9$ implies

$$\left[\frac{\omega}{\eta}\right]_3 = \left[\frac{\omega}{\pi}\right]_3 \text{ and } \left[\frac{1-\omega}{\eta}\right]_3 = \left[\frac{1-\omega}{\pi}\right]_3.$$

So, automatically we have that

$$\left[\frac{a_j}{\eta}\right]_3 = \left[\frac{a_j}{\pi}\right]_3 \quad \forall j = 1, \ldots, r,$$

which implies that none of the a_i's is a cube modulo $N(\pi)$.

We also claim that if $p = N(\pi)$, then for all $i = 1, \dots, r$

$$\left(\frac{a_i}{p}\right) = \left(\frac{a_i}{q}\right) = -1.$$

Indeed since $\pi = \eta + 3L\alpha$ for a suitable $\alpha \in \mathbb{Z}[\omega]$, we have $p = N(\pi) \equiv q \bmod 3L$ and by applying one more time the quadratic reciprocity law, we obtain the claim. $\square$

If $\eta, L' \in \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ are the elements in Lemma 28, then let

$$f(X) = N(\eta + \alpha X) = N(L')X^2 + L' \operatorname{Tr}(\eta)X + q \in \mathbb{Z}[X].$$

It is clear from the definition of L' and η that $f(X) \equiv 1 \bmod 3$ and whenever $x \in \mathbb{N}$ is such that $p = f(x)$ is prime, then each of $a_i, \dots, a_r$ is both a cubic and a quadratic non residue modulo p. Furthermore let

$$g(X) = \begin{cases} (f(X)-1)/6 & \text{if } \ell \equiv 3 \bmod 4; \\ (f(X)-1)/12 & \text{if } \ell \equiv 5 \bmod 8; \\ (f(X)-1)/24 & \text{if } \ell \equiv 1 \bmod 8. \end{cases}$$

In a very similar way as we did above, we can check that the conditions of Schinzel's Hypothesis H in [19] are satisfied for f and g; therefore, there exists infinitely many x such that $f(x)$ and $g(x)$ are both primes. These primes p have the form

$$p = \begin{cases} 1 + 6q & \text{if } \ell \equiv 3 \bmod 4; \\ 1 + 12q & \text{if } \ell \equiv 5 \bmod 8; \\ 1 + 24q & \text{if } \ell \equiv 1 \bmod 8, \end{cases}$$

where q is also prime and moreover none of the a_i's is either a square or a cube modulo p.

Let now p be sufficiently large so that none of the a_i's can have as order a divisor of 24. Since in this case for each i, $a_i^{(p-1)/2} \equiv -1 \bmod p$ and $a_i^{(p-1)/3} \not\equiv 1 \bmod p$, each a_i is a primitive root modulo p and this concludes the proof on the Theorem.

Chapter 5

A Characterization for Schinzel-Wójcik Problem for "Odd Rationals" under Hypothesis H

5.1 Introduction

In this Chapter, I am going to introduce a characterization, under Hypothesis H, of the r-tuples of off rational numbers (i.e. rational numbers supported at odd primes) for which the *Schinzel-Wójcik problem* has an affimative answer. That is,

Theorem 29. *Let* $\{a_1, \ldots, a_r\} \subset \mathbb{Q}^* \setminus \{\pm 1\}$, $v_2(a_i) = 0 \,\text{for all}\, i = 1, \ldots, r$. *Assuming Hypothesis H, then Schinzel-Wójcik problem has an affimative answer for* $\{a_1, \ldots, a_r\}$ *if and only if at least one of the following two conditions is satisfied :*

1. $-1 \notin \langle a_1, \ldots, a_r \rangle$ *;*
2. *For every* $\nu_1, \ldots, \nu_r \in \mathbb{Z}$, *if* $a_1^{\nu_1} \cdots a_r^{\nu_r} = 1$, *then* $\nu_1 + \cdots + \nu_r \equiv 0 \pmod 2$.

Let us recall two results that are already had proved and represent some parts of the characterization. One is due to *Wójcik* in 1996.

Theorem 30. *Wójcik (1996)[23]. Let $K/\mathbb{Q}$ be a finite extension and $a_1, \cdots, a_r \in K \setminus \{0,1\}$ be such that the multiplicative group $\langle a_1, \ldots, a_r\rangle \subset K$ is torsion free. Then, the Schinzel* Hypothesis H *implies that there exist infinitely many primes $\mathfrak{p}$ of degree 1 such that* $\operatorname{ord}_{\mathfrak{p}} a_1 = \cdots = \operatorname{ord}_{\mathfrak{p}} a_r$.

The other one is due to *F. Pappalardi* and *A.Susa* in 2006.

Proposition 31. *[16] Let $\{a_1, \ldots, a_r\} \subset \mathbb{Q}^* \setminus \{0, \pm 1\}$ be such that both the following properties are satisfied:*

(i) *there exist $\omega_1, \ldots, \omega_r \in \mathbb{Z}$ with $a_1^{\omega_1} \cdots a_r^{\omega_r} = -1$;*

(ii) *there exist $\nu_1, \ldots, \nu_r \in \mathbb{Z}$ with $\nu_1 + \cdots + \nu_r$ is odd and $a_1^{\nu_1} \cdots a_r^{\nu_r} = 1$.*

Then the Schinzel–Wójcik problem for $a_1, \ldots, a_r$ has a negative answer.

Proof. Assume that $\delta = \operatorname{ord}_p a_1 = \ldots = \operatorname{ord}_p a_r$ for some $p > 2$. Since $-1 = a_1^{\omega_1} \cdots a_r^{\omega_r}$ for suitable $\omega_1, \ldots, \omega_r \in \mathbb{Z}$, we have $(-1)^\delta \equiv a_1^{\delta\omega_1} \cdots a_r^{\delta\omega_r} \equiv 1 \mod p$. This implies that $2 \mid \delta$. For each $i = 1, \ldots, r$, $a_i^{\delta/2} \equiv -1 \mod p$. Therefore, we have $1 = (a_1^{\nu_1} \cdots a_r^{\nu_r})^{\delta/2} \equiv (-1)^{\nu_1 + \cdots + \nu_r} \mod p$ which is a contradiction to the second hypothesis. □

It is clear that to complete the proof of Theorem 29, in light of Theorem 30, Theorem 32 and Proposition 31, we need to prove the following:

Theorem 32. *Let $\{a_1, \ldots, a_r\} \subset \mathbb{Q}^* \setminus \{\pm 1\}$, $v_2(a_i) = 0$ for all $i = 1, \cdots, r$ such that*

1. $-1 \in \langle a_1, \ldots, a_r\rangle$ *;*

2. For every $\nu_1, \ldots, \nu_r \in \mathbb{Z}$, if $a_1^{\nu_1} \cdots a_r^{\nu_r} = 1$, then $\nu_1 + \cdots + \nu_r \equiv 0 \,(\mathrm{mod}\, 2)$,

then Hypothesis H *implies the existence of infinitely many prime numbers p such that*

$$\langle a_1 \mod p \rangle = \langle a_2 \mod p \rangle = \cdots = \langle a_r \mod p \rangle .$$

5.2 Lemmata

We shall follow the approach of the proof of Theorem 30 from [23].

