National Library
of Canada

Acquisitions and
Bibliographic Services Branch

395 Wellington Street
Ottawa, Ontario
K1A 0N4

Bibliothèque nationale
du Canada

Direction des acquisitions et
des services bibliographiques

395, rue Wellington
Ottawa (Ontario)
K1A 0N4

Your file Votre référence

Our file Notre référence

NOTICE

The quality of this microform is heavily dependent upon the quality of the original thesis submitted for microfilming. Every effort has been made to ensure the highest quality of reproduction possible.

If pages are missing, contact the university which granted the degree.

Some pages may have indistinct print especially if the original pages were typed with a poor typewriter ribbon or if the university sent us an inferior photocopy.

AVIS

La qualité de cette microforme dépend grandement de la qualité de la thèse soumise au microfilmage. Nous avons tout fait pour assurer une qualité supérieure de reproduction.

S'il manque des pages, veuillez communiquer avec l'université qui a conféré le grade.

La qualité d'impression de certaines pages peut laisser à désirer, surtout si les pages originales ont été dactylographiées à l'aide d'un ruban usé ou si l'université nous a fait parvenir une photocopie de qualité inférieure.

Canada

On Artin's Conjecture for Primitive Roots

by

Francesco Pappalardi *

Department of Mathematics and Statistics

A thesis submitted in partial fulfillment

of the requirements of the degree of

Doctor of Philosophy at McGill University

February 1993

ISBN 0-315-87877-0

Canada

ACKNOWLEDGMENTS

There are many people who I would like to thank at this point:

My Master thesis Supervisor Marco Fontana for having trusted me and supported my choice to come to Canada. Professor Paulo Ribenboim for having always advised me on my choices and his precious mathematical teaching.

Professors Jal Choksi, Ian Connell, Hershy Kisilevsky, John Labute, V. Seshadri and Georg Schmidt, whose help and politeness made my time at McGill pleasant.

Raffaella Bruno who corrected the english of this thesis. None of my problems were ever unsolvable for her.

Valerie McConnell, Elaine Tremblay for never having denied a smile and their valuable help.

My friends Mark Fels and Djordje Čubrić, the first having shown me the human side of being a graduate student, and the second , with whom I shared an office was a true gentleman and a solid office-mate. It will not be easy to find others like them.

Masato Kuwata, who has helped me considerably with the computers and Damien Roy who helped me with the theory of Kummer's Extensions.

My wife Claudia and my daughter Silvia, the first for support and encouragement during these difficult years, and the second for having waited that extra week necessary to finish this thesis.

Last but certainly not least I would like to thank my supervisor Ram Murty. He is an exceptional man, who placed his trust in me and guided me to many of the problems which lead to this thesis. His teaching did not cover only Mathematics but he has also been a precious counsellor on any issue that I have brought to him. I hope to be able to pass on what I have learned from Professor Murty to others in the future.

ABSTRACT

Various generalizations of the Artin's Conjecture for primitive roots are considered. It is proven that for at least half of the primes p, the first $\log p$ primes generate a primitive root. A uniform version of the Chebotarev Density Theorem for the field $\mathbf{Q}(\zeta_l, 2^{1/l})$ valid for the range $l < \log x$ is proven. A uniform asymptotic formula for the number of primes up to x for which there exists a primitive root less than s is established. Lower bounds for the exponent of the class group of imaginary quadratic fields valid for density one sets of discriminants are determined.

RESUMÉ

Nous considérons différentes généralisations de la conjecture d'Artin pour les racines primitives. Nous démontrons que pour au moins la moitié des nombres premiers p, les premiers $\log p$ nombres premiers engendrent une racine primitive. Nous démontrons une version uniforme du Théorème de Densité de Chebotarev pour le corps $\mathbf{Q}(\zeta_l, 2^{1/l})$ pour l'intervalle $l < \log x$. On établit une formule asymptotique uniforme pour les nombres de premiers plus petits que x tels qu' il existe une racine primitive plus petite que s. Nous déterminons des minorants pour l'exposant du groupe de classe des corps quadratiques imaginaires valides pour ensembles de discriminants de densité 1.

Contents

INTRODUCTION

The famous Artin Conjecture for primitive roots states that any integer $a \neq \pm 1$ which is not a perfect square is a primitive root for infinitely many primes. More precisely, if $N_a(x)$ is the set of such primes up to x, then

$$N_a(x) \sim A(a)\pi(x)$$

where $A(a) \neq 0$.

Artin also gave an explicit formula for $A(a)$ and his intuition was based on the following heuristic argument (see [1]):
For any prime p less than x, let $P_a(q)$ be the probability that the prime q divides the index $[\mathbf{F}_p^* : \langle a \rangle]$; then,by considering such instances independent, we have

$$A(a) = \prod_q (1 - P_a(q)).$$

In order to have $q|[\mathbf{F}_p^* : \langle a \rangle]$, the two necessary and sufficient conditions

$$p \equiv 1 (\mathrm{mod} q) \text{ and } a^{(p-1)/q} \equiv 1 (\mathrm{mod} p) \tag{1}$$

must be satisfied.

Now consider the field $L_q = \mathbf{Q}(\zeta_q, a^{1/q})$, let p be a rational prime that splits completely in L_q and let $\mathcal{P}$ be a prime over p. The residue field at $\mathcal{P}$ has p elements, therefore (1) holds. Conversely if (1) holds for p, then p splits completely in L_q.

The Chebotarev Density Theorem indeed states that the probability that p splits completely in a normal extension K, equals $1/[K : \mathbf{Q}]$ and therefore the probability $P_a(q)$ is $1/q(q-1)$ and

$$A(a) = \prod_q \left(1 - \frac{1}{q(q-1)}\right).$$

Later, calculations made by D. H. Lehmer and E. Lehmer (see [35]) suggested that in some cases the expression of $A(a)$ was not correct and the factors of the product expansion of $A(a)$ corresponding to the prime divisors of a had to be replaced by other expressions.

In 1965, C. Hooley (see [26]) used the linear sieve to prove that if the validity of the Generalized Riemann Hypothesis is assumed for the Dedekind zeta function of the fields L_q then the Artin's Conjecture is true, with the corrections indicated by Lehmer.

The main tool used by Hooley is the effective version of the Chebotarev density Theorem valid under the assumption of the Riemann Hypothesis for the Dedekind zeta function of K. That is

$$\#\{p \leq x \mid p \text{ splits completely in } K\} = \frac{1}{n_K}\mathrm{li}(x) + O(x^{1/2}(\log x + \log d_K^{1/n_K})),$$

where $n_K = [K : \mathbf{Q}]$ and d_K is the discriminant.

This version of the Chebotarev Density Theorem has been for a long time the only effective one available until 1977 when J. C. Lagarias and A. M. Odlyzko proved a version of the Theorem valid with the condition (see [29]):

$$\sqrt{\frac{\log x}{n_K}} \gg \max\left\{d_K^{1/n_K}, \log d_K\right\}.$$

For a Kummer's extension of the type L_q, this is equivalent to $q < \log^{1/6} x$.

Such a discovery, unfortunately, does not allow one to eliminate the use of the Riemann Hypothesis on the proof of the Theorem of Hooley, however it gives a uniform result for $q < \log^{1/6} x$.

In 1984 R. Gupta and R. Murty (see [15]) published the first result in which the validity of the Artin Conjecture is established for at least one value of a. Indeed, they constructed a set of 13 numbers for which at least one is primitive root for a

number of primes p up to x which is $\gg \frac{x}{\log^2 x}$. This result was later sharpened by Heath-Brown (see [21]) to a set of 3 elements.

The idea of Gupta and Murty also allowed them to deal with the analogous statement of the Artin Conjecture for rational points on Elliptic Curves (see. [17]). This is the Lang-Trotter Conjecture. From this they were led to consider a high-rank version of the Artin Conjecture.

Given $a_1, \ldots, a_r \in \mathbf{Z}$, we say that $a_1, \ldots, a_r$ are **multiplicatively independent** if, whenever there are integers $n_1, \ldots, n_r$ such that

$$a_1^{n_1} \cdots a_r^{n_r} = 1,$$

we have $n_1 = n_2 = \cdots = n_r = 0$.

It makes sense to ask if

$$\langle a_1, \ldots, a_r \mod p \rangle = \mathbf{F}_p^* \tag{2}$$

for infinitely many primes p and to speculate whether the density of such primes can be calculated. It is necessary to express the condition for a prime q to divide the index of the group generated by $a_1, \ldots, a_r$ in terms of splitting conditions on some fields. The natural generalization of Artin's original idea is in:

Theorem 1 *Let $\langle a_1, \ldots, a_r \rangle$ be the subgroup of $\mathbf{F}_p^*$ generated by the multiplicatively independent $a_1, \ldots, a_r$. For any prime q*

$$q \left| [\mathbf{F}_p^* : \langle a_1, \ldots, a_r \rangle] \right. \iff p \text{ splits completely in } \mathbf{Q}\left(\zeta_q, a_1^{1/q}, \ldots, a_r^{1/q}\right). \square$$

This result and the consequent application of the Chebotarev Density Theorem suggests that the density of primes for which (2) holds equals

$$\prod_q \left(1 - \frac{1}{q^r(q-1)}\right). \tag{3}$$

In Chapter 1 we prove that if the Generalized Riemann Hypothesis holds for the fields in Theorem 1, then

$$N_{a_1,\dots,a_r}(x) = \#\left\{p \le x \mid \langle a_1,\dots,a_r\rangle = \mathbf{F}_p^*\right\} \sim A_{a_1,\dots,a_r}\pi(x), \tag{4}$$

where the constant $A_{a_1,\dots,a_r}$ equals the product in (3), up to finitely many factors. The complete formulas, with the analogous corrections of those suggested by Lehmer for the Artin Conjecture, are worked out in Section 2.1 by the use of some properties of Kummer's extension.

The proof follows the original one of Hooley but now the estimate for the number of primes for which there is a large prime divisor of the index is made using a Lemma due to C.R. Matthews which is an application of the pigeon-hole principle.

The new parameter given by the rank, suggests to take r as a function of x and try to adapt the proof to obtain a result independent of the Riemann Hypothesis. This is done in Section 3.1 and the conclusion is that for a positive density of primes p, $\mathbf{F}_p^*$ can be generated by about $\log p$ multiplicatively independent integers.

The main obstacle comes from those primes for which the index

$$[\mathbf{F}_p^* : \langle a_1,\dots,a_r\rangle]$$

has some prime divisor in the interval $[\log^{1/6} x, \log^2 x]$.

The range $[\log^{1/6} x, \log x]$ is dealt by using a version of Chebotarev Density Theorem for the field $\mathbf{Q}(\zeta_l, 2^{1/l})$ valid for a range of l up to $\log x/(\log\log x)^2$ which is proven in Chapter 2. Such a proof uses properties of the single non-Abelian L-function of $\mathbf{Q}(\zeta_l, 2^{1/l})$, and is of course stronger than the one of Lagarias and Odlyzko of [29].

This establishes a Conjecture of H. Zassenhaus of 1969 (see [1]).

In Section 3.3, we work out the bound of $r \ge \log^2 p$ for a set of density one of primes p for which $\mathbf{F}_p^*$ is generated by r elements. Such a result is stronger than

the one that was known as a consequence of the work of Burgess and Elliot (see Proposition 1.11) and uses the Large Sieve Inequality.

The Lemma of Matthews used in the proof of the asymptotic formula in (4) allows one to conclude that for almost all primes p the index

$$[\mathbf{F}_p^* : \langle a_1, \ldots, a_r \rangle] \geq \frac{p^{r/(r+1)}}{\log p}.$$

In Appendix A, we improve such a lower bound to

$$[\mathbf{F}_p^* : \langle a_1, \ldots, a_r \rangle] \geq p^{r/(r+1)} \exp\{\log^\delta p\}. \tag{5}$$

This is done by deducing an upper bound for the number of primes p for which $p-1$ has a divisor in the range $(x^h, x^h \exp\{\log^\delta p\})$ which is due to Murty and Erdös (see [14]) and proven here with the uniformity conditions that allow estimates of the type (5) uniform with respect to r.

Next we take into consideration the problem of determining an asymptotic formula for the number of primes for which two given numbers (or more in general s given numbers) are simultaneously primitive roots. An heuristic argument similar to Artin's suggests a density

$$\delta = \prod_{q \text{ prime}} \left(1 - \frac{2q-1}{q^2(q-1)}\right),$$

and again this is proven to be the right one up to finitely many factors. Complete formulas are worked out in the case where the given numbers are primes. We later discovered that a general version of this statement has been proven by K. R. Matthews in his Ph.D. Thesis (see [36]). However, our proof is different and by the use of a Tauberian Theorem, we get a better uniform error term.

This result has, as an application, a uniform asymptotic formula for the number of primes for which the least prime primitive root is less than a parameter y. Such a formula has applications to the problem of the distribution of least primitive roots.

In Appendix B, we consider the problem of the exponent of the class group of imaginary quadratic fields.

If $e(d)$ is the exponent of the ideal classgroup of the imaginary quadratic fields $\mathbf{Q}(\sqrt{-d})$, the Iwasawa Conjecture states that

$$\lim_{d \to +\infty} e(d) = +\infty.$$

In 1972, D.W. Boyd and H. Kisilevsky (see [3]) proved that if the Extended Riemann Hypothesis holds for certain Dirichlets L-functions, then the Iwasawa Conjecture is true.

The proof consists on noticing a link between the least prime p for which $-d$ is a quadratic residue and $e(d)$ (this is $p^{e(d)} \gg d$) and then use the Riemann Hypothesis to prove that $p \ll \log^2 d$. This argument establishes the bound

$$e(d) \gg \frac{\log d}{\log \log d}. \tag{6}$$

We prove unconditionally that (6) holds for a set of discriminants of density one, by calculating uniform asymptotic formulas for the number of integers (resp. square-free integers) $d < x$ for which the least prime p with $\left(\frac{-d}{p}\right) = 1$ is smaller than s.

1 ON HOOLEY'S THEOREM

1.1 A generalization of Hooley's Theorem

Suppose $a_1, \ldots, a_r$ are multiplicatively independent integers and let Γ be the subgroup of $\mathbf{Q}^\times$ generated by $a_1, \ldots, a_r$. For all but finitely many primes p, it makes sense to consider the reduction of Γ modulo p which we indicate by Γ_p which can be viewed as a subgroup of $\mathbf{F}_p^*$.

In the case $r = 1$, Hooley has shown that if the generalized Riemann Hypothesis holds for the Dedekind zeta function of the fields $\mathbf{Q}(\zeta_l, a_1^{1/l})$, with l prime, then the set of primes p for which $\mathbf{F}_p^* = \Gamma_p$ has non zero density (see [26]).

We will consider the following generalization first introduced by R. Gupta and R. Murty in [15].

Theorem 1.1 *Let Γ be as above, $n_m = [\mathbf{Q}(\zeta_m, a_1^{1/m}, \ldots, a_r^{1/m}) : \mathbf{Q}]$ and let*

$$\delta_\Gamma = \sum_{m=1}^{\infty} \frac{\mu(m)}{n_m}$$

if the Generalized Riemann Hypothesis holds for the Dedekind zeta function of the fields $\mathbf{Q}(\zeta_l, a_1^{1/l})$, l prime, then

$$N_\Gamma(x) = \#\{p \leq x | \mathbf{F}_p^* = \Gamma_p\} \sim \delta_\Gamma \frac{x}{\log x}.$$

Remark: a) Note that

$$n_m \geq [\mathbf{Q}(\zeta_m, a_1^{1/m}) : \mathbf{Q}] \gg \phi(m)m, \tag{1}$$

therefore δ_Γ is a convergent series and thus a well defined number. We will prove in the second section that $\delta_\Gamma \neq 0$.

b) Theorem 1.1 can also be proven on the weaker assumption that there exists $a \in \Gamma$ with the property that all the Dedekind zeta functions of the fields $\mathbf{Q}(\zeta_l, a^{1/l})$ (l large prime) have no zeroes in the region

$$\sigma > 1 - \frac{1}{r+1}.$$

Proof: Let us assume $r > 1$. The first steps of the proof follow the original idea of Hooley who considered the following functions:

$$N_\Gamma(x,y) = \#\{p \leq x \mid \forall l,\ l \leq y,\ l \not| \ [\mathbf{F}_p^* : \Gamma_p]\},$$

$$M_\Gamma(x,y,z) = \#\{p \leq x \mid \exists l,\ y \leq l \leq z, l| \ [\mathbf{F}_p^* : \Gamma_p]\},$$

$$M_\Gamma(x,z) = \#\{p \leq x \mid \exists l,\ l \geq z, l| \ [\mathbf{F}_p^* : \Gamma_p]\},$$

where $y = \frac{1}{6r+8} \log\log x$ and $z = x^{1/(r+1)} \log x$.

Clearly,

$$N_\Gamma(x,y) \geq N_\Gamma(x) \geq N_\Gamma(x,y) - M_\Gamma(x,y,z) - M_\Gamma(x,z), \tag{2}$$

and establishing the following:

$$\begin{aligned} &a) \quad N_\Gamma(x,y) = \delta_\Gamma \tfrac{x}{\log x} + o(\tfrac{x}{\log x}); \\ &b) \quad M_\Gamma(x,y,z) = o(\tfrac{x}{\log x}); \\ &c) \quad M_\Gamma(x,z) = o(\tfrac{x}{\log x}), \end{aligned}$$

the Theorem would be proven.

In his original work, Hooley used the GRH to treat both the main term $N_\Gamma(x,y)$ and the term $M_\Gamma(x,y,z)$. In this proof we will show that a choice of $y = \frac{1}{6r+8} \log\log x$ enables to remove the GRH from the treatment of the main term. This is a key element for subsequent applications.

a) By the inclusion-exclusion formula,

$$N_\Gamma(x,y) = \sum_m^* \mu(m)\pi_m(x)$$

where μ is the Möbius function, the upper $*$ means that the sum is extended to all the integers m whose prime divisors are distinct and less than y (note that this forces $m \leq \prod_{q<y} q = e^{\theta(y)} < e^{2y}$, the last inequality being implied by the Prime Number Theorem) and

$$\pi_m(x) = \#\{p \leq x \mid \forall q,\ q|m,\ q|\ [\mathbf{F}_p^*, \Gamma_p]\}.$$

Now recall that

$$q \mid [\mathbf{F}_p^* : \Gamma_p] \iff p \text{ splits completely in } \mathbf{Q}(\zeta_q, a_1^{1/q}, \ldots, a_r^{1/q}),$$

and if a prime splits completely in two fields then it does also in their compositum. Hence if $L_m = \mathbf{Q}(\zeta_m, a_1^{1/m}, \ldots, a_r^{1/m})$, we have

$$\pi_m(x) = \#\{p \leq x \mid p \text{ splits completely in } L_m\}. \tag{3}$$

The result that gives an asymptotic formula for (3) and makes possible to handle this step without the use of the GRH is the Chebotarev Density Theorem, with the error term described in page 243 of [39]:

Lemma 1.2 (Chebotarev Density Theorem): *If L is a Galois extension of $\mathbf{Q}$ with discriminant d_L and degree n_L, then there exists an absolute constant c such that for*

$$\sqrt{\log x} \geq c\, n_L^{1/2} \max(\log|d_L|, |d_L|^{1/n_L}),$$

one has

$$\#\{p \leq x \mid p \text{ splits completely in } L\} = \frac{1}{n_L}\mathrm{li}(x) + O(x \exp -An_L^{-1/2}\sqrt{\log x})$$

where A is constant depending only on c.□

Now, let d_m be the discriminant of L_m and n_m its degree. The Hensel inequality (see. page. 259 of [42]) states that

$$\log |d_m| \leq n_m \sum_{q|d_m} \log q. \tag{4}$$

therefore

$$d_m^{1/n_m} \leq \prod_{q|d_m} q \leq m a_1 \dots a_r \leq n_m \leq \log d_m$$

since indeed in any field $\log d \geq n$. We can also prove the following.

Corollary 1.3 *If* $m \leq (\log x)^{\frac{1}{3r+4}}$ *then*

$$\pi_m(x) = \frac{\mathrm{li}(x)}{n_m} + O(x \exp -A(\log x)^{1/3})$$

for some absolute positive constant A.

Proof of Corollary 1.3: The inequality assumed for m and the Hensel inequality in (4), imply ($n_m \leq m^{r+1}$):

$$c\, n_m^{1/2} \log d_m \leq c\, n_m^{3/2} \sum_{q|d_m} \log q \leq m^{\frac{3r+4}{2}} \leq (\log x)^{1/2}.$$

Hence, Lemma 1.2 gives

$$\pi_m(x) - \frac{\mathrm{li}(x)}{n_m} = O\left(x \exp\left(-A\left(\frac{\log x}{n_m}\right)^{1/2}\right)\right)$$

$$= O\left(x \exp\left(-A(\log x)^{\frac{1}{2}-\frac{r+1}{2(3r+4)}}\right)\right) = O\left(x \exp\left(-A(\log x)^{1/3}\right)\right). \square$$

The choice made for y allows us to apply Corollary 1.3 to all the $m \leq e^{2y} = (\log x)^{\frac{1}{3r+4}}$. Using the estimate (1) for the degree n_m, we get:

$$N_\Gamma(x,y) = \sum_m{}^{\cdot} \mu(m) \left(\frac{1}{n_m}\mathrm{li}(x) + O(x \exp -A(\log x)^{1/3})\right) =$$

$$= \sum_{m=1}^{\infty} \frac{\mu(m)}{n_m} \mathrm{li}(x) + \mathrm{O}\left(\sum_{m>y} \frac{1}{m\phi(m)} \mathrm{li}(x) \right) + \mathrm{O}(e^y x \exp -A(\log x)^{1/3})$$

$$= \sum_{m=1}^{\infty} \frac{\mu(m)}{n_m} \frac{x}{\log x} + \mathrm{o}(\mathrm{li}(x)) + \mathrm{O}((\log x)\, x \exp(-A(\log x)^{1/3}))$$

$$= \delta_r \frac{x}{\log x} + \mathrm{o}\left(\frac{x}{\log x} \right).$$

c) To deal with the last term, we will make use of the following result due to Matthews (see [37]):

Lemma 1.4

$$\#\{p \mid |\Gamma_p| \leq t\} = \mathrm{O}(t^{1+1/r} \sum_i \log a_i)$$

where the constants involved in the O *symbol do not depend on* t *nor* r, *nor on* $\{a_1, \ldots, a_r\}$.

Proof of Lemma 1.4: Consider the set $\mathcal{S} = \{a_1^{n_1} \cdot \ldots \cdot a_r^{n_r} \mid 0 \leq n_i \leq t^{1/r}\}$. As $a_1, \ldots, a_r$ are multiplicatively independent, the number of elements of $\mathcal{S}$ exceeds

$$([t^{1/r}] + 1)^r > t.$$

If p is prime such that $|\Gamma_p| \leq t$, then two distinct elements of $\mathcal{S}$ are congruent $(\mathrm{mod} p)$. Hence, p divides the numerator N of

$$a_1^{m_1} \cdots a_r^{m_r} - 1$$

for some $m_1, m_2, \ldots, m_r$ satisfying $|m_1| \leq t^{1/r}, 1 \leq i \leq r$.

For a fixed choice of $m_1, m_2, \ldots, m_r$, the number of such primes is bounded by

$$\log N \leq t^{1/r} \sum_{i=1}^{r} \log a_i$$

Taking in account the number of possibilities for $m_1, m_2, \ldots, m_r$, the total number of primes p cannot exceed

$$\mathrm{O}(t^{1+1/r} \sum_{i=1}^{r} \log a_i).$$

This completes the proof of the Lemma.□

Now note that

$$M_\Gamma(x,z) \le \#\left\{p \le x \mid \exists\, l \ge z,\ l \middle| \frac{p-1}{|\Gamma_p|}\right\}$$

$$\le \#\left\{p \le x \mid |\Gamma_p| \le \frac{x}{z}\right\}$$

and applying Lemma 1.4 (no dependence on r is required here), we get

$$M_\Gamma(x,z) = O\left(\frac{x^{(1-1/(r+1))(1+1/r)}}{(\log x)^{1+1/r}}\right) = o\left(\frac{x}{\log x}\right).$$

b) For the middle term we assume the GRH which allows to state the following version of the Chebotarev Density Theorem (a proof can be found in [26] or also in [30]):

$$\#\{p \le x \mid p \text{ splits completely in } \mathbf{Q}(\zeta_l, a_1^{1/l})\} = \frac{1}{l(l-1)}\mathrm{li}(x) + O(x^{1/2}\log xl) \quad (5)$$

Now, as in the main term, $l|[\mathbf{F}_p^* : \Gamma_p]$ if and only if p splits completely in the Kummer extension $\mathbf{Q}(\zeta_l, a_1^{1/l}, \ldots, a_r^{1/l})$ and thus, in particular, p splits completely in $\mathbf{Q}(\zeta_l, a_1^{1/l})$. From this we get:

$$M_\Gamma(x,y,z) \le \#\{p \le x \mid \exists\, l,\ y \le l \le z, p \text{ splits completely in } \mathbf{Q}(\zeta_l, a_1^{1/l})\}$$

$$\le \sum_{y \le l \le z}\left(\frac{1}{l(l-1)}\mathrm{li}(x) + O(x^{1/2}\log xl)\right).$$

As $\sum_{l \ge y} \frac{1}{l(l-1)}$ is the tail of a convergent sequence and

$$\sum_{l<z} x^{\frac{1}{2}}\log xl \ll x^{\frac{1}{2}+\frac{1}{r+1}}\log x,$$

for $r > 1$ this yields to an estimate of the type:

$$M_\Gamma(x,y,z) \ll \frac{1}{y}\mathrm{li}(x) + O(x^{\frac{1}{2}+\frac{1}{r+1}}\log x) \quad (6)$$

which is $o(\log x/x)$, and this completes the proof for $r > 1$.

For completeness we add the the proof of the remain case $r = 1$. Estimate (6) has no meaning anymore. We have that

$$M_\Gamma(x, y, x^{1/2}\log x) \leq M_\Gamma(x, y, x^{1/2}/\log^3 x) + M_\Gamma(x, x^{1/2}/\log^3 x, x^{1/2}\log x).$$

The first term is treated as the general case and leads to the coresponding estimate of (6) that in this case is $o\left(\frac{x}{\log x}\right)$. For the second term we proceed as Hooley and we note that $z = x^{1/2}\log x$ and

$$M_\Gamma(x, x^{1/2}/\log^3 x, x^{1/2}\log x) \ll \sum_{x^{1/2}/\log^3 x < l < x^{1/2}\log x} \pi(x, l, 1)$$

$$\ll \frac{x}{\log x} \sum_{x^{1/2}/\log^3 x < l < x^{1/2}\log x} \frac{1}{l} = O\left(\frac{x\log\log x}{\log^2 x}\right).$$

the last by the Brun-Titchmarsh Theorem and the Merten's formula.□

1.2 Computation of the Densities

The density δ_r can always be expressed as an Euler product. Doing so one can prove that the density is not zero. In this section we will calculate δ_r in the case when $a_i = p_i$ is an odd prime for any $i \geq 1$, we will also be able to prove that in this particular case

$$\lim_{r \to \infty} \delta_r = 1.$$

The first step is to calculate the degrees of L_m over $\mathbf{Q}$.

