Analytic Problems for Number Fields and Elliptic Curves

Amir Akbary

Abstract

These are the lecture notes of a series of six lectures given in the WAMS Research School in "Topics in Analytic and Transcendental Number Theory" at the Institute for Advanced Studies in Basic Sciences (IASBS), Zanjan, Iran in July 2017. The author would like to thank Dakota Duffy and Sahar Siavashi for typing these notes.

1 Analytic Methods in Number Fields

The Riemann Zeta Function.

We start by reviewing some basic facts from analytic number theory over $\mathbb{Q}$. The fundamental object in this case is the Riemann zeta function. For $\Re(s) > 1$, let

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

This is an absolutely convergent series. In a seminal eight page paper written in 1859, Riemann proved that $\zeta(s)$ has an analytic (meromorphic) continuation to the whole complex plane $\mathbb{C}$ with the exception of a simple pole of residue 1 at $s = 1$. Moreover, he proved that this series satisfies a functional equation which relates the values of $\zeta(s)$ and $\zeta(1-s)$.

In his paper (known as Riemann's Memoire), Riemann described a program in which one can prove the prime number theorem by exploiting the analytic properties of $\zeta(s)$. Let

$$\pi(x) = \#\{p \leq x;\ p \text{ is prime}\}.$$

In the 18^{th} century, Legendre and Gauss conjectured that

$$\pi(x) \sim \frac{x}{\log x}, \quad \text{as } x \to \infty.$$

Following Riemann's program, this conjecture was proved in 1896, independently by Hadamard and de la Vallee Poussin. Shortly after that, de la Vallee Poussin proved a more precise version of this theorem, which involved an error. Using Chebychev's auxiliary function,

$$\psi(x) = \sum_{p^m \leq x} \log p$$

the prime number theorem with the remainder states that

$$\psi(x) = x + \mathrm{O}\left(xe^{-c\sqrt{\log x}}\right),$$

where $c > 0$ is an absolute constant.

Exercise 1. *Does de la Vallee Poussin's theorem imply that*

$$\psi(x) = x + \mathrm{O}\left(x^{1-\epsilon}\right)$$

for some $\epsilon > 0$? How about

$$\psi(x) = x + \mathrm{O}\left(\frac{x}{(\log x)^{\alpha}}\right)$$

for any $\alpha > 0$?

It is conjectured that $\psi(x) = x + \mathrm{O}\left(x^{1/2}(\log x)^2\right)$. This is the celebrated Riemann Hypothesis. We are not planning to describe the above topics in detail, but here we prove a useful general theorem on analytic continuation of Dirchlet series.

Theorem 2. *Let $\{a_m\}_{m=1}^{\infty}$ be a sequence of complex numbersAhat*

$$A(x) = \sum_{m \le x} a_m = \mathrm{O}\left(x^{\delta}\right) \text{ for some } \delta \ge 0.$$

Then the series $\displaystyle\sum_{m=1}^{\infty} \frac{a_m}{m^s}$ converges for $\Re(s) > \delta$ and in this half-plane we have

$$\sum_{m=1}^{\infty} \frac{a_m}{m^s} = s \int_1^{\infty} \frac{A(x)}{x^{s+1}}\, dx.$$

Proof. By the partial summation formula we have

$$\sum_{m \le x} \frac{a_m}{m^s} = \frac{1}{x^s}\left(\sum_{m \le x} a_m\right) + s\left[\int_1^x \left(\sum_{m \le t} a_m\right) \frac{dt}{t^{s+1}}\right]$$

$$= \frac{A(x)}{x^s} + s\left(\int_1^x \frac{A(t)}{t^{s+1}}\, dt\right).$$

Let $s = \sigma + it$ and assume that $\sigma > \delta$. Then, for $C > 0$,

$$\lim_{x \to \infty} \frac{|A(x)|}{x^{\sigma}} \le C \lim_{x \to \infty} \frac{x^{\delta}}{x^{\sigma}} = 0.$$

The above inequality implies that

$$\lim_{x \to \infty} \frac{A(x)}{x^{\sigma}} = 0.$$

On the other hand,

$$\left|\int_1^\infty \frac{A(t)dt}{t^{s+1}}\right| \le \int_1^\infty \frac{dt}{t^{\sigma+1-\delta}} < \infty$$

as $\sigma > \delta$. Thus, sending $x \to \infty$ yields the result. □

Exercise 3. *Prove the following properties of $\zeta(s)$.*

(i) For $\Re(s) > 1$, $\zeta(s) = \prod_p (1 - \frac{1}{p^s})^{-1}$.

(ii) For $\Re(s) > 1$, $\zeta(s) \neq 0$.

(iii) For $\Re(s) > 0$,

$$\zeta(s) = \frac{s}{s-1} - s\int_1^\infty \frac{\{x\}}{x^{s+1}}\,dx,$$

where $\{x\} = x - [x]$.

(iv) The function $\zeta(s)$ has a simple pole of residue 1 at $s = 1$.

The Dedekind Zeta Function.

An extension of the theory of the Riemann zeta function to number fields was initiated by Dedekind in the latter part of the 19^{th} century; however, most of the fundamental results in this subject (conjectured by Dedekind) were proved by Hecke in the early 20^{th} cenutry.