Lemma 33. *Suppose that $k, F \in \mathbb{N}$ are such that $k \mid F$. Suppose that $\ell_1, \ldots, \ell_n$ are odd prime numbers such that $\ell_j \nmid k$ for all $j = 1, \ldots, n$. For all rational integers $x_1, \ldots, x_n \in \mathbb{Z}/k\mathbb{Z}$, and for every integer $t \equiv 1 \bmod k$ such that $\gcd(t, F) = 1$, with the property that there exists infinitely many primes $\mathfrak{q}$ in $\mathbb{Q}(\zeta_k)$ of degree one such that:*

$$\left[\frac{\ell_i}{\mathfrak{q}}\right]_k = \zeta_k^{x_i} \quad (1 \leq i \leq m), \qquad N\mathfrak{q} \equiv t \mod F.$$

Proof. Let $\zeta_k = e^{2\pi i/k}$. Since

$$L = \mathbb{Q}\left(\zeta_k, \ell_1^{1/k}, \ell_2^{1/k}, \ldots, \ell_n^{1/k}\right)$$

is finite abelian Galois extension of $\mathbb{Q}(\zeta_k)$, by Kummer Theory, we have

$$\begin{aligned}\mathrm{Gal}(L/\mathbb{Q}(\zeta_k)) &\cong \langle \ell_1, \ldots, \ell_n\rangle\,(\mathbb{Q}(\zeta_k)^*)^k/(\mathbb{Q}(\zeta_k)^*)^k \\ &\cong \prod_{j=1}^{n} \langle \ell_j\rangle\,(\mathbb{Q}(\zeta_k)^*)^k/(\mathbb{Q}(\zeta_k)^*)^k.\end{aligned}$$

We deduce that $[L : \mathbb{Q}(\zeta_k)] = |\,\mathrm{Gal}\, L/\mathbb{Q}(\zeta_k)\,| = k^n$, since by the hypothesis that $\ell_j \nmid 2k$,

$$\langle \ell_j\rangle(\mathbb{Q}(\zeta_k)^*)^k/(\mathbb{Q}(\zeta_k)^*)^k \cong \mathbb{Z}/k\mathbb{Z} \quad j = 1, \ldots, n.$$

Furthermore

$$[L(\zeta_F) : \mathbb{Q}] = k^n \varphi(F)$$

and, if $x_1, \cdots, x_n \in \mathbb{Z}/k\mathbb{Z}$ and $\overline{s} \in \mathrm{Gal}(\mathbb{Q}(\zeta_F)/\mathbb{Q})$, then there exists $\sigma \in \mathrm{Gal}(L(\zeta_F)/\mathbb{Q})$ such that

$$\sigma(\zeta_F) = s(\zeta_F), \qquad \sigma(\ell_i^{1/k}) = \zeta_k^{x_i}\ell_i^{1/k}, \quad i = 1, \cdots, n.$$

By Chebotarev's Density Theorem, there exist infinitley many degree one prime ideals $\mathfrak{q}$ in $\mathbb{Q}(\zeta_k)$ such that $\left[\frac{L}{\mathfrak{q}}\right] = \sigma$, where $\left[\frac{L}{\mathfrak{q}}\right]$ denotes the Artin symbol.

If $N(\mathfrak{q})$ is sufficiently large, we obtain

$$\left[\frac{\ell_i}{\mathfrak{q}}\right]_k \ell_i^{1/k} \equiv \ell_i^{(N(\mathfrak{q})-1)/k}\ell_i^{1/k} \equiv \left(\ell_i^{1/k}\right)^{N(\mathfrak{q})} \equiv \left[\frac{L}{\mathfrak{q}}\right]\ell_i^{1/k} \equiv \zeta_k^{x_i}\ell_i^{1/k} \pmod{\mathfrak{q}}.$$

and

$$\zeta_F^{N(\mathfrak{q})} \equiv \left[\frac{L}{\mathfrak{q}}\right]_k \zeta_F \equiv \zeta_F^t \pmod{\mathfrak{q}}$$

Hence,

$$\left[\frac{\ell_i}{\mathfrak{q}}\right]_k = \zeta_k^{x_i} \quad \text{and} \quad N(\mathfrak{q}) \equiv t \pmod{F}.$$

$\square$

The following lemma is due to *Wójcik* in [23, Lemma 5].

Lemma 34. *[23] Suppose that $k, F \in \mathbb{N}$ satisfy the condition $k^{\varphi(k)+1}(2\varphi(k))! \mid F$. Let q_0 be a prime such that*

$$q_0 \equiv 1 \mod k, \quad q_0 \nmid F \quad \textit{and} \quad \gcd(\frac{q_0 - 1}{k}, F) = 1.$$

Then there exists a polynomial $f(X) \in \mathbb{Z}[X]$ such that $f(X)$ and $(f(X)-1)/k$ satisfy the assumptions of Hypothesis H *and, if $q = f(x)$ is prime for $x \in \mathbb{N}$, then $\mathfrak{q} \sim \mathfrak{q}_0^{-1} \mod F$ where $\mathfrak{q}$ and $\mathfrak{q}_0$ are primes of $\mathbb{Q}(\zeta_k)$ such that $q_0 = N(\mathfrak{q}_\circ)$ and $q = N(\mathfrak{q})$.*

5.3 Proof of Theorem 32

Proof. Let $k = 2^\alpha$ where α is large enough be determined later and let $F \in \mathbb{N}$ be such that Lemma 34 can be applied. Suppose that $\{a_1, \ldots, a_r\} \in \mathbb{Q}^* \setminus \{\pm 1\}$ are such that $-1 \in \langle a_1, \ldots, a_r \rangle$ for all $j \in \{1, \ldots, r\}$. Let

$$\mathcal{L} = \{\ell \text{ prime } : v_\ell(a_j) \neq 0 \text{ for some } j \in 1, \ldots, r\}.$$

Write $\mathcal{L} = \{\ell_1, \ldots, \ell_n\}$ and, for each $j = 1, \ldots, r$,

$$a_j = (-1)^{e_{0j}} \cdot \ell_1^{e_{1j}} \cdot \ell_2^{e_{2j}} \cdots \ell_n^{e_{nj}}$$

where $e_{ij} \in \mathbb{Z}$ for all $1 \leqslant i \leqslant n, 1 \leqslant j \leqslant r$. Define the matrix

$$A := \begin{pmatrix} e_{11} & \cdots & e_{n1} \\ \vdots & & \vdots \\ e_{1r} & \cdots & e_{nr} \end{pmatrix}.$$

Next set $t = 1 + k \in \mathbb{N}$ and suppose that $x_1, \ldots, x_n \in \mathbb{Z}/k\mathbb{Z}$ have the property that there exist prime ideal $\mathfrak{q}_0$ in $\mathbb{Q}(\zeta_k)$ of degree one ($N\mathfrak{q}_0 := q_0$) with the properties:

$$\left[\frac{\ell_i}{\mathfrak{q}_0}\right]_k = \zeta_k^{x_i} \quad 1 \leq i \leq m, \qquad N\mathfrak{q}_0 \equiv t \mod F.$$