Theorem 1.5 *Let $p_1, \ldots, p_r$ be odd primes, m a square-free integer and let*

$$n_m = [\mathbf{Q}(\zeta_m, p_1^{1/m}, \ldots, p_r^{1/m}) : \mathbf{Q}].$$

Suppose $(m, p_1 \cdots p_r) = p_{i_1} \cdots p_{i_t}$, then $n_m = \frac{\phi(m) m^r}{2^\alpha}$, where

$$\alpha = \begin{cases} 0 & m \text{ is odd or } t = 0 \\ t & \text{if } p_{i_1} \equiv p_{i_2} \equiv \cdots \equiv p_{i_t} \equiv 1 \pmod 4 \\ t-1 & \text{otherwise.} \end{cases}$$

Proof: Fix $m > 1$, we may assume without loss of generality that $p_1 \cdots p_t = (p_1 \cdots p_r, m)$, we let $K = \mathbf{Q}(\zeta_m)$, $A = K(p_1^{1/m}, \ldots, p_t^{1/m})$ and for any $1 \leq i \leq r - t$, let $B_i = A(p_{t+1}^{1/m}, \ldots, p_{t+i}^{1/m})$. We have that

$$n_m = [B_{r-t} : \mathbf{Q}] = [B_{r-t} : A][A : K][K : \mathbf{Q}]$$

and clearly $[K : \mathbf{Q}] = \phi(m)$.

Step 1): We claim that $[B_{r-t} : A] = m^{r-t}$.

Since the polynomial $x^m - p_{t+1}$ splits completely in $B_1 = A(p_{t+1}^{1/m})$, we know that $[B_1 : A] = \frac{m}{d}$. Let $q|d$ be a prime, then $[A(p_{t+1}^{1/q}) : A] = 1$ or q. If it was q, we would have $q = [A(p_{t+1}^{1/q}) : A][B_1 : A] = \frac{m}{d}$, which is a contradiction since m is square-free.

Therefore $p_{t+1}^{1/q} \in A$, which implies that p_{t+1} ramifies in $A/\mathbf{Q}$, but, from Kummer's Theory, we know that the only primes that ramify in A are $p_1, \ldots, p_t$ and those that divide m, and since $(p_{t+1}, m) = 1$, we conclude that $d = 1$. Now, by induction, we have that

$$[B_{r-t} : A] = [B_{r-t} : B_{r-t-1}][B_{r-t-1} : A] = [B_{r-t} : B_{r-t-1}]m^{r-t-1},$$

and again, $[B_{r-t} : B_{r-t-1}] = \frac{m}{d}$ and since $(p_r, m) = 1$, we conclude that $d = 1$. Hence $[B_{r-t} : A] = m^{r-t}$.

Step 2) Let $A_i = K(p_1^{1/m}, \ldots, p_i^{1/m})$, then $A_{i+1} = A_i(p_{i+1}^{1/m})$, and for the same reason as above, $[A_{i+1} : A_i] = \frac{m}{e}$. We claim that $e = 1$ or 2.
Let $q|e$ be a prime divisor and consider $A_i(p_{i+1}^{1/q})$, since m is square-free, we have that $p_{i+1}^{1/q} \in A_i$. If $p_{i+1}^{1/q} \in K$, then we would have a cyclic extension of prime degree (over $\mathbf{Q}$) $\mathbf{Q}(p_{i+1}^{1/q}) \subset K$ and this is only possible when $q = 2$. Therefore we may assume that $p_{i+1}^{1/q} \notin K$, having extensions:

$$K \subseteq K(p_{i+1}^{1/q}) \subseteq A_i.$$

Note that $\mathrm{Gal}(A_i/K)$ is the direct product of cyclic groups and a general subgroup of order q has as fixed field $K((p_{s_1} \cdots p_{s_k})^{1/q})$, with $1 \leq s_1 \leq \cdots \leq s_k \leq i-1$. Therefore, $K(p_{i+1}^{\frac{1}{q}}) = K((p_{s_1} \cdots p_{s_k})^{1/q})$ and from Lemma 3 in page 160 of Cassels and Fröhlich [7], we have that there exists $0 \leq i \leq q-1$ such that

$$\left(\frac{p_{i+1}}{(p_{s_1} \cdots p_{s_k})^i}\right)^{1/q} \in K,$$

and again this implies that $q = 2$.

Therefore, if m is odd, $[A_{i+1} : A_i] = m$ for every i, and thus $[A_t : K] = m^t$.

From the Theory of Cyclotomic Fields, we know that the general quadratic subfield of K has the form $\mathbf{Q}\left(\sqrt{\left(\frac{-1}{D}\right)D}\right)$, where D is a positive divisor of m. We gather that if $p_i \equiv 1 \pmod 4$, $1 \leq i \leq t$, then $\left(\frac{-1}{p_i}\right) = 1$, hence $\sqrt{p_i} \in K$.

Step 3) If $p_1 \equiv p_2 \equiv \cdots \equiv p_t \equiv 1 \pmod 4$,

then let ζ_m be a primitive m-th root of unity, then $\mathrm{Gal}(A_1/K)$ is generated by $\sigma : p_1^{1/m} \mapsto \zeta_m^2 p_1^{1/m}$, (Note that $\sigma(\sqrt{p_1}) = (\sigma(p_1^{1/m}))^{m/2} = (\zeta_m^2)^{m/2} p_1^{(1/m)(m/2)} = \sqrt{p_1}$) and hence, $|\mathrm{Gal}(A_1/K)| = [A_1 : K] = \frac{m}{2}$.

Similarly $\mathrm{Gal}(A_{i+1}/A_i)$ is generated by $\sigma : p_{i+1}^{1/m} \mapsto \zeta_m^2 p_{i+1}^{1/m}$, therefore $[A_{i+1} : A_i] = \frac{m}{2}$ and $[A : K] = \frac{m^t}{2^t}$.

Step 4) If it exists $1 \leq i \leq t$ such that $p_i \equiv 3 \pmod 4$,

then we can suppose without loss of generality that $p_1 \equiv 3 \pmod 4$. Let us consider $A_i = K(p_1^{1/m})$. We have that $[A_1 : K] = m$ (If not, we would have $K(\sqrt{p_1}) = K$, but this only happens when $p_1 \equiv 1 \pmod 4$, which is a contradiction). Now consider $i > 1$, and $A_i = A_{i-1}(p_i^{1/m})$. We claim that $[A_i : A_{i-1}] = \frac{m}{2}$. Indeed either $p_i \equiv 1 \pmod 4$ or $p_i \equiv 3 \pmod 4$; in the first case $\sqrt{p_i} \in K$, in the second case $\sqrt{p_1 p_i} \in K$. In any case, $\mathrm{Gal}(A_i/A_{i-1})$ is always generated by $\sigma : p_i^{1/m} \mapsto \zeta_m^2 p_i^{1/m}$. Finally we get $[A_i : A_{i-1}] = \frac{m}{2}$ and $[A : K] = \frac{m^t}{2^{t-1}}$.

This concludes the proof of the Theorem.□

Corollary 1.6 *With the same notation of Theorem 1.5, we have*

$$n_m \geq m^r \phi(m)/2^{\min(r,\nu(m)-1)}$$

(where $\nu(m)$ is the number of distinct prime divisors of m), furthermore such a lower bound is the best possible.□

We are now ready to express the density as an Euler product. The case $r = 1$ has been dealt with by C. Hooley in [26]. He proved that:

Lemma 1.7 *Let p be a prime, $n_m = [\mathbf{Q}(\zeta_m, p^{1/m}) : \mathbf{Q}]$ and let*

$$A = \prod_{l \text{ prime}} \left(1 - \frac{1}{l(l-1)}\right)$$

be the Artin's constant, then we have:

$$\sum_{m=1}^{\infty} \frac{\mu(m)}{n_m} = \begin{cases} A & \text{if } p \not\equiv 1 \pmod 4, \\ A\left(1 + \frac{1}{p^2-p-1}\right) & \text{if } p \equiv 1 \pmod 4. \end{cases}$$

Proof: If $p \not\equiv 1 \pmod 4$, then $n_m = m\phi(m)$ for every m and the result follows from the definition of the Artin's constant. We can therefore assume that $p \equiv 1 \pmod 4$, having:

$$\sum_{m=1}^{\infty} \frac{\mu(m)}{n_m} = \Sigma_o + \Sigma_e,$$

where Σ_o is the sum extended to the odd values of m and Σ_e to the even values. Clearly $\Sigma_o = 2A$ and $\Sigma_e = -\frac{1}{2}\Sigma'_e$, with

$$\Sigma'_e = \sum_{\substack{m=1 \\ (m,2p)=1}}^{\infty} \frac{\mu(m)}{m\phi(m)} + 2 \sum_{\substack{m=1 \\ p|m, m\text{odd}}}^{\infty} \frac{\mu(m)}{m\phi(m)} =$$

$$2A + \frac{-1}{p(p-1)} \sum_{\substack{m=1 \\ (m,2p)=1}} \frac{\mu(m)}{m\phi(m)} = 2A + \frac{-1}{p(p-1)} \frac{2A}{\left(1 - \frac{1}{p(p-1)}\right)} = 2A - \frac{2A}{p^2-p-1}.$$

Finally $\Sigma_o + \Sigma_e = A\left(1 + \frac{1}{p^2-p-1}\right)$. □

The general case is similar but a little more complicated:

Theorem 1.8 *Let $p_1, \ldots, p_r$ be odd primes, $n_m = [\mathbb{Q}(\zeta_m, p_1^{1/m}, \ldots, p_r^{1/m}) : \mathbb{Q}]$, let $\alpha_i = p_i^r(p_i - 1) - 1$ and define the r-dimensional incomplete Artin's constant to be:*

$$A(r) = \prod_{l \text{ odd prime}} \left(1 - \frac{1}{l^r(l-1)}\right),$$

then:

$$\sum_{m=1}^{\infty} \frac{\mu(m)}{n_m} = A(r)\left\{1 - \frac{1}{2^{r+1}}\left[\prod_{i=1}^{r}\left(1 - \left(\frac{-1}{p_i}\right)\frac{1}{\alpha_i}\right) + \prod_{i=1}^{r}\left(1 - \frac{1}{\alpha_i}\right)\right]\right\}.$$

Proof: As in the case $r = 1$, note that if m is odd, then $n_m = m^r\phi(m)$, thus we can write:

$$\sum_{m=1}^{\infty} \frac{\mu(m)}{n_m} = A(r) - \Sigma$$

where Σ is the sum extended to the even values of m.

Let $P = p_1 \cdots p_r$ and $\tilde{P} = \prod_{i=1,\ p_i \equiv 1(4)}^{r} p_i$, if m is an odd positive integer and $Q = (m, P)$ then, by Theorem 1.5, we have

$$n_{2m} = \begin{cases} 2^r \frac{m^r\phi(m)}{2^{\nu(Q)}} & \text{if } Q|\tilde{P} \\ 2^r \frac{m^r\phi(m)}{2^{\nu(Q)-1}} & \text{otherwise.} \end{cases}$$

For any $Q|P$, let $S(Q) = \{m \in \mathrm{N} |\ (m, P) = Q\}$. We have that $\mathrm{N} = \bigcup_{Q|P} S(Q)$, and the union is disjoint. Therefore,

$$\Sigma = \sum_{Q|P} \sum_{m \in S(Q)} \frac{\mu(2m)}{n_{2m}}.$$

Now divide the set of divisors of P into two sets; the divisors of $\tilde{P}$, and its complement. It follows that

$$\Sigma = \sum_{Q|\tilde{P}} \sum_{m \in S(Q)} \frac{\mu(2m)2^{\nu(Q)}}{2^r m^r \phi(m)} + \sum_{\substack{Q|P \\ Q \nmid \tilde{P}}} \sum_{m \in S(Q)} \frac{\mu(2m)2^{\nu(Q)-1}}{2^r m^r \phi(m)} =$$

$$\frac{1}{2^{r+1}} \left\{ \sum_{Q|\tilde{P}} 2^{\nu(Q)} \sum_{m \in S(Q)} \frac{\mu(2m)}{m^r \phi(m)} + \sum_{Q|P} 2^{\nu(Q)} \sum_{m \in S(Q)} \frac{\mu(2m)}{m^r \phi(m)} \right\}.$$

The sum over $m \in S(Q)$ is easy to evaluate,

$$\sum_{m \in S(Q)} \frac{\mu(2m)}{m^r \phi(m)} = -\frac{(-1)^{\nu(Q)}}{Q^r \phi(Q)} \sum_{(m,2P)=1} \frac{\mu(m)}{m^r \phi(m)} = -\frac{(-1)^{\nu(Q)}}{Q^r \phi(Q)} A(r) \prod_{i=1}^{r} \left(1 - \frac{1}{\alpha_i + 1}\right)^{-1}.$$

Substituting we get:

$$\Sigma = \frac{-A(r)}{2^{r+1}} \prod_{i=1}^{r} \left(1 - \frac{1}{\alpha_i + 1}\right)^{-1} \left(\sum_{Q|\tilde{P}} \frac{(-2)^{\nu(Q)}}{Q^r \phi(Q)} + \sum_{Q|P} \frac{(-2)^{\nu(Q)}}{Q^r \phi(Q)} \right) =$$

$$\frac{-A(r)}{2^{r+1}}\prod_{i=1}^{r}\left(\frac{\alpha_i+1}{\alpha_i}\right)\left(\prod_{\substack{i=1\\ p_i\equiv 1(4)}}^{r}\left(1-\frac{2}{\alpha_i+1}\right)+\prod_{i=1}^{r}\left(1-\frac{2}{\alpha_i+1}\right)\right)=$$

$$\frac{-A(r)}{2^{r+1}}\left(\prod_{\substack{i=1\\ p_i\equiv 1(4)}}^{r}\left(1-\frac{1}{\alpha_i}\right)\prod_{\substack{i=1\\ p_i\equiv 3(4)}}^{r}\left(1+\frac{1}{\alpha_i}\right)+\prod_{i=1}^{r}\left(1-\frac{1}{\alpha_i}\right)\right).$$

The claim is therefore deduced.□

Corollary 1.9 *Let $\{a_i\}_{i>1}$ be a sequence of odd primes and let δ_r be the density of the set of primes p for which $\mathbf{F}_p^*$ is generated by $a_1,\ldots,a_r$, then*

$$\lim_{r\to\infty}\delta_r = 1.\square$$

Remark:

The method just exposed can be easily extended to any set of r multiplicatively independent numbers which are pairwise coprime. The first step of the induction in the general form is in [26]. It is also conceivable that for any *infinite sequence of multiplicatively independent integers* (that is a sequence of integers such that $a_i < a_{i+1}$ and for any r, $a_1,\ldots,a_r$ are multiplicatively independent), one has that $\lim_{r\to\infty}\delta_r = 1$. Not being able to provide a proof of this property here, we will include it in the hypothesis when ever needed.

1.3 The Main Problem

Suppose $f(p)$ is a monotone function of p that tends to infinity with p and let $\{a_n\}_{n\in\mathbf{N}}$ be an infinite sequence of multiplicatively independent integers. Let

$$\Gamma_{f,p} = \langle a_i \pmod p \mid 1 \le i \le f(p)\rangle.$$

Question:

Does a function exist f such that, $\Gamma_{f,p} = \mathbf{F}_p^*$ for almost all primes p ?

Using Theorem 1.1, we can prove:

Theorem 1.10 *Let $\{a_i\}_{i\in\mathbf{N}}$ be a sequence of multiplicatively independent integers such that $\lim_{r\to\infty}\delta_\Gamma = 1$ (We noticed in the last section that when the a_i's are all primes this is true) suppose the Generalized Riemann Hypothesis holds for the Dedekind function of the field $\mathbf{Q}(\zeta_l, a_1^{1/l})$, l prime, then for any monotone function $f(p)$ that tends to infinity, we have that*

$$\#\{p \le \mid \Gamma_{f,p} = \mathbf{F}_p^*\} \sim \pi(x).$$

Proof: Let us fix $r \in \mathbf{N}$. For all but finitely many primes p, we have:

$$\Gamma_{f,p} \supset \Gamma_p = \langle a_1, \ldots, a_r\rangle.$$

Therefore

$$\mathcal{A} = \#\{p \le x \mid \Gamma_{f,p} = \mathbf{F}_p^*\} \ge \#\{p \le x \mid \Gamma_p = \mathbf{F}_p^*\} + O(1).$$

From Theorem 1.1, we get:

$$\overline{\lim_{x\to\infty}} \frac{\mathcal{A}}{\frac{x}{\log x}} \ge \delta_\Gamma.$$

Now let r tend to infinity and prove the statement.□

Our intention in the following Chapters is to prove statements of the type of Theorem 1.10, restricting our assumptions only on the rate of growth of f. For example it is not difficult to prove:

Proposition 1.11 *Let $f(p) = \log^{2+\epsilon} p$ then there exists a sequence of multiplicatively independent integers such that, for almost all primes p, $\Gamma_{f,p} = \mathbf{F}_p^*$.*

Proof: This is a consequence of a Theorem of Burgess and Elliott (see [5]) on the average of the least primitive root. They proved that if $g(p)$ is the least primitive root, then for large x,

$$\pi(x)^{-1} \sum_{p \le x} g(p) \ll \log^2 x (\log\log x)^2.$$

If U is the number of primes up to x for which $g(p) \ge f(p)$, we get that:

$$U \log^{2+\epsilon} x \ll \sum_{\frac{x}{\log x} \le p \le x} g(p) + o\left(\pi(x) \log^{2+\epsilon} x\right) \ll \pi(x) \log^2 x (\log\log x)^2$$

which is equivalent to saying that for almost all primes $g(p) \le f(p)$.
Now let $a_i = p_i$ be the i-th prime number, since $g(p) \le \log^{2+\epsilon} p$, every prime that divide $g(p)$ is also less than $f(p)$, therefore $\Gamma_{f,p}$ contains a primitive root for almost all primes p.□

2 ON THE ARTIN L-FUNCTIONS OF $\mathbf{Q}(\zeta_l, 2^{1/l})$

2.1 Introduction

Let $L = \mathbf{Q}(\zeta_l, 2^{1/l})$ and $G = \mathrm{Gal}(L/\mathbf{Q})$. If

$$\begin{array}{rcl} \tau : L & \longrightarrow & L \\ 2^{1/l} & \mapsto & \zeta_l 2^{1/l} \\ \zeta_l & \mapsto & \zeta_l \end{array} \quad \text{and} \quad \begin{array}{rcl} \nu : L & \longrightarrow & L \\ 2^{1/l} & \mapsto & 2^{1/l} \\ \zeta_l & \mapsto & \zeta_l^g \end{array}$$

(where g is a primitive root modulo p), then G is generated by τ and ν, more precisely,

$$G = < \tau,\ \nu \mid \tau^l = \nu^{l-1} = 1,\ \nu^{-1}\tau\nu = \tau^{g^*} >$$

is a presentation (here g^* is any integer such that $gg^* \equiv 1 \bmod p$).

Hence G is the semidirect product of a cyclic group of order l by a cyclic group of order $l-1$. Note also that τ generates the Galois group of $L/\mathbf{Q}(\zeta_l)$ and the subgroup generated by ν has as fixed field, the non-Galois field $K = \mathbf{Q}(2^{1/l})$.

For any $t = 1, \ldots, l-1$, the map

$$\chi_t : G \to G, \tau \mapsto 1, \nu \mapsto e^{\frac{2\pi i t}{l-1}}$$

is clearly a character and a quick computation shows that G has l conjugate classes and the remaining character of G can be calculated via the orthogonality relations. That is

$$\chi_l(\tau^a \nu^b) = \begin{cases} (l-1) & \text{If } a = b = 0 \\ 0 & \text{If } b \neq 0 \\ -1 & \text{If } b = 0, \text{ and } a \neq 0. \end{cases}$$

Note also that χ_l is induced by any non-trivial character of the normal subgroup generated by τ and if $\phi_t : \nu \mapsto e^{2\pi i t/(l-1)}, t < l-1$ is a character of the subgroup $\langle \nu \rangle$,

then $\mathrm{ind}_{(\nu)}^{G}\phi_t = \chi_t + \chi_l$.

Hence $\chi_1, \ldots, \chi_l$ is a complete list of the irreducible characters of G.

Let us now take a step back and describe the concept of non-Abelian Artin L-function. Let E/F be a Galois extension and ρ a representation of $\mathrm{Gal}(E/F)$, we define the Artin L-function of ρ to be

$$L(s, \rho, E/F) = \prod_{\mathfrak{p}} L_{\mathfrak{p}}(s)$$

where, if $\mathfrak{p}$ does not ramify, the Artin symbol $\sigma_{\mathfrak{p}}$ is the conjugacy class in $\mathrm{Gal}(E/F)$ determined by the Frobenius automorphism of the residue field of any prime of E over $\mathfrak{p}$ (note also that, if $\mathfrak{p}$ does not ramify in E, then $\sigma_{\mathfrak{p}} = \{1\}$ if and only if $\mathfrak{p}$ splits completely in E) and $L_{\mathfrak{p}}(s)$ is the characteristic polynomial of $\sigma_{\mathfrak{p}}$ evaluated at $N(\mathfrak{p})^{-s}$, i.e.

$$L_{\mathfrak{p}}(s) = \det(I - N(\mathfrak{p})^{-s}\rho(\sigma_{\mathfrak{p}}))^{-1}$$

and, if $\mathfrak{p}$ is ramified, $L_{\mathfrak{p}}(s)$ is the characteristic polynomial of the Frobenius element at $\mathfrak{p}$ acting on the subspace fixed by the inertia group $\mathrm{I}_{\mathfrak{p}}$ evaluated at $N(\mathfrak{p})^{-s}$.

Simple arguments on the bounds of the eigenvalues of the representation show that $L(s, \rho, E/F)$ converges absolutely for $\Re(s) > 1$. Since the determinant of a matrix is the product of its eigenvalues, we also have that:

$$\log L(s, \rho, E/F) = \sum_{\mathfrak{p},\, m} \frac{\mathrm{tr}(\rho(\sigma_{\mathfrak{p}})^m)}{m\mathfrak{p}^{ms}}$$

Sometimes, we might indicate $L(s, \rho, E/F)$ by $L(s, \chi, E/F)$ where χ is the character of ρ.

We describe here the basic properties of L-functions. For a more complete picture, see [33] Chapter XII.

PROPERTIES:

A) If $Z_F(s)$ is the usual Dedekind zeta function of the field F, then

$$Z_F(s) = L(s, 1, E/F);$$

B) If χ_1, χ_2 are two characters of $\mathrm{Gal}(E/F)$, then

$$L(s, \chi_1 + \chi_2, E/F) = L(s, \chi_1, E/F) + L(s, \chi_2, E/F);$$

C) If $E' \supset E \supset F$, where E'/F is also Galois, then any character of $\mathrm{Gal}(E/F)$ can be viewed as a character of $\mathrm{Gal}(E'/F)$ (by composing $\mathrm{Gal}(E'/F) \longrightarrow\!\!\!\!\!\rightarrow \mathrm{Gal}(E/F) \xrightarrow{\chi}$ C), and we have

$$L(s, \chi, E/F) = L(s, \chi, E'/F);$$

D) If $E \supset E' \supset F$ then $\mathrm{Gal}(E/E') \subset \mathrm{Gal}(E/F)$, therefore any character χ of $\mathrm{Gal}(E/E')$ induces a character $\mathrm{Ind}(\chi)$ of $\mathrm{Gal}(E/F)$ and one has:

$$L(s, \mathrm{Ind}(\chi), E/F) = L(s, \chi, E/E');$$

E) If E/F is an abelian extension then for every character χ, $L(s, \chi, E/F)$ has an extension to an entire function and verifies a functional equation;

F) If χ_{reg} is the character of the regular representation of $\mathrm{Gal}(E/F)$, then

$$L(s, \chi_{\mathrm{reg}}, E/F) = Z_E(s).$$

(This is a consequence of the fact that the regular representation is induced by the trivial character on the trivial identity subgroup which is the Galois group of L/L therefore, D) and A) give this claim);

G) The Brauer Theorem for characters, states that any character is equal to a sum with integer coefficients of characters induced from elementary subgroups (see

[46] Chapter X). By properties B), C), and D) this implies that any Artin L-function can be written as product of powers with integer exponents of entire functions, and therefore, any such a function is certainly meromorphic. Artin had actually conjectured that these functions are always entire whenever χ does not contain the trivial character;

H) Whenever the Galois group of an extension has the property that every character is induced by the character of an abelian subgroups (such characters are called monomials) then the Artin Conjecture holds for such an extension. This is the case of nilpotent extensions (as well as supersolvable extensions).

2.2 Artin L-functions of $L/\mathbf{Q}$

The Galois group G of $L/\mathbf{Q}$ is certainly supersolvable. Thus all the Artin L-functions of G are entire and by the properties F), D) and A), we have the following factorization:

$$Z_L(s) = \zeta(s) \left(\prod_{t=1}^{l-2} L(s, \chi_t, L/\mathbf{Q}) \right) L(s, \chi_l, L/\mathbf{Q})^{l-1}.$$

On the other hand, if $K = \mathbf{Q}(2^{1/l})$,

$$Z_L(s) = L(s, \chi_{\text{reg}}, L/K) = Z_K(s) \prod_{t=1}^{l-2} L(s, \phi_t, L/K) =$$

$$Z_K(s) \prod_{t=1}^{l-2} L(s, \chi_t, L/\mathbf{Q}) L(s, \chi_l, L/\mathbf{Q}),$$

the last identity being obtained noticing that $\text{Ind}(\phi_t) = \chi_t + \chi_l$ and applying properties B) and D). Putting the two together, we get

$$Z_K(s) = \frac{Z_L(s)}{\left(\prod_{t=1}^{l-2} L(s, \chi_t, L/\mathbf{Q}) \right) L(s, \chi_l, L/\mathbf{Q})^{l-2}}$$

$$= \frac{\zeta(s) \left(\prod_{t=1}^{l-2} L(s, \chi_t, L/\mathbf{Q}) \right) L(s, \chi_l, L/\mathbf{Q})^{l-1}}{\left(\prod_{t=1}^{l-2} L(s, \chi_t, L/\mathbf{Q}) \right) L(s, \chi_l, L/\mathbf{Q})^{l-2}} = \zeta(s) L(s, \chi_l, L/\mathbf{Q}).$$

Therefore the zeroes of $L(s, \chi_l, L/\mathbf{Q})$ are in particular zeroes of $Z_K(s)$ and

$$L(1, \chi_l, L/\mathbf{Q}) = \mathrm{Res}_{s=1} Z_K(s) \neq 0$$

The identity also allows us to compute the functional equation for $L(s, \chi_l, L/\mathbf{Q})$. It is indeed a classical result that if K is any number field, and

$$F_K(s) = A^s \Gamma\left(\frac{s}{2}\right)^{r_1} \Gamma(s)^{r_2} Z_K(s) \tag{1}$$

(where $A = 2^{-r_2} d_K^{1/2} \pi^{-n_K/2}$, r_1 and r_2 are respectively the number of real and complex embeddings of K, d_K is the absolute value of the discriminant of K and n_K its degree over $\mathbf{Q}$) then $F_K(s) = F_K(1-s)$.

In our case $d_K = 2^{l-1} l^l$, $n_K = l$, $r_1 = 1$, $r_2 = (l-1)/2$, and

$$Z_K(s) = \zeta(s) L(s, \chi_l, L/\mathbf{Q}),$$

so we get:

$$F_K(s) = \left(\frac{l}{\pi}\right)^{(l/2)s} \Gamma\left(\frac{s}{2}\right) \Gamma(s)^{(l-1)/2} \zeta(s) L(s, \chi_l, L/\mathbf{Q}).$$

Using the fact that the value of $\pi^{s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s)$ does not change if we substitute s with $1-s$, we get that if

$$G(s) = \left(\frac{l}{\pi}\right)^{(l/2)s} \pi^{s/2} \Gamma(s)^{\frac{l-1}{2}} L(s, \chi_l, L/\mathbf{Q}) \tag{2}$$

then $G(s) = G(1-s)$, which is the functional equation.