We start by setting up our notation. Let K be a number field. Thus, K is a finite extension of $\mathbb{Q}$. We let $n = [K : \mathbb{Q}]$ be the degree of K over $\mathbb{Q}$ and $\mathfrak{O}_K$ be the ring of integers of K. For a prime $p \in \mathbb{Z}$, the ideal generated by p in $\mathfrak{O}_K$ is denoted by $p\mathfrak{O}_K$. Since $\mathfrak{O}_K$ is a Dedekind domain, we have

$$p\mathfrak{O}_K = \mathfrak{p}_1^{e_1} ... \mathfrak{p}_g^{e_g}$$

where each $\mathfrak{p}_i$ is a prime ideal of $\mathfrak{O}_K$. Since each $\mathfrak{p}_i$ is also a maximal ideal of $\mathfrak{O}_K$, we have that $\mathfrak{O}_K/\mathfrak{p}_i$ is a finite field. In fact, $\mathfrak{O}_K/\mathfrak{p}_i$ is a finite extension of $\mathbb{Z}/p\mathbb{Z}$. Let

$$f_i = [\mathfrak{O}_K/\mathfrak{p}_i : \mathbb{Z}/p\mathbb{Z}].$$

The number e_i is called the ramification index of $\mathfrak{p}_i$, and f_i is called the degree of $\mathfrak{p}_i$ above p (or the decomposition index of $\mathfrak{p}_i$, or the degree of the residue field extension of $\mathfrak{p}_i$). The fundamental relation between these parameters is

$$n = \sum_{i=1}^{g} e_i f_i.$$

Note that this relation implies that $g \le n$. For an ideal $\mathfrak{a}$ of $\mathfrak{O}_K$, we let $\mathrm{N}\mathfrak{a} = |\mathfrak{O}_K/\mathfrak{a}|$. It is known that $\mathrm{N}\mathfrak{a}$ is finite, and moreover $\mathrm{N}\mathfrak{a}$ is completely multiplicative; that is,

$$\mathrm{N}(\mathfrak{a}_1\mathfrak{a}_2) = \mathrm{N}(\mathfrak{a}_1)\mathrm{N}(\mathfrak{a}_2) \text{ for any ideals } \mathfrak{a}_1, \mathfrak{a}_2 \subseteq \mathfrak{O}_K.$$

Furthermore, if $\mathfrak{a} = \langle\alpha\rangle$ is the principal ideal generated by α, then

$$\mathrm{N}(\mathfrak{a}) = \mathrm{N}(\langle\alpha\rangle) = \left|\mathrm{N}_{K/\mathbb{Q}}(\alpha)\right|.$$

Here, $\mathrm{N}_{K/\mathbb{Q}}(\alpha) = \sigma_1(\alpha)\ldots\sigma_n(\alpha)$, where $\sigma_i(\alpha)$ denotes a conjugate of α (Each σ_i denotes an embedding of K to $\mathbb{C}$). Note that for a prime ideal $\mathfrak{p}$ of degree f above p, we have

$$\mathrm{N}\mathfrak{p} = p^f.$$

Example 4. *Let $K = \mathbb{Q}(i)$ be the field of Gaussian rationals; that is,*

$$\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}.$$

It is known that the ring of integers of $K = \mathbb{Q}(i)$ is $\mathfrak{O}_K = \mathbb{Z}[i]$ and that $\mathbb{Q}(i)$ has disciminant $d_K = -4$. Thus, $p = 2$ is the only prime that ramifies in $\mathfrak{O}_K$. Moreover, for any odd prime, we have one of the following:

(i) If $\left(\frac{-4}{p}\right) = \left(\frac{-1}{p}\right) = 1$ then $\mathfrak{p}\mathfrak{O}_K = \mathfrak{p}_1\mathfrak{p}_2$, where $\mathfrak{p}_1 \neq \mathfrak{p}_2$. Thus, $n = 2$, $e_1 = e_2 = 1$, and $f_1 = f_2 = 1$. In this case, we say p splits in $\mathfrak{O}_K$.This happens if $p = 4k + 1$ for some $k \in \mathbb{Z}$.

(ii) If $\left(\frac{-4}{p}\right) = \left(\frac{-1}{p}\right) = -1$ then $\mathfrak{p}\mathfrak{O}_K$ is a prime ideal of $\mathfrak{O}_K$. So, $n = 2$, $e = 1$, and $f = 2$. In this case, we say that p is inert in $\mathfrak{O}_K$. This happens of $p = 4k + 3$ for some $k \in \mathbb{Z}$.

A classical theorem due to Fermat states that an odd prime p is the sum of two squares if and only if $p \equiv 1 \pmod 4$. Fermat's theorem can be regarded as a theorem on the splitting of primes in $\mathbb{Q}(i)$. For example, $5 = 1^2 + 2^2 = (1 + 2i)(1 - 2i)$ and $5\mathfrak{O}_K = \langle 1 + 2i\rangle\langle 1 - 2i\rangle$. Furthermore, we can show that $\langle 1 + 2i\rangle \neq \langle 1 - 2i\rangle$ are distinct prime ideals in $\mathfrak{O}_K$.