Then, $\left[\frac{-1}{\mathfrak{q}_0}\right]_k = (-1)^{(N\mathfrak{q}_0 - 1)/k} = -1$ and

$$\begin{aligned} \left[\frac{a_j}{\mathfrak{q}_0}\right]_k &= \left[\frac{-1}{\mathfrak{q}_0}\right]_k^{e_{0j}} \cdot \left[\frac{\ell_1}{\mathfrak{q}_0}\right]_k^{e_{1j}} \cdots \left[\frac{\ell_n}{\mathfrak{q}_0}\right]_k^{e_{nj}} \\ &= (-1)^{e_{0j}} \zeta_k^{x_1 e_{1j}} \zeta_k^{x_2 e_{2j}} \cdots \zeta_k^{x_n e_{nj}} \\ &= (-1)^{e_{0j}} \zeta_k^{e_{1j} x_1 + \cdots + e_{nj} x_n}. \end{aligned}$$

To prove that $\left[\frac{a_j}{\mathfrak{q}_0}\right]_k = -1 = \zeta_k^{k/2}$, it is equivalent to prove that the following system of congruences is solvable:

$$A \cdot \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix} \equiv \begin{pmatrix} 2^{\alpha-1}(1+e_{10}) \\ \vdots \\ 2^{\alpha-1}(1+e_{r0}) \end{pmatrix} (\mathrm{mod} 2^\alpha). \tag{5.1}$$

By applying the method that has been introduced in Chapter 2, we get the following equivalent system:

$$\begin{cases} d_1x_1 & \equiv & k_1 & (\mathrm{mod} 2^\alpha) \\ & \vdots & & \\ d_sx_s & \equiv & k_s & (\mathrm{mod} 2^\alpha) \\ 0 & \equiv & k_{s+1} & (\mathrm{mod} 2^\alpha) \\ & \vdots & & \\ 0 & \equiv & k_n & (\mathrm{mod} 2^\alpha) \end{cases}$$

with $d_i = 2^{\beta_i}, i = 1, \ldots, s$ and $k_i \in \{0, 2^{\alpha-1}\}$, $i = 1, \ldots, n$.

The second condition in the statement of Theorem 32 implies that, in order to obtain zero on the left side above, an even number of raws have to be added. Hence $k_i = 0$ for $i = s+1, \ldots, n$.

Furthermore, since k_i is 0 or $2^{\alpha-1}$ for all $i = 1, \ldots, s$, if we choose α sufficiently large so that $d_i < 2^{\alpha-1}$ for all $i = 1, \ldots, s$, we obtain a compatible system of cogruences. Therefore, by Lemma 33, $\left[\frac{a_j}{\mathfrak{q}_0}\right]_k = -1$ for all $j = 1, \dots, r$.

By applying Lemma 34, we deduce that there are infinitely many x such that $q = f(x)$ and $p = (f(x) - 1)/k$ are both primes. Moreover, $\mathfrak{q} \sim \mathfrak{q}_0^{-1} \mod F$ where $\mathfrak{q}$ and is primes of $\mathbb{Q}(\zeta_k)$ such that $q = N(\mathfrak{q})$. Hence,

$$a_j^{\frac{q-1}{k}} \equiv \left[\frac{a_j}{\mathfrak{q}}\right]_k = \left[\frac{a_j}{\mathfrak{q}_0}\right]_k^{-1} = -1 \pmod{\mathfrak{q}} \qquad \text{for all } j = 1, \dots, r.$$

Therefore,

$$a_j^p \equiv -1 \pmod{\mathfrak{q}} \qquad \text{for all } j = 1, \dots, r.$$

Thus,

$$a_j^p \equiv -1 \pmod{q} \qquad \text{for all } j = 1, \dots, r.$$

Hence,

$$a_j^{2p} \equiv 1 \pmod{q} \qquad \text{for all } j = 1, \dots, r.$$

For sufficiently large $q = 2^\alpha p + 1$,

$$\langle a_1 \mod q\rangle = \langle a_2 \mod q\rangle = \cdots = \langle a_r \mod q\rangle = 2p.$$

$\square$

Chapter 6

The Average of Schinzel–Wójcik problem

6.1 Introduction

One of the famous standard problems in Multiplicative Number Theory is studying the average of the values of an arthematic functions. The average of the famous arthimetic functions like $\varphi(n), \tau(n), \sigma(n), \Omega(n), \omega(n)$ has been considered extremely. I will recall again some results on the average version of *Artin's* conjecture on primitive roots and some generalizations of *Artin's* conjecture then I will introduce my work on the Average of Schinzel–Wójcik problem.

In 1969, *P.J. Stephens* [21] proved, free of any hypothesis, that *Artin's* conjecture on average holds. More preciesly,

Theorem 35. *[21] If* $T > \exp(4(\log x \log\log x)^{\frac{1}{2}})$, *then*

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

where $A = \prod_{\ell} \left(1 - \frac{1}{\ell(\ell-1)}\right)$ *is Artin's constant, and the constant* $D > 1$ *is arbitrary.*

Also, he proved the following:

Theorem 36. *[21] Let* A *be Artin's constant, and* $E > 2$ *be an arbitrary real number. Then, for* $T > \exp(6(\log x \log\log x)^{\frac{1}{2}})$*, we have*

$$\frac{1}{T} \sum_{a \leq T} \{N_a(x) - A \operatorname{li} x\}^2 \ll \frac{x^2}{(\log x)^E} \qquad (\textit{as } x \longrightarrow \infty)\,.$$

Moreover, by using the normal order method of Turan, he proved that the number of exceptions is bounded by $O(T)$ when $T > \exp(6(\log x \log\log x)^{\frac{1}{2}})$ and as T, x tends to infinity.

In 2015, *C. Pehlivan* and *L. Menici* [13] studied the average behaviour of $N_{\Gamma,m}(x)$, which is defined in Chapter 1, where $\Gamma = \langle a_1, \cdots, a_r \rangle \subseteq \mathbb{Z}^r$. They proved the following results:

Theorem 37. *[13] Assume* $T^* := \min\{T_i : i = 1, \ldots, r\} > \exp(4(\log x \log\log x)^{\frac{1}{2}})$ *and* $m \leq (\log x)^D$ *for an arbitrary positive constant* D*. Then*

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

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

Theorem 38. *[13] if* $T^* > \exp(6(\log x \log\log x)^{\frac{1}{2}})$*, then*

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

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

By using the *Euler* product expansion and some properties of *Euler* function, they showed that

$$C_{r,m} = \frac{1}{m^{r+1}} \prod_{p \mid m} \left(1 - \frac{p}{p^{r+1} - 1}\right)^{-1} C_r$$

where $C_r = \prod_{\ell} \left(1 - \frac{1}{\ell^r - 1}\right)$ is r-rank *Artin* constant. They also proved that, for $T_i > \exp(4(\log x \log\log x)^{\frac{1}{2}})$ for all $i = 1, \ldots, r$, $m \leq (\log x)^D$ and any constant $M > 2$,

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

where $J_r(n)=n^r\prod_{\ell|n}(1-1/\ell^r)$ is the so called *Jordan's totient function*. The above is a generalization of Moree's result in [10].