An asymmetric functional equation can also be deduced using the formula:

$$\Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin \pi s};$$

which is

$$L(1-s, \chi_l, L/\mathbf{Q}) = \frac{l^{l(s-1/2)}}{\pi^{(l-1)s}} (\sin \pi s)^{(l-1)/2} \Gamma(s)^{l-1} L(s, \chi_l, L/\mathbf{Q}) \tag{3}$$

These results can be used to determine all the zeroes of $L(s, \chi_l, L/\mathbf{Q})$ outside of the critical strip. Indeed $L(s, \chi_l, L/\mathbf{Q})$ has just a zero of order $\frac{l-1}{2}$ for $s = 0, -1, -2, \ldots$ and is non-vanishing elsewhere (outside the critical strip).

We conclude this Section with a classical general result that we will use later (this result can be found in [31], in that version, though, are missing all the uniformity conditions which are necessary for subsequent applications).

Lemma 2.1 *Let K be a number field, $n = [K : \mathbf{Q}]$, d the absolute value of the discriminant and let $Z_K(s)$ be its Dedekind zeta function. There exists a positive absolute numerical constant c_1 such that in the region*

$$\sigma \geq 1 - \frac{c_1}{\log d(t+2)^n}, \quad t \geq 0$$

$Z_K(s)$ has no zeroes.

Proof of Lemma 2.1: We will follow the classical proof for the Riemann Zeta function (See. [6] §13). Let $H_K(s) = \frac{1}{2}s(s-1)F_K(s)$ where $F_K(s)$ has been defined in (1). $H_K(s)$ is an integral function of order 1, verifies $H_K(1-s) = H_K(s) = \overline{H_K(\bar{s})}$ and admits the following Weierstrass product expansion:

$$H_K(s) = e^{a+bs} \prod_{\rho} \left(1 - \frac{s}{\rho}\right) e^{s/\rho} \tag{4}$$

where the product is extended to all the non-trivial zeroes of $Z_K(s)$.

Taking the logarithmic derivative and using the functional equation, we get

$$\frac{H_K'}{H_K}(s) = b + \sum_{\rho} \left(\frac{1}{s-\rho} + \frac{1}{\rho}\right) = -b - \sum_{\rho} \left(\frac{1}{1-s-\bar{\rho}} + \frac{1}{\bar{\rho}}\right) = -\frac{\overline{H_K'}}{\overline{H_K}}(1-\bar{s}).$$

Since, if ρ is a root then also $1 - \bar{\rho}$ is, we deduce that

$$\Re\left(b + \frac{1}{2}\sum_{\rho}\left(\frac{1}{\rho} + \frac{1}{\bar{\rho}}\right)\right) = 0,$$

therefore

$$\Re\left(\frac{H_K'}{H_K}(s)\right) = \sum_\rho \Re\left(\frac{1}{s-\rho}\right).$$

Substituting inside the real part of the logarithmic derivative of (1), we have the identity:

$$\sum_\rho \Re\left(\frac{1}{s-\rho}\right) = \Re\left(\frac{1}{s} + \frac{1}{s-1} + \log A + \frac{r_1}{2}\frac{\Gamma'(s/2)}{\Gamma(s/2)} + r_2\frac{\Gamma'(s)}{\Gamma(s)} + \frac{Z_K'(s)}{Z_K(s)}\right). \quad (5)$$

Now consider this expression for $s = \sigma, \sigma+it, \sigma+2it$, $1 < \sigma \leq 2$, $t \geq 0$. Since $\log(A) \ll \log d$ and since

$$\Re\left(\frac{1}{s-\rho}\right) = \frac{\sigma-\beta}{|s-\rho|^2} > 0,$$

there exist three absolute positive constants c_2, c_3, c_4 such that if we take $t = \gamma$ to be the ordinate of the zero $\rho = \beta + i\gamma$, then

$$-\Re\frac{Z_K'(\sigma)}{Z_K(\sigma)} < \frac{1}{\sigma-1} + c_2\log(d);$$

$$-\Re\frac{Z_K'(\sigma+it)}{Z_K(\sigma+it)} < c_3\log(d(t+2)^n) - \frac{1}{\sigma-\beta};$$

$$-\Re\frac{Z_K'(\sigma+2it)}{Z_K(\sigma+2it)} < c_4\log(d(t+2)^n)$$

because of the Stirling formula for the Gamma function. Finally the standard inequality

$$3\left[-\frac{Z_K'(\sigma)}{Z_K(\sigma)}\right] + 4\left[-\Re\frac{Z_K'(\sigma+it)}{Z_K(\sigma+it)}\right] + \left[-\Re\frac{Z_K'(\sigma+2it)}{Z_K(\sigma+2it)}\right] \geq 0$$

implies

$$\frac{4}{\sigma-\beta} < \frac{3}{\sigma-1} + c_5\log(d(t+2)^n).$$

A choice of $\sigma = 1 + \frac{\delta}{\log(d(t+2)^n)}$ yields, for an opportune δ

$$\beta < 1 - \frac{c_1}{\log(d(t+2)^n)}$$

which is equivalent to the statement.□

2.3 On the non-Abelian L-function of $\mathbf{Q}(\zeta_l, 2^{1/l})$

Just for this Section, we will use the notation $L(s) = L(s, \chi_l, L/\mathbf{Q})$, the main goal of this Section is to prove the following:

Theorem 2.2 *With the same notations as above, there exists a positive absolute constant A such that uniformly*

$$\pi(x, \chi_l) = \sum_{p \leq x} \chi_l(\sigma_p) \ll xl \exp\left(-A\sqrt{\frac{\log x}{l}}\right).$$

Proof: In the spirit of the classical Prime Number Theorem (See. Davenport [6]), if we define

$$\Lambda_l(n) = \begin{cases} \chi_l(\sigma_p) \log p & \text{if } n \text{ is a power of a prime } p \\ 0 & \text{otherwise,} \end{cases}$$

then it is sufficient to prove that

$$\psi(x, \chi_l) = \sum_{n \leq x} \Lambda_l(n) \ll xl \exp\left(-A\sqrt{\frac{\log x}{l}}\right).$$

for some absolute positive constant A.

We will need some lemmas.

Lemma 2.3 *Let $N(T, \chi_l)$ be the number of zeroes $\sigma + it$ of $L(s, \chi_l, L/\mathbf{Q})$ such that $0 \leq \sigma \leq 1$ and $0 < t \leq T$ then if d_K is the absolute value of the discriminant of $K = \mathbf{Q}(2^{1/l})$,*

$$N(T, \chi_l) = (l-1)\frac{T}{2\pi} \log \frac{T}{2\pi} - (l-1)\frac{T}{2\pi} + \left(\frac{\log d_K}{2\pi}\right) T + O(\log d_K T^l).$$

Proof of the Lemma: If $N_K(T)$ and $N(T)$ are respectively the number of zeroes of $Z_K(s)$ and $\zeta(s)$ in the region in question, then we have that $N(T, \chi_l) = N_K(T) - N(T)$ and since, from the classical theory, we know that

$$N(T) = \frac{T}{2\pi}\log\frac{T}{2\pi} - \frac{T}{2\pi} + O(\log T).$$

It is enough to show that

$$N_K(T) = l\frac{T}{2\pi}\log\frac{T}{2\pi} - l\frac{T}{2\pi} + \left(\frac{\log d_K}{2\pi}\right)T + O(\log d_K T^l).$$

Also, in the same way as in the classical result, we can write

$$4\pi N_K(T) = \Im\left(\int_{\mathcal{R}} \frac{H_K'}{H_k}(s)ds\right) \tag{6}$$

where $H_K(s)$ is the function defined during the proof of the lemma in the last Section and $\mathcal{R}$ is the rectangle, described counterclockwise, having as vertices:

$$5/2 - iT,\ \ 5/2 + iT,\ \ -3/2 + iT,\ \ -3/2 - iT\ .$$

Since $H_K(s) = \frac{1}{2}s(s-1)F_K$, by the residue theorem, we can write that (6) is equal to

$$\Im\left(\int_{\mathcal{R}}\left(\frac{1}{s} + \frac{1}{s-1} + \frac{F_K'}{F_K}(s)\right)ds\right) = 4\pi + \Im\left(\int_{\mathcal{R}}\frac{F_K'}{F_K}(s)ds\right) \tag{7}$$

If $\mathcal{L}$ denotes the line from $5/2$ to $5/2+iT$ and then to $\frac{1}{2}+iT$, then using the functional equation, we quickly get that (7) equals:

$$4\pi + 4\Im\int_{\mathcal{L}}\frac{F_K'}{F_K}(s)ds = 4\pi + 4T\log A + 4\Im\int_{\mathcal{L}}\left(r_1/2\frac{\Gamma'(s/2)}{\Gamma(s/2)} + r_2\frac{\Gamma'(s)}{\Gamma(s)} + \frac{Z_K'(s)}{Z_K(s)}\right)ds$$

and, by the Stirling formula we know that

$$\Im\left(\int_{\mathcal{L}}\frac{\Gamma'(s/2)}{\Gamma(s/2)}ds\right) = 2\Im\log\Gamma\left(\frac{1}{4} + i\frac{T}{2}\right) = T\log\frac{T}{2} - T - \frac{\pi}{4} - O\left(\frac{1}{T}\right),$$

and

$$\Im\left(\int_{\mathcal{L}}\frac{\Gamma'(s)}{\Gamma(s)}ds\right) = \Im\log\Gamma\left(\frac{1}{2} + iT\right) = T\log T - T + O\left(\frac{1}{T}\right).$$

This yields

$$N_K(T) = l\frac{T}{2\pi}\log\frac{T}{2\pi} - l\frac{T}{2\pi} + \left(\frac{\log d_K}{2\pi}\right)T + \frac{8-r_1}{8} + O\left(\frac{l}{T}\right) + 4\Im\left(\int_{\mathcal{L}}\frac{Z_K'(s)}{Z_K(s)}ds\right).$$

The problem amounts to proving that

$$\Im\left(\int_{\mathcal{L}}\frac{Z_K'(s)}{Z_K(s)}ds\right) = O(\log d_K T^l). \tag{8}$$

Since $Z_K(s)$ is real on the reals, we have that $\Delta_L \arg(Z_K(s)) = \arg Z_K(\frac{1}{2}+iT)$. As in the classical case:

Lemma 2.4 *For all $T > 0$, we have that*

$$\sum_\rho \frac{1}{1+(T-\gamma)^2} = O(\log d_K(T+2)^l)$$

where ρ runs over all the non-trivial zeroes of $Z_K(s)$.

Proof of Lemma 2.4: From the same argument used in the proof of Lemma 2.1, we know that for $1 < \sigma \leq 2$ and $t > 0$, there exists an absolute positive constant c_0 such that

$$-\Re\frac{Z_K'(s)}{Z_K(s)} < c_0\log(d_K(t+2)^l) - \sum_\rho \Re\frac{1}{\sigma-\beta}.$$

Since for a choice of $s = 2+iT$, we have

$$\left|\frac{Z_K'}{Z_K}(2+iT)\right| \ll \log d_K.$$

we obtain

$$\sum_\rho \Re\frac{1}{\sigma-\beta} < c_1\log(d_K(T+2)^l).$$

Finally note that

$$\Re\frac{1}{\sigma-\beta} = \frac{2-\beta}{(2-\beta)^2+(T-\gamma)^2} \gg \frac{1}{1+(T-\gamma)^2}$$

and prove the Lemma.□

As in the classical case we have the following implications:

Corollary 2.5 *For $T \geq 2$, we have that* .

$$a) \quad N(T+1) - N(T-1) = O(\log d_K T^n);$$
$$b) \quad \sum_{\rho, |\gamma - T| > 1} \frac{1}{(T-\gamma)^2} = O(\log d_K T^n). \square$$

Now we are ready to prove (8). Take the identity (5) for $s = \sigma + iT$ and $s = 2 + iT$, subtract and get:

$$\frac{Z_K'(\sigma+iT)}{Z_K(\sigma+iT)} = \frac{Z_K'(2+iT)}{Z_K(2+iT)} + O(\log T^l) + \sum_{\rho} \left(\frac{1}{\sigma+iT-\rho} - \frac{1}{2+iT-\rho} \right) \ll \quad (9)$$

$$O(\log d_K T^l) + \sum_{\rho, |T-\gamma|<1} \frac{1}{\sigma+iT-\rho},$$

the last estimate because for $|T-\gamma| > 1$,

$$\left| \frac{1}{\sigma+iT-\rho} - \frac{1}{2+iT-\rho} \right| \leq \frac{3}{|\gamma - T|},$$

and

$$\sum_{\rho, |T-\gamma|<1} \frac{1}{2+iT-\rho} \leq N(T+1) - N(T-1) = O(\log d_K T^n).$$

Finally,

$$\Im \left(\int_{\mathcal{L}} \frac{Z_K'(s)}{Z_K(s)} ds \right) = \Im \left(- \int_{\frac{1}{2}+iT}^{2+iT} \frac{Z_K'(\sigma+iT)}{Z_K(\sigma+iT)} d\sigma \right) + \Im \left(\int_2^{2+iT} \frac{Z_K'(s)}{Z_K(s)} ds \right).$$

By (9), the absolute value of the second integral is $\ll$ than

$$\sum_{\rho, |T-\gamma|<1} \left| \int_{\frac{1}{2}+iT}^{2+iT} \Im(\sigma+iT-\rho)^{-1} \right| d\sigma + O(\log d_K T^n) = \sum_{\rho, |T-\gamma|<1} |\arg(\sigma+iT-\rho)|_{\frac{1}{2}+iT}^{2+iT}$$

$$\leq \pi \left(N(T+1) - N(T-1) \right) + O(\log d_K T^n),$$

while the first integral is in absolute value

$$|\log(|Z_K(2+iT)|/|Z_K(2)|)|$$

which is $O(l)$.$\square$

Lemma 2.6 *Let x be an integer and $2 \leq T < x$, then*

$$\psi(x, \chi_l) = -\sum_{|\gamma| \leq T} \frac{x^\rho}{\rho} + O\left(\frac{xl}{T}(\log lxT)^2 + l^2 \log^2 l\right). \tag{10}$$

where the sum is extended over all those zeroes ρ whose imaginary part γ is in absolute value less or equal than T

Proof of Lemma 2.6: As in the classical case of the zeta function, $\psi(x, \chi_l)$ is the sum of the coefficients of the logarithmic derivative, more precisely, if $c > 1$ and T is large, then the Lemma in §17 of [6] gives that if:

$$J(x,T) = \frac{1}{2\pi i}\int_{c-iT}^{c+iT}\left[-\frac{L'(s)}{L(s)}\right]\frac{x^s}{s}ds,$$

then

$$\psi(x,\chi_l) = J(x,T) + O\left(\sum_{\substack{n=1\\ n\neq x}}^{\infty}\left(\Lambda_l(n)\left(\frac{x}{n}\right)^c \frac{1}{T|\log(x/n)|}\right) + \frac{c\Lambda_l(x)}{T}\right) + O(l\log x) \tag{11}$$

If we choose $c = 1 + 1/\log x$ ($x^c = ex$) and we treat the four ranges separately:

$$(n \leq \tfrac{3}{4}x,\ n \geq \tfrac{5}{4}x)\quad (\tfrac{3}{4}x < n < x-2)\quad (x-2 \leq n \leq x+2)\quad (x+2 < n < \tfrac{5}{4}x).$$

For the values of n, the first range, we have that $|\log(x/n)| \gg 1$ therefore the contribution of these terms in the sum in(11) is

$$\ll \frac{x}{T}\left[-\frac{L'(c)}{L(c)}\right] \ll \frac{x}{T} l\log l, \tag{12}$$

where we just noticed that for $c > 1$

$$-\frac{L'(c)}{L(c)} = -\left(\frac{Z_K'(c)}{Z_K(c)} - \frac{\zeta'(c)}{\zeta(c)}\right) = \frac{1}{c-1} - \frac{1}{c-1} + O(\log d_K) = O(l\log l).$$

and that $d_K = 2^{l-1}l^l$.

For the values of n, the second range, set $[x]-n=r$, and note that $1\le r\le x/4$ therefore

$$\log\left(\frac{x}{n}\right)=\log\left(\frac{x}{[x]-r}\right)\ge\left|\log\left(1-\frac{r}{[x]}\right)\right|\ge\frac{r}{2x}.$$

We gather that the contribution of these terms in (11) is

$$\ll\frac{x}{T}\sum_{1\le r\le x/4}\Lambda_l(x-r)r^{-1}\ll\frac{xl\log x}{T}\sum_{1\le r\le x/4}r^{-1}\ll\frac{xl\log^2 x}{T}\tag{13}$$

Analogously, for the values of n in the fourth range, set $n-[x]=r'$ (now $2\le r'<\frac{x}{4}+1$) and thus

$$\left|\log\left(\frac{x}{n}\right)\right|=-\log\left(1-\frac{n-x}{n}\right)\gg\frac{r}{x}$$

and the contribution of these terms in (11) is

$$\ll\frac{xl\log^2 x}{T}.\tag{14}$$

Finally for the (at most five) values of n in the third range, we have a contribution which is $\ll l\log x$. Putting this together with the estimates in (12), (13) and (14), we get:

$$\psi(x,\chi_l)=J(x,T)+O\left(\frac{xl}{T}(\log^2 x+\log l)\right).\tag{15}$$

Now we replace the vertical segment of integration by the other three sides of the rectangle with vertices

$$c-iT,\quad c+iT,\quad -U+iT,\quad -U-iT$$

where U is a large half integer (i.e. $U=m/2$, m odd integer). If $T\neq\gamma$ for any zero $\rho=\beta+i\gamma$ of $L(s)$ is the critical strip, the residue Theorem gives

$$\begin{aligned}\psi(x,\chi_l) &= -\sum_{|\gamma|<T}\frac{x^\rho}{\rho}-\operatorname*{Res}_{s=0}\left(\frac{x^s}{s}\frac{L'(s)}{L(s)}\right)-\frac{l-1}{2}\sum_{m=1}^{U}\frac{x^{-m}}{-m}+\\ &\quad+O\left(\frac{xl}{T}(\log^2 x+\log l)\right)+\\ &\quad+\frac{1}{2\pi i}\left\{\left(\int_{c-iT}^{-U-iT}+\int_{-U-iT}^{-U+iT}+\int_{-U+iT}^{c+iT}\right)-\frac{L'(s)}{L(s)}\frac{x^s}{s}\right\}\end{aligned}\tag{16}$$

since by the functional equation in (2), the integrand in $J(x,T)$ has simple poles at $s=\rho$, poles of order $(l-1)/2$ at $s=-m$ $(m\geq 1)$, and an extra pole of order 2 at $s=0$.

The residue at $s=0$ can be estimated as follows: Since $L(s)=Z_k(s)/\zeta(s)$, and since $x^s/s=1/s+\log x+\ldots$, we have

$$\operatorname*{Res}_{s=0}\left(\frac{x^s}{s}\frac{L'(s)}{L(s)}\right)=\operatorname*{Res}_{s=0}\left(\frac{1}{s}\frac{Z_K'(s)}{Z_K(s)}\right)+\mathrm{O}(\log x). \tag{17}$$

From the functional equation in (1) and the Weierstrass product expansion in (4) we get that

$$\operatorname*{Res}_{s=0}\left(\frac{1}{s}\frac{Z_K'(s)}{Z_K(s)}\right)=b-\log A+1-(l/2)\frac{\Gamma'(1)}{\Gamma(1)}=b+\mathrm{O}(l\log l). \tag{18}$$

If we substitute $s=2$ in (4), use the functional equation again and note that $Z_K'(2)/Z_K(2)\ll l$, we deduce that

$$b=\sum_{\rho}\left(\frac{1}{2-\rho}+\frac{1}{\rho}\right)+\mathrm{O}(l\log l). \tag{19}$$

For the terms of this series with $|\gamma|\geq 1$, we have

$$\sum_{|\gamma|\geq 1}\left|\frac{1}{2-\rho}+\frac{1}{\rho}\right|=2\sum_{|\gamma|\geq 1}\frac{1}{|\rho(2-\rho)|}\ll\sum_{\rho}\frac{1}{|2-\rho|^2}\ll l\log l. \tag{20}$$

The last sum being estimated as $\mathrm{O}(\log d_k)$ using Lemma 2.4 with $t=0$. The same estimate applies to

$$\sum_{|\gamma|<1}\frac{1}{2-\rho},$$

since for $|\gamma|<1$ we have $|2-\rho|\gg|2-\rho|^2$.

Finally, for $|\gamma|<1$, we know that $c_8/\log d_K<\beta<1-c_8/\log d_K$, therefore

$$\rho^{-1}\ll\log d_K.$$

and being the number of zeroes in question $\ll \log d_K$ by Lemma 2.3 with $T = 1$, we have

$$\sum_{|\gamma|<1} \frac{1}{\rho} = \mathrm{O}(\log^2 d_K) = \mathrm{O}(l^2 \log^2 l). \tag{21}$$

Putting together the estimates (17), (18), (19), (20) and (21) we gather

$$\operatorname*{Res}_{s=0} \left(\frac{x^s}{s} \frac{L'(s)}{L(s)} \right) = \mathrm{O}(l^2 \log^2 l) + \mathrm{O}(\log x). \tag{22}$$

From Corollary 2.5, we see that the number of non-trivial zeroes ρ of $Z_K(s)$ for which $|\gamma - T| < 1$ is $\mathrm{O}(l \log lT)$, thus the differences of the ordinates of these zeroes cannot be all $\mathrm{o}(1/(l \log lT))$. Hence, we can choose T (varying it by a bounded amount, if necessary) so that $|\gamma - T| \gg (l \log lT)^{-1}$ for all the zeroes ρ. This allows us to determine a good bound for $-L'(s)/L(s)$ for $s = \sigma + iT$, T large and $-1 \leq \sigma \leq 2$, that is

$$\frac{L'(s)}{L(s)} = \frac{Z'(s)}{Z(s)} - \frac{\zeta'(s)}{\zeta(s)} = \sum_{\rho, |\gamma - T| < 1} \frac{1}{s - \rho} + \mathrm{O}(\log d_K T^l) \ll l \log^2 lT \tag{23}$$

where we have used (9), the fact that by our choice of T we have $|\gamma - T| \gg (\log d_K T^l)^{-1}$ for all ρ and the fact that the number of summands is here $\ll \log d_K T^l$.

To obtain a bound for $\sigma \leq -1$, we use the asymmetric functional equation (3) whose logarithmic derivative is

$$-\frac{L'(1-s)}{L(1-s)} = l \log l + \frac{l-1}{2} \left(2 \log \pi + \pi \cot \pi s + \frac{\Gamma'(s)}{\Gamma(s)} \right) + \frac{L'(s)}{L(s)}. \tag{24}$$

We know that $\cot \pi s$ is bounded if $|s - m| \geq 1/3$, that is if

$$|(1 - s) + (m + 1)| \geq \frac{1}{3}.$$

If $1 - \sigma \leq -1$, then $\Gamma'(s)/\Gamma(s) = \mathrm{O}(\log 2|1 - s|)$ by the Stirling formula, while the last term (24) is $\mathrm{O}(l)$. Thus

$$\frac{L'(s)}{L(s)} \ll \log 2|s| + l \log l \quad (\sigma \leq 1), \tag{25}$$

provided that circles of radius $1/3$ around the trivial zeroes $s = -m$ of $L(s)$ are excluded.

Using (23) and (25) we have

$$\int_{-U\pm iT}^{c\pm iT} \ll \frac{l\log^2 lT}{T}\int_{-\infty}^{c} x^{\sigma}d\sigma \ll \frac{xl\log^2 lT}{T\log x},$$

while (25) gives

$$\int_{-U-iT}^{-U+iT} \ll \frac{l\log^2 lU}{U}\int_{-T}^{T} x^{U}dt \ll \frac{Tl\log^2 lU}{Ux^{U}} = o(1), \quad (\text{for } U\to\infty).$$

Inserting these estimates in (16) we get the wanted claim.□

Proof of Theorem 2.2: The zero-free region proved for $Z_K(s)$ in Lemma 2.1 holds also for $L(s)$, therefore, if $\rho = \beta + i\gamma$ is a zero of $L(s)$ with $\gamma < T < x$ we have that

$$\beta < 1 - \frac{c}{l\log lT}$$

where c is an absolute positive constant.

We gather that

$$|x^{\rho}| = x^{\beta} < x\exp\left(-c\frac{\log x}{l\log lT}\right). \tag{26}$$

The sum $\sum_{\gamma<T}\frac{1}{\rho}$ extended over all the zeroes with $|\gamma| > 1$ can be estimated by partial summation as follows

$$\sum_{|\gamma|<T}\frac{1}{\gamma} = \int_0^T t^{-1}dN_l(t) = \frac{N_l(T)}{T} + \int_0^T t^{-2}N_l(t)dt$$

$$\ll \log T(l\log T + \log d_K) \ll l^2\log^2 lT.$$

The same sum over the zeroes ρ with $|\gamma| \le 1$ is $O(l^2\log^2 l)$ as we noted in (21). Putting these two facts and (26) together with Lemma 2.6 we get

$$\psi(x,\chi_l) \ll xl^2\log^2 lT\exp\left(-c\frac{\log x}{l\log lT}\right) + \frac{xl}{T}(\log lxT)^2. \tag{27}$$

We minimize it by choosing T such that

$$l \log^2 lT = \log x,$$

and we get that (27) is

$$\ll xl \exp\left(-c/2\sqrt{\frac{\log x}{l}}\right)$$

which by partial summation is equivalent to statement.□

Remark: If we assume the strong Hypothesis that for any prime l, the Dedekind zeta function $Z_K(s)$ has the zero-free region

$$\sigma > 1 - \frac{c}{\log T}, \quad T \geq 0$$

then, using exactly the same method we would be able to prove that uniformly for $l < x$

$$\pi(x, \chi_l) \ll xl \exp\left(-c\sqrt{\log x}\right). \tag{28}$$

2.4 An Application to Chebotarev Density Theorem

In this Section we apply Theorem 2.2 to the Chebotarev Density Theorem, obtaining for the special case of $\mathbf{Q}(\zeta_l, 2^{1/l})$ a stronger result than Lemma 1.2. This will be used later in Theorem 3.1, which is actually a motivation for such a result.

Theorem 2.7 *There exists a constant B such that uniformly for all l with*

$$l < \frac{\log x}{B(\log\log x)^2},$$

we have

$$\begin{aligned} P(x,l) &= \#\{p \leq x \mid p \text{ splits completely in } \mathbf{Q}(\zeta_l, 2^{1/l})\} \\ &= \frac{1}{l(l-1)}\mathrm{li}(x) + O\left(x \exp\left(-Al^{-1/2}\sqrt{\log x}\right)\right), \end{aligned}$$

where A is an absolute positive constant.