Definition 5. *Let K be a number field. For $\Re(s) > 1$ the* Dedekind zeta function *$\zeta_K(s)$ of the number field K is defined by*

$$\zeta_K(s) = \sum_{\mathrm{N}\mathfrak{a} \neq 0} \frac{1}{(\mathrm{N}\mathfrak{a})^s}.$$

We need to show that the above expression is well-defined. Since $\mathrm{N}\mathfrak{a}$ is completely multiplicative and $\mathfrak{O}_K$ is a Dedekind domain for $\Re(s) > 1$, we have

$$\begin{aligned}
\left|\sum_{\mathrm{N}\mathfrak{a} \leq x} \frac{1}{(\mathrm{N}\mathfrak{a})^s}\right| &\leq \sum_{\mathrm{N}\mathfrak{a} \leq x} \frac{1}{(\mathrm{N}\mathfrak{a})^\sigma} \\
&\leq \prod_{\mathrm{N}\mathfrak{p} \leq x} \left(1 + \frac{1}{(\mathrm{N}\mathfrak{p})^\sigma} + \frac{1}{(\mathrm{N}\mathfrak{p})^{2\sigma}} + \ldots\right) \\
&= \prod_{\mathrm{N}\mathfrak{p} \leq x} \left(1 - \frac{1}{(\mathrm{N}\mathfrak{p})^\sigma}\right)^{-1}.
\end{aligned}$$

Note that there are at most $[K:\mathbb{Q}]$ prime ideals above a rational prime p. So,

$$\prod_{\mathrm{N}\mathfrak{p}\leq x}\left(1-\frac{1}{(\mathrm{N}\mathfrak{p})^{\sigma}}\right)^{-1} \leq \prod_{p\leq x}\prod_{i=1}^{g}\left(\frac{1}{1-\frac{1}{p^{f_i\sigma}}}\right)$$

$$\leq \prod_{p\leq x}\left(\frac{1}{1-\frac{1}{p^{\sigma}}}\right)^{g} \leq \prod_{p\leq x}\left(\frac{1}{1-\frac{1}{p^{\sigma}}}\right)^{[K:\mathbb{Q}]}.$$

By sending $x\to\infty$ we get

$$|\zeta_K(s)| \leq |\zeta_K(\sigma)| \leq \zeta(\sigma)^{[K:\mathbb{Q}]}.$$

Thus, $\zeta_K(s)$ is well-defined in the half-plane $\Re(s)>1$.

Exercise 6. *Prove that for $\Re(s)>1$,*

$$\zeta_K(s) = \prod_{\mathfrak{p}}\left(1-\frac{1}{(\mathrm{N}\mathfrak{p})^{s}}\right)^{-1}.$$

Conclude that $\zeta_K(s)\neq 0$ in this half-plane.

Finding an analytic continuation of $\zeta_K(s)$ is a more difficult problem. In fact, it is closely related to counting the ideals of a given norm. Here, we consider it for the special case $K=\mathbb{Q}(i)$.

Theorem 7. *Let $K=\mathbb{Q}(i)$. Then $\zeta_K(s)$ extends analytically to $\Re(s)>\frac{1}{2}$, with an exception of a simple pole of residue $\frac{\pi}{4}$ at $s=1$.*

Proof. Let a_n denotes the number of ideals $\mathfrak{a}$ such that $\mathrm{N}\mathfrak{a}=n$. Then we have

$$\zeta_K(s) = \sum_{\mathfrak{a}}\frac{1}{(\mathrm{N}\mathfrak{a})^{s}} = \sum_{n=1}^{\infty}\frac{a_n}{n^s}.$$

Note that any ideal of $\mathbb{Q}(i)$ has a unique generator $a+ib$, with $a\geq 0$ and $b\geq 0$. This is true since if $\mathfrak{a}=\langle a+bi\rangle$ with $a,b<0$, then $\mathfrak{a}=\langle -a-bi\rangle$. Also if $\mathfrak{a}=\langle a+bi\rangle$ with $a<0$ and $b\geq 0$, then $\mathfrak{a}=\langle -i(a+bi)\rangle=\langle b-ia\rangle$. Thus, to compute

$$A(x)=\sum_{n\leq x}a_n,$$

we only need to compute the number of lattice points (a,b) in the first quadrant inside the disk $a^2+b^2\leq x$. We can show that E

$$A(x)=\frac{\pi}{4}x+\mathrm{O}\left(\sqrt{x}\right)=\frac{\pi}{4}x+E(x).$$

By Theorem 2 we have, for $\sigma > 1$,

$$\zeta_K(s) = s\int_1^\infty \frac{1}{x^{s+1}}\left(\frac{\pi}{4}x + E(x)\right)dx$$

$$= \left(\frac{s}{s-1}\right)\frac{\pi}{4} + s\left(\int_1^\infty \frac{E(x)}{x^{s+1}}\,dx\right).$$

Multiplying both sides of the above equation by $s-1$ yields the identity

$$(s-1)\zeta_K(s) = \frac{\pi s}{4} + s(s-1)\left(\int_1^\infty \frac{E(x)}{x^{s+1}}\,dx\right).$$

Now since $E(x) = \mathrm{O}\left(\sqrt{x}\right)$, for $\Re(s) > \frac{1}{2}$ we have

$$\left|s(s-1)\int_1^\infty \frac{E(x)}{x^{s+1}}\,dx\right| \le |s||s-1|\int_1^\infty \frac{dx}{x^{\sigma+\frac{1}{2}}} < \infty.$$

The proof is complete. □

Exercise 8. *Let $A(x)$ be the number of non-zero lattice points (a,b) that lie within the first quadrant inside the disk $a^2+b^2 \le (\sqrt{x})^2$. Show that*

$$A(x) = \frac{\pi}{4}x + \mathrm{O}\left(\sqrt{x}\right).$$

We next give a desciption for the Dedekind zeta function of the quadratic number field $K = \mathbb{Q}\left(\sqrt{d}\right)$, where d is square free. The disciminant d_K of this field is given by the following formula:

$$d_K = \begin{cases} d & \text{if } d \equiv 1 \pmod 4, \\ 4d & \text{if } d \not\equiv 1 \pmod 4. \end{cases}$$

In order to describe $\zeta_K(s)$, we need the following definition.