6.2 Schinzel–Wójcik Problem on Average

Now, let us discuss *Schinzel–Wójcik* problem on average. Define the counting function

$$S_{\underline{a},m}(x)=\#\left\{p\leqslant x:\mathrm{ord}_p a_1=\ldots=\mathrm{ord}_p a_r=\frac{p-1}{m}\right\},\quad \text{where } \underline{a}=(a_1,\cdots,a_r)\,.$$

Define

$$M_m(x):=\sum_{p\le x}\left(\frac{\varphi((p-1)/m)}{(p-1)/m}\right)^r,\quad f(k)=\sum_{\substack{(d_1,\ldots,d_r)\in\mathbf{N}^r\\ k=[d_1,\cdots,d_r]}}\frac{\mu(d_1)\cdots\mu(d_r)}{d_1\cdots d_r}$$

and

$$g(k)=\sum_{\substack{(d_1,\ldots,d_r)\in\mathbb{N}^r\\ k=[d_1,\cdots,d_r]}}\frac{\mu^2(d_1)\cdots\mu^2(d_r)}{d_1\cdots d_r}.$$

It is clear that f and g are multiplicative in k, they are zero for any non-square free integer, $f(\ell)=(1-\frac{1}{\ell})^r-1$, $g(\ell)\le\dfrac{2^r}{\ell}$ for any prime number ℓ and $g(k)\le\dfrac{2^{r\omega(k)}}{k}$ for any $k\in\mathbb{N}$.

Lemma 39.

$$\sum_{k>T}\frac{2^{r\omega(k)}}{k^2}\ll\frac{(\log T)^{2^r-1}}{T}$$

for sufficiently large T.

Proof. By using Wirsing Theorem [11], it is simple to show that

$$A(X):=\sum_{n\le X}2^{r\omega(n)}\sim c_rX(\log X)^{2^r-1},\quad\text{for some constant } c_r$$

Then by using *partial sumation*, we get

$$\sum_{k>T} \frac{2^{r\omega(k)}}{k^2} = -\frac{A(T)}{T^2} + 2\int_T^\infty \frac{A(t)dt}{t^3} \le 2\int_T^{T^2} \frac{A(t)dt}{t^3} + 2\int_{T^2}^\infty \frac{A(t)dt}{t^3}$$

and since for large T, we have

$$\int_{T^2}^\infty \frac{A(t)dt}{t^3} \le \int_{T^2}^\infty \frac{dt}{t^{3/2}} \ll \frac{1}{T}$$

and

$$\int_T^{T^2} \frac{A(t)dt}{t^3} \le \log^{2^r-1} T^2 \int_T^{T^2} \frac{dt}{t^2} \ll \frac{(\log T)^{2^r-1}}{T}.$$

Therefore,

$$\sum_{k>T} \frac{2^{r\omega(k)}}{k^2} \ll \frac{(\log T)^{2^r-1}}{T}$$

□

Lemma 40.

$$M_m(x) = \frac{\mathrm{li}(x)}{\varphi(m)} \prod_\ell \left(1 + \frac{\varphi((m,\ell))f(\ell)}{\varphi(\ell)(m,\ell)}\right) + O\left(\frac{x}{\log^{\min\{C-1,B\}} x}\right)$$

for any positve integers B *and* C.

Proof.

$$M_m(x) = \sum_{p\le x} \left(\sum_{d|\frac{p-1}{m}} \frac{\mu(d)}{d}\right)^r = \sum_{p\le x} \sum_{\substack{d_1,\ldots,d_r\in\mathbb{N} \\ [d_1,\ldots,d_r]|\frac{p-1}{m}}} \frac{\mu(d_1)\cdots\mu(d_r)}{d_1\cdots d_r}$$

$$= \sum_{\substack{d_1,\ldots,d_r\in\mathbb{N} \\ d_1\le x,\ldots,d_r\le x}} \frac{\mu(d_1)\cdots\mu(d_r)}{d_1\cdots d_r}\pi(x,1;m[d_1,\ldots,d_r])$$

$$= \sum_{\substack{d_1,\ldots,d_r\in\mathbb{N} \\ m[d_1,\ldots,d_r]\le\log^{B+2^r-1} x}} \frac{\mu(d_1)\cdots\mu(d_r)}{d_1\cdots d_r}\pi(x,1;m[d_1,\ldots,d_r]) + E_B(x,m),$$

where

$$E_B(m,x) \le \sum_{\substack{d_1,\ldots,d_r\in\mathbb{N} \\ [d_1,\ldots,d_r]>(\log^{B+2^r-1} x)/m}} \frac{\pi(x,1;m[d_1,\ldots,d_r])\mu^2(d_1)\cdots\mu^2(d_r)}{d_1\cdots d_r}$$

$$
\begin{aligned}
&\le \sum_{\substack{d_1,\ldots,d_r\in\mathbb{N}\\ [d_1,\ldots,d_r]>(\log^{B+2^r-1}x)/m}} \frac{\#\{n\le x : m[d_1,\ldots,d_r]\mid n-1\}\mu^2(d_1)\cdots\mu^2(d_r)}{d_1\cdots d_r}\\
&\le \frac{x}{m}\sum_{\substack{d_1,\ldots,d_r\in\mathbb{N}\\ [d_1,\ldots,d_r]>(\log^{B+2^r-1}x)/m}} \frac{\mu^2(d_1)\cdots\mu^2(d_r)}{[d_1,\ldots,d_r]d_1\cdots d_r}\\
&= \frac{x}{m}\sum_{k>(\log^{B+2^r-1}x)/m} \frac{g(k)}{k}\\
&\le \frac{x}{m}\sum_{k>(\log^{B+2^r-1}x)/m} \frac{2^{r\omega(k)}}{k^2}.
\end{aligned}
$$

By Lemma 39, we deduce

$$E_B(m,x) \ll \frac{x}{m}\frac{(\log\log x)^{2^r-1}}{\log^{B+2^r-1}x} \ll \frac{x}{\log^B x}.$$

Consider the main term

$$\sum_{\substack{d_1,\ldots,d_r\in\mathbb{N}\\ m[d_1,\ldots,d_r]\le\log^{B-2^r+1}x}} \frac{\mu(d_1)\cdots\mu(d_r)}{d_1\cdots d_r}\pi(x,1;m[d_1,\ldots,d_r]).$$