Proof Let χ_G be the character of the regular representation. That is:

$$\chi_G(x) = \begin{cases} |G| = l(l-1) & \text{if } x = 1, \\ 0 & \text{otherwise.} \end{cases}$$

We have that

$$\frac{1}{l(l-1)} \sum_{p \leq x} \chi_G(\sigma_p) = \#\{p \leq x \mid \sigma_p \text{ is trivial}\} = \#\{p \leq x \mid p \text{ splits completely in } L\}.$$

On the other hand, $\chi_G = \chi_1 + \ldots + \chi_{l-1} + (l-1)\chi_l$ is the canonical decomposition of the regular character, therefore:

$$\frac{1}{l(l-1)} \sum_{p \leq x} \chi_G(\sigma_p) = \frac{1}{l(l-1)} \sum_{p \leq x} \sum_{i=1}^{l-1} \chi_i(\sigma_p) + \frac{1}{l} \sum_{p \leq x} \chi_l(\sigma_p).$$

The orthogonality relations for the characters of the subgroup $H < G$ give:

$$\frac{1}{l-1} \sum_{i=1}^{l-1} \chi_i(h) = \begin{cases} 1 & \text{if } h = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Therefore, the first $l-1$ characters count the number of primes up to x such that their Artin symbol is trivial modulo H. These are the primes that split completely in the Cyclotomic field $\mathbf{Q}(\zeta_l)$ (whose Galois group is isomorphic to H). Finally, if $\pi(x, l, 1) = \{p \leq x \mid p \equiv 1 \bmod l\}$, then

$$P(x, l) = \frac{1}{l} \left(\pi(x, l, 1) + \pi(x, \chi_l) \right).$$

The Siegel-Walfisz Theorem (see [6] in §22) states that given any positive constant C, if $l \leq (\log x)^C$, one has

$$\pi(x, l, 1) = \#\{p \leq x \mid p \equiv 1 \bmod l\} = \frac{1}{l-1} \mathrm{li}(x) + O(x \exp(-A\sqrt{\log x}))$$

for some constant $A = A(C)$, uniformly in l.

This result with $C = 2$ and Theorem 2.2 gives the wanted claim.□

We conclude with the following statement whose proof is a consequence of the Remark at the end of the last Section.

Theorem 2.8 *Assuming the strong Hypothesis that for any prime l and for any non-trivial zero $\beta + i\gamma$ of the Dedekind zeta function $Z_K(s)$, $\beta < 1 - \frac{c}{\log \gamma}$, then given any positive constant C, uniformly for $l \leq (\log x)^C$, we have*

$$P(x, l) = \frac{1}{l(l-1)}\mathrm{li}(x) + O\left(x \exp\left(-A\sqrt{\log x}\right)\right),$$

for some constant $A = A(C)$.□

3 ON THE NUMBER OF PRIMES GENERATING $\mathbf{F}_p^*$

3.1 Extending Hooley's Method

In this Section we will extend the ideas illustrated in Chapter 1 proving the following

Theorem 3.1 *Suppose Γ_p is the subgroup of $\mathbf{F}_p^*$ generated by the classes of the first $\log p$ primes, let*

$$N(x) = \#\{p \leq x \mid \Gamma_p = \mathbf{F}_p^*\}$$

then

$$\overline{\lim_{x\to\infty}} \frac{N(x)}{\frac{x}{\log x}} \geq 1 - \log 2.$$

Proof: If we assume $p \geq x^{1/2}$, then, for every x,

$$\Gamma_p \supseteq \Gamma_{r,p} = \langle p_1, \ldots, p_r \rangle, \text{ with } r = [\frac{1}{2}\log x]$$

and

$$N(x) \geq \tilde{N}(x) = \#\{p \leq x \mid \Gamma_{r,p} = \mathbf{F}_p^*\}. \tag{1}$$

Now, as in the standard Hooley's case, we define for given η_1 and η_2:

$$\begin{aligned}
\tilde{N}(x,\eta_1) &= \#\{p \leq x \mid \forall l,\ l \leq \eta_1,\ \ l \not| [\mathbf{F}_p^* : \Gamma_{r,p}]\};\\
M(x,\eta_1,\eta_2) &= \#\{p \leq x \mid \exists l,\ \eta_1 \leq l \leq \eta_2,\ l | [\mathbf{F}_p^* : \Gamma_{r,p}]\};\\
M(x,\eta_2) &= \#\{p \leq x \mid \exists l,\ l \geq \eta_2,\ l | [\mathbf{F}_p^* : \Gamma_{r,p}]\},
\end{aligned}$$

and clearly

$$\tilde{N}(x) \geq \tilde{N}(x,\xi_1) - M(x,\xi_1,\xi_2) - M(x,\xi_2,\xi_3) - M(x,\xi_3) \tag{2}$$

where $\xi_1 = 1/4\sqrt{\log\log x}$, $\xi_2 = \frac{\log x}{B(\log\log x)^2}$ and $\xi_3 = (\log^2 x)(\log\log x)^2$ and B is a fixed positive number to be chosen later.

- The last term of (2) can be treated as in Theorem 1.1 using Lemma 1.4. We have that

$$M(x,\xi_3) \le \#\left\{p \le x \mid |\Gamma_{r,p}| \le \frac{x}{(\log^2 x)(\log\log x)^2}\right\}$$

and since $\sum_i \log p_i = O(p_r) = O(r\log r)$, Lemma 1.4 gives

$$\begin{aligned} M(x,\xi_3) &\ll \frac{x}{(\log^2 x)(\log\log x)^2}\left(\frac{x}{(\log^2 x)(\log\log x)^2}\right)^{1/r} r\log r \\ &\ll \frac{x}{\log x}\frac{1}{\log\log x}. \end{aligned} \tag{3}$$

- To handle the third term of (2), we will make use of the already quoted Siegel-Walfisz Theorem, which states that given any positive constant C, then if $l \le (\log x)^C$, one has

$$\pi(x,l,1) = \#\{p \le x \mid p \equiv 1 \bmod l\} = \frac{1}{l-1}\mathrm{li}(x) + O(x\exp(-A\sqrt{\log x})) \tag{4}$$

for some constant $A = A(C)$, uniformly in l.

This result yields to,

$$\begin{aligned} M(x,\xi_2,\xi_3) &\le \#\{p \le x \mid \exists l,\ \xi_2 < l < \xi_3,\ p \equiv 1 \bmod l\} \le \sum_{\xi_2<l<\xi_3} \pi(x,l,1) \\ &= \sum_{\xi_2<l<\xi_3}\left(\frac{1}{l-1}\mathrm{li}(x) + O(x\exp(-A\sqrt{\log x}))\right) \end{aligned} \tag{5}$$

where we have chosen $C = 3$ say.

Now recall the Merten's Theorem that states that for any two positive numbers a and b,

$$\sum_{a<l<b}\frac{1}{l} = \log\left(\frac{\log b}{\log a}\right) + O\left(\frac{1}{\log b}\right).$$

It follows that:

$$\sum_{a<l<b}\frac{1}{l-1} = \sum_{a<l<b}\frac{1}{l} + \sum_{a<l<b}\frac{1}{l(l-1)} = \log\left(\frac{\log b}{\log a}\right) + O\left(\frac{1}{\log b}\right). \tag{6}$$

Using this result in (5), we get

$$M(x,\xi_2,\xi_3) \le \mathrm{li}(x)\left(\log\left(\frac{\log\xi_3}{\log\xi_2}\right)+\mathrm{O}((\log\xi_2)^{-1})\right)+\mathrm{O}\left(\xi_3 x\exp-c\sqrt{\log x}\right)$$

$$\le \frac{x}{\log x}\left(\log 2+\log\left(\frac{1+\log\log\log x/\log\log x}{1-(\log B+2\log\log\log x)/\log\log x}\right)\right)+\mathrm{o}\left(\frac{x}{\log x}\right)$$

$$=\frac{x}{\log x}\log 2+\mathrm{o}\left(\frac{x}{\log x}\right) \tag{7}$$

- Theorem 2.7 in Chapter 2 is the ingredient to the estimate of the second term of (2). Indeed, $l<\xi_2$ yields to

$$\begin{aligned} M(x,\xi_1,\xi_2,) &\le \sum_{\xi_1<l<\xi_2}\#\{p\le x \mid p \text{ splits completely in } \mathbf{Q}(\zeta_l,2^{1/l})\} \\ &= \sum_{\xi_1<l<\xi_2}\left(\frac{1}{l(l-1)}\mathrm{li}(x)+\mathrm{O}(xl\exp\left(-Al^{-1/2}\sqrt{\log x}\right)\right) \\ &\ll \frac{1}{\xi_1}\mathrm{li}(x)+x\xi_2^2\exp\left(-A\xi_2^{-1/2}\sqrt{\log x}\right) \\ &\ll \frac{1}{\xi_1}\mathrm{li}(x)+\frac{x\log^2 x}{(\log\log x)^4\log^{AB/2}x}=\mathrm{o}\left(\frac{x}{\log x}\right), \end{aligned} \tag{8}$$

where B has been chosen to be larger than $6/A$, say.

- To treat the main term of (2), let us set $t=[(\log r)^{1/2}]$, and note that if

$$N_0(x,\xi_1)=\#\{p\le x \mid \forall l,\ l\le\xi_1,\ \ l\nmid[\mathbf{F}_p^*:\Gamma_{t,p}]\},$$

then $\tilde{N}(x,\xi_1)\ge N_0(x,\xi_1)$, and

$$\hat{N}(x,\xi_1)=\sum_m^* \mu(m)\pi_m(x),$$

where again the sum is extended to all the square free integers m whose prime divisors are less then ξ_1 (Note $m\le e^{\xi_1}$), and

$$\pi_m(x)=\#\{p\le x \mid p \text{ splits completely in } \mathbf{Q}(\zeta_m,p_1^{1/m},\dots,p_t^{1/m})\}.$$

Finally, the Hensel inequality (see (4) of Section 1.1) gives

$$c\, n_m^{1/2} \log d_m \leq m^{\frac{3}{2}t+1}(\log m + \sum_{i\leq t} \log p_i) \leq m^{2t} \leq e^{2\xi_1 t} \leq \sqrt{\log x}.$$

Therefore the Chebotarev Density Theorem (see Lemma 1.2 of Section 1.1) gives

$$N_0(x,\xi_1) = \sum_m^{\cdot} \mu(m) \left(\frac{1}{n_m} \mathrm{li}(x) + O\left(x \exp\left(-A\sqrt{\frac{\log x}{n_m}} \right) \right) \right)$$

$$= \sum_{m=1}^{\infty} \frac{\mu(m)}{n_m} \frac{x}{\log x} + O\left(\sum_{m>\xi_1} \frac{1}{m^{t+1}} \mathrm{li}(x) \right) + O\left(e^{\xi_1} x \exp\left(-A\sqrt{\frac{\log x}{(\log x)^{1/2}}} \right) \right)$$

$$= \delta_\Gamma \frac{x}{\log x} + O\left(\frac{1}{\xi_1} \frac{x}{\log x} \right), \tag{9}$$

where δ_Γ is as in Section 1.1 and where we used the fact that in this range of m, $n_m \leq e^{2t\xi_1} \leq \sqrt{\log x}$.

Putting together the estimates (3), (7), (8) and (9) and using (1) and (2), we get

$$N(x) \geq N_0(x,\xi_1) - M(x,\xi_1,\xi_2) - M(x,\xi_2,\xi_3) - M(x,\xi_3)$$

$$\geq \delta_\Gamma \frac{x}{\log x} + o\left(\frac{x}{\log x} \right) - \log 2 \frac{x}{\log x} + o\left(\frac{x}{\log x} \right).$$

Therefore, by Corollary 1.9

$$\overline{\lim_{x\to\infty}} \frac{N(x)}{x/\log x} \geq \lim_{x\to\infty} (\delta_\Gamma - \log 2 + o(1)) \geq 1 - \log 2$$

which is the wanted claim.□

The estimate in (8) is the real obstacle to achieve an asymptotic formula for $N(x)$. Such estimate is connected with the range of validity of the Chebotarev Density Theorem of the field $K = \mathbb{Q}(\zeta_l, 2^{1/l})$. As we have seen in Chapter 2, such a range depends on the determination of zero-free regions for $L(s,\chi_l)$ and thus of the Dedekind zeta function $Z_K(s)$. Indeed we have

Theorem 3.2 *Assuming in the strong Hypothesis that for any prime l and for any non-trivial zero $\beta + i\gamma$ of the Dedekind zeta function $Z_K(s)$, $\beta < 1 - \frac{c}{\log T}$, then for almost all primes p, $\mathbf{F}_p^*$ is generated by the first $[2\log p]$ primes.*

Proof. Using exactly the same notation of Theorem 3.1, we now choose $\xi_1 = 1/4\sqrt{\log\log x}$, $\xi_2 = \log^2 x$ and $\xi_3 = (\log^2 x)(\log\log x)^2$.

The estimate of the main and last terms in (2) is the same, for the third term, again we use the Siegel-Walfisz Theorem (4) and Merten's formula (6),

$$\begin{aligned} M(x,\xi_2,\xi_3) &\leq \sum_{\xi_2<l<\xi_3}\left(\frac{1}{l-1}\mathrm{li}(x) + \mathrm{O}\left(x\exp\left(-A\sqrt{\log x}\right)\right)\right) \\ &\leq \frac{x}{\log x}\log\left(\frac{2\log\log x + \log\log\log x}{2\log\log x}\right) + \mathrm{o}\left(\frac{x}{\log x}\right) \\ &= \mathrm{o}\left(\frac{x}{\log x}\right). \end{aligned}$$

Finally for the second term we use Theorem 2.8, and gather that

$$\begin{aligned} M(x,\xi_1,\xi_2,) &\leq \sum_{\xi_1<l<\xi_2}\left(\frac{1}{l(l-1)}\mathrm{li}(x) + \mathrm{O}\left(xl\exp\left(-A\sqrt{\log x}\right)\right)\right) \\ &= \mathrm{o}\left(\frac{x}{\log x}\right), \end{aligned}$$

and this concludes the proof.□

Remark: It can be proven that the minimal assumption necessary to prove that $N(x) \sim \pi(x)$ in Theorem 3.1 is that the Dedekind zeta function $Z_K(s)$ has a zero-free region of the type

$$\sigma > 1 - \frac{c}{l^{1/2}\log d_K^{1/l}T}, \quad T \geq 0,$$

for any prime l large enough and for some absolute positive constant c.

Indeed this would yield to a version of Chebotarev Density Theorem for K valid up to $l < (\log x)^2$, and the rest of the proof would work as in Theorem 3.2.

Finally note that using this approach improvements, in terms of determining a significantly smaller set of generators of $\mathbf{F}_p^*$ for almost all p, are not possible. The choice $r = \log p$ is in fact imposed by the statement of Lemma 1.4. The next Section is devoted to analyzing this aspect in a more detailed manner.

3.2 Relaxation of the Hypothesis and Improvements

Our first intention is to prove a version of Theorem 3.1 in which the number of generators is optimal with respect to the method used. As we have already remarked, the choice of the minimal number of generators of $\mathbf{F}_p^*$ for a positive proportion of p's is imposed by Lemma 1.4. Precisely

Theorem 3.3 a) *Let f be a (monotone) function of p with $f(p) \to +\infty$ for $p \to \infty$ and let Γ_p be the subgroup of $\mathbf{F}_p^*$ generated by the classes of the first*

$$f(p)\frac{\log p}{\log\log p}$$

primes, then for a set of primes of density greater than $1 - \log 2$, we have $\Gamma_p = \mathbf{F}_p^*$.

b) *Let α be a real number with $0 < \alpha < e - 2$ and let Γ'_p be the subgroup of $\mathbf{F}_p^*$ generated by the classes of the first*

$$\frac{\log p}{\alpha \log\log p}$$

primes, then for a set of primes of density greater than $1 - \log(2 + \alpha)$, it follows that $\Gamma'_p = \mathbf{F}_p^*$.

Proof: a) The proof starts in the same way as in Theorem 3.1, where we assumed $p \geq x^{1/2}$ and noticed that, for every x,

$$\Gamma_p \supseteq \Gamma_{r,p} =< p_1, \ldots, p_r >, \text{ with } r = \left[\frac{f(x)}{2}\frac{\log x}{\log\log x}\right]$$

and

$$\#\{p \le x \mid \Gamma_p = \mathrm{F}_p^*\} \ge \tilde{N}(x, \xi_1) - M(x, \xi_1, \xi_2) - M(x, \xi_2, \xi_3) - M(x, \xi_3) \qquad (10)$$

where the notations, ξ_1 and ξ_2 are the same as in Theorem 3.1 and ξ_3 will be chosen later.

The estimate of the main term and the second term are exactly the same, while this time the estimate of the last term of (10) using Lemma 1.4 is the following:

$$\begin{aligned} M(x, \xi_3) &\le \#\left\{p \le x \mid |\Gamma_{r,p}| \le \frac{x}{\xi_3}\right\} \ll \frac{x}{\xi_3}\left(\frac{x}{\xi_3}\right)^{1/r} r \log r \\ &\ll \frac{x}{\xi_3}(\log x)^{2/f(x)} f(x) \log x \ll \frac{x(\log x)^{1+\epsilon(x)}}{\xi_3} \end{aligned} \qquad (11)$$

where we have put $\epsilon = \epsilon(x) = 2/f(x) + (\log f)/\log\log x$ and assumed that $f(x) \ll \log\log x$, say.

If we now choose $\xi_3 = (\log x)^{2+\epsilon} \log\log x$, we get that (11) is

$$\ll \frac{x}{\log x \log\log x}.$$

Finally we deal with the third term similarly as we did in Theorem 3.1, using the Siegel-Walfisz Theorem and the Merten's Formula:

$$\begin{aligned} M(x, \xi_2, \xi_3) &\le \sum_{\xi_2 < l < \xi_3} \left(\frac{1}{l-1}\mathrm{li}(x) + \mathrm{O}(x \exp(-A\sqrt{\log x}))\right) \\ &\le \mathrm{li}(x)\left(\log\left(\frac{\log \xi_3}{\log \xi_2}\right) + \mathrm{O}((\log \xi_2)^{-1})\right) + \mathrm{O}\left(\xi_3 x \exp -c\sqrt{\log x}\right) \\ &\le \frac{x}{\log x}\left(\log 2 + \log\left(\frac{1 + \epsilon(x)/2}{1 - \log(B(\log\log x)^2)/\log\log x}\right)\right) + \mathrm{o}\left(\frac{x}{\log x}\right) \\ &= \frac{x}{\log x}\log 2 + \mathrm{o}\left(\frac{x}{\log x}\right), \end{aligned}$$

and this concludes the proof of a).

b) In this case we need to be a little more careful with the definition of r. We can assume that $p \geq x^{1-\epsilon(x)}$ where $\epsilon(x)$ is a given function which is $o(\frac{\log\log x}{\log x})$, and therefore we define

$$r = \left[(1-\epsilon(x))\frac{\log x}{\alpha \log\log x}\right]$$

and the rest is as in a).

The last term is

$$M(x,\xi_3) \leq \#\left\{p \leq x \mid |\Gamma'_{r,p}| \leq \frac{x}{\xi_3}\right\} \ll \frac{x}{\xi_3}\left(\frac{x}{\xi_3}\right)^{1/r} r\log r \ll \frac{x}{\xi_3}(\log x)^{1+\alpha/(1-\epsilon(x))},$$

and choosing $\xi_3 = (\log x)^{2+\alpha/(1-\epsilon(x))}\log\log x$, we would make it $o(x/\log x)$. Finally the estimate for the third term is:

$$\begin{aligned} M(x,\xi_2,\xi_3) &\leq \mathrm{li}(x)\left(\log\left(\frac{\log\xi_3}{\log\xi_2}\right) + O((\log\xi_2)^{-1})\right) + O\left(\xi_3 x \exp -c\sqrt{\log x}\right) \\ &\leq \frac{x}{\log x}\log\left(2+\frac{\alpha}{1-\epsilon(x)}\right) + o\left(\frac{x}{\log x}\right) \\ &= \frac{x}{\log x}\log(2+\alpha) + o\left(\frac{x}{\log x}\right) \end{aligned}$$

and this completes the proof.□

Now we turn our attention to another aspect. Note that neither the proof of Theorem 3.1 nor the one of Theorem 3.3 use in any way the fact that each Γ_p is generated by the first $[\log p]$ primes except for the fact that the sum of their logarithms is $\ll \log p \log\log p$ and that $\lim_{r\to\infty}\delta_\Gamma = 1$. The statement remains true if we consider a sequence $a_1, a_2 \ldots$ of multiplicatively independent integers such that for any r,

$$\sum_{i=1}^{r}\log a_i \ll r\log r \text{ and } \lim_{r\to\infty}\delta_\Gamma = 1.$$

It is conceivable to ask if a choice of $a_1,\ldots,a_r$ exists for which we could prove a stronger Theorem. That would amount to having a better estimate for the sum of the logarithms. For this purpose one could set

$$\Upsilon(r) = \min\left\{\sum_{i=0}^{r}\log a_i \mid a_1,\ldots,a_r, \text{ multiplicatively independent } r\text{-tuple}\right\}.$$

The following holds:

Proposition 3.4

$$\Upsilon(r) = r \log r \ + O(r).$$

Proof: For any multiplicatively independent $a_1, \ldots, a_r$, we can assume $a_1 \geq 1, \ldots, a_r \geq r$, therefore

$$\sum_{i=1}^{r} \log a_i \geq \sum_{i=1}^{r} \log i = \log r! = r \log r - r + \mathrm{O}(\log r)$$

the last identity, by the Stirling formula. Thus

$$\Upsilon(r) \geq r \log r \ + \mathrm{O}(r).$$

The choice $a_1 = 2, \ldots, a_r = p_r$, the r^{th} prime, and the Prime Number Theorem, prove that

$$\Upsilon(r) \leq \sum_{i=0}^{r} \log p_r = p_r + \mathrm{O}(p_r \exp -A\sqrt{\log p_r}) = r \log r \ + \mathrm{O}(r \exp -A\sqrt{\log r}).\square$$

Although many of the results that we will state can be extended to any sequence of multiplicatively independent integers, from now on we will only consider the sequence of the prime numbers.

It is now clear that the problem amounts to estimating the number of those primes $p \leq x$ for which $[\mathrm{F}_p^* : \Gamma_r]$ has a prime divisor in the range $(\log^{1-\epsilon_1(x)} x, \log^{2+\epsilon_2(x)} x)$ where $\epsilon_i(x) = \mathrm{o}(1)$. We note that it is enough to restrict our attention to those primes for which the prime divisor is in $(\log x, \log^2 x)$, since by the argument we already used more than once (the Siegel-Walfisz Theorem and the Mertens Formula), that the number of primes p for which $p-1$ has a prime divisor in $(\log^{1-\epsilon_1(x)} x, \log x)$ or in $(\log^2 x, \log^{2+\epsilon_2(x)} x)$ is $\mathrm{o}(\pi(x))$.

We can also assume that $[\mathbf{F}_p^* : \Gamma_r]$ has exactly one prime divisor in $(\log x, \log^2 x)$. Indeed, if p is a prime in the set under consideration for which this is not the case, we would have

$$\exists l_1, l_2. \quad l_1 l_2 \left| [\mathbf{F}_p^* : \Gamma_r] \right| \Longrightarrow |\Gamma_p| \leq \frac{p-1}{l_1 l_2} \leq \frac{x}{\log^2 x}$$

and an application of Lemma 1.4 shows that the number of such primes is $o(\pi(x))$. Finally for the same reason we can assume no divisors of $[\mathbf{F}_p^* : \Gamma_r]$ are $> \log^2 x$.

Putting these remarks together, we have the following

Proposition 3.5 *With the same notation of Theorem 3.3, for almost all primes p up to x either*

$$\mathbf{F}_p^* = \Gamma_r$$

or the index $[\mathbf{F}_p^* : \Gamma_r]$ has exactly one prime divisor in the range $(\log x, \log^2 x)$ and no divisor $> \log^2 x$, i.e.

$$N(x) = \frac{x}{\log x} - A(x) + o\left(\frac{x}{\log x}\right),$$

where

$$A(x) = \left\{ p \leq x \mid \exists! l \in \left(\log x, \log^2 x\right),\ l | [\mathbf{F}_p^* : \Gamma_r],\ \textit{and}\ [\mathbf{F}_p^* : \Gamma_r] \leq \log^2 x \right\}. \square$$

This fact will be used in Section 3.3. We conclude the Section mentioning how this argument can be extended to the case of any $r \to \infty$, in particular the following holds:

Theorem 3.6 *Let r be a function of p that tends to ∞, then for almost all primes p, either $\Gamma_r = \mathbf{F}_p^*$ or*

$$\exists! l,\ l | [\mathbf{F}_p^* : \Gamma_r] \textit{ with } l \in \left(\log p, r p^{1/r} \log p\right), \quad \textit{and } [\mathbf{F}_p^* : \Gamma_r] < r p^{1/r} \log p. \square$$

Corollary 3.7 *Let $\alpha > 0$ be fixed. For almost all primes p either $\mathbf{F}_p^*$ is generated by the classes of the first $\frac{1}{\alpha}\frac{\log p}{\log\log p}$ primes, or*

$$\exists! l,\ l|[\mathbf{F}_p^* : \Gamma_p] \text{ with } l \in \left(\log p, \log^{2+\alpha} p\right), \quad \text{and } [\mathbf{F}_p^* : \Gamma_p] < \log^{2+\alpha} p.\square$$

As we have seen in Proposition 3.5, the problem is now to determine upper bounds for the quantity:

$$A(x) = \left\{p \leq x \mid \exists! l \in \left(\log x, \log^2 x\right),\ l|[\mathbf{F}_p^* : \Gamma_r], \text{ and } [\mathbf{F}_p^* : \Gamma_r] \leq \log^2 x\right\}$$

where we can suppose $r \gg \log x$. We already noticed that the Siegel-Walfisz Theorem and the Merten's Formula, give:

$$A(x) \leq \log 2\frac{x}{\log x} + o\left(\frac{x}{\log x}\right).$$

The idea that allows one to improve this upper bound is coming from the Brun's Sieve, more precisely we will use the following result:

Lemma 3.8 *Let $B_n(x)$ be the number of primes up to x for which $p-1$ is not divisible by any of the primes in the interval $(\log x, \log^n x)$, then we have*

$$B_n(x) \sim \frac{1}{n}\pi(x).$$

Proof: It is an application of the version of the Brun's Sieve that is on Theorem 2.5′ at page 83 of [18] to the set:

$$\mathcal{A} = \{p - 1 \mid p \text{ is primes}, p \leq x\}.$$

Hypothesis (R_0) and $(R_1(k,a))$ are easily satisfied, the latter using the Bombieri-Vinogradov Theorem.□

The application to our problem with the following:

Corollary 3.9 *With the same notation as above, for any r,*

$$A(x) \leq \frac{1}{2}\frac{x}{\log x} + o\left(\frac{x}{\log x}\right).$$

Proof: We have that

$$A(x) \leq \left\{p \leq x \mid \exists l \in \left(\log x, \log^2 x\right),\ l|[\mathbf{F}_p^* : \Gamma_r]\right\} = \pi(x) - B_2(x) \sim \frac{1}{2}\pi(x).\square$$

We conclude with

Theorem 3.10 a) *Let f be a (monotone) function of p with $f(p) \to +\infty$ for $p \to \infty$ and let Γ_p be the subgroup of $\mathbf{F}_p^*$ generated by the classes of the first*

$$f(p)\frac{\log p}{\log\log p}$$

primes, then for at least half of the primes p, we have $\Gamma_p = \mathbf{F}_p^*$.

b) *Let α be a real number with $0 < \alpha$ and let Γ'_p be the subgroup of $\mathbf{F}_p^*$ generated by the classes of the first*

$$\frac{\log p}{\alpha \log\log p}$$

primes, then for a set of primes of density greater than $\frac{1}{2+\alpha}$, it results $\Gamma'_p = \mathbf{F}_p^*$.$\square$

Proof of b): The proof goes as the one in Theorem 3.3, except that to estimate the third term we make use of Lemma 3.8 with $n = 2 + \alpha$.$\square$

3.3 A Density One Result

We will discuss in this section a method to find an estimate for the size of the set

$$H_{m,r}(x) = \left\{ p \leq x \mid |\Gamma_r| = \frac{p-1}{m} \right\}$$

where m is a given integer greater than one and r a function of p that tends to infinity.