Definition 9. *For a nonzero integer a and a positive integer $n = p_1^{e_1}\dots p_k^{e_k}$, the* Kronecker symbol $\left(\frac{a}{n}\right)$ *is defined by*

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{k}\left(\frac{a}{p_i}\right)^{e_i},$$

where $\left(\frac{a}{p_i}\right)$ is the Legendre symbol if p_i is odd and

$$\left(\frac{a}{2}\right) = \begin{cases} 0 & \text{if } a \text{ is even}, \\ 1 & \text{if } a \equiv \pm 1 \pmod 8, \\ -1 & \text{if } a \equiv \pm 3 \pmod 8. \end{cases}$$

Next note that, for $\Re(s) > 1$ and $K = \mathbb{Q}\left(\sqrt{d}\right)$, we have

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{(\mathrm{N}\mathfrak{a})^s} = \sum_{n=1}^{\infty} \frac{a_n}{n^s},$$

where a_n is the number of ideals of $\mathfrak{O}_K$ with norm n.

Exercise 10. *For a prime p, show that $a_p = 1 + \left(\frac{d_K}{p}\right)$ and $a_{p^n} = \sum_{k=0}^{n} \left(\frac{d_K}{p^k}\right)$.*

Theorem 11. *Let $K = \mathbb{Q}\left(\sqrt{d}\right)$. For $\Re(s) > 1$, we have*

$$\zeta_K(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \sum_{\delta | n} \left(\frac{d_K}{\delta}\right) = \zeta(s) \sum_{n=1}^{\infty} \frac{\left(\frac{d_K}{n}\right)}{n^s}.$$

Proof. Let a_n be the number of ideals of norm n. Since the norm is completely multiplicative a_n is also completely multiplicative and thus

$$\zeta_K(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} = \prod_p \left(1 + \frac{a_p}{p^s} + \frac{a_{p^2}}{p^{2s}} + \cdots\right).$$

Replacing the value of a_p from Exercise 10 and employing the multiplicative property of the Kronecker symbol, we have

$$\zeta_K(s) = \prod_p \left(1 + \frac{1 + \left(\frac{d_K}{p}\right)}{p^s} + \frac{1 + \left(\frac{d_K}{p}\right) + \left(\frac{d_K}{p^2}\right)}{p^{2s}} + \cdots\right) = \sum_{n=1}^{\infty} \frac{1}{n^s} \sum_{\delta | n} \left(\frac{d_K}{\delta}\right).$$

□

Theorem 12. *Let $K = \mathbb{Q}\left(\sqrt{d}\right)$ and a_n denote the number of ideals of $\mathfrak{O}_K$ with norm n. Assume*

$$\sum_{\delta \leq |d_K|} \left(\frac{d_K}{\delta}\right) = 0,$$

then we have

$$\sum_{n \leq x} a_n = cx + \mathrm{O}\left(\sqrt{x}\right) \text{ where } c = \sum_{\delta=1}^{\infty} \frac{1}{\delta} \left(\frac{d_K}{\delta}\right).$$

Proof. We employ the Dirichlet hyperbola method. From the proof of Theorem 11, we have

$$\sum_{n\le x} a_n = \sum_{n\le x}\sum_{\delta|n}\left(\frac{d_K}{\delta}\right) = \sum_{\delta e\le x}\left(\frac{d_K}{\delta}\right) = \sum_{\substack{\delta e\le x\\ \delta\le\sqrt{x}}}\left(\frac{d_K}{\delta}\right) + \sum_{\substack{\delta e\le x\\ \delta>\sqrt{x}}}\left(\frac{d_K}{\delta}\right)$$

$$= \sum_{\delta\le\sqrt{x}}\left(\frac{d_K}{\delta}\right)\sum_{e\le\frac{x}{\delta}} 1 \;+\; \sum_{e\le\sqrt{x}}\;\sum_{\substack{\delta\;>\sqrt{x}\\ \delta\le\frac{x}{e}}}\left(\frac{d_K}{\delta}\right)$$

$$= \sum_{\delta\le\sqrt{x}}\left(\frac{d_K}{\delta}\right)\left[\frac{x}{\delta}\right] + \sum_{e\le\sqrt{x}}\left(\sum_{\delta\le\frac{x}{e}}\left(\frac{d_K}{\delta}\right) - \sum_{\delta\le\sqrt{x}}\left(\frac{d_K}{\delta}\right)\right)$$

$$= \sum_{\delta\le\sqrt{x}}\left(\frac{d_K}{\delta}\right)\left(\frac{x}{\delta}+\mathrm{O}(1)\right) \;+\; \sum_{e\le\sqrt{x}}\;\sum_{\delta\le\frac{x}{e}}\left(\frac{d_K}{\delta}\right) - \sum_{e\le\sqrt{x}}\;\sum_{\delta\le\sqrt{x}}\left(\frac{d_K}{\delta}\right).$$

Applying our assumption we conclude that $\left|\sum_{\delta\le x}\left(\frac{d_K}{\delta}\right)\right| \le |d_K|$, and thus the above becomes

$$\sum_{n\le x} a_n = \left(\sum_{\delta\le\sqrt{x}}\frac{\left(\frac{d_K}{\delta}\right)}{\delta}\right)x + \mathrm{O}\left(\sqrt{x}\right) = \left(\sum_{\delta=1}^{\infty}\frac{\left(\frac{d_K}{\delta}\right)}{\delta}\right)x - \left(\sum_{\delta>x}^{\infty}\frac{\left(\frac{d_K}{\delta}\right)}{\delta}\right)x + \mathrm{O}(\sqrt{x}).$$