By applying Siegel-Walfisz Theorem [22] for primes in an arithmetic progression which states that

$$\pi(x,1;m[d_1,\ldots,d_r]) = \frac{\mathrm{li}(x)}{\varphi(m[d_1,\ldots,d_r])} + O\left(\frac{x}{\log^C x}\right)$$

provided that $m[d_1,\ldots,d_r] < \log^{B+2^r-1}x$ where $B+2^r-1$ and C are arbitrary positive constants, we obtain:

$$M_m(x) = \mathrm{li}(x)\sum_{\substack{d_1,\ldots,d_r\in\mathbb{N}\\ [d_1,\ldots,d_r]\le(\log^{B-2^r+1}x)/m}} \frac{\mu(d_1)\cdots\mu(d_r)}{\varphi(m[d_1,\ldots,d_r])d_1\cdots d_r} + O\left(\frac{x}{\log^{C-1}x}+\frac{x}{\log^B x}\right)$$

$$= \mathrm{li}(x)\sum_{d_1,\ldots,d_r\in\mathbb{N}} \frac{\mu(d_1)\cdots\mu(d_r)}{\varphi(m[d_1,\ldots,d_r])d_1\cdots d_r} + O\left(\frac{x}{\log^{\min\{C-1,B\}}x}\right)$$

$$+O\left(\sum_{\substack{d_1,\ldots,d_r\in\mathbb{N}\\ [d_1,\ldots,d_r]>(\log^{B+2^r-1}x)/m}}\frac{\mu^2(d_1)\cdots\mu^2(d_r)}{[d_1,\ldots,d_r]d_1\cdots d_r}\frac{x}{m\log x}\right)$$

$$\begin{aligned}
&= \mathrm{li}(x)\sum_{k\geqslant 1}\frac{1}{\varphi(mk)}\sum_{\substack{(d_1,\ldots,d_r)\in\mathbb{N}^r\\ k=[d_1,\ldots,d_r]}}\frac{\mu(d_1)\cdots\mu(d_r)}{d_1\cdots d_r}+O\left(\frac{x}{\log^{\min\{C-1,B\}}x}\right)\\
&= \frac{\mathrm{li}(x)}{\varphi(m)}\sum_{k\geqslant 1}\frac{\varphi((m,k))}{\varphi(k)(m,k)}\sum_{\substack{(d_1,\ldots,d_r)\in\mathbb{N}^r\\ k=[d_1,\ldots,d_r]}}\frac{\mu(d_1)\cdots\mu(d_r)}{d_1\cdots d_r}+O\left(\frac{x}{\log^{\min\{C-1,B\}}x}\right)
\end{aligned}$$

$$=\frac{\mathrm{li}(x)}{\varphi(m)}\sum_{k\geqslant 1}\frac{\varphi((m,k))}{\varphi(k)(m,k)}f(k)+O\left(\frac{x}{\log^{\min\{C-1,B\}}x}\right).$$

By multiplicativity and the properties of f, we get

$$M_m(x)=\frac{\mathrm{li}(x)}{\varphi(m)}\prod_{\ell}\left(1+\sum_{\alpha\geqslant 1}\frac{\varphi((m,\ell^\alpha))f(\ell^\alpha)}{\varphi(\ell^\alpha)(m,\ell^\alpha)}\right)+O\left(\frac{x}{\log^{\min\{C-1,B\}}x}\right).$$

$$=\frac{\mathrm{li}(x)}{\varphi(m)}\prod_{\ell}\left(1+\frac{\varphi((m,\ell))f(\ell)}{\varphi(\ell)(m,\ell)}\right)+O\left(\frac{x}{\log^{\min\{C-1,B\}}x}\right).$$

□

Lemma 41. *Given $m\in\mathbb{N}$, we have*

$$\sum_{p\leq x}\tau\left(\frac{p-1}{m}\right)^r\ll\frac{1}{\varphi(m)}x\left(\log x\right)^{2^r-1}.$$

Proof.

$$\begin{aligned}
\sum_{p\leq x}\tau\left(\frac{p-1}{m}\right)^r &= \sum_{p\leq x}\left(\sum_{e\mid\frac{p-1}{m}}1\right)^r\\
&= \sum_{p\leq x}\sum_{\substack{(d_1,\ldots,d_r)\in\mathbb{N}^r\\ d=[d_1,\ldots,d_r]\mid\frac{p-1}{m}}}1
\end{aligned}$$

$$= \sum_{\substack{(d_1,\ldots,d_r)\in\mathbb{N}^r \\ md\le x-1}} \sum_{\substack{p\le x \\ p\equiv 1 (\mathrm{mod}\, md)}} 1.$$

By using Dirichlet hyperbola method, we get

$$\sum_{p\le x} \tau\left(\frac{p-1}{m}\right)^r = 2 \sum_{\substack{(d_1,\ldots,d_r)\in\mathbb{N}^r \\ md\le \sqrt{x-1}}} \sum_{\substack{k\le \frac{x-1}{md} \\ kmd=p-1}} 1 - \sum_{\substack{(d_1,\ldots,d_r)\in\mathbb{N}^r \\ md\le \sqrt{x-1}}} \sum_{\substack{k\le \sqrt{x-1} \\ kmd=p-1}} 1$$

$$= 2 \sum_{\substack{(d_1,\ldots,d_r)\in\mathbb{N}^r \\ md\le \sqrt{x-1}}} \sum_{\substack{p\le x \\ p\equiv 1 (\mathrm{mod}\, md)}} 1 - \sum_{\substack{(d_1,\ldots,d_r)\in\mathbb{N}^r \\ md\le \sqrt{x-1}}} \sum_{\substack{p\le md\sqrt{x-1}+1 \\ p\equiv 1 (\mathrm{mod}\, md)}} 1$$

$$= 2 \sum_{\substack{(d_1,\ldots,d_r)\in\mathbb{N}^r \\ md\le \sqrt{x-1}}} \pi\left(x, 1; md\right) - \sum_{\substack{(d_1,\ldots,d_r)\in\mathbb{N}^r \\ md\le \sqrt{x-1}}} \pi\left(md\sqrt{x-1}+1, 1; md\right).$$

Define $\mathrm{LCM}(d;r) := \#\left\{(d_1,\ldots,d_r)\in\mathbb{N}^r : [d_1,\ldots,d_r]=d\right\}$. As in [3], we have

$$\mathrm{LCM}(p_1^{n_1}\cdots p_t^{n_t};r) = \prod_{i=1}^{t} \left(n_i+1\right)^r - n_i^r.$$

Therefore, we get

$$\sum_{p\le x} \tau\left(\frac{p-1}{m}\right)^r = 2 \sum_{\substack{d\in\mathbb{N} \\ md\le \sqrt{x-1}}} \mathrm{LCM}(d;r)\,\pi\left(x,1;md\right) - \sum_{\substack{d\in\mathbb{N} \\ md\le \sqrt{x-1}}} \mathrm{LCM}(d;r)\,\pi\left(md\sqrt{x-1}+1,1;md\right)$$

$$\le 2 \sum_{\substack{d\in\mathbb{N} \\ md\le \sqrt{x-1}}} \mathrm{LCM}(d;r)\,\pi\left(x,1;md\right).$$