The idea is that Γ_r is a subgroup of the cyclic group $\mathbf{F}_p^*$ and therefore is itself cyclic. For any integer m, $m \equiv 1 (\bmod p)$, the subgroup of m-th powers is a subgroup of $\mathbf{F}_p^*$ of order $(p-1)/m$ and since a finite cyclic group has a unique subgroup for every divisor of its order, we deduce that Γ_r is the group of m-th powers mod p. Since a group is made out of m-th powers if and only if it is generated by m-th powers, this implies:

$$H_{m,r}(x) = \{ p \leq x \mid p \equiv 1 (\bmod m) \text{ and } p_i \text{ is an } m\text{-th power } (\bmod p)\ \forall i = 1, \ldots, r \}.$$

If $n_m(p)$ is the least prime which is not congruent to an m-th power $(\bmod p)$, then we can also write:

$$H_{m,r}(x) = \{ p \leq x \mid p \equiv 1 (\bmod m) \text{ and } n_m(p) > p_r \}.$$

As r grows, the possibility that all the p_i's are m-th powers becomes less probable. The idea is to find the minimum r such that $H_{m,r}(x)$ is $o(\frac{1}{m}\pi(x))$. We will do this making use of the large sieve, the proof of which can be found in [6] or [2], that is:

Lemma 3.11 (The Large Sieve)
Let $\mathcal{N}$ be a set of integers contained in the interval $\{1, \ldots, z\}$ and for any prime $p \leq x$, let $\Omega_p = \{h (\bmod p) \mid \forall n \in \mathcal{N}, n \not\equiv h (\bmod p)\}$ and

$$L = \sum_{q \leq x} \mu^2(q) \prod_{p \mid q} \frac{|\Omega_p|}{p - |\Omega_p|},$$

then

$$|\mathcal{N}| \leq \frac{z + 3x^2}{L}. \square$$

In our case, let $\mathcal{N} = \{n \leq z \mid \forall q | n, q < p_r\}$ and note that if $p \in \mathrm{H}_{m,r}(x)$, then

$$\Omega_p \supset \{h(\mathrm{mod}p) \mid h \text{ is not an } m\text{-th power } (\mathrm{mod}p)\}$$

therefore, for such p's, $|\Omega_p| \geq p - 1 - (p-1)/m$ and

$$L \geq \sum_{p \in \mathrm{H}_{m,r}(x)} \frac{|\Omega_p|}{p - |\Omega_p|} \geq \frac{m-1}{2} |\mathrm{H}_{m,r}(x)|.$$

Applying the Large Sieve with $z = x^2$, we get:

Theorem 3.12 *Let* $\Psi(s,t) = \#\{n \leq s \| \ \forall q | n, \ q < t\}$, *then*

$$H_{m,r}(x) \leq \frac{8x^2}{(m-1)\Psi(x^2, p_r)}.\square$$

Estimating the function $\Psi(z,y)$ is a classical problem in Number Theory. In 1985, D. Hensley proved (see [22]) the following:

Lemma 3.13 *Let* $u = \frac{\log z}{\log y}$ *and let* $\rho(u)$ *be the function determined by:*

$$\begin{cases} \rho(u) = 1 & \text{if } \ 0 \leq u \leq 1; \\ u\rho'(u) = -\rho(u-1) & \text{if } \ u > 1, \end{cases}$$

then, for $1 + \log\log z \leq \log y \leq (\log\log z)^2$, *and* $\epsilon > 0$,

$$\Psi(z,y) \gg z\rho(u)\exp(-u\exp(-(\log y)^{(3/5-\epsilon)})).\square$$

In our case, this gives:

Corollary 3.14 *Let* r *be a function of* x *such that* $\log p_r \in [1 + \log\log x^2, (\log\log x^2)^2]$ *and let* $u = 2\log x / \log p_r$, *then*

$$H_{m,r}(x) \ll m^{-1}\frac{1}{\rho(u)}\exp\left(u\exp\left(-u\exp\left(-\log^{(3/5-\epsilon)} p_r\right)\right)\right).\square$$

An asymptotic formula for $\rho(u)$ was found by de Bruijn in [10] and is the following:

Lemma 3.15 *Let $u > 0$. then*

$$\rho(u) = \exp\left\{-u\left(\log u + \log\log u - 1 + \frac{(\log\log u) - 1}{\log u} + O\left(\frac{(\log\log u)^2}{\log^2 u}\right)\right)\right\}.\square$$

In our case we get the following:

Theorem 3.16 *If $p_r \geq \log^2 x$ then*

$$H_{m,r}(x) \ll \frac{1}{m}\,\frac{x}{\exp\left\{\frac{\log x}{2\log\log x}\right\}} = o(\pi(x)).$$

Proof: From Corollary 3.14 and the asymptotic formula of Lemma 3.15, we can write the estimate:

$$H_{m,r}(x) \ll \frac{1}{m}\exp(u(\log u + \log_2 u - 1 + O\left(\frac{\log\log u}{\log u}\right))).$$

where $u = 2\frac{\log x}{\log p_r}$. Now, take $p_r \geq \log^2 x$, and note that

$$u = \tfrac{\log x}{\log_2 x};\quad \log u = \log_2 x - \log_3 x;\quad \log_2 u = \log_3 x + \log\left(1 - \tfrac{\log_3 x}{\log_2 x}\right)$$
$$\text{and}\qquad \log u \asymp \log_2 x;\qquad \log_2 u \leq \log_3 x - \tfrac{\log_3 x}{\log_2 x} \asymp \log_3 x.$$

Therefore

$$mH_{m,r}(x) \ll \exp\left\{\frac{\log x}{\log_2 x}\left(\log_2 x - \log_3 x + (\log_3 x - \frac{\log_3 x}{\log_2 x}) - 1 + O\left(\frac{\log_3 x}{\log_2 x}\right)\right)\right\} \ll$$

$$\exp\left\{\log x\left(1 - \frac{1}{\log_2 x} + O\left(\frac{\log_3 x}{\log_2^2 x}\right)\right)\right\} \ll \frac{x}{\exp\left\{\frac{\log x}{2\log\log x}\right\}} = o(\pi(x)).\square$$

Remark:

The choice of $p_r = \log^2 x$ is not optimal in Theorem 3.16. A simple but long calculation shows that if $p_r = \left(\frac{\log x}{e}\right)^2$, then the asymptotic formula on Lemma 3.15 gives the estimate

$$\frac{1}{\rho(u)} \ll x^{\left(1+O\left(\frac{\log_3^2 x}{\log_2^3 x}\right)\right)},$$

which is useless to our purpose. However, if we fix $\delta < 1$ and set $p_r = \left(\frac{\log x}{e^\delta}\right)^2$, then the same calculation gives

$$\frac{1}{\rho(u)} \ll x^{\left(1-\frac{1-\delta}{\log_2 x}-\frac{1-\delta^2}{\log_2^2 x}+O\left(\frac{\log_3^2 x}{\log_2^3 x}\right)\right)},$$

which is a valid estimate and is the optimal one.

We are now ready to prove:

Theorem 3.17 *Let $\Gamma_r = \langle p_1, \ldots, p_r \rangle$ be the subgroup of $\mathbf{F}_p^*$ generated by all the primes up to $p_r = \log^2 p$ ($r \sim \frac{\log^2 p}{\log\log p}$), then for almost all primes p,*

$$\Gamma_r = \mathbf{F}_p^*$$

Proof: We want to estimate the size of the set

$$S = \left\{p \leq x \mid \left[\mathbf{F}_p^* : \Gamma_r\right] > 1\right\}.$$

The index $\left[\mathbf{F}_p^* : \Gamma_r\right]$ can be at most x since it is a divisor of $p-1$.

Since we may suppose $p > x^{1-\epsilon}$, we can take $p_r = \log^2 p > (1-\epsilon)^2 \log^2 x$ and apply Theorem 3.16. to S,

$$S = \sum_{m=1}^{x} \mathrm{H}_{m,r}(x) = \left(\sum_{m=1}^{x} \frac{1}{m}\right) \frac{x}{\exp\left\{\frac{\log x}{2\log\log x}\right\}} = o(\pi(x)).\square$$

Remarks:

a) This is an improvement with respect to the result of Burgess and Elliot of [5] deduced in Proposition 1.11 where for almost all primes $\leq x$, the size of p_r (least primitive root) was proven to be $\geq \log^2 x (\log\log x)^4$;

b) Improvements to this result using this approach do not stay in the possibility to apply a stronger version of Lemma 3.13 (which exists in the literature, see for example the work of A. Hildebrand in [23] or Canfield, Erdös and Pomerance in [8]). It is the asymptotic formula of De Bruijn for the function $\rho(u)$ that forces a choice p_r of size close to $\log^2 x$.

4 MORE ON PRIMITIVE ROOTS

This Chapter is devoted to the problem of finding a uniform asymptotic formula for the number of primes p up to x such that s distinct numbers (which for simplicity we suppose to be prime) are all at the same time primitive roots (mod$p$). It turns out that, under the assumption of the G.R.H., there is always a positive density of primes with such a property.

Heuristically, the probability that a prime l divides one the indexes $[\mathbf{F}_p^* : \langle p_1 \rangle]$ or $[\mathbf{F}_p^* : \langle p_2 \rangle]$ is the probability that p splits completely in the fields $\mathbf{Q}(\zeta_l, p_1^{1/l})$ and $\mathbf{Q}(\zeta_l, p_2^{1/l})$, minus the probability that p splits completely in the compositum $\mathbf{Q}(\zeta_l, p_1^{1/l}, p_2^{1/l})$. By the Chebotarev density Theorem, we get that the probability that l does not divide both the indexes is

$$1 - \left(\frac{1}{[\mathbf{Q}(\zeta_l, p_1^{1/l}) : \mathbf{Q}]} + \frac{1}{[\mathbf{Q}(\zeta_l, p_2^{1/l}) : \mathbf{Q}]} - \frac{1}{[\mathbf{Q}(\zeta_l, p_1^{1/l}, p_2^{1/l}) : \mathbf{Q}]} \right).$$

Multiplying for all primes l, we get the formula:

$$\delta = \prod_{l \text{ prime}} \left(1 - \frac{2l-1}{l^2(l-1)} \right).$$

A natural generalization of this argument to the case of r distinct primes with the application of an inclusion exclusion principle, yields to:

$$\delta = \prod_{l \text{ prime}} \left(1 - \frac{1}{l-1} \left[1 - \left(1 - \frac{1}{l} \right)^s \right] \right).$$

We will prove that this heuristic argument is correct with the assumption of the Generalized Riemann Hypothesis and some adjustments of the same type of those noticed by Lehmer in the case of the Artin Conjecture for primitive roots. This will be applied in Section 4.3 to the problem of determining the least prime primitive root mod$p$ for almost all primes p.

4.1 Another Generalization of Hooley's Theorem

We present in this section a very natural generalization of Hooley's Theorem for primitive roots.

Theorem 4.1 *Let $\mathcal{P} = \{p_1, \ldots, p_s\}$ be a set of odd primes, $L(d_1, \ldots, d_s)$ be the compositum field:*

$$L(d_1, \ldots, d_s) = \prod_{i=1}^{s} \mathbf{Q}(\zeta_{d_i}, p_i^{1/d_i}),$$

$n_{d_1,\ldots,d_s} = [L(d_1, \ldots, d_s) : \mathbf{Q}]$, *and let*

$$\delta_{\mathcal{P}} = \sum_{d_1=1,\ldots,d_s=1}^{\infty} \frac{\mu(d_1)\cdots\mu(d_s)}{n_{d_1,\ldots,d_s}}.$$

Define

$$N_{\mathcal{P}}(x) = \#\{p \leq x \mid \forall i = 1, \ldots, s \;\; p_i \text{ is a primitive root } \pmod p\}.$$

Then, if the Generalized Riemann Hypothesis holds for the fields $L(d_1, \ldots, d_s)$, we have that

$$N_{\mathcal{P}}(x) = \delta_{\mathcal{P}} \frac{x}{\log x} + O\left(\frac{x \log\log x}{\log^2 x} c_0^s \sum_{i=1}^{s} \log p_i\right)$$

for some absolute constant c_0, uniformly respect to $s = |\mathcal{P}|$ and $p_1, \ldots, p_s$.

Remark: It is not straightforward to see that $\delta_{\mathcal{P}}$ is well defined nor that it is non zero. Indeed, the series defining the density, converges absolutely. We will assume it for the moment and prove it in the next section in Corollary 4.12.

Proof: We will follow the same approach of Hooley who first noticed that in order $p_1, \ldots, p_s$ be all primitive roots for the same prime p, one has to have that

$$\forall l \text{ prime}, \; l \not| [\mathbf{F}_p^* : \langle p_i \rangle]. \forall i = 1, \ldots, s,$$

therefore

$$N_{\mathcal{P}}(x) = N_{\mathcal{P}}(x, y) + M_{\mathcal{P}}(x, y)$$

where

$$N_{\mathcal{P}}(x,y) = \#\left\{p \le x \mid \forall l \text{ prime}, l < y \text{ and } \forall i = 1,\ldots,s \ l \nmid [\mathbf{F}_p^* : \langle p_i \rangle]\right\}$$

and

$$M_{\mathcal{P}}(x,y) = \#\left\{p \le x \mid \exists l \text{ prime}, l > y \text{ with } l|[\mathbf{F}_p^* : \langle p_i \rangle], \text{ for some } i = 1,\ldots,s\right\}.$$

We choose $y = \frac{1}{6s}\log x$ for a reason that will become clear later.

Step 1): $M_{\mathcal{P}}(x,y) \ll \dfrac{x \log\log x}{\log^2 x} s \sum_{i=1}^{s} \log p_i$.

Clearly

$$M_{\mathcal{P}}(x,y) \le \sum_{i=1}^{s} M_{\{p_i\}}(x,y),$$

therefore it is enough to show that, uniformly with respect to $\mathcal{P}$,

$$M_{\{q\}}(x,y) \ll \frac{x \log\log x}{\log^2 x} s \log q.$$

This was proven already by Hooley in his original paper [26], and we will report it here just for completeness.

Note that

$$M_{\{q\}}(x,y) \le |A| + |B| + |C|,$$

where

$$A = \left\{p \in M_{\{q\}}(x,y) |\ \exists l | [\mathbf{F}_p^* : \langle q \rangle], l > x^{1/2}\log x\right\};$$
$$B = \left\{p \in M_{\{q\}}(x,y) |\ \exists l | [\mathbf{F}_p^* : \langle q \rangle], \tfrac{x^{1/2}}{\log^2 x} < l \le x^{1/2}\log x\right\};$$
$$C = \left\{p \in M_{\{q\}}(x,y) |\ \exists l | [\mathbf{F}_p^* : \langle q \rangle], y \le l \le \tfrac{x^{1/2}}{\log^2 x}\right\}.$$

$|A|$ can be estimated as follows:

$l|[\mathbf{F}_p^* : \langle q \rangle]$ implies that

$$q^{\frac{p-1}{l}} \equiv 1 \pmod{p}.$$

Therefore, since $l > x^{1/2}\log x$ and $p \leq x$, any prime in A must divide the positive product

$$\prod_{m \leq x^{1/2}\log^{-1} x} (q^m - 1).$$

Now note that the number of divisors of a natural number N is $O(\log N)$, therefore

$$|A| \ll \sum_{m \leq x^{1/2}\log^{-1} x} m \log q \ll \frac{x}{\log^2 x} \log q.$$

$|B|$ can be estimated as follows:

Retaining only the condition $l|p-1$ for the primes $p \in B$, we get

$$|B| \leq \sum_{\frac{x^{1/2}}{\log^2 x} < l \leq x^{1/2}\log x} \pi(x, l, 1).$$

By the Brun-Titchmarsh Theorem, we know that

$$\pi(x, l, 1) \ll \frac{x}{(l-1)\log(x/l)}.$$

We therefore deduce that

$$|B| \ll \frac{x}{\log x} \sum_{\frac{x^{1/2}}{\log^2 x} < l \leq x^{1/2}\log x} \frac{1}{l} \ll \frac{x}{\log^2 x} \sum_{\frac{x^{1/2}}{\log^2 x} < l \leq x^{1/2}\log x} \frac{\log l}{l},$$

from which it follows from the easier Merten's formula that

$$|B| \ll \frac{x}{\log^2 x}\left(\log\left(x^{1/2}\log x\right) - \log\left(\frac{x^{1/2}}{\log^2 x}\right) + O(1)\right) = O\left(\frac{x \log\log x}{\log^2 x}\right).$$

$|C|$ can be estimated as follows:

We have already noticed that $l|[\mathbf{F}_p^* : \langle q \rangle]$ is equivalent to the statement that p splits completely in the field $\mathbf{Q}(\zeta_l, q^{1/l})$, the version of the Chebotarev Density Theorem that assumes the validity of the Generalized Riemann Hypothesis for such fields is:

$$P(x, l) = \#\{p \leq x \mid p \text{ splits completely in } \mathbf{Q}(\zeta_l, q^{1/l})\} =$$

$$\frac{1}{l(l-1)}\mathrm{li}(x) + O(x^{1/2}\log x \cdot l \cdot q).$$

If we use this formula we get:

$$|C| = \sum_{y \le l \le \frac{x^{1/2}}{\log^2 x}} P(x,l) = \sum_{y \le l \le \frac{x^{1/2}}{\log^2 x}} \left[\frac{1}{l(l-1)}\mathrm{li}(x) + O(x^{1/2}\log x \cdot l \cdot q)\right] =$$

$$O\left(\frac{1}{y}\frac{x}{\log x}\right) + O\left(\frac{x}{\log^2 x}\log q\right).$$

Taking into account that $y = \frac{1}{6s}\log x$, we get

$$|C| = O\left(\frac{x}{\log^2 x} s \log q\right),$$

which is the desired estimate.

Step 2): We can now turn our attention to $N_{\mathcal{P}}(x,y)$. We claim that

$$N_{\mathcal{P}}(x,y) = \sum_{a_1}^{*} \cdots \sum_{a_s}^{*} \mu(a_1)\cdots\mu(a_s) P(x, a_1, \ldots, a_s) \tag{1}$$

where the $*$ over the sums means that the sums are extended to those values of a_i for which all its prime divisors are less than y (note that this implies $a_i < e^{2y} = x^{1/3s}$), and

$$P(x, a_1, \ldots, a_s) = \#\left\{p \le x \mid a_i \left| [\mathbf{F}_p^* : \langle p_i \rangle] \ \ \forall i = 1, \ldots, s\right.\right\}.$$

This claim can be proven by induction on s: If $s = 1$ then we have the standard inclusion-exclusion principle:

$$N_{\{p_1\}}(x,y) = \pi(x) - \sum_{l<y} P(x,l) + \sum_{l<y, l'<y} P(x, ll') - \cdots = \sum_{a_1=1}^{*} \mu(a_1) P(x, a_1).$$

Similarly, for $0 \le t \le s$, define

$$P_t(x, a_{t+1}, \ldots, a_s) = \#\{p \in N_{\{p_1,\ldots,p_t\}}(x,y) \left| a_i \right| [\mathbf{F}_p^* : \langle p_i \rangle] \ \ \forall i = t+1, \ldots, s\}.$$

Clearly

$$P_0(x, a_1, \ldots, a_s) = P(x, a_1, \ldots, a_s)$$

and the recursive relation holds:

$$P_t(x, a_{t+1}, \ldots, a_s) = \sum_{a_t}^{*} \mu(a_t) P_{t-1}(x, a_t, \ldots, a_s).$$

Hence inductively

$$N_{\mathcal{P}}(x, y) = P_s(x) = \sum_{a_s}^{*} \mu(a_s) \ldots \sum_{a_1}^{*} \mu(a_1) P_0(x, a_1, \ldots, a_s).$$

Now note that the condition $a_i \left| [\mathbf{F}_p^* : \langle p_i \rangle] \right.$ is equivalent to

$$p \text{ splits completely in } \mathbf{Q}(\zeta_{a_i}, p_i^{1/a_i}),$$

and that a prime splits completely in a set of fields if and only if it splits completely in their compositum.

Therefore $a_i \left| [\mathbf{F}_p^* : \langle p_i \rangle] \right.$ for all $i = 1, \ldots, s$, if and only if p splits completely in

$$\prod_{i=1}^{s} \mathbf{Q}(\zeta_{a_i}, p_i^{1/a_i}) = \mathbf{Q}(\zeta_{[a_1, \ldots, a_s]}, p_1^{1/a_1}, \ldots, p_s^{1/a_s}).$$

We gather that

$$P(x, a_1, \ldots, a_s) = \# \{ p \leq x \mid p \text{ splits completely in } L(a_1, \ldots, a_s) \}$$

and the Generalized Riemann Hypothesis allows us to write the Chebotarev Density formula:

$$P(x, a_1, \ldots, a_s) = \frac{1}{n_{a_1, \ldots, a_s}} \mathrm{li}(x) + O\left(x^{1/2} \left(\log x + \frac{\log D_{a_1, \ldots, a_s}}{n_{a_1, \ldots, a_s}} \right) \right).$$

where $D_{a_1, \ldots, a_s}$ is the discriminant of $L(a_1, \ldots, a_s)$. Recall that by the Hensel Inequality (See page 259 of [42]) we can write

$$\frac{\log D_{a_1, \ldots, a_s}}{n_{a_1, \ldots, a_s}} \leq \log [a_1, \ldots, a_s] + \sum_{i=1}^{s} \log p_i.$$

since only $p_1, \ldots, p_s$ and the primes dividing $[a_1, \ldots, a_s]$ ramify in $L(a_1, \ldots, a_s)$. Now substitute inside (1) and get:

$$N_{\mathcal{P}}(x,y) = \sum^{*}_{a_1} \cdots \sum^{*}_{a_s} \mu(a_1) \cdots \mu(a_s) \left\{ \frac{\mathrm{li}(x)}{n_{a_1,\ldots,a_s}} + \mathrm{O}\left(x^{1/2} \left(\log x + \frac{\log D_{a_1,\ldots,a_s}}{n_{a_1,\ldots,a_s}} \right) \right) \right\} =$$

$$\delta_{\mathcal{P}} \mathrm{li}(x) + \mathrm{O}\left(\sum_{(a_1,\ldots,a_s)\in S} \frac{\mu^2(a_1)\cdots\mu^2(a_s)}{n_{a_1,\ldots,a_s}} \right) \mathrm{li}(x) +$$

$$\mathrm{O}\left(\sum_{a_1 < e^{2y}, \ldots, a_s < e^{2y}} x^{1/2} \left(\log x + \sum_{i=1}^{s} \log p_1 + \log[a_1, \ldots, a_s] \right) \right) \qquad (2)$$

where S is the set of s-tuples of positive integers where at least one of the component is greater that y. We will prove later in Proposition 4.4 that

$$\sum_{(a_1,\ldots,a_s)\in S} \frac{\mu^2(a_1)\cdots\mu^2(a_s)}{n_{a_1,\ldots,a_s}} \ll \frac{c_1^s}{y},$$

for some absolute constant c_1 . In our case $1/y \ll s/\log x$ therefore (2) is equal to

$$\delta_{\mathcal{P}} \frac{x}{\log x} + \mathrm{O}\left(\frac{x}{\log^2 x} s c_1^s \sum_{i=1}^{s} \log p_i \right) + \mathrm{O}\left(x^{1/2} \sum_{a_1 < e^{2y} \ldots a_s < e^{2y}} \log[a_1, \ldots, a_s] \right).$$

Finally note that if $a_1, \ldots, a_s$ are square-free numbers with prime divisors less than y, then also $[a_1, \ldots, a_s]$ has the same property, thus

$$\sum_{a_1 < e^{2y} \ldots a_s < e^{2y}} \log[a_1, \ldots, a_s] \ll \sum_{a_1 < e^{2y} \ldots a_s < e^{2y}} y \ll y e^{2sy} \ll x^{1/3} \log x$$

Hence

$$N_{\mathcal{P}}(x,y) = \delta_{\mathcal{P}} \frac{x}{\log x} + \mathrm{O}\left(\frac{x}{\log^2 x} c_0^s \sum_{i=1}^{s} \log p_i \right).$$

which, together with step 1) proves the Theorem.□

4.2 Calculation of the Densities

We can now give the expression for the density δ_P, and as we did in Section 1.2, the first step is to calculate the dimension of the fields

$$L = L_{a_1,\ldots,a_s} = \prod_{i=1}^{s} \mathbf{Q}\left(\zeta_{a_i}, p^{1/a_i}\right) = \mathbf{Q}(\zeta_{[a_1,\ldots,a_s]}, p_1^{1/a_1}, \ldots, p_s^{1/a_s}),$$

for any s-tuple $a_1, \ldots, a_s$ of square-free integers. This is done in the following:

Theorem 4.2 *Let $n = n_{a_1,\ldots,a_s} = [L : \mathbf{Q}], M = [a_1, \ldots, a_s]$ and suppose P is the product of those p_i such that $p_i | M$ and a_i is even. Let t be the number of prime factors of P, then*

$$n = \frac{\phi(M) a_1 \cdots a_s}{2^\alpha},$$

with

$$\alpha = \begin{cases} t & \text{if } \forall q | P, q \equiv 1 \pmod 4, \\ t-1 & \text{if } \exists q | P, \text{with } q \equiv 3 \pmod 4. \end{cases}$$

Proof: The argument is similar to the one in the proof of Theorem 1.5. We can suppose, with out loss of generality, that $P = p_1 \cdots p_t$, and define

$$C_0 = \mathbf{Q}(\zeta_M), \qquad C_i = C_{i-1}(p_i^{1/a_i}).$$

Clearly $L = C_s$ and

$$[L : \mathbf{Q}] = [C_s : C_{s-1}] \cdots [C_2 : C_1] \phi(M).$$

Step 1): For $1 \leq i \leq s$, it results $[C_i : C_{i-1}] = a_i$ or $a_i/2$.
Since $x^{a_1} - p_i$ splits into linear factors over C_{i-1}, we have that $[C_i : C_{i-1}] = \frac{a_i}{d}$, if $q | d$ is a prime, then we have the fields:

$$C_{i-1} \subseteq C_{i-1}(p_i^{1/q}) \subseteq C_i.$$

Now, either $q = 1$ or

$$[C_{i-1}(p_i^{1/q}) : C_{i-1}] \,|\, [C_i : C_{i-1}] = \frac{a_i}{d}$$

and since a_i is square-free, we deduce that $p_i^{\frac{1}{q}} \in C_{i-1}$. Either $p_i \in C_0$ which imply $q = 2$ since the only subfields of a cyclotomic field of the type $\mathbf{Q}(p_i^{1/q})$ are quadratic, or $C_0(p_i^{1/q})$ is a Kummer extension of degree q of C_0. Now by Galois Theory, we get that such an extension has to be of the following type:

$$C_0(p_i^{1/q}) = C_0\left((p_{s_1} \cdots p_{s_k})^{1/q}\right),$$

where $1 \leq s_1 \leq s_2 \cdots \leq s_k \leq i-1$ Finally, the Theory of Kummer extensions, (See Lemma 3 at page 160 of Cassels and Fröhlich [7]) implies that there exists $0 \leq i \leq q-1$ such that

$$\left(\frac{p_i}{(p_{s_1} \cdots p_{s_k})^i}\right)^{1/q} \in C_0,$$

which again implies $q = 2$.