Noting that $\left|\sum_{\delta>x}\left(\frac{d_K}{\delta}\right)\right| \le |d_K|$, yields

$$\sum_{n\le x} a_n = cx + \mathrm{O}(\sqrt{x}).$$

Note that since $\sum_{\delta\le x}\left(\frac{d_K}{\delta}\right)$ is bounded, the series defining c is convergent. □

Exercise 13. *If K is a quadratic field show that $\zeta_K(s)$ extends to an analytic function on the half-plane $\Re(s) > \frac{1}{2}$, with an exception of a simple pole of residue*

$$c = \sum_{\delta=1}^{\infty}\frac{1}{\delta}\left(\frac{d_K}{\delta}\right).$$

2 Group Characters in Number Fields

The Kronecker symbol $\left(\frac{d_K}{n}\right)$ considered as a function

$$\left(\frac{d_K}{\cdot}\right) \; : \; \mathbb{N} \to \mathbb{C}$$
$$n \longmapsto \left(\frac{d_K}{n}\right)$$

is a completely multiplicative function of period $|d_K|$, with the property that $\left(\frac{d_K}{n}\right) = 0$ if and only if $(n, d_K) \neq 1$. Thus, $\left(\frac{d_K}{n}\right)$ is an example of a (quadratic) Dirichlet character mod $|d_K|$.

Definition 14. *Let $\chi : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$ be a homomorphism of the multiplicative group $(\mathbb{Z}/m\mathbb{Z})^\times$ to the multiplicative group $\mathbb{C}^\times$. We extend χ to $\mathbb{N}$ as follows:*

$$\chi(a) = \begin{cases} \chi(a \bmod m) & \text{if } (a,m) = 1, \\ 0 & \text{if } (a,m) \neq 1\ . \end{cases}$$

Then χ is called a Dirichlet character mod m. *If $\chi(a) = 1$ for all $(a,m) = 1$ and $\chi(a) = 0$ otherwise, then χ is called the* trivial (or principal) character mod m.

Example 15. *(i) The unique non-trivial character mod 3 is*

$$\chi_3(m) = \left(\frac{m}{3}\right) = \begin{cases} 1 & \text{if } m \equiv 1 \pmod 3, \\ -1 & \text{if } m \equiv 2 \pmod 3, \\ 0 & \text{if } m \equiv 0 \pmod 3. \end{cases}$$

(ii) The unique non-trivial character mod 4 is

$$\chi_4(m) = \left(\frac{-4}{m}\right) = \begin{cases} 1 & \text{if } m \equiv 1 \pmod 4, \\ -1 & \text{if } m \equiv 3 \pmod 4, \\ 0 & \text{if } m \equiv 0, 2 \pmod 4. \end{cases}$$

(iii) We have $(\mathbb{Z}/5\mathbb{Z})^\times = \left\{2, 2^2, 2^3, 2^4\right\} = \{2,4,3,1\}$. Thus, for $(m,5) = 1$ we have $m \equiv 2^{\nu_2(m)} \pmod 5$. Define

$$\chi_5(m) = (-1)^{\nu_2(m)} = \begin{cases} 1 & \text{if } m \equiv 1, 4 \pmod 5, \\ -1 & \text{if } m \equiv 2, 3 \pmod 5, \\ 0 & \text{if } m \equiv 0 \pmod 5. \end{cases}$$

Therefore, $\chi_5(m) = \left(\frac{m}{5}\right)$. This is the only real character mod 5.

The set of Dirchlet characters with multiplication forms a group. In general, there are $\varphi(m)$ characters mod m.

Proposition 16. *Dirchlet characters have the following properties.*

(i) Let χ be a nontrivial character mod m. Then we have

$$\left|\sum_{n\le x}\chi(n)\right| \le m.$$

(ii) We have

$$\sum_{\chi \,(\mathrm{mod}\, m)} \overline{\chi}(a)\chi(b) = \begin{cases}\varphi(m) & \text{if } (a,m)=1 \text{ and } a\equiv b \;(\mathrm{mod}\, m),\\ 0 & \text{otherwise .}\end{cases}$$

Proof. (i) Since χ is a non-trivial, there is an $n_0\in\mathbb{N}$ such that $\chi(n_0)\neq 1$. Now let

$$S=\sum_{n\le m}\chi(n) \;=\; \sum_{\substack{n\le m\\ (n,m)=1}}\chi(n).$$

We have

$$\chi(n_0)S=\sum_{\substack{n\le m\\ (n,m)=1}}\chi(n_0 n)=S.$$

Thus, $(\chi(n_0)-1)\,S=0$. Since $\chi(n_0)\neq 1$, we have $S=0$. Now writing $[x]=km+m_0$ for $0\le m_0<m-1$ yields

$$\left|\sum_{n\le x}\chi(n)\right| = \left|\sum_{1\le n\le m_0}\chi(n)\right| \le m_0\le m.$$

(ii) If $(a,m)\neq 1$, then $\overline{\chi}(a)=0$ for all χ and the result follows. Assume that $(a,m)=1$. Then $a\in(\mathbb{Z}/m\mathbb{Z})^\times$ and a^{-1} exists. In this case

$$\overline{\chi}(a)\chi(a)=|\chi(a)|^2=1=\chi(a)\chi(a^{-1}).$$

Therefore, $\overline{\chi}(a)=\chi(a^{-1})$ and we have

$$\sum_{\chi\,(\mathrm{mod}\, m)}\overline{\chi}(a)\chi(b) \;=\; \sum_{\chi\,(\mathrm{mod}\, m)}\chi(a^{-1}b). \tag{1}$$