By using Brun-Titchmarsh theorem [12], we get

$$\sum_{p\le x} \tau\left(\frac{p-1}{m}\right)^r \le 2x \sum_{\substack{d\in\mathbb{N} \\ md\le \sqrt{x-1}}} \frac{\mathrm{LCM}(d;r)}{\log\frac{x}{md}\,\varphi\left(md\right)}$$

$$\le \frac{4x}{\log x} \sum_{\substack{d\in\mathbb{N} \\ md\le \sqrt{x-1}}} \frac{\mathrm{LCM}(d;r)}{\varphi\left(md\right)}$$

$$\leq \frac{4x}{\log x}\frac{1}{\varphi(m)} \sum_{\substack{d\in\mathbb{N}\\ d\leq \frac{\sqrt{x-1}}{m}}} \frac{\mathrm{LCM}(d;r)}{\varphi(d)}$$

$$\leq \frac{4x}{\log x}\frac{1}{\varphi(m)} \sum_{\substack{d\in\mathbb{N}\\ d\leq \frac{\sqrt{x-1}}{m}}} \frac{\mathrm{LCM}(d;r)}{\varphi(d)}.$$

Since $\mathrm{LCM}(d;r)$ is multiplicative function, therefore

$$\sum_{p\leq x}\tau\left(\frac{p-1}{m}\right)^r \leq \frac{4x}{\log x}\frac{1}{\varphi(m)}\prod_{\ell\leq\sqrt{x-1}}\left(1+\frac{2^r-1}{\ell-1}+\frac{3^r-2^r}{\ell(\ell-1)}+\frac{4^r-3^r}{\ell^2(\ell-1)}+\dots\right)$$

$$\leq \frac{4x}{\log x}\frac{1}{\varphi(m)}\prod_{\ell\leq\sqrt{x-1}}\left(1+\frac{2^r}{\ell}+\frac{3^r}{\ell^2}+\dots\right)$$

$$\leq \frac{4x}{\log x}\frac{1}{\varphi(m)}\prod_{\ell\leq\sqrt{x-1}}\left(1+\frac{2^r}{\ell}+O\left(\frac{1}{\ell^2}\right)\right)$$

$$\leq \frac{4x}{\log x}\frac{1}{\varphi(m)}\exp\left(\sum_{\ell\leq\sqrt{x-1}}\log\left(1+\frac{2^r}{\ell}+O\left(\frac{1}{\ell^2}\right)\right)\right)$$

$$\ll \frac{x}{\log x}\frac{1}{\varphi(m)}\exp\left(\sum_{\ell\leq\sqrt{x-1}}\frac{2^r}{\ell}+O\left(\sum_{\ell\leq\sqrt{x-1}}\frac{1}{\ell^2}\right)\right)$$

$$\ll \frac{x}{\log x}\frac{1}{\varphi(m)}\exp\left(\log\left(\log\sqrt{x-1}\right)^{2^r}\right)$$

$$\ll \frac{1}{\varphi(m)}x\left(\log x\right)^{2^r-1}. \qquad \square$$

Notations.

- $\underline{a}$ means $(a_1,\cdots,a_r)$.
- $\underline{a}\leq\underline{T}$ means $a_i\leq T$ for all $i=1,\cdots,r$.
- $\underline{\chi}$ means $(\chi_1,\dots,\chi_r)$.
- $\underline{\chi_0}$ means the r-tuple $(\chi_0,\dots,\chi_0)$.

Theorem 42. *Assume* $T > \exp\left(4\left(\log x \log\log x\right)^{\frac{1}{2}}\right)$, *then for every* $k > 1$, *we have*

$$\frac{1}{T^r}\sum_{\underline{a}\leq\underline{T}} S_{\underline{a},m}(x) = \delta_m \operatorname{li}(x) + O\left(\frac{x}{(\log x)^k}\right),$$

where $\delta_m = \frac{1}{m^r\varphi(m)}\prod_{\ell}\left(1+\frac{\varphi((m,\ell))f(\ell)}{\varphi(\ell)(m,\ell)}\right)$ *and* $f(\ell) = \left(1-\frac{1}{\ell}\right)^r - 1$

Proof.

$$\frac{1}{T^r}\sum_{\underline{a}\leq\underline{T}} S_{\underline{a},m}(x) = \frac{1}{T^r}\sum_{\underline{a}\leq\underline{T}}\sum_{\substack{p\leqslant x\\ p\equiv 1 \pmod m}} t_{p,m}\left(\underline{a}\right),$$

where

$$t_{p,m}\left(\underline{a}\right) = \begin{cases} 1 & \text{if } \operatorname{ord}_p a_1 = \cdots = \operatorname{ord}_p a_r = \frac{p-1}{m}; \\ \\ 0 & \text{otherwise.}\end{cases}$$

Which can be written as following

$$t_{p,m}\left(\underline{a}\right) = \sum_{\underline{\chi}} c_m\left(\underline{\chi}\right)\underline{\chi}\left(\underline{a}\right).$$

Therefore,

$$c_m\left(\underline{\chi}\right) = \frac{1}{(p-1)^r}\sum_{\substack{\underline{a}\in(\mathbb{Z}/p-1\mathbb{Z})^r\\ \operatorname{ord}_p \underline{a}=\frac{p-1}{m}}}\underline{\chi}\left(\underline{a}\right).$$

So,

$$\frac{1}{T^r}\sum_{\underline{a}\leqslant\underline{T}} S_{\underline{a},m}(x) = \frac{1}{T^r}\sum_{\substack{p\leqslant x\\ p\equiv 1 \pmod m}}\sum_{0<\underline{a}\leqslant\underline{T}} t_{p,m}\left(\underline{a}\right)$$

$$= \frac{1}{T^r}\sum_{\substack{p\leqslant x\\ p\equiv 1 \pmod m}}\sum_{0<\underline{a}\leqslant\underline{T}}\sum_{\underline{\chi}} c_m\left(\underline{\chi}\right)\underline{\chi}\left(\underline{a}\right)$$

$$= \frac{1}{T^r}\sum_{\substack{p\leqslant x\\ p\equiv 1 \pmod m}}\sum_{0<\underline{a}\leqslant\underline{T}} c_m\left(\underline{\chi}_0\right)\underline{\chi}_0\left(\underline{a}\right) + E_m(x),$$

where

$$E_m(x) = \frac{1}{T^r}\sum_{\substack{p\leqslant x\\ p\equiv 1 \pmod m}}\sum_{0<\underline{a}\leqslant\underline{T}}\sum_{\underline{\chi}\neq\underline{\chi}_0} c_m(\underline{\chi})\underline{\chi}\left(\underline{a}\right).$$

Let us talk about the main term

$$\frac{1}{T^r}\sum_{\substack{p\leqslant x\\ p\equiv 1 (\mathrm{mod}\, m)}}\sum_{0<\underline{a}\leqslant \underline{T}} c_m\left(\underline{\chi}_0\right)\underline{\chi}_0\left(\underline{a}\right)$$