Step 2): $[C_i : C_{i-1}] = a_i$ for $t < i \leq s$.

In the case a_i odd then clearly Step 1) implies Step 2), thus suppose a_i is even and $[C_i : C_{i-1}] = a_i/2$. In this case, we have that $\sqrt{p_i}$ is in C_{i-1} because a_i is square-free ($[C_{i-1}(\sqrt{p_i}) : C_{i-1}] \,|\, a_i/2$). This implies that p_i ramifies in C_{i-1}, but since, by the Kummer Theory, the only primes that ramify in C_{i-1} are $p_1, \ldots, p_{i-1}$ and those dividing M, we get a contradiction and conclude that $[C_i : C_{i-1}] = a_i$.

This also implies that $[C_s : C_t] = a_{t+1} \cdots a_s$.

Step 3): If every prime dividing P is $\equiv 1 (\bmod 4)$, then $[C_i : C_{i-1}] = a_i/2$ for every $1 \leq i \leq t$.

From the Theory of Cyclotomic fields we know that a generic quadratic subfield of $C_0 = \mathbf{Q}(\zeta_M)$ is of the following type:

$$\mathbf{Q}\left(\sqrt{\left(\frac{-1}{D}\right) D}\right), \text{ where } D \,|\, M,$$

since $\left(\frac{-1}{q}\right) = 1$ if and only if $q \equiv 1(\mathrm{mod}4)$, we deduce that $\sqrt{q_i} \in C_0$ and the Galois group of C_i over C_{i-1} is generated by the map

$$\sigma : p_i^{1/a_i} \mapsto \zeta_{a_i}^2 p_i^{1/a_i}$$

(note that $\sigma(\sqrt{p_i}) = (\sigma(p_i^{1/a_i}))^{a_i/2} = \sqrt{p_i}$), which has clearly order $a_i/2$.
In this case we have $[C_t : C_0] = a_1 \cdots a_t/2^t$.

Step 4): If it exists $q \mid P$ with $q \equiv 3(\mathrm{mod}\,4)$ (we assume, without loss of generality, that $q = p_1$), then $[C_1 : C_0] = a_1$ and $[C_i : C_{i-1}] = a_i/2$ for every $1 < i \leq t$.
The assumption $[C_1 : C_0] = a_1/2$ would imply again that $\sqrt{p_1} \subset C_0$. By the same argument of Step 3), this implies that the Legendre symbol $\left(\frac{-1}{p_1}\right) = 1$; which is a contradiction. Therefore we are left to show the second part of the statement of this Step.
If $1 < i \leq t$ then $\sqrt{p_i} \in C_1$ because, either $p_i \equiv 1(\mathrm{mod}4)$ and thus $\sqrt{p_i} \in C_0 \subset C_1$, or $p_i \equiv 3(\mathrm{mod}4)$ and $\sqrt{p_1 p_i} \in C_0$ hence $\sqrt{p_i} = \sqrt{p_1 p_i}/\sqrt{p_1} \in C_1$. In both cases, the Galois group of C_i over C_{i-1} is generated by the map

$$\sigma : p_i^{1/a_i} \mapsto \zeta_{a_i}^2 p_i^{1/a_i}$$

which again has order $a_i/2$.
Finally, in this case we have $[C_t : C_0] = a_1 \cdots a_t/2^{t-1}$ and this concludes the proof.□

Corollary 4.3 *We have the following lower bound for the dimension $n_{a_1,\ldots,a_s}$ of the field $L_{a_1,\ldots,a_s}$ over* **Q**:

$$n_{a_1,\ldots,a_s} \geq \frac{\phi([a_1,\ldots,a_s])a_1 \cdots a_s}{2^s}.\square$$

We have now enough tools to prove the property we used during the proof of Theorem 4.1.

Proposition 4.4 *Recall that* $\mathcal{S} = \{(a_1, \ldots, a_s) \in \mathbb{N}^s \mid \exists i \text{ with } a_i > y\}$. *It results that*

$$\sum_{(a_1,\ldots,a_s)\in\mathcal{S}} \frac{\mu^2(a_1)\cdots\mu^2(a_s)}{n_{a_1,\ldots,a_s}} \ll \frac{c_1^s}{y} \tag{3}$$

for some absolute constant c_1.

Before proving Proposition 4.4, we need the following technical Lemma:

Lemma 4.5 *Consider the multiplicative function* $d_t(n)$ *defined as the number of ways to write* n *as product of* t *natural numbers, and denote:*

$$\sigma(t) = \prod_{l \text{ prime}} \left(1 + \frac{1}{l}\sum_{k\geq 1} \frac{d_t(l^k)}{l^k}\right).$$

we have:

$$\sigma(t) \leq \zeta(2)^{2t}.$$

Proof: Note that $d_t(l^{2k-1}) \leq d_t(l^{2k})$, therefore

$$1 + \frac{1}{l}\left(\frac{d_t(l)}{l} + \frac{d_t(l^2)}{l^2} + \cdots\right) \leq 1 + 2\left(\frac{d_t(l^2)}{l^2} + \frac{d_t(l^4)}{l^4} + \cdots\right)$$

$$\leq \left(1 + \frac{d_t(l^2)}{l^2} + \frac{d_t(l^4)}{l^4} + \cdots\right)^2 = \left(1 + \frac{1}{l^2} + \frac{1}{l^4} + \cdots\right)^{2t}.$$

Hence

$$\sigma(t) \leq \prod_{l \text{ prime}} \left(1 + \frac{1}{l^2} + \frac{1}{l^4} + \cdots\right)^{2t} = \zeta(2)^{2t}.\square$$

Proof of Proposition 4.4: First note that from Corollary 4.3, we get that

$$n_{a_1,\ldots,a_s} \geq \frac{\phi([a_1, \ldots, a_s])a_1 \cdots a_s}{2^s},$$

therefore (3) is

$$\ll 2^s \sum_{\mathcal{S}} \frac{\mu^2(a_1)\cdots\mu^2(a_s)}{a_1 \cdots a_s \phi([a_1, \ldots, a_s])}, \tag{4}$$

But the sum on (4) is completely symmetric on the a_i's, therefore is

$$\ll 2^s s \sum_{\substack{a_1>y \\ (a_2,\dots,a_s)\in\mathbb{N}^{s-1}}} \frac{\mu^2(a_1)\cdots\mu^2(a_s)}{a_1\cdots a_s \phi([a_1,\dots,a_s])}$$

$$\ll 2^s s \sum_{a_1>y} \frac{\mu^2(a)}{a} \sum_{(a_2,\dots,a_s)\in\mathbb{N}^{s-1}} \frac{1}{a_2\cdots a_s \phi([a_2,\dots,a_s])}. \tag{5}$$

Using the multiplicative function defined above and the function γ defined as

$$\gamma(n) = \prod_{p|n} p.$$

we can write that (5) is equal to:

$$2^s s \sum_{a>y} \frac{\mu^2(a)}{a} \sum_{b=1}^{\infty} \frac{d_{s-1}(b)}{\phi(\gamma(ab))} = 2^s s \sum_{a>y} \frac{\mu^2(a)}{\phi(a)a} \sum_{b=1}^{\infty} \frac{d_{s-1}(b)\phi((a,b))}{\phi(\gamma(b))}.$$

Since all functions inside the second sum are multiplicative, we can write (5) as

$$2^s s \sum_{a>y} \frac{\mu^2(a)}{\phi(a)a} \prod_{l \text{ prime}} \left\{ 1 + \frac{\phi((a,l))}{\phi(l)} \left(\frac{d_{s-1}(l)}{l} + \frac{d_{s-1}(l^2)}{l^2} + \cdots \right) \right\} \ll$$

$$2^s s\sigma(s-1) \sum_{a>y} \frac{\mu^2(a)}{\phi(a)a} \left(\prod_{l|a} \sum_{k\geq 0} \frac{d_{s-1}(l^k)}{l^k} \right).$$

If we can prove the estimate:

$$\sum_{a>y} \frac{f(a)}{a^2} \ll \frac{\sigma(s-1)}{y} \tag{6}$$

where

$$f(a) = \frac{a\mu^2(a)}{\phi(a)} \prod_{l|a} \sum_{k\geq 0} \frac{d_{s-1}(l^k)}{l^k} = \mu^2(a) \left(\frac{a}{\phi(a)} \right)^s,$$

then the estimate for the function $\sigma(t)$ of Lemma 4.5 would imply the claim.

From the Theory of Dirichlet series, we know that (6) is

$$\ll \int_y^{\infty} \frac{F(x)}{x^3} dx,$$

where $F(x) = \sum_{n \leq x} f(n)$ is the average of f. If we could prove the asymptotic formula:

$$F(x) \sim \sigma(s-1)x, \tag{7}$$

for x that tends to infinity, then we would have that (6) is

$$\ll \int_y^{\infty} \frac{\sigma(s-1)x}{x^3} dx = \frac{\sigma(s-1)}{y}.$$

To prove (7), we make use of the Dirichlet series:

$$H(z) = \sum_{n=1}^{\infty} \frac{f(n)}{n^z}. \tag{8}$$

Since $f(n) \ll (\log\log n)^s$, we know that $H(z)$ converges in the semi-plane $\Re(z) > 1$ and we can write the Euler product expansion:

$$H(z) = \prod_l \left(1 + \frac{1}{l^z} \frac{l}{l-1} \sum_{k \geq 0} \frac{d_{s-1}}{l^k}\right) = \zeta(z)K(z)$$

where

$$K(z) = \prod_l \left(1 + \frac{1}{l^z} \frac{l}{l-1} \sum_{k \geq 0} \frac{d_{s-1}}{l^k}\right)\left(1 - \frac{1}{l^z}\right)$$

converges for $\Re(z) > 0$. This decomposition gives an analytic continuation for $H(z)$ and therefore we can calculate the residue at $z = 1$ of $H(z)$ which is going to be

$$\lim_{z \to 1}(z-1)\zeta(z)K(z) = K(1) = \prod_l \left(1 - \frac{1}{l} + \frac{1}{l}\left(1 + \sum_{k \geq 1} \frac{d_{s-1}(l^k)}{l^k}\right)\right) = \sigma(s-1).$$

The Ikehara Tauberian Theorem (see [33], page 311) implies the claim of (7) and the Proposition results proven.□

Remark: The details used in the last part of the proof of Proposition 4.4 are missing from the original proof of Hooley in the case $s = 1$. In that circumstance the level of precision that we need here for the application on Section 4.3 was not required.

If $n_{d_1,\dots,d_s}$ is the dimension over $\mathbf{Q}$ of $\prod_{i=1}^{s} \mathbf{Q}(\zeta_{d_i}, p_i^{1/d_i})$ then we have seen that whenever $([d_1,\dots,d_s], p_1\cdots p_s) = 1$, it results

$$n_{d_1,\dots,d_s} = d_1\cdots d_s \phi([d_1,\dots,d_s]),$$

this leads us to consider the function:

$$\Delta_s = \sum_{a_1=1}^{\infty}\cdots\sum_{a_s=1}^{\infty} \frac{\mu(a_1)\cdots\mu(a_s)}{a_1\cdots a_s \phi([a_1,\dots,a_s])}.$$

Our goal is to show that $\Delta_s \neq 0$ and that $\lim_{s\to\infty}\Delta_s = 0$, the best way to do this is again to express Δ_s as an Euler product. This will also confirm the heuristic argument illustrated at the beginning of this Chapter.

Proposition 4.6

$$\Delta_s = \prod_{l \text{ prime}} \left(1 - \frac{1}{l-1}\left[1 - \left(1-\frac{1}{l}\right)^s\right]\right).$$

We need two lemmas:

Lemma 4.7 *For any prime l, let it be given a function α_l, and define*

$$\Gamma_{t+1}(\alpha_l) = \sum_{a_1=1}^{\infty}\cdots\sum_{a_{t+1}=1}^{\infty}\left(\frac{\mu(a_1)\dots\mu(a_{t+1})}{a_1\cdots a_{t+1}} \prod_{l\mid[a_1,\dots,a_{t+1}])}\alpha_l\right), \tag{9}$$

(note that $\Gamma_s(1/(l-1)) = \Delta_s$) then:

$$\Gamma_{t+1}(\alpha_l) = \Gamma_t\left(\alpha_l\frac{l-1}{l-\alpha_l}\right)\prod_{q \text{ prime}}\left(1-\frac{\alpha_q}{q}\right).$$

Proof: The right hand side of (9) is equal to:

$$\sum_{a_1=1}^{\infty}\cdots\sum_{a_t=1}^{\infty}\left(\frac{\mu(a_1)\dots\mu(a_t)}{a_1\cdots a_t}\prod_{l\mid[a_1,\dots,a_t])}\alpha_l\right)\left(\sum_{x=1}^{\infty}\frac{\mu(x)}{x}\prod_{l\left|\frac{[a_1,\dots,a_t,x]}{[a_1,\dots,a_t]}\right.}\alpha_l\right), \tag{10}$$

where we just renamed a_{t+1} to be x. Note that for any multiplicative function $f(n)$ and $H \in \mathbb{N}$, if we define

$$F(n) = \mu(n) f([H,n]/H),$$

then $F(n)$ is again multiplicative. If we take $H = [a_1, \ldots, a_t]$ and $f(n) = \prod_{l|n} \alpha_l$, we get that (10) is equal to

$$\sum_{a_1=1}^{\infty} \cdots \sum_{a_t=1}^{\infty} \left(\frac{\mu(a_1) \cdots \mu(a_t)}{a_1 \cdots a_t} \prod_{l|[a_1,\ldots,a_t]} \alpha_l \right) \prod_{q \text{ prime}} \left(1 - \frac{1}{q} \left(\prod_{l \left| \frac{[a_1,\ldots,a_t,q]}{[a_1,\ldots,a_t]} \right.} \alpha_l \right) \right). \qquad (11)$$

Since $l \left| \frac{[H,q]}{H} \right.$ if and only if $l = q$ and $q \not| H$, we gather that (11) is equal to:

$$\sum_{a_1=1}^{\infty} \cdots \sum_{a_t=1}^{\infty} \left(\frac{\mu(a_1) \cdots \mu(a_t)}{a_1 \cdots a_t} \prod_{l|[a_1,\ldots,a_t]} \alpha_l \right) \prod_{l|[a_1,\ldots,a_t]} \left(1 - \frac{1}{l} \right) \prod_{\substack{q \text{ prime} \\ q|[a_1,\ldots,a_t]}} \left(1 - \frac{\alpha_q}{q} \right).$$

Multiplying and dividing by the missing terms, we get the claim.□

Lemma 4.8 *Define inductively the functions $\beta_i = \beta_i(l)$ in the following :*

$$\beta_1 = \frac{1}{l-1} \quad \textit{and} \quad \beta_n = \beta_{n-1} \frac{l-1}{l - \beta_{n-1}},$$

then:

$$\Delta_s = \prod_{l \text{ prime}} \prod_{n=1}^{s} \left(1 - \frac{\beta_n(l)}{l} \right).$$

Proof: By induction on s, the case $s = 1$ being the definition of the Artin constant. Lemma 4.7 implies that:

$$\Delta_s = \Gamma_s(\beta_1) = \Gamma_{s-1}(\beta_2) \prod_{l \text{ prime}} \left(1 - \frac{\beta_1(l)}{l} \right) =$$

$$\Gamma_{s-2}(\beta_3) \prod_{l \text{ prime}} \left(1 - \frac{\beta_1(l)}{l} \right) \left(1 - \frac{\beta_2(l)}{l} \right) =$$

$$\vdots$$

$$\Gamma_1(\beta_s) \prod_{l \text{ prime}} \left[\prod_{i=1}^{s-1} \left(1 - \frac{\beta_i(l)}{l} \right) \right].$$

Finally

$$\Gamma_1(\beta_s) = \sum_{a=1}^{\infty} \frac{\mu(a)}{a} \prod_{l|a} \beta_s(l) = \prod_{l \text{ prime}} \left(1 - \frac{\beta_s(l)}{l}\right),$$

and the claim follows.□

First Proof of Proposition 4.6: Note that by the inductive definition of the β_i's, we have that

$$\left(1 - \frac{\beta_i(l)}{l}\right)\left(1 - \frac{\beta_{i+1}(l)}{l}\right) = \left(1 - \beta_i(l)\left(1 - \left(1 - \frac{1}{l}\right)^2\right)\right)$$

and, more in general

$$\left(1 - \frac{\beta_i(l)}{l}\right)\left(1 - \beta_{i+1}(l)\left(1 - \left(1 - \frac{1}{l}\right)^k\right)\right) = \left(1 - \beta_i(l)\left(1 - \left(1 - \frac{1}{l}\right)^{k+1}\right)\right).$$

Finally

$$\Delta_s = \prod_{l \text{ prime}} \left[\left(1 - \frac{\beta_1(l)}{l}\right) \cdots \left(1 - \frac{\beta_{s-1}(l)}{l}\right)\left(1 - \frac{\beta_s(l)}{l}\right)\right] =$$

$$\prod_{l \text{ prime}} \left[\left(1 - \frac{\beta_1(l)}{l}\right) \cdots \left(1 - \frac{\beta_{s-2}(l)}{l}\right)\left(1 - \beta_{s-1}(l)\left(1 - \left(1 - \frac{1}{l}\right)^2\right)\right)\right]$$

$$\vdots$$

$$\prod_{l \text{ prime}} \left[\left(1 - \frac{\beta_1(l)}{l}\right)\left(1 - \beta_2(l)\left(1 - \left(1 - \frac{1}{l}\right)^{s-1}\right)\right)\right].$$

Substitute $\beta_1(l) = 1/(l-1)$, and get the claim.□

Second Proof of Proposition 4.6: If we define

$$f(m) = \sum_{\substack{a_1,\ldots,a_s \\ [a_1,\ldots,a_s]=m}} \frac{\mu(a_1)\cdots\mu(a_s)}{a_1 \cdots a_s},$$

then it results

$$\Delta_s = \sum_{m=1}^{\infty} \frac{\mu^2(m) f(m)}{\varphi(m)}$$

since the lowest common multiple of square-free integers is itself square-free.

We now claim that $f(m)$ is multiplicative, which imply:

$$\Delta_s = \prod_{l \text{ prime}} \left(1 + \frac{f(l)}{l-1}\right). \tag{12}$$

Indeed, if m and m' are coprime integers, then the map

$$(a_1,\ldots,a_s),(b_1,\ldots,b_s)\longmapsto(a_1b_1,\ldots,a_sb_s)$$

is a bijection from the set of s-tuples of integers with lowest common multiple m cross the set of r-tuples of integers with lowest common multiple m' to the set of s-tuples of integers with lowest common multiple mm', whose inverse map is given by:

$$(c_1,\ldots,c_s)\longmapsto((c_1,m),\ldots,(c_s,m)),((c_1,m'),\ldots,(c_s,m')).$$

We gather that

$$f(m)f(m')=\sum_{\substack{a_1,\ldots,a_s\\[a_1,\ldots,a_s]=m}}\sum_{\substack{b_1,\ldots,b_s\\[b_1,\ldots,b_s]=m'}}\frac{\mu(a_1b_1)\cdots\mu(a_sb_s)}{a_1b_1\cdots a_sb_s}=$$

$$\sum_{\substack{c_1,\ldots,c_s\\[c_1,\ldots,c_s]=mm'}}\frac{\mu(c_1)\cdots\mu(c_s)}{c_1\cdots c_s}=f(mm').$$

Finally, if $[a_1,\ldots,a_s]=p$, then each a_i can be equal to 1 or to p, and each possibility is possible except $a_i=1\forall i=1,\ldots,s$. Hence

$$f(p)=s\frac{-1}{p}+\binom{s}{2}\frac{1}{p^2}+\cdots+\binom{s}{k}\frac{(-1)^k}{p^k}+\cdots+\frac{(-1)^s}{p^s}=\left(1-\frac{1}{p}\right)^s-1.$$

Substitute in (12) and get the claim.□

Corollary 4.9 *With the same notation of Theorem 4.1, we have that:*

$$\Delta_s=O\left(2^{-s}\frac{1}{\log s}\right).$$

Proof: For any fixed $N>0$, we have that:

$$2^s\Delta_s\le\prod_{\substack{l<N\\l\neq2}}\left(1-\frac{f(l)}{l-1}\right)$$

where $f(l) = \left(1 - \left(1 - \frac{1}{l}\right)^s\right)$. Note that in such a range for l it results

$$f(l) \geq \left(1 - \left(1 - \frac{1}{N}\right)^s\right) \sim 1 - e^{-\frac{s}{N}},$$

as N tends to infinity. Hence

$$2^s \Delta_s \leq \exp\left\{\sum_{\substack{l<N \\ l\neq 2}} \log\left(1 - \frac{f(N)}{l-1}\right)\right\} \ll \exp - \left\{\sum_{\substack{l<N \\ l\neq 2}} \left(\frac{1}{l-1}\right) f(N)\right\} \ll$$

$$\exp - \left\{(\log\log N)(1 - e^{-\frac{s}{N}})\right\}.$$

Now take $N = s/\log s$ and get

$$2^s \Delta_s \ll \frac{1}{\log s} \exp\left(\log\log(s/\log s) s^{-1}\right) \ll \frac{1}{\log s}. \square$$

Theorem 4.10 *Let $\mathcal{P} = \{p_1, \ldots, p_s\}$ be a set of odd primes, suppose $\tilde{\mathcal{P}}$ is the subset of $\mathcal{P}$ of those primes congruent to $1 (\mathrm{mod}\, 4)$. With the same notation of Theorem 4.2 and Proposition 4.6, it results*

$$\delta_{\mathcal{P}} = \sum_{a_1=1}^{\infty} \cdots \sum_{a_s=1}^{\infty} \frac{\mu(a_1)\cdots\mu(a_s)}{n_{a_1,\ldots,a_s}} = \frac{1}{2}\Delta_s \left\{\prod_{p\in\mathcal{P}} \frac{1}{1+\alpha_p} + \prod_{p\in\tilde{\mathcal{P}}} \frac{1 + \alpha_p - \left(\frac{-1}{p}\right)\alpha_p}{1+\alpha_p}\right\},$$

where $\alpha_p = \frac{1}{p-1}\left(\left(1 - \frac{1}{p}\right)^s - 1\right)$.

Proof: To make the notation lighter, we will indicate the s-tuple $(a_1, \ldots, a_s)$ by $\underline{a}$, the product $a_1 \cdots a_s$ by $\overline{a}$ and $\mu(a_1)\cdots\mu(a_s)$ by $\mu(\underline{a})$. We also say that $\underline{a}$ is odd if all its components are odd.

Furthermore, for any subset I of $[s] \stackrel{def}{=} \{1, \ldots s\}$, we denote by P_I the product of elements in I and by $\tilde{I}$ the subset of I of those i's for which $p_i \equiv 1 (\mathrm{mod}\, 4)$. Now call $[a]^I$ the set of s-tuples of integers for which a_i is even for all $i \in I$ and a_i is odd for all $i \notin I$. It is clear that $\{[a]^I\}_{I\in[s]}$ is a partition of $\mathbb{N}^s$, therefore

$$\delta_{\mathcal{P}} = \sum_{\underline{a}} \frac{\mu(\underline{a})}{n_{\underline{a}}} = \sum_{I\subseteq[s]} \sum_{\underline{a}\in[a]^I} \frac{\mu(\underline{a})}{n_{\underline{a}}} = \sum_{I\subseteq[s]} \frac{(-1)^{|I|}}{2^{|I|}} \sum_{\underline{a}\ \mathrm{odd}} \frac{2^{3I}\mu(\underline{a})}{\overline{a}\phi([\underline{a}])}$$

where, if $Q = (P_I, [\underline{a}])$,

$$\beta_I = \begin{cases} \nu(Q) & \text{if } Q \,|\, P_{\bar{I}} \\ \nu(Q) - 1 & \text{otherwise} \end{cases}$$

the possibility $Q = 1$ belonging to the first case. We gather that

$$\sum_{\underline{a} \text{ odd}} \frac{2^\beta \mu(\underline{a})}{\overline{a}\phi([\underline{a}])} = \sum_{J \subseteq I} \sum_{\substack{\underline{a} \text{ odd} \\ P_J = (P_I, [\underline{a}])}} \frac{2^\beta \mu(\underline{a})}{\overline{a}\phi([\underline{a}])} = \sum_{J \subseteq \bar{I}} 2^{\nu(P_J)} \sum_{\substack{\underline{a} \text{ odd} \\ P_J = (P_I, [\underline{a}])}} \frac{\mu(\underline{a})}{\overline{a}\phi([\underline{a}])} + \sum_{\substack{J \not\subseteq \bar{I} \\ J \subseteq I}} 2^{\nu(P_J)-1} \sum_{\substack{\underline{a} \text{ odd} \\ P_J = (P_I, [\underline{a}])}} \frac{\mu(\underline{a})}{\overline{a}\phi([\underline{a}])}$$

$$= \frac{1}{2} \left\{ \sum_{J \subseteq \bar{I}} 2^{\nu(P_J)} \sum_{\substack{\underline{a} \text{ odd} \\ P_J = (P_I, [\underline{a}])}} \frac{\mu(\underline{a})}{\overline{a}\phi([\underline{a}])} + \sum_{J \subseteq I} 2^{\nu(P_J)} \sum_{\substack{\underline{a} \text{ odd} \\ P_J = (P_I, [\underline{a}])}} \frac{\mu(\underline{a})}{\overline{a}\phi([\underline{a}])} \right\}.$$

Now note that for $J \subseteq I$, the condition $P_J = (P_I, [\underline{a}])$ is equivalent to $P_J | [\underline{a}]$ and $([\underline{a}], P_{I-J}) = 1$. As we did during the second proof of Proposition 4.6, we can write

$$\sum_{\substack{\underline{a} \text{ odd} \\ P_J = (P_I, [\underline{a}])}} \frac{\mu(\underline{a})}{\overline{a}\phi([\underline{a}])} = \sum_{\substack{m=1 \\ m \text{ odd}, P_J | m, (m, P_{I-J})=1}}^{\infty} \frac{\mu^2(m)}{\phi(m)} \sum_{\substack{\underline{a} \text{ odd} \\ [\underline{a}]=m}} \frac{\mu(\underline{a})}{\overline{a}}, \tag{13}$$

again the function inside is multiplicative, thus we can write that (13) is equal to

$$\sum_{\substack{m=1 \\ m \text{ odd}, P_J | m, (m, P_{I-J})=1}}^{\infty} \frac{\mu^2(m)}{\phi(m)} \prod_{l|m} \left[\left(1 - \frac{1}{l}\right)^s - 1 \right]$$

$$= \frac{1}{\phi(P_J)} \prod_{l|P_J} \left[\left(1 - \frac{1}{l}\right)^s - 1 \right] \sum_{\substack{m=1 \\ m \text{ odd}, (P_I, m)=1}}^{\infty} \frac{\mu^2(m)}{\phi(m)} \prod_{l|m} \left[\left(1 - \frac{1}{l}\right)^s - 1 \right] =$$

$$2^s \Delta_s \prod_{p|P_J} \alpha_p \prod_{p|P_I} \frac{1}{1+\alpha_p}.$$

Putting everything together,

$$\delta_P = 2^s \Delta_s \sum_{I \subseteq [s]} \frac{(-1)^{|I|}}{2^{|I|+1}} \left\{ \sum_{J \subseteq I} 2^J \prod_{p|P_J} \alpha_p \prod_{p|P_I} \frac{1}{1+\alpha_p} + \sum_{J \subseteq \bar{I}} 2^J \prod_{p|P_J} \alpha_p \prod_{p|P_I} \frac{1}{1+\alpha_p} \right\}.$$

Finally

$$\sum_{I \subseteq [s]} \frac{(-1)^{|I|}}{2^{|I|}} \sum_{J \subseteq I} 2^J \prod_{p|P_J} \alpha_p \prod_{p|P_I} \frac{1}{1+\alpha_p} = \sum_{I \subseteq [s]} \frac{(-1)^{|I|}}{2^{|I|}} \prod_{p|P_I} \frac{1+2\alpha_p}{1+\alpha_p} = \frac{1}{2^s} \prod_{i=1}^{s} \frac{1}{1+\alpha_{p_i}}$$

and similarly

$$\sum_{I\subseteq[s]}\frac{(-1)^{|I|}}{2^{|I|}}\sum_{J\subseteq\bar{I}}2^{J}\prod_{p|P_J}\alpha_p\prod_{p|P_I}\frac{1}{1+\alpha_p}=\sum_{I\subseteq[s]}\frac{(-1)^{|I|}}{2^{|I|}}\prod_{p|P_I}(1+2\alpha_p)\prod_{p|P_I}\frac{1}{1+\alpha_p}=$$

$$\frac{1}{2^s}\prod_{\substack{i=1\\ p_i\equiv 1 \bmod 4}}^{s}\frac{1}{1+\alpha_p}\prod_{\substack{i=1\\ p_i\equiv 3 \bmod 4}}^{s}\left(2-\frac{1}{1+\alpha_p}\right)=\prod_{i=1}^{s}\left(1-\left(\frac{-1}{p}\right)\frac{\alpha_p}{1+\alpha_p}\right)$$

therefore the claim.□

We conclude this Section with two Corollaries:

Corollary 4.11 *Under tha same assumptions of Theorem 4.1, if every prime in $\mathcal{P}$ is congruent to* $1 \pmod 4$ *then the density of primes for which all elements of $\mathcal{P}$ are primitive roots, is*

$$\prod_{l\notin\mathcal{P}}(1+\alpha_l).\square$$

Corollary 4.12 *For any set of odd primes $\mathcal{P}$, $\delta_{\mathcal{P}}$ is a well defined number.*□

4.3 An Application to the Least Prime Primitive Root

In this last section we apply Theorem 4.1 to the classical problem of the study of the function $G(p)$ defined as the least prime primitive root $(\mathrm{mod} p)$. More precisely, by the use of the inclusion exclusion principle, we determine a uniform asymptotic formula for the number of primes $p \leq x$ such that $G(p) < r$.