Now if $a\equiv b\;(\mathrm{mod}\, m)$, then (1) is equal to $\varphi(m)$. Now let $c=a^{-1}b$, and assume that $c\neq 1$. Then there exists a Dirchlet character χ' such that $\chi'(c)\neq 1$ (why?). Let

$$S \;=\; \sum_{\chi\,(\mathrm{mod}\, m)}\chi(a^{-1}b)=\sum_{\chi\,(\mathrm{mod}\, m)}\chi(c).$$

This implies that

$$\chi'(c)S \;=\; \sum_{\chi \pmod m} (\chi'\chi)(c) \;=\; S.$$

Thus, $(\chi'(c)-1)S = 0$. Since $\chi'(c) \neq 1$, we have $S = 0$.

□

Definition 17. *For $\Re(s) > 1$ the* Dirichlet L-function $L(s,\chi)$ *associated to the Dirichlet character χ is defined as*

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}.$$

Exercise 18. *Prove the following properties of Dirchlet L-functions.*

(i) *Show that $L(s,\chi)$ converges absolutely for $\Re(s) > 1$.*

(ii) *If χ is non-trivial, show that $L(s,\chi)$ extends to an analytic function for $\Re(s) > 0$. What can we say for the trivial character χ_0?*

(iii) *For $\Re(s) > 1$, show that*

$$L(s,\chi) = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}.$$

(iv) *For $\Re(s) > 1$, show that*

$$\log L(s,\chi) = \sum_p \frac{\chi(p^n)}{np^{ns}}.$$

The Dirichlet L-functions naturally appear as factors of the Dedekind zeta function of cyclotomic fields. If ζ_m is a primitive mth root of unity we call $K = \mathbb{Q}(\zeta_m)$ a *cyclotomic field*. We can show that

$$\zeta_K(s) = \zeta(s) \prod_{\chi \neq \chi_0} L(s,\chi).$$

It is clear that this identity shows that, for $\Re(s) > 1$

$$\prod_{\chi \pmod m} L(s,\chi)$$

is a Dirichlet series with non-negative coefficients. Since we have not established this identity, we will provide a direct proof of this fact.

Proposition 19. *For $\Re(s) > 1$, if*

$$f(s) = \prod_{\chi} L(s,\chi) = \sum_{n=1}^{\infty} \frac{c_n}{n^s},$$

then $c_n \geq 0$.

Proof. We have

$$\log f(s) = \sum_{\chi} \log L(s,\chi) = \sum_{\chi}\sum_{p,n} \frac{\chi(p^n)}{np^{ns}}.$$

Applying Proposition 16 (ii) with $a = 1$, we have

$$\log f(s) \quad = \sum_{\substack{p,n \\ p^n \equiv 1 \pmod m}} \frac{\varphi(m)}{np^{ns}}.$$

Thus,

$$f(s) = \exp\left(\sum_{\substack{p,n \\ p^n \equiv 1 \pmod m}} \frac{\varphi(m)}{np^{ns}} \right),$$

which is a Dirichlet series with non-negative coefficients. □

From the theory of Dirichlet series we know that to any Dirchlet series we can correspond a half-plane $\sigma > \sigma_c$ of convergence and a half-plane $\sigma > \sigma_a$ of absolute convergence. One can prove that $\sigma_c - \sigma_a \leq 1$. σ_c (resp. σ_a) is called the abscissa of convergence (resp. the abscissa of absolute convergence) of the Dirichlet series.

A good reference for Dirichlet series is Titchmarsh's "Theory of Functions," which includes a proof of the following theorem of Landau regarding abscissa of convergence of a Dirichlet series with non-negative coefficients.

Theorem 20 (Landau). *Let $\{a_n\}_{n=1}^{\infty}$ be a sequence of non-negetive real numbers and let*

$$f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s},$$

be the Dirichlet series corrsponding to this sequence. If $f(s)$ has abscissa of convergence σ_c, then $f(s)$ is holomorphic in $\Re(s) > \sigma_c$ and $s = \sigma_c$ is a singular point of $f(s)$.

Theorem 21. *Let $L(s,\chi)$ be a Dirichlet L-function and $\chi \neq \chi_0$. Then $L(1,\chi) \neq 0$.*

Proof. From Proposition 19, we know that

$$f(s) = \prod_{\chi} L(s,\chi) = \exp\left(\sum_{\substack{p,n \\ p^n \equiv 1 \pmod m}} \frac{\varphi(m)}{np^{ns}} \right),$$

is a Dirichlet series with non-negetive coefficients. Assume that there exists a non-trivial character χ such that $L(1,\chi) = 0$. Then $f(s)$ will be holomorphic on $\Re(s) > 0$ (the zero of $L(s,\chi)$ at $s = 1$ will cancel the simple pole of $L(s,\chi_0)$ at $s = 1$). However,

$$f\left(\frac{1}{\varphi(m)}\right) = \exp\left(\varphi(m) \sum_{\substack{p,n \\ p^n \equiv 1 \pmod m}} \frac{1}{np^{\frac{n}{\varphi(m)}}} \right) \geq \exp\left(\sum_{p \nmid m} \frac{1}{p} \right) = \infty.$$

This is a contradiction, as f is holomorphic on $\Re(s) > 0$. Thus, $L(s,\chi) \neq 0$ for all $\chi \neq \chi_0$. □