Since $|c_m(\underline{\chi}_0)| \leqslant 1$ and

$$c_m(\underline{\chi}_0) = \frac{1}{(p-1)^r}\sum_{\substack{\underline{a}\in(\mathbb{Z}/p-1\mathbb{Z})^r\\ \mathrm{ord}_p\,\underline{a}=\frac{p-1}{m}}}\underline{\chi}_0\left(\underline{a}\right)$$

$$= \frac{1}{(p-1)^r}\sum_{\substack{\underline{a}\in(\mathbb{Z}/p-1\mathbb{Z})^r\\ \mathrm{ord}_p\,a_1=\cdots=\mathrm{ord}_p\,a_r=\frac{p-1}{m}}} 1$$

$$= \frac{1}{(p-1)^r}\left(\#\left\{a\leqslant p-1 : \mathrm{ord}_p\,a = \frac{p-1}{m}\right\}\right)^r$$

$$= \frac{1}{(p-1)^r}\varphi\left(\frac{p-1}{m}\right)^r,$$

and

$$\frac{1}{T^r}\sum_{0<\underline{a}\leqslant \underline{T}}\underline{\chi}_0(\underline{a}) = \frac{1}{T^r}\left([T]-\left[\frac{T}{p}\right]\right)^r$$

$$= \frac{1}{T^r}\left(T-\frac{T}{p}+O(1)\right)^r$$

$$= \left(\left(1-\frac{1}{p}\right)+O(\frac{1}{T})\right)^r$$

$$= \left(1-\frac{1}{p}\right)^r + O\left(\sum_{i=1}^{r}\frac{1}{T^i}\right)$$

$$= 1+O\left(\frac{1}{p}\right)+O\left(\frac{1}{T}\right),$$

therefore

$$\frac{1}{T^r}\sum_{\substack{p\leqslant x\\ p\equiv 1 (\mathrm{mod}\, m)}}\sum_{0<\underline{a}\leqslant \underline{T}} c_m(\underline{\chi}_0)\underline{\chi}_0(\underline{a}) = \sum_{\substack{p\leqslant x\\ p\equiv 1 (\mathrm{mod}\, m)}} c_m(\underline{\chi}_0)\left(1+O\left(\frac{1}{p}\right)+O\left(\frac{1}{T}\right)\right)$$

$$= \sum_{\substack{p\leqslant x\\ p\equiv 1(\mathrm{mod}\, m)}} c_m(\underline{\chi}_0) + O\left(\sum_{\substack{p\leqslant x\\ p\equiv 1(\mathrm{mod}\, m)}} \frac{1}{p}\right) + O\left(\frac{1}{T}\sum_{\substack{p\leqslant x\\ p\equiv 1(\mathrm{mod}\, m)}} 1\right)$$

$$= \sum_{\substack{p\leqslant x\\ p\equiv 1(\mathrm{mod}\, m)}} \frac{1}{m^r}\left(\frac{\phi\left(\frac{p-1}{m}\right)}{\frac{p-1}{m}}\right)^r + O\left(\log\log x\right) + O\left(\frac{1}{T}\frac{x}{\log x}\right)$$

$$= \frac{1}{m^r}\sum_{\substack{p\leqslant x\\ p\equiv 1(\mathrm{mod}\ m)}} \left(\frac{\phi\left(\frac{p-1}{m}\right)}{\frac{p-1}{m}}\right)^r + O\left(\log\log x\right) + O\left(\frac{1}{T}\frac{x}{\log x}\right)$$

$$= \frac{1}{m^r}M_m(x) + O\left(\log\log x\right) + O\left(\frac{1}{T}\frac{x}{\log x}\right)$$

By lemma 40,

$$= \delta_m \operatorname{li}(x) + O\left(\frac{x}{\log^{\min\{C-1,B\}} x}\right) + O\left(\log\log x\right) + O\left(\frac{1}{T}\frac{x}{\log x}\right),$$

for any positve integers B and C, where $\delta_m = \dfrac{1}{m^r\varphi\left(m\right)}\displaystyle\prod_{\ell\, prime}\left(1+\frac{\varphi((m,\ell))f(\ell)}{\varphi(\ell)(m,\ell)}\right)$.

Now, let us consider the error term

$$E_m(x) = \frac{1}{T^r}\sum_{\substack{p\leqslant x\\ p\equiv 1(\mathrm{mod}\, m)}}\sum_{0<\underline{a}\leqslant \underline{T}}\sum_{\underline{\chi}\neq\underline{\chi}_0} c_m\left(\underline{\chi}\right)\underline{\chi}\left(\underline{a}\right)$$

$$|E_m(x)| \leq \frac{1}{T^r}\sum_{j=1}^{r}\sum_{\substack{p\leqslant x\\ p\equiv 1(\mathrm{mod}\, m)}}\sum_{\substack{\underline{\chi}\\ \chi_j\neq\chi_0}} |c_m\left(\underline{\chi}\right)| * |\sum_{0<\underline{a}\leqslant\underline{T}}\underline{\chi}\left(\underline{a}\right)|$$

$$= \frac{1}{T^r}\sum_{j=1}^{r}\sum_{\substack{p\leqslant x\\ p\equiv 1(\mathrm{mod}\, m)}}\left(\prod_{\substack{k=1\\ k\neq j}}^{r}\sum_{\chi}\left(\frac{1}{p-1}\sum_{\substack{a\in\mathbb{Z}/(p-1)\mathbb{Z}\\ \mathrm{ord}_p a=\frac{p-1}{m}}}\chi\left(a\right)\right)|\sum_{0<a\leqslant T}\chi\left(a\right)|\right).$$

$$*\left(\sum_{\chi\neq\chi_0}\left(\frac{1}{p-1}\sum_{\substack{a\in\mathbb{Z}/(p-1)\mathbb{Z}\\ \mathrm{ord}_p a=\frac{p-1}{m}}}\chi\left(a\right)\right)|\sum_{0<a\leqslant T}\chi\left(a\right)|\right)$$

$$= \frac{1}{T}\sum_{j=1}^{r} \sum_{\substack{p\leqslant x\\ p\equiv 1(\bmod m)}} \left(\prod_{\substack{k=1\\ k\neq j}}^{r}\sum_{\chi}\frac{1}{\mathrm{ord}\chi^{m}}\right) * \left(\sum_{\chi\neq\chi_0}\frac{1}{\mathrm{ord}\chi^{m}} * \left|\sum_{0<a\leqslant T}\chi(a)\right|\right)$$

$$\leq \frac{r}{T} \sum_{\substack{p\leqslant x\\ p\equiv 1(\bmod m)}} \tau\left(\frac{p-1}{m}\right)^{r-1}\left(\sum_{\chi\neq\chi_0}\frac{1}{\mathrm{ord}\chi^{m}} * \left|\sum_{0<a\leqslant T}\chi(a)\right|\right).$$

$$= \frac{r}{T} \sum_{\substack{p\leqslant x\\ p\equiv 1(\bmod m)}} \sum_{\chi\neq\chi_0}\frac{\tau\left(\frac{p-1}{m}\right)^{r-1}}{\mathrm{ord}\chi^{m}} * \left|\sum_{0<a\leqslant T}\chi(a)\right|.$$