Theorem 4.13 *With the same notation and hypothesis of Theorem 4.1, let q_n be the n-th odd prime,*

$$\mathcal{T}_r(x) = \#\{p \leq x \mid \exists i \leq r \mid q_i \text{ is a prime primitive root } \pmod p\},,$$

and

$$\hat{\delta}_r = \sum_{\mathcal{P} \subseteq \{p_1, \ldots, p_r\}} (-1)^{|\mathcal{P}|} \delta_{\mathcal{P}}$$

($\delta_\emptyset = 1$). We have that

$$\mathcal{T}_r(x) = (1 - \hat{\delta}_r)\frac{x}{\log x} + O\left(\frac{x \log\log x}{\log^2 x} C_2^r\right)$$

for some absolute constant C_2, uniformly respect to r.

Proof: Let $\mathcal{S}_r$ be the number of primes p up to x such that none of the first r primes is a primitive root $\mathrm{mod} p$.

As a straightforward application of the inclusion exclusion principle, we get that

$$\mathcal{S}_r = \sum_{\mathcal{P} \subseteq \{p_1, \ldots, p_r\}} (-1)^{|\mathcal{P}|} N_{\mathcal{P}}(x)$$

where as in Theorem 4.1,

$$N_{\mathcal{P}} = \#\{p \leq x \mid \forall q \in \mathcal{P}, q \text{ is a primitive root } (\mathrm{mod} q)\}$$

and $N_\emptyset(x) = \pi(x)$.

Applying Theorem 4.1, we get for a suitable positive constant c_0,

$$\mathcal{S}_r = \sum_{\mathcal{P}\subseteq\{p_1,\dots,p_r\}} (-1)^{|\mathcal{P}|}\left(\delta_{\mathcal{P}}\frac{x}{\log x} + O\left(\frac{x\log\log x}{\log^2 x}c_0^{|\mathcal{P}|}\right)\right) =$$

$$\hat{\delta}_r\frac{x}{\log x} + O\left(\frac{x\log\log x}{\log^2 x}C^r\right)$$

where we have taken $C = 2c_0$, say. Finally, noticing that $\mathcal{T}_r = \pi(x) - \mathcal{S}_r$, we get the claim.□

Corollary 4.14 *Let $f(x)$ be any monotone function of x that tends to infinity. Suppose also that $f(x) = o(\log\log x)$, then, if the generalized Riemann Hypothesis holds, we have that $G(p) \le f(x)$ for all primes with the exception of a set of primes of size*

$$\hat{\delta}_{f(x)}\frac{x}{\log x} + O\left(\frac{x\log\log x}{\log^2 x}C_2^{f(x)}\right).$$

Proof: It is enough to notice that by the assumption made on f, the error term is $o(\pi(x))$.□

The problem now amounts to estimating the behaviour of the function $\hat{\delta}_r$. Computer calculations suggest that $\hat{\delta}_r = O\left(\frac{1}{\log r}\right)$, but we do not hazard in any precise claim.

We are not even able to present a direct proof of the fact that

$$\lim_{r\to\infty}\hat{\delta}_r = 0,$$

which, of course would imply that $G(p) < f(p)$ for almost all p ($f \to \infty$), under the Riemann Hypothesis.

The latter assertion has been proven by L. Murata in [38] and is equivalent, under the Riemann Hypothesis, to $\hat{\delta}_r = o(1)$.

Upper and Lower estimates for $\hat{\delta}_r$ would allow to determine (under the Riemann Hypothesis) $\Omega_{\pm}$-type of estimates for the size of set of primes p for which $G(p) \prec f(p)$.

We do feel that such a problem is not too difficult and we are planning to address these questions in the near future.

Finally we would like to mention that in principle this approach could be extened to the analogous problem for the function $g(p)$, the least primitive root $(\mathrm{mod} p)$. We found out just recently that a general form of Theorem 4.1 has been found by K. R. Matthews in [36]. The asymptotic formula found by Matthews is not uniform and provides a weeker error term than Theorem 4.1, however the proof can be adjusted to yield to an analogous result of Corollary 4.14 for $g(p)$. The expression for the density in this case would be much more complicated and even computer calculations seem at the moment very hard to perform.

APPENDIX A: ON DIVISORS OF $p-1$

We recall that Lemma 1.4 states that for any given sequence of multiplicatively independent integers, the number of primes for which the group generated by the first r elements of the sequence is smaller than t is

$$O\left(t^{1+1/r} r \log r\right),$$

uniformly with respect to r.

(Note that we are using the statement of Proposition 3.4 according to which the sum of the logarithms of the first r elements of a sequence of multiplicatively independent numbers in asymptotic to $r \log r$). A consequence of this is that, if r is fixed, then for almost all primes,

$$|\Gamma_r| \geq \frac{p^{\frac{r}{r+1}}}{\log p}.$$

Indeed, if we take $t = x^{r/(r+1)}/\log x$, in Lemma 1.4, we get that the number of primes for which $|\Gamma_r| < p^{r/(r+1)}/\log p \leq t$ is $O(\pi(x)/\log^{1/r} x)$, therefore for almost all primes we have the desired inequality. It is natural to ask what would be an estimate of $|\Gamma_r|$ uniform respect to r? Using the same method of the fixed r case, we get that, if $f(p)$ is any divergent function, then

$$|\Gamma_r| \geq \left(\frac{p}{f(p)\log p\, r \log r}\right)^{\frac{r}{r+1}}$$

for almost all primes, uniformly respect to r. We need of course to ensure certain growing conditions to be met.

The goal of this section is to improve the preceding results making use of the following:

Theorem A. 1 *It exist, β and δ positive such that, for all $h \in [\log^{-\beta} x, 1 - \log^{-\beta} x]$, and $y = x^h$, one has uniformly on h:*

$$\#\left\{p \leq x \mid \exists u | p-1, \text{ with } u \in [y, y \exp \log^{\delta} x]\right\} = o\left(\frac{x}{\log x}\right)$$

where the constant implied by the o symbol is absolute.

Before starting the proof of the Theorem we need some preliminary lemmas:

Lemma A. 2 (Erdös) *Let $\Omega(n)$ be the number of prime divisors counted with multiplicity of a natural number n than the normal order of $\Omega(p-1)$ is $\log\log p$; more precisely, for every $\epsilon > 0$, it exists $\eta = \eta(\epsilon)$ such that the number of p up to x for which $\Omega(p-1) > \epsilon \log\log p$ is*

$$o\left(\frac{x}{\log x}\right).$$

Proof: See [12].□

Lemma A. 3 (de Bruijn) *Let $\Psi(x, y)$ be the number of natural numbers up to x whose greatest prime divisor is less than y, then*

$$\Psi(x, y) \ll x \exp\left\{-c_1 \frac{\log x}{\log y}\right\}.$$

Proof: See [11].□

Lemma A. 4 (Hardy-Ramanujan) *For any $0 < \epsilon < 1$ there exists $\tau > 0$ such that the number of integers n up to x such that $\Omega(n) < \epsilon \log\log x$ is*

$$O\left(\frac{x}{\log^{\tau} x}\right).$$

Proof: See [19].□

Lemma A. 5 Murty (Weak Brun's sieve) *For any natural number $m < x$, denote by $N(x,m)$ the number of solutions of*

$$p - 1 = qm$$

where p and q are prime numbers $\leq x$. Then for some absolute constant $B > 0$, we have

$$N(x,m) \leq \frac{Bx(\log\log x/m)^2}{\phi(m)\log^2(x/m)}.$$

Proof: See [43].□

We are now ready to prove Theorem A.1:

Proof: Let $\mathcal{S} = \left\{p \leq x \mid \exists u | p-1, \text{ with } u \in [y, y\exp\log^\delta x]\right\}$. Without loss, we can assume that $p \geq \frac{x}{\log^2 x}$, and for a suitable δ to be chosen later, $p \in \mathcal{S}$ means that

$$p - 1 = uv \qquad \text{with} \qquad u \in \left[y, y\exp\log^\delta x\right] \quad \text{and} \quad v \in \left[\frac{x}{y}\exp\log^\delta x, \frac{x}{y}\right].$$

If $\Omega(u) > \frac{2}{3}\log\log x$ and $\Omega(v) > \frac{2}{3}\log\log x$ then $\Omega(p-1) > \frac{4}{3}\log\log x$, the number of $p \in \mathcal{S}$ for which this holds is certainly less then

$$\#\left\{p \leq x \mid \Omega(p-1) > \frac{4}{3}\log\log x\right\}$$

and for Lemma A.2, this is $o(\pi(x))$.

Remark: A stronger statement than Lemma A.2 can be found in [39]. Using such a statement, our proof would yield to $|S| \ll x/\log^\alpha x$. For the purpose of the application that will follow, our assumption is enough.

On the other hand, for a fixed u, the number of v's for which the maximum prime divisor is less then z is, by Lemma A.3,

$$O\left(\frac{x}{u}\exp\left\{-c_1\frac{\log(x/u)}{\log z}\right\}\right).$$

Fix $\epsilon > 0$, let $\beta > 0$ be a number to be chosen later and put $\log z = \log^{1-\beta-\epsilon} x$. We notice that $u < y \exp \log^{\delta} x = x^h \exp \log^{\delta} x$ and thus we get that the number we are estimating is

$$\ll \frac{x}{u} \exp\left\{-c_1 \frac{\log x - \log y - \log^{\delta} x}{\log^{1-\beta-\epsilon} x}\right\}$$

$$\ll \frac{x}{u} \exp\left\{-c_2 \frac{(1-h)\log x - \log^{\delta} x}{\log^{1-\beta-\epsilon} x}\right\} \ll \frac{x}{u} \exp\left\{-c_3 \log^{\epsilon} x\right\}.$$

(Note that this put the constraint $1 - \beta > \delta$.)

Therefore, the number of $p \in S$ for which this holds is

$$\ll \sum_u{}' \frac{x}{u} \exp\left\{-c_3 \log^{\epsilon} x\right\} \ll x \exp\left\{-c_3 \log^{\epsilon} x\right\} \sum_u{}' \frac{1}{u}$$

$$\ll x \exp\left\{-c_4 \log^{\epsilon} x\right\}$$

(here the dash on the sum sign means that the sum is extended to all the values of u for $p \in S$). A similar argument shows that $h > \log^{-\beta} x$ implies that we can also exclude the possibility that the maximum prime divisor of u is smaller than $\exp\left(\log^{1-\beta-\epsilon} x\right)$. Therefore we can assume that
$p - 1 = u_1 v_1 q$, with u_1 and v_1 in the desired range, $q > \exp\left(\log^{1-\beta-\epsilon} x\right)$ and $\Omega(u_1)$ or $\Omega(v_1)$ is less than $\frac{2}{3} \log\log x$.

From Lemma A.5, we get that for fixed u_1 and v_1, the number of possible solutions is

$$\ll \frac{x(\log\log \frac{x}{u_1 v_1})^2}{u_1 v_1 \log^2(x/u_1 v_1)} \ll \frac{x(\log\log x)^2}{u_1 v_1 \log^2(x/u_1 v_1)}.$$

As $u_1 v_1 \leq x \exp(-\log^{1-\beta-\epsilon} x)$ and $(\log\log x)^2 \ll \log^{\epsilon} x$, the number is

$$\ll \frac{x}{u_1 v_1 \log^{2-2\beta-3\epsilon} x}.$$

As applications of Lemma A.4 we know that

$$\#\left\{n \leq x \mid \Omega(n) < \frac{2}{3}\log\log x\right\} = O\left(\frac{x}{\log^{\tau} x}\right)$$

for some $\tau > 0$. Partial summation implies that, if
$S(t) = \#\left\{n \le t \mid \Omega(n) < \frac{2}{3}\log\log t\right\}$, then

$$\sum_{\Omega(n)<(2/3)\log\log x} \frac{1}{n} = S(x)/x - \int_1^x \frac{S(t)}{t^2}dt \ll \log^{1-\tau} x,$$

therefore the number of $p \in \mathcal{S}$ with the required properties is

$$\ll \frac{x}{\log^{2-2\beta-3\epsilon} x}\left(\sum_{\Omega(v_1)<(2/3)\log\log x}\sum_{u_1}{}' \frac{1}{u_1 v_1} + \sum_{\Omega(u_1)<(2/3)\log\log x}\sum_{v_1}{}' \frac{1}{u_1 v_1}\right)$$

$$\ll \frac{x}{\log^{1+\tau-2\beta-3\epsilon} x}\left(\sum_{u_1}{}' \frac{1}{u_1} + \sum_{v_1}{}' \frac{1}{v_1}\right) \ll \frac{x}{\log^{1-2\beta-3\epsilon+\tau-\delta} x}.$$

So that if we take $\delta + 2\beta < \tau$ (for example $\beta = \delta = \frac{1}{4}\tau$) we obtain the desired result and this completes the proof of the Theorem.□

Remark: The result just proven is a $p-1$-version of a Theorem of Erdös (See [13]). For a general statement on estimates of the number of $n \le x$ with a divisor in a given range see [49].

We are now ready to give a good estimate of $|\Gamma_r| = |\langle p_1, \ldots, p_r\rangle|$. More precisely:

Theorem A. 6 *Let r be a fixed positive number, then it exists $\delta > 0$ such that for almost all primes,*

$$|\Gamma_r| \ge p^{\frac{r}{r+1}} \exp\left(\log^{\delta} p\right).$$

Proof: From Lemma 1.4, we know that

$$\#\{p \le x \mid |\Gamma_r| < t\} = O\left(t^{1+\frac{1}{r}}\right),$$

if we take $t = x^{\frac{r}{r+1}}/\log x$, then

$$\#\left\{p \le x \mid |\Gamma_r| < \frac{p^{\frac{r}{r+1}}}{\log p}\right\} \ll \#\left\{p \le x \mid |\Gamma_r| < \frac{x^{\frac{r}{r+1}}}{\log x}\right\} \ll \frac{x}{\log x \log^{1/r} x} = o(\pi(x)).$$

Hence $|\Gamma_r| \geq \frac{p^{\frac{r}{r+1}}}{\log p}$ for almost all p's.

Now set

$$y = \frac{x^{\frac{r}{r+1}}}{\log x} = x^{\frac{r}{r+1} - \frac{\log\log x}{\log x}}$$

and note that $\frac{r}{r+1} - \frac{\log\log x}{\log x} < 1 - \frac{1}{\log^\beta x}$ for x large enough. Theorem A.2 gives that there exists δ such that if

$$\mathcal{T} = \left\{ p \leq x \mid \exists l | p-1,\ l \in \left[\frac{x^{\frac{r}{r+1}}}{\log x}, x^{\frac{r}{r+1}} \exp\left(\log^\delta x\right) \right] \right\}$$

then $|\mathcal{T}| = o(\pi(x))$. Finally, since

$$\left\{ p \leq x \mid |\Gamma_r| \in \left[\frac{x^{\frac{r}{r+1}}}{\log x}, x^{\frac{r}{r+1}} \exp\left(\log^\delta x\right) \right] \right\} \subset \mathcal{T},$$

we get that for almost all primes p,

$$|\Gamma_r| \geq x^{\frac{r}{r+1}} \exp(\log^\delta x) \geq p^{\frac{r}{r+1}} \exp(\log^\delta p). \square$$

The case in which r grows with p can be treated in an analogous fashion. The only care is to consider the version of Lemma 1.4 which is uniform with respect to r. In particular:

Theorem A. 7 *There exist β and δ such that if $r \leq (\log^\beta p) - 1$, then for almost all primes p,*

$$|\Gamma_r| \geq p^{\frac{r}{r+1}} \exp(\log^\delta p).$$

Proof: The uniform version of Lemma 1.4 states that

$$\#\{p \leq x \mid |\Gamma_r| < t\} = O\left(t^{1+\frac{1}{r}} r \log r\right),$$

if we take $t = \frac{x^{\frac{r}{r+1}}}{r \log^2 x}$, we get

$$\# \left\{ p \leq x \mid |\Gamma_r| < p^{\frac{r}{r+1}} \frac{1}{r \log^2 p} \right\} \ll \frac{x}{\log^2 x \log^{\frac{2}{r}} x} r^{-\frac{1}{r}} \log r = o(\pi(x)).$$

Now set

$$\frac{x^{\frac{r}{r+1}}}{r\log^2 x} = x^{\frac{r}{r+1}-\frac{2\log\log x}{\log x}-\frac{\log r}{\log x}} = x^h = y$$

and note that $h = \frac{r}{r+1} - \frac{2\log\log x}{\log x} - \frac{\log r}{\log x} < 1 - \frac{1}{\log^3 x}$

if $r \leq (\log^\beta p) - 1$ and x is large enough.

Therefore Theorem A.1 gives

$$\#\left\{p \leq x \mid \frac{p^{\frac{r}{r+1}}}{r\log^2 p} \leq |\Gamma_r| \leq p^{\frac{r}{r+1}}\exp(\log^\delta p)\right\} = o(\pi(x))$$

which clearly implies the claim.□

Remark: If $l|[\mathbf{F}_p^* : |\Gamma_r|]$, then Theorem A.7 puts the constraint

$$l < \frac{p-1}{\Gamma_r} < p^{-\frac{1}{r+1}}\exp(-\log^\delta p)$$

for almost all primes p.

Unfortunately the position $r = (\log p)^\beta - 1$ and the constraint $\beta + \delta < 1$ remarked during the proof of Theorem A.1, implies that

$$l < \exp\left(\log^{1-\beta} p - \log^\delta p\right) \leq \exp\left(\frac{1}{2}\log^{1-\beta} p\right).$$

Such a bound is too high to make possible the use of any of our techniques for th range of r's under consideration.

APPENDIX B: ON THE EXPONENT OF THE IDEAL CLASS GROUP OF $\mathbf{Q}(\sqrt{-d})$

Let d be a positive square-free integer and let $m(d)$ denote the exponent of the class group of $\mathbf{Q}(\sqrt{-d})$, i.e. $m(d)$ is the least positive integer m, such that $x^m = 1$ for every x in the class group.

In 1972 D.W. Boyd and H. Kisilevsky (see [3]) proved that if the Extended Riemann Hypothesis holds, then for any $\eta > 0$, and d sufficiently large,

$$m(d) > \frac{\log d}{(2+\eta)\log\log d} \tag{1}$$

which of course implies that $m(d) \to \infty$ as $d \to \infty$.

The goal of this note is to establish unconditional inequalities of the type (1) for density-one sets of values of d. Before doing this, let us review the method used by Boyd and Kisilevsky to prove (1).

First they noticed that if α is an integer of $\mathbf{Q}(\sqrt{-d})$ which is not in $\mathbf{Z}$, then $N(\alpha) \geq d/4$ and that if p is a rational prime that splits in $\mathbf{Q}(\sqrt{-d})$ and ϖ is a prime ideal above p, then $\varpi^{m(d)}$ is a principal ideal (α) thus

$$N(\varpi)^{m(d)} = p^{m(d)} = N(\alpha)^{m(d)} \geq (d/4)^{m(d)}.$$

In conclusion,

$$\left(\frac{-d}{p}\right) = 1 \quad \Longrightarrow \quad p \geq (d/4)^{1/m(d)}. \tag{2}$$

Then they proved that

If the Extended Riemann Hypothesis holds then, for any integer d, there exists a prime less then $\log^{2+\eta} d$ for which $-d$ is a quadratic residue and this gives (1).

Now, let us take $p = 3$ and ask how often is a square-free d a quadratic residue (mod3)? This happens when $d \equiv 1 \bmod 3$, and the density of such d's is certainly positive

For a positive proportion of square-free integers d,

$$m(d) \geq \frac{\log d/4}{\log 3}.$$

In general we will be able to prove that

Theorem B. 1 *For any $d < x$ there exists a prime $< \log d$ for which d is a quadratic residue with at the most $O\left(x^{1-A(\log\log x)^{-1}}\right)$ exceptions.*

This is an consequence of Theorem B.3 below and by (2) implies

Corollary B. 2 *For all discriminant $d < x$, we have that*

$$m(d) > \frac{\log d/4}{\log\log d}$$

with at most $O\left(x^{1-A(\log\log x)^{-1}}\right)$ exceptions.

For an integer n, let $\mathcal{M}(n)$ be the least prime for which n is quadratic residue, i.e.

$$\mathcal{M}(n) = \min\left\{p \;\middle|\; p \text{ is prime and } \left(\frac{n}{p}\right) = 1\right\}.$$

Let $K(x,s)$ (respectively $K_1(x,s)$) be the set of numbers (resp. square-free numbers) up to x such that $\mathcal{M}(n) > s$. We have that

Theorem B. 3 *Let $k(x,s) = |K(x,s)|$ and $k_1(x,s) = |K_1(x,s)|$, then*

$$a)\quad k(x,s) = \frac{x}{2^{\pi(s)}} \prod_{p \leq s}\left(1 + \frac{1}{p} - \frac{2}{p^2}\right) + O\left(\frac{e^{\theta(s)}\log^3 s}{2^{\pi(s)}}\right);$$

$$b)\quad k_1(x,s) = \frac{6}{\pi^2}\frac{x}{2^{\pi(s)}} \prod_{p \leq s}\left(1 + \frac{1}{p+1}\right) + O\left(\frac{x^{1/2}e^{\theta(s)}}{2^{\pi(s)}\log s}\right).$$

uniformly with respect to s (where as usual $\pi(s)$ and $\theta(s)$ are respectively the number of primes up to s and the sum of the logarithms of the primes up to s).

Proof: Let us define P to be the product of all primes up to s.

b) In order for a square-free number $n \leq x$ to be in $K_1(x,s)$, one must have $\left(\frac{n}{p}\right) = 0$ or -1 for all primes p up to s. For any divisor Q of P, let A_Q be the set of $n \in K_1(x,s)$ such that

$$\left(\frac{n}{p}\right) = 0 \text{ for any } p|Q \text{ and } \left(\frac{n}{p}\right) = -1 \text{ for any } p\left|\frac{P}{Q}\right.,$$

Clearly

$$K_1(x,s) = \overset{\circ}{\bigcup_{Q|P}} A_Q \tag{3}$$

where the union is disjoint. Note also that

$$|A_Q| = \overset{\prime\prime}{\pi}\left\{n \leq \frac{x}{Q} \;\middle|\; (n,Q)=1, n \text{ square-free}, \left(\frac{n}{p}\right) = -\left(\frac{Q}{p}\right) \text{ for any } p\left|\frac{P}{Q}\right.\right\} \tag{4}$$

$$= \sum{}^{*}\overset{\prime\prime}{\pi}\left\{n \leq \frac{x}{Q} \mid (n,Q)=1, n \text{ square-free}, n \equiv g_i (\mathrm{mod} q_i), i = 1, \ldots, t\right\}$$

where we have put $\frac{P}{Q} = q_1 \cdots q_t$ and $\sum^{*}$ means that the sum is extended to all the t-tuples $(g_1, \ldots, g_t)$, g_i being a congruence class modq_i such that $\left(\frac{a}{q_i}\right) = -\left(\frac{Q}{q_i}\right)$.

By the Chinese remainder Theorem, for each t-tuple $(g_1, \ldots, g_t)$, there exists a unique congruence class $M = M(g_1, \ldots, g_t)(\mathrm{mod}\frac{P}{Q})$ such that

$$n \equiv g_i (\mathrm{mod} q_i), \forall i = 1, \ldots, t \quad \Longleftrightarrow \quad n \equiv M \left(\mathrm{mod}\frac{P}{Q}\right)$$

therefore (4) equals

$$\sum{}^{*}\overset{\prime\prime}{\pi}\left\{n \leq \frac{x}{Q} \;\middle|\; (n,Q)=1, n \text{ square-free}, n \equiv M \left(\mathrm{mod}\frac{P}{Q}\right)\right\}. \tag{5}$$

Now we need the following two Lemmas:

Lemma B. 4 *Let R_1, R_2, R_3 be positive integers with $(R_1, R_3) = (R_2, R_3) = 1$ and define*

$$B_{R_1,R_2,R_3}(y) = \#\{n \leq y \mid (n, R_1) = 1,\ n \equiv R_2 (\mathrm{mod} R_3)\}$$

then, uniformly with respect to $R_1, R_2, R_3 < y$, we have

$$B_{R_1,R_2,R_3}(y) = y\frac{\varphi(R_1)}{R_1 R_3} + O(\vartheta(R_1)),$$

where $\vartheta(R_1)$ is the number of square-free divisors of R_1.

Lemma B. 5 *Let Q_1, Q_2, Q_3 be positive integers with $(Q_1, Q_2) = (Q_2, Q_3) = 1$ and define*

$$C_{Q_1,Q_2,Q_3}(z) = \#\{n \leq z \mid n \text{ square-free},\ (n, Q_1) = 1,\ n \equiv Q_3 (\mathrm{mod} Q_2)\},$$

then, uniformly respect to $Q_1, Q_2, Q_3 < z$, we have

$$C_{Q_1,Q_2,Q_3}(z) = \frac{6}{\pi^2} z \frac{\varphi(Q_1)}{Q_1 Q_2} \prod_{p \mid Q_1 Q_2} \left(1 - \frac{1}{p^2}\right)^{-1} + O\left(z^{1/2}\vartheta(Q_1)\right).$$

Remark: Lemma B.4 and B.5 are due respectively Cohen (See [9]) and to Landau (See p. 633-636 of [30]). Their version is slightly less general though the proof is similar. One might think that a stronger version of Lemma B.4, say valid on a range of R_1 of the same order of the range given by the Brun's Sieve, would yield a better error term in Theorem B.3. On the contrary, it will become clear how this is not influential to the main goal of our discussion.