In the above proof, we have used the fact that

$$\sum_p \frac{1}{p} = \infty.$$

Euler proved this for the first time and concluded that the set of primes is infinite. With his proof Euler pioneered the use of analytic techniques in number theory. The starting point of his proof is the product formula (which is now known as the Euler product), for $\zeta(s)$. Assume $s \in \mathbb{R}$. Then,

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}.$$

Taking the natural lograthim of both sides, we have

$$\log \zeta(s) = -\sum_p \log\left(1 - \frac{1}{p^s}\right) = \sum_p \sum_{n=1}^{\infty} \frac{1}{np^{ns}}.$$

By splitting the last sum, we arrive at

$$\log \zeta(s) = \sum_p \frac{1}{p^s} + \sum_{p,n\geq 2} \frac{1}{np^{ns}}. \tag{2}$$

Observe that,

$$\left|\sum_{p,n\geq 2} \frac{1}{np^{ns}}\right| \leq \sum_{p,n\geq 2} \frac{1}{p^{ns}} = \sum_p \frac{\frac{1}{p^{2s}}}{1-\frac{1}{p^s}} = \sum_p \frac{1}{p^s(p^s-1)}.$$

Now as $s \to 1^+$, we have

$$\lim_{s\to 1^+} \sum_p \frac{1}{p^s(p^s-1)} = \sum_p \frac{1}{p(p-1)} < \infty.$$

Thus, sending s to 1^+, in both sides of (2), we get

$$\lim_{s\to 1^+} \log \zeta(s) = \sum_p \frac{1}{p} + \sum_{p,n\geq 2} \frac{1}{np^n}.$$

Since $\lim\limits_{s\to 1^+} \zeta(s) = \infty$ and the sum over $p, n \geq 2$ is convergent, we conclude that

$$\sum_p \frac{1}{p} = \infty.$$

In early 19th century, Dirichlet adapted the above argument to show that, for $(m,a) = 1$, there are infinitely many primes in the arithmetic progression $p \equiv a \pmod{m}$.

Theorem 22 (Dirichlet). *For $(m,a) = 1$ we have*

$$\sum_{p\equiv a \ (\mathrm{mod}\ m)} \frac{1}{p} = \infty.$$

Proof. The proof is basically Euler's proof, which instead of $\zeta(s)$ one considers

$$\prod_{\chi \pmod m} L(s,\chi)^{\overline{\chi}(a)}.$$

For real $s>1$ we have

$$\sum_{\chi \pmod m} \overline{\chi}(a)\log L(s,\chi) = \sum_{\chi \pmod m} \overline{\chi}(a) \sum_{p,n} \frac{\chi(p^n)}{np^{ns}}.$$

Thus,

$$\sum_{\chi \pmod m} \overline{\chi}(a)\log L(s,\chi) = \sum_{p,n} \frac{1}{np^{ns}} \left(\sum_{\chi \pmod m} \overline{\chi}(a)\chi(p^n) \right)$$

$$= \sum_{p^n\equiv a \pmod m} \frac{\varphi(m)}{np^{ns}}.$$

Similar to Euler's proof, we split the last sum to get

$$\frac{1}{\varphi(m)} \sum_{\chi \pmod m} \overline{\chi}(a)\log L(s,\chi) = \sum_{p\equiv a \pmod m} \frac{1}{p^s} + \sum_{\substack{n\geq 2 \\ p^n\equiv a \pmod m}} \frac{1}{np^{ns}}. \tag{3}$$

Now by Theorem 21, $L(1,\chi)\neq 0$ for $\chi\neq\chi_0$. Also,

$$L(s,\chi_0) = \prod_{p|m} \left(1-\frac{1}{p^s}\right)\zeta(s)$$

has a simple pole of residue $\frac{\varphi(m)}{m}$ at $s=1$. Therefore the left-hand-side of the above identity approaches ∞, as $s\to 1^+$. On the other hand the sum over $n\geq 2$ in the right-hand-side converges as $s\to 1^+$. Thus, sending $s\to 1^+$ in the above identity implies the result. □

Definition 23. *Let S be a subset of primes. We say that S has* Dirichlet density *α if*

$$\lim_{s\to 1^+} \frac{\sum_{n\in S} \frac{1}{n^s}}{\log\zeta(s)} = \alpha.$$

Here, we consider s as a real variable.

Exercise 24. *Show that*

(i) If S has a positive Dirichlet density, then S is infinite.

(ii) Theorem 22 implies that the Dirichlet density of primes congruent to a mod m is $\frac{1}{\varphi(m)}$.

Hecke L-functions are a generalization of Dirichlet L-functions to number fields. These L-functions are attached to charachters of the ideal class group or more generally generalized ideal class group (ray class group). By using Hecke L-functions, we can formulate and prove a generalization of Dirichlet's theorem as a statement on Dirichlet density of prime ideals in a certain generalized ideal class. We will not pursue this line of thoughts any further, instead we are going to consider another generalization of Dirichlet's theorem by using the charachters of $\mathrm{Gal}(\mathbb{Q}(\zeta_m):\mathbb{Q})$. But before doing this we will describe some applications of primes in arithmetic progressions in certain problems in classical number theory.