By holder inequality, we have

$$\leq \frac{r}{T}\left\{\sum_{\substack{p\leqslant x\\ p\equiv 1(\bmod m)}} \sum_{\chi\neq\chi_0}\left(\frac{\tau\left(\frac{p-1}{m}\right)^{r-1}}{\mathrm{ord}\chi^{m}}\right)^{\frac{2s}{2s-1}}\right\}^{\frac{2s-1}{2s}} * \left\{\sum_{\substack{p\leqslant x\\ p\equiv 1(\bmod m)}} \sum_{\chi\neq\chi_0}\left(\left|\sum_{0<a\leqslant T}\chi(a)\right|\right)^{2s}\right\}^{\frac{1}{2s}}.$$

By using lemma 5 in [21], we have

$$\ll \frac{1}{T}\left\{\sum_{\substack{p\leqslant x\\ p\equiv 1(\bmod m)}} \tau\left(\frac{p-1}{m}\right)^{\frac{2s(r-1)}{2s-1}+1}\right\}^{\frac{2s-1}{2s}} * \left(x^2+T^s\right)^{\frac{1}{2s}} T^{\frac{1}{2}}\left(\log eT^{s-1}\right)^{\frac{s^2-1}{2s}}$$

By using lemma 41, we have

$$\ll \frac{1}{T^{\frac{1}{2}}}\left\{\frac{1}{\varphi(m)}x(\log x)^{2^r-1}\right\}^{\frac{2s-1}{2s}}\left(x^2+T^s\right)^{\frac{1}{2s}}\left(\log eT^{s-1}\right)^{\frac{s^2-1}{2s}}$$

$$\ll \frac{1}{T^{\frac{1}{2}}}x^{1-\frac{1}{2s}}(\log x)^{2^r-1}\left(x^2+T^s\right)^{\frac{1}{2s}}\left(\log eT^{s-1}\right)^{\frac{s^2-1}{2s}}.$$

By choosing the parameter s as in [21] and by the same technique and by the hypothesis $T>\exp\left(4(\log x\log\log x)^{\frac{1}{2}}\right)$, we get

$$E_m(x) \ll \frac{x}{(\log x)^k} \quad \text{for every } k>1.$$

Therefore, for every $k>1$, we have

$$\frac{1}{T^r}\sum_{\underline{a}\leqslant\underline{T}} S_{\underline{a},m}(x) = \delta_m \operatorname{li}(x) + O\left(\frac{x}{\log^{\min\{C-1,B\}} x}\right) + O\left(\log\log x\right) + O\left(\frac{1}{T}\frac{x}{\log x}\right) + O\left(\frac{x}{(\log x)^k}\right).$$

Since $T > \exp\left(4\left(\log x \log\log x\right)^{\frac{1}{2}}\right)$, therefore, for every $k > 1$, we have

$$\frac{1}{T^r}\sum_{\underline{a}\leqslant\underline{T}} S_{\underline{a},m}(x) = \delta_m \operatorname{li}(x) + O\left(\frac{x}{(\log x)^k}\right).$$

$\square$

Chapter 7

Future Work

I will try to conclude the characterization of *Schinzel–Wójcik* problem under Hypothesis H which had discussed in Chapter 5 and continue studying *Schinzel–Wójcik* problem on average ingeneral. More precisely, I will try to study

$$\frac{1}{T^r}\sum_{\underline{a}\leq \underline{T}} S_{\underline{a}}(x), \text{ where } S_{\underline{a}}(x) = \{p \leqslant x : \mathrm{ord}_p a_1 = \cdots = \mathrm{ord}_p a_r\}.$$

Moreover, I will study the Average n- dimensional *Artin*'s Conjecture ,that is,

$$\frac{1}{T^r}\sum_{\underline{a}\leq \underline{T}} \#\left\{p \leqslant x : \mathrm{ord}_p a_1 \,|\, \mathrm{ord}_p a_2 \cdots |\mathrm{ord}_p a_r\right\}.$$

In addition, I will study the Average of *Schinzel–Wójcik* constant $\delta_{a_1,\cdots,a_r}$, which is defined in Theorem 9 [16] as

$$\delta_{a_1,\ldots,a_r} = \sum_{\substack{m\in\mathbb{N}\\ \underline{k}\in\mathbb{N}^r}} \frac{\mu(\underline{k})}{\varphi(mk)} \frac{\#\tilde{\Gamma}_{\underline{k}}(mk)}{\#\Gamma_{\underline{k}}(mk)}.$$

More precisely, I will try to prove (the same result, under GRH, in Theorem 12 [16]), free of any hypothesis, that

$$\frac{1}{T^r}\sum_{\underline{a}\leq \underline{T}} \delta_{a_1,\ldots,a_r} = \delta + \underline{o}\,(1)\,, \quad \text{where} \quad \delta = \prod_{\ell}\left(1 - \frac{\ell(\ell^r - (\ell-1)^r - 1)}{(\ell-1)(\ell^{r+1}-1)}\right).$$

Bibliography

[1] ADHIKARI, S. D, *The early reciprocity laws: from Gauss to Eisenstein. Cyclotomic fields and related topics (Pune, 1999)*, 55–74. Bhaskaracharya Pratishthana, Pune, 2000.

[2] ANWAR, M. AND PAPPALARDI, F., *On simultaneous primitive roots.* Acta Arith. **180** (2017) 35–43.

[3] BAGDASAR, O., *On some functions involving the lcm and gcd of integer tuples.* Appl. Maths. Inform. and Mech. **6.2** (2014) 91–100.

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

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

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

[7] IRELAND, K. AND ROSEN, M., *A classical introduction to modern number theory. Graduate Texts in Mathematics 84.* Springer-Verlag, New York, 2nd edition, 1990.

[8] LANG, S., *Algebra. Graduate texts in mathematics 211.* Springer-Verlag, New York, 2002.

[9] MATTHEWS, K. R., *A generalisation of Artin's conjecture for primitive roots.* Acta Arith. **29**(2) (1976) 113–146.

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

[11] Montgomery, H. and Vaughan R, C., *Multiplicative Number Theory I: Classical Theory. Graduate Texts in Mathematics* . Cambridge University Press, New York, 2006.

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

[13] Menici, L., Pehlivan, C. *Average r–rank Artin Conjecture.* Acta Arithmetica, **174** (2016), 255–276.

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

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

[16] Pappalardi, F. and Susa, A., *On a problem of Schinzel and Wójcik, involving equalities between multiplicative orders.* Math. Proc. Cambridge Philos. Soc., 146(2), 303–319.

[17] Ribenboim, P., *Classical theory of algebraic numbers*, *Universitext*, Springer-Verlag, New York, 2001.

[18] Samuel, P., *Algebraic Theory of numbers.*, *Universitext*, Hermann, 1970.

[19] Schinzel, A. and Sierpiński, W., *Sur certaines hypothèses concernant les nombres premiers.* Acta Arith. **4** (1958), 185–208; erratum, **5** (1958) 259.

[20] Schinzel, A. and Wójcik, J., *On a problem in elementary number theory.* Math. Proc. Cambridge Philos. Soc., **112** (1992), no. 2, 225–232.

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

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

[23] Wójcik, J., *On a problem in algebraic number theory.* Math. Proc. Cambridge Philos. Soc., **119** (1996), no. 2, 191–200. 75–102.