Proof of Lemma B.4: We have that

$$\begin{aligned} B_{R_1,R_2,R_3}(y) &= \sum_{d \mid R_1} \mu(d) \#\{n \leq y \mid d \mid n, \text{ and } n \equiv R_2 (\mathrm{mod} R_3)\} \\ &= \sum_{d \mid R_1} \mu(d) \#\left\{n \leq \frac{y}{d} \mid n \equiv R_2 d^* (\mathrm{mod} R_3)\right\} \\ &= \sum_{d \mid R_1} \mu(d) \left[\frac{y}{d R_3}\right] \end{aligned}$$

where d^* is the unique congruence class mod R_3 defined by $dd^* \equiv 1 \bmod R_3$ (Such a class exists since we have assumed that $(R_1, R_3) =$ and $d|R_3$). Finally

$$B_{R_1,R_2,R_3}(y) = \sum_{d|R_1} \mu(d) \left(\frac{y}{dR_3} + O(1) \right)$$

$$= y \frac{\varphi(R_1)}{R_1 R_3} + O(\vartheta(R_1)). \square$$

Proof of Lemma B.5: This is based on the identity

$$\mu^2(n) = \sum_{d^2|n} \mu(d),$$

We have that

$$\begin{aligned} C_{Q_1,Q_2,Q_3}(z) &= \sum_{\substack{n \le z \\ (n,Q_1)=1 \\ n \equiv Q_3 (\mathrm{mod} Q_2)}} \mu^2(n) = \sum_{\substack{d^2\delta \le z \\ (d,Q_1)=(\delta,Q_1)=1 \\ d^2\delta \equiv Q_3 (\mathrm{mod} Q_2)}} \mu(d) \\ &= \sum_{\substack{d \le z^{1/2} \\ (d,Q_1)=(d,Q_2)=1}} \mu(d) \sum_{\substack{\delta \le \frac{z}{d^2} \\ (\delta,Q_1)=1 \\ \delta \equiv Q_3 d^{*2} (\mathrm{mod} Q_2)}} 1 = \\ &= \sum_{\substack{d \le z^{1/2} \\ (d,Q_1)=(d,Q_2)=1}} \mu(d) B_{Q_1, Q_3 d^{*2}, Q_2}(z/d^2) \end{aligned} \tag{6}$$

where the condition $(Q_2, Q_3) = 1$ implies $(d, Q_2) = 1$ and d^* has the same meaning as in the proof of Lemma B.4. Now apply Lemma B.4 and get that (6) equals

$$\sum_{\substack{d \le z^{1/2} \\ (d,Q_1Q_2)=1}} \mu(d) \left(\frac{z}{d^2} \frac{\varphi(Q_1)}{Q_1 Q_2} + O(\vartheta(Q_1)) \right) =$$

$$= \frac{z\varphi(Q_1)}{Q_1 Q_2} \sum_{\substack{d=1 \\ (d,Q_1Q_2)=1}}^{\infty} \frac{\mu(d)}{d^2} + O\left(\sum_{d > z^{1/2}} \frac{z\varphi(Q_1)}{d^2 Q_1 Q_2} \right) + O\left(z^{1/2} \vartheta(Q_1) \right)$$

and since clearly $\frac{\varphi(Q_1)}{Q_1} < \vartheta(Q_1)$ and

$$\sum_{\substack{d=1 \\ (d,Q_1Q_2)=1}}^{\infty} \frac{\mu(d)}{d^2} = \frac{6}{\pi^2} \prod_{p|Q_1Q_2} \left(1 - \frac{1}{p^2} \right)^{-1},$$

the claim is deduced.□

Now we can apply Lemma B.5 to (4) with $Q_1 = Q, Q_2 = P/Q, Q_3 = M$ and $z = x/Q$. Note that the number of summands in (5) is $\varphi(\frac{P}{Q})/\vartheta(\frac{P}{Q})$, therefore

$$|A_Q| = \frac{\varphi(\frac{P}{Q})}{\vartheta(\frac{P}{Q})}\left\{\frac{6}{\pi^2}\frac{x}{Q}\frac{\varphi(Q)}{P}\prod_{p|P}\left(1-\frac{1}{p^2}\right)^{-1} + O\left(\left(\frac{x}{Q}\right)^{1/2}\vartheta(Q)\right)\right\} \tag{7}$$

$$= \frac{6}{\pi^2}\frac{x}{2^{\pi(s)}}\prod_{p|P}\left(1+\frac{1}{p}\right)^{-1}\frac{\vartheta(Q)}{Q} + O\left(\frac{x^{1/2}}{2^{\pi(s)}}\frac{\vartheta^2(Q)}{Q^{1/2}\varphi(Q)}\frac{e^{\theta(s)}}{\log s}\right),$$

where we just noticed that $\vartheta(P) = 2^{\pi(s)}$ and $\varphi(P) \ll \frac{e^{\theta(s)}}{\log s}$. Now use (3) and get

$$\begin{aligned} k_1(x,s) &= \sum_{Q|P}|A_Q| \\ &= \frac{6}{\pi^2}\frac{x}{2^{\pi(s)}}\prod_{p|P}\left(1+\frac{1}{p}\right)^{-1}\sum_{Q|P}\frac{\vartheta(Q)}{Q} + O\left(\frac{x^{1/2}}{2^{\pi(s)}}\frac{e^{\theta(s)}}{\log s}\sum_{Q|P}\frac{\vartheta^2(Q)}{Q^{1/2}\varphi(Q)}\right) \qquad (8) \\ &= \frac{6}{\pi^2}\frac{x}{2^{\pi(s)}}\prod_{p|P}\left(1+\frac{1}{p}\right)^{-1}\prod_{p|P}\left(1+\frac{2}{p}\right) + O\left(\frac{x^{1/2}}{2^{\pi(s)}}\frac{e^{\theta(s)}}{\log s}\right) \end{aligned}$$

The last identity follows since $\sum_{Q|P}\frac{\vartheta^2(Q)}{Q^{1/2}\varphi(Q)}$ converges as $s \to \infty$. This concludes the proof of b).□

a) This is simpler than b). For any $Q|P$, define A_Q to be the set of $n \in K(x,s)$ such that

$$\left(\frac{n}{p}\right) = 0 \text{ for any } p|Q \quad \text{and} \quad \left(\frac{n}{p}\right) = -1 \text{ for any } p\left|\frac{P}{Q}\right.$$

Again

$$k(x,s) = \sum_{Q|P}|A_Q| \tag{9}$$

and now

$$|A_Q| = \dot{\sum}\#\left\{n \le \frac{x}{Q} \mid n \equiv g_i(\mathrm{mod}\, q_i), i = 1,\ldots,t\right\}$$

$$= \sum{}^{\cdot}\#\left\{n \le \frac{x}{Q} \;\middle|\; n \equiv M(\mathrm{mod}\,\frac{P}{Q})\right\}.$$

where the $g_i, i = 1, \ldots, t$ and $M = M(g_1, \ldots, g_t)$ are defined as above. Now apply Lemma B.4 with $R_1 = Q, R_2 = M, R_3 = P/Q$ and $y = \frac{x}{Q}$ and get

$$|A_Q| = \frac{\varphi(\frac{P}{Q})}{\vartheta(\frac{P}{Q})} \left\{ \frac{x}{Q} \frac{\varphi(Q)}{P} + O(\vartheta(Q)) \right\} = 2^{-\pi(s)} \left(x \frac{\varphi(P)}{P} \frac{\vartheta(Q)}{Q} + O\left(\frac{e^{\vartheta(s)}}{\log s} \frac{\vartheta^2(Q)}{\varphi(Q)} \right) \right).$$

Finally by (9),

$$k(x,s) = 2^{-\pi(s)} \left(x \prod_{p \le s} \left(1 - \frac{1}{p}\right) \left(1 + \frac{2}{p}\right) + O\left(\frac{e^{\vartheta(s)}}{\log s} \prod_{p \le s} \left(1 + \frac{1}{p-1}\right) \right) \right)$$

$$= 2^{-\pi(s)} \left(x \prod_{p \le s} \left(1 + \frac{1}{p} - \frac{2}{p^2}\right) + O\left(e^{\vartheta(s)} \log^3 s\right) \right)$$

Which is the claim of a).□

Proof of Theorem B.1: We want to estimate

$$\# \{ d \le x \mid \mathcal{M}(d) > \log d \} \tag{10}$$

Note that, since the contribution for $d < x^{1/2}$ is $O(x^{1/2})$, we have that (10) equals

$$\begin{aligned} & \# \left\{ d : x^{1/2} \le d \le x \mid \mathcal{M}(d) > \log d \right\} + O(x^{1/2}) \\ \le \; & \# \left\{ d \le x \mid \mathcal{M}(d) > \frac{1}{2} \log x \right\} + O(x^{1/2}). \end{aligned} \tag{11}$$

Now apply Theorem 3 a), with $s = \frac{1}{2} \log x$ and get that (11) is $\ll$ then

$$2^{-\pi(\frac{1}{2}\log x)} \left(x \log\log x + e^{\vartheta(\frac{1}{2}\log x))} (\log\log x)^3 \right)$$

$$\ll x \exp(-A \log x / \log\log x)$$

where we took $A < \frac{1}{2} \log 2$, say, and this proves the claim.□

Remark: Note that although in Theorem B.1 we consider discriminants of imaginary quadratic fields which are by definition squarefree numbers, statement b) of Theorem B.3. does not give anything more than statement a). This is due to the fact that square-free numbers have non-zero density.

Theorem B.3 b) can be improved using a version of Lemma B.5 in which the error term depends on Q_2. This has been done by K. Prachar in [45] for the case $Q_1 = 1$, and his proof can adapted to proof the following:

Lemma B. 6 *With the same notations of Lemma B.5 we have that, uniformly respect to the parameters,*

$$C_{Q_1,Q_2,Q_3}(z) = \frac{6}{\pi^2} z \frac{\varphi(Q_1)}{Q_1 Q_2} \prod_{p|Q_1Q_2} \left(1 - \frac{1}{p^2}\right)^{-1} + O\left((z^{1/2} Q_2^{-1/4+\epsilon} + Q_2^{1/2+\epsilon})\vartheta(Q_1)\right),$$

for any $\epsilon > 0$.□

Corollary B. 7 *With the same notation as above, we have that*

$$k_1(x,s) = \frac{6}{\pi^2} \frac{x}{2^{\pi(s)}} \prod_{p \le s} \left(1 + \frac{1}{p+1}\right) + O\left(\left(\frac{x^{1/2}}{e^{\theta(s)(1/4-\epsilon)}} + e^{\theta(s)(1/2+\epsilon)}\right) \frac{e^{\theta(s)}}{2^{\pi(s)} \log s}\right).$$

Proof: It is similar to the proof of Theorem B.1 b), but in this case we have

$$|A_Q| = \frac{6}{\pi^2} \frac{x}{2^{\pi(s)}} \prod_{p|P} \left(1 + \frac{1}{p}\right)^{-1} \frac{\vartheta(Q)}{Q} +$$

$$O\left(\left(\frac{x^{1/2}}{Q^{1/2}} P^{-1/4+\epsilon} Q^{1/4-\epsilon} + \frac{P^{1/2+\epsilon}}{Q^{1/2+\epsilon}}\right) \frac{\vartheta^2(Q)}{2^{\pi(s)} \varphi(Q)} \frac{e^{\theta(s)}}{\log s}\right)$$

and therefore

$$k_1(x,s) = \sum_{Q|P} |A_Q|$$

$$= \frac{6}{\pi^2} \frac{x}{2^{\pi(s)}} \prod_{p \le s} \left(1 + \frac{1}{p+1}\right) +$$

$$+O\left(\left(\frac{x^{1/2}}{P^{-1/4+\epsilon}} \sum_{Q|P} \frac{\vartheta^2(Q)}{Q^{1/2-1/4+\epsilon} \varphi(Q)} + P^{1/2+\epsilon} \sum_{Q|P} \frac{\vartheta^2(Q)}{Q^{1/2+\epsilon} \varphi(Q)}\right) \frac{e^{\theta(s)}}{2^{\pi(s)} \log s}\right)$$

$$= \frac{6}{\pi^2} \frac{x}{2^{\pi(s)}} \prod_{p \le s} \left(1 + \frac{1}{p+1}\right) + O\left(\left(\frac{x^{1/2}}{e^{\theta(s)(1/4-\epsilon)}} + e^{\theta(s)(1/2+\epsilon)}\right) \frac{e^{\theta(s)}}{2^{\pi(s)} \log s}\right).$$

The last identity because both the series $\sum_{Q|P} \frac{\mu^2(Q)}{Q^{1/2+\varepsilon}\varphi(Q)}$ and $\sum_{Q|P} \frac{\mu^2(Q)}{Q^{1/2-1/4+\varepsilon}\varphi(Q)}$ converge as $s \to \infty$.□

Remark A general form of Theorem B.1 can also be proven. It is a uniform asymptotic formula for $k_{m-1}(x, s)$, the number of m-free numbers d up to x for which $\mathcal{M}(d) < s$. The m-free version of Lemma B.6 is also in [45]. Finally, the results of Prachar have been improved by Hooley in [24] and the use of this last one would give a further improvement of Theorem B.3.

APPENDIX C: OPEN QUESTIONS AND FUTURE RESEARCH

Variants of the Bombieri-Vinogradov Theorem

A form of the famous Bombieri-Vinogradov Theorem for primes in arithmetic progression states that

For any real number $A > 0$, it exists a $B > 0$ such that

$$\sum_{m \leq \frac{x^{1/2}}{\log^A x}} \left| \psi(x, m, 1) - \frac{1}{\phi(m)} x \right| \ll \frac{x}{\log^B x}$$

where $\psi(x, m, 1) = \sum_{\substack{p \leq x \\ p \equiv 1 \bmod m}} \log p$.

This important result provides us with an estimate on average of the error term for the prime number Theorem for primes in arithmetic progressions which is as strong as the one that could be deduced useing the Extended Riemann Hypothesis for the Dirichlet L-functions of all the characters mod$m$.

Such a Theorem can be interpreted as an estimate on average of the error term of the Chebotarev Density Theorem for cyclotomic fields. More precisely, let us consider the following statement:

For every integer m, let us suppose K_m is a given finite Galois extension of $\mathbf{Q}$ *and let $n(m) = [K_m : \mathbf{Q}]$. Further, set*

$$\psi(x, K_m) = \sum_{\substack{p \leq x \\ p \text{ splits completely in } K_m}} \log p.$$

We have that

$$\sum_{m \leq \frac{x^{1/2}}{\log^A x}} \left| \psi(x, K_m) - \frac{1}{n(m)} x \right| \ll \frac{x}{\log^B x} \qquad (1)$$

Let us note the following facts:

- If the Generalized Riemann Hypothesis holds for all the (non-abelian) Artin L-functions of K_m then the statement is true.

- If, for any m, K_m is the cyclotomic field $\mathbf{Q}(\zeta_m)$, then the statement is a consequence of the famous Bombieri-Vinogradov Theorem.

- If, for any m, K_m is the Galois Extension $\mathbf{Q}(\zeta_m, a^{1/m})$ and the statement is true, then the Artin Conjecture for primitive roots is true for the number a.

The last fact has been noticed by R. Murty in his thesis and he gave a result which is in the spirit of this approach.

We can refer to (1) as the *general non-abelian Bombieri-Vinogradov Theorem* and ask for which families K_m it holds

A proof of the general statements is certainly a very difficult problem, and to our knowledge, the Theorem of R. Murty and K. Murty in [41] is the only significant contribution toward this direction and it states that:

If $\pi_K(x,q)$ is the number of primes p up to x such that p splits completely in a given fixed Galois extension K of $\mathbf{Q}$ and $p \equiv 1 (\mathrm{mod} q)$ (i.e. p splits completely in $K(\zeta_q)$), then for any $A > 0$, there exists $B = B(A)$ such that

$$\sum_{q \leq x^{\alpha}(\log x)^{-B}} \left| \pi_K(x,q) - \frac{1}{[K(\zeta_q) : \mathbf{Q}]} \mathrm{li}(x) \right| \ll \frac{x}{\log^A x}$$

where $\alpha = \min\left(\frac{2}{[K:\mathbf{Q}]}, \frac{1}{2}\right)$ and the sum is extended to all the values of q for which $K \cap \mathbf{Q}(\zeta_q) = \mathbf{Q}$.

In general, one could try to settle for something less and restrict the sum in (1) to $m \leq \log^C x$ for some fixed positive integer C. We would get a weaker statement but with still quite a few interesting arithmetical consequences. For example, if we prove

the statement with $C = 2$ ($C = 1$ is actually Theorem 2.7), then it can be proven the following substantial improovement of Theorem 3.1:

For amost all primes p, the $\frac{\log p}{\log\log p}$ primes generate $\mathbf{F}_p^*$.

Such a problem admits an analogous situation where we substitute the Artin L-function with the L-series attached to modular forms.

The Lang-Trotter Conjecture for Abelian Varieties

In 1977 J.-P. Serre (see [47]) has proven the following result:
Let E be an elliptic curve defined over $\mathbf{Q}$ and let $K_n = \mathbf{Q}(E[n])$ where by $E[n]$ we denote the set of n-points of E (i.e. $Q \in E$ such that $[n]Q = 0$). Let us put

$$\delta = \sum_{n=1}^{\infty} \frac{\mu(n)}{[K_n : \mathbf{Q}]},$$

where $\mu(n)$ denotes the μ function of Möbius. If the Generalized Riemann Hypothesis holds for K_n, then

$$\#\{p \leq x \mid \bar{E}(\mathbf{F}_p^*) \text{ is cyclic}\} \sim \delta \frac{x}{\log x}$$

This result has been reconsidered by R. Murty and R. Gupta. In 1990 (see [16]) without any unproved hypothesis they have characterized elliptic curves for which $E(\mathbf{F}_p^*)$ is cyclic for infinitely many values of p.

Gupta and Murty considered as well a similar problem to Serre's Theorem, namely The Lang-Trotter Conjecture (see [34]):

Let E be an elliptic curve defined over $\mathbf{Q}$ and let P be a rational point of E with infinite order. We denote by $N(x, P)$ the number of primes p up to x such that $\langle P \rangle = E(\mathbf{F}_p^*)$, then

$$N(x, P) \sim \delta_E(P) \frac{x}{\log x}$$

where $\delta_E(P)$ can be expressed in terms of the decomposition of primes in the extensions $\mathbf{Q}(E[n], n^{-1}P)$ over $\mathbf{Q}$.

Both this result and the statement of Serre's Theorem are analogous to the Artin's Conjecture for primitive roots.

Many of these conjectures admit a very natural generalization to the case of abelian varieties. The problem can be stated as follows:

Let A be an abelian variety defined over $\mathbf{Q}$ and let $P \in A$ be a rational point (with infinite order). For all (but finitely many) prime numbers p, it makes sense to consider the reduction of A modulo p that we can denote by $A(\mathbf{F}_p^*)$.

$A(\mathbf{F}_p^*)$ is a finite group and we can indicate with $\bar{P} \in A(\mathbf{F}_p^*)$ the reduction of P modulo p. Various questions can be formulated, for example:

- Under which conditions $A(\mathbf{F}_p^*)$ is cyclic (or more particularly $\langle \bar{P} \rangle = A(\mathbf{F}_p^*)$) for infinitely many p?
- What is the distribution of the prime numbers with this property ?
- Is it possible to write a formula for the density of such sets of primes?

In the case $\dim A = 1$, (i.e. A is an elliptic curve), then the Lang-Trotter conjecture toghether with the Theorem of Serre and the contribution of Gupta and Murty, provide with a precise indication on what should be the answer to these questions.

In the case $\dim A > 1$, there are not, at the moment in the literature conjectures that give any answer to this question, nevertheless it is natural to suspect that many of the arguments that worked in the case of elliptic curves, extend to the general case and the first problem is as usual to express, for any prime number l, the condition

$$l \Big| \big[A[\mathbf{F}_p^*] : \langle P \rangle \big]$$

in terms of particular decompositions of p in algebraic extensions $K(l, P)$.

Similarly as in the case of elliptic curves in which it has been necessary to distinguish between Complex Multiplication curves and curves without Complex Multiplication (see [17]), it is natural to expect that the properties under consideration depend heavily on the structure of the ring $\mathrm{End}_{\mathbf{Q}} A$.

References

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

[2] E. Bombieri, *Le grande crible dans la théorie analytique des nombres* - Astérisque 18, (1974).

[3] D. W. Boyd and H. Kisilevsky, *On the exponent of the Ideal Class Groups of Complex Quadratic Fields* Amer. Math. Soc. Proc. (1972) 433-436.

[4] H. Brown and H. Zassenhaus, *Some Empirical Observations on Primitive Roots*, J. Number Theory 3(1971) 306-309

[5] D. A. Burgess and T. A. Elliott, *The average of least primitive root* - Mathematika 15 (1968), 39-50.

[6] H. Davenport, *Multiplicative Number Theory* - GTM 74 - Springer Verlag, (1980).

[7] J. W. S. Cassels and A.Fröhlich, *Algebraic Number Theory*, Academic Press, (1967).

[8] E. R. Canfield, P. Erdös and C. Pomerance, *On a problem of Oppenheim concerning "Factorization Numerorum"*, J. Number Theory 17(1983), 1-28.

[9] E. Cohen, *Remark on a Set of Integers*, Acta Sci. Math. (Szeged) 25 (1964), 179-180.

[10] N.G. de Bruijn, *The asymptotic behavior of a function occurring in the theory of primes*, J. Indian Math. Soc. (N. S.) 15 (1951), 25-32.

[11] N.G. de Bruijn, *On the number of positive integers $\leq x$ and free of prime factors $> y$*. Indag. Math. 13, (1951) 50-60.

[12] P. Erdös, *On the normal number of prime factors of $p-1$ and some related problems concerning Euler's ϕ-function*, Quarterly Journal of Mathematics, (Oxford Ser.) 6 (1935), 205-213.

[13] P. Erdös and R. R. Hall, *On the Möbius function*, J. reine angew. Math. 315, (1980).

[14] P. Erdös and M. R. Murty, *On the order of $a \pmod p$*, unpublished.

[15] R. Gupta and M. R. Murty, *A remark on Artin's Conjecture*, Inventiones Math. 78 (1984), 127-130.

[16] R. Gupta and M. R. Murty, *Cyclicity and generation of points* mod p *on elliptic curves*. Invent. math. 101, (1990) 225-235.

[17] R. Gupta and M. R. Murty, *Primitive points on elliptic curves*, Comp. Mathematica 58, (1986) 13-44.

[18] H. Halberstam and H.E. Richert, *Sieve Methods*, Academic Press, London/New York (1974).

[19] G. H. Hardy and S. Ramanujan, Quarterly Journal of Mathematics, (Oxford Ser.) 48 (1917), 76-92.

[20] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, second Ed. Oxford at the Clarendon Press, (1945).

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

[22] D.R. Hensley, *The number of positive integers $\leq x$ and free of prime divisors $> y$*. J. Number Theory **21**(1985), 286-298.

[23] A. Hildebrand, *On the number of positive integers $\leq x$ and free of prime divisors $> y$*, J. Number Theory **22**(1986), 289-307.

[24] C. Hooley, *A note on Square-Free Numbers in Arithmetic Progressions*, Bull. London Math. Soc., 7 (1975), 133-138.

[25] C. Hooley, *Application of Sieve methods to the Theory of Numbers*, Cambridge University Press - (1976).

[26] C. Hooley, *On Artin's Conjectures* - J. Reine Angew. Math. - **226** (1967), 207-220.

[27] A. Ivić, *The Riemann Zeta-function*, John Wiley & Sons, (1985).

[28] J.C. Lagarias, H.L. Montgomery, A.M. Odlyzko, *A Bound for the Least Prime Ideal in the Chebotarev Density Theorem* - Inventiones math. - **54**(1979), 271-296.

[29] J.C. Lagarias and A.M. Odlyzko, *Effective versions of the Chebotarev Density Theorem in Algebraic Number Fields*, Ed. A. Fröhlich. Academic press, New York, (1977) 409-464.

[30] E. Landau, *Algebraische Zahlen* Verlag und Druck Von B. G. Teubner, Leipzig (1927).

[31] E. Landau, *Einführung in die Elementare und Analytische Theorie der Algebraischen Zahlen und der ideale.* - Verlag und Druck Von B. G. Teubner, Leipzig und Berlin (1918).

[32] S. Landau, *Handbuch der Lehre von der Verteilung der Primzahlen*, Leipzig und Berlin (1909), Vol. 2.

[33] S. Lang, *Algebraic Number Theory* - GTM **110**- Springer Verlag, (1986).

[34] S. Lang and H. Trotter, *Primitive points on elliptic curves*, Bull. Amer. Math. Soc. **83**, (1977) 289-292.

[35] D. H Lehmer and E. Lehmer *Heuristics Anyone?* - Selected Papers, Vol 1, Winnipeg. Canada (1981).

[36] K. R. Matthews, *A generalisation of Artin's conjecture for primitive roots*, Acta Arithmetica **XXIX** (1976), 113-146.

[37] C.R. Matthews, *Counting points modulo p for some finitely generated subgroups of algebraic group* - Bulletin London Math. Soc. 14 (1982), 149-154.

[38] Leo Murata, *On the magnitude of the least prime primitive root*, J. Number Theory **37**, (1991) 47-66.

[39] M. R. Murty, *An analogue of Artin's conjecture for Abelian extensions* - J. of Num. Theory - **18** (1984), 241-248.

[40] M. R. Murty, *Finitely Generated Groups* (mod p), to appear in Proc. Amer. Math. Soc.

[41] M. R. Murty and V. K. Murty, *A variant of the Bombieri-Vinogradov Theorem* - Canadian Math. Soc. Conference Proceedings - **7** (1987), 243-271.

[42] M. R. Murty, V. K. Murty, N. Saradha, *Modular forms and Chebotarev density Theorem* - Am. J. of Math. - **110** (1988), 252-281.

[43] M. R. Murty and N. Saradha *On the Sieve of Eratosthenes* Can. J. Math. Vol. XXXIX, **5** (1987), 1107-1122.

[44] V. K. Murty, *Explicit Formulae and Lang-Trotter Conjecture* Rocky Mountain J. of Math. **15**(1985), 535-551.

[45] K. Prachar, *Über die kleinste quadratfreie Zahl einer arithmetishen Reihe*, Monatsh. Math, **62** (1958), 173-176.

[46] J.-P. Serre, *Linear Representations of Finite Groups* - GTM 42 - Springer Verlag, (1982).

[47] J. -P. Serre, *Resumé de cours* (1977), See: Oeuvres. Berlin-Heidelberg- New York: Springer (1986).

[48] D. Suryanarayana and R. Sita Rama Chandra Rao *Uniform O-estimates for k-free integers*, J. Reine Angew. Math. **261**, 146-152.

[49] G. Tenenbaum, *Sue la probabilité qu'un entier possède un diviseur dans un intervalle donné.* Comp. Math. **51**(1984) 243-263.