3 Primes in Arithmetic Progressions

Shortly after the proof of the prime number theorem, de la Vallee Poussin proved a stronger version of Dirichlet's theorem. He proved that the set of primes congruent to a mod m in fact has natural density $\frac{1}{\varphi(m)}$. In other words, for $(a,m)=1$,

$$\lim_{x\to\infty} \frac{\#\ \{p \leq x \mid p \equiv a \pmod{m}\}}{\#\ \{p \leq x\}} = \frac{1}{\varphi(m)}.$$

We denote $\#\ \{p\leq x\} = \pi(x)$ and $\#\ \{p \leq x \mid p \equiv a \pmod{m}\} = \pi(x;m,a)$. Having this notation,de la Vallee Poussin's theorem can be written as:

Theorem 25 (de la Vallee Poussin). *For $(a,m)=1$, we have*

$$\pi(x;m,a) = \frac{\pi(x)}{\varphi(m)}(1+o(1)), \text{ as } x\to\infty.$$

An important issue here is the uniformity of the above estimate as m varies. In other words we would like to have estimates with constants independent of m. We follow with the statement of three important theorems and one conjecture in this topic.

Theorem 26 (Brun-Titchmarsch). *The inequality*

$$\pi(x;m,a) \leq \frac{2x}{\varphi(m)\log(\frac{x}{m})}$$

holds for all $1\leq a < m$ with $(a,m)=1$ and $m \leq x$.

Theorem 27 (Siegel-Walfisz). *Let $A>0$ be any fixed constant. Then there exists a positive constant $B = B(A)$ depending on A, such that*

$$\pi(x;m,a) = \frac{\pi(x)}{\varphi(m)} + \mathrm{O}\left(x\exp\left(-B\sqrt{\log x}\right)\right)$$

holds for large values of x uniformly for $1\leq a < m$ with $(a,m)=1$ and $m < (\log x)^A$.

Conjecture 28 (GRH). *As $x \to \infty$, we have*

$$\pi(x;m,a) = \frac{\pi(x)}{\varphi(m)} + \mathrm{O}(x^{1/2}\log mx),$$

for all integers $1 \le a < m$, with $(a,m) = 1$.

Note that the above asymptotic relation is non-trivial for only $m \le x^{1/2-\varepsilon}$. In fact Conjecture 28 does not imply Theorem 26. The following theorem shows that Conjecture 28 holds on average.

Theorem 29 (Bombieri-Vinogradov). *For every constant $A > 0$, there exists a positive constant $B = B(A)$ depending on A, such that for large values of x, we have*

$$\sum_{m < \frac{x^{1/2}}{(\log x)^B}} \max_{\substack{1\le a<m \\ (a,m)=1 \\ y\le x}} \left| \pi(y;m,a) - \frac{\pi(y)}{\varphi(m)} \right| \ll \frac{x}{(\log x)^A}.$$

Note. The above theorem can be stated in terms of the logarithmic integral

$$\mathrm{Li}(x) = \int_2^x \frac{dt}{\log t},$$

instead of $\pi(x)$. The above statement can also be expressed in terms of $\theta(x)$ or $\psi(x)$.

An integer a with $(a,p) = 1$ is called a *primitive root mod p*, if $\langle a\rangle = (\mathbb{Z}/p\mathbb{Z})^\times$. In othe words a is a primitive root mod p if order of a mod $p = \mathrm{ord}_p(a) = p-1$. For a given prime p, we have $\varphi(p-1)$ primitive roots. Thus, $\frac{\varphi(p-1)}{p-1}$ is the average number of primitive roots mod p. In other words for fixed p, the proportion of primitive roots mod p is $\frac{\varphi(p-1)}{p-1}$. In the next theorem, we find the proportion of primitive roots mod p on average over p.

Theorem 30. *We have*

$$\frac{1}{\pi(x)} \sum_{p\le x} \frac{\varphi(p-1)}{p-1} \sim \prod_p \left(1 - \frac{1}{p(p-1)}\right),$$

as $x \to \infty$. The constant $A = \prod_p \left(1 - \frac{1}{p(p-1)}\right)$ is called the Artin constant.

Proof. First of all observe that

$$\frac{\varphi(n)}{n} = \prod_{p|n}(1-\frac{1}{p}) = \sum_{d|n}\frac{\mu(d)}{d}.$$

By employing this identity, we have

$$\sum_{p\le x}\frac{\varphi(p-1)}{p-1} = \sum_{p\le x}\sum_{d|p-1}\frac{\mu(d)}{d} = \sum_{d\le x-1}\frac{\mu(d)}{d} \sum_{\substack{p\le x \\ p\equiv 1 \ (\mathrm{mod}\ d)}} 1.$$

Thus,

$$\sum_{p\leq x}\frac{\varphi(p-1)}{p-1}=\sum_{d\leq x-1}\frac{\mu(d)}{d}\pi(x;d,1).$$

Now by Theorem 27 (Siegel-Walfisz), for $A>1$, there exists $B=B(A)>0$ such that

$$\sum_{d\leq(\log x)^A}\frac{\mu(d)}{d}\left(\frac{\mathrm{Li}(x)}{\varphi(d)}+\mathrm{O}\left(xe^{-B\sqrt{\log x}}\right)\right)+\sum_{d>(\log x)^A}\frac{\mu(d)}{d}\pi(x;d,1). \tag{4}$$

Now we observe the trivial bound

$$\pi(x;d,1)\leq\frac{x}{d}.$$

By an application of this bound in (4), for any $\alpha>0$, we have

$$\sum_{p\leq x}\frac{\varphi(p-1)}{p-1}=\mathrm{Li}(x)\sum_{d\leq(\log x)^A}\frac{\mu(d)}{d\varphi(d)}+\mathrm{O}\left(\frac{x\log x}{(\log x)^\alpha}\right)+\mathrm{O}\left(x\sum_{d>(\log x)^A}\frac{1}{d^2}\right).$$

Therefore, by employing $\varphi(d)\gg\frac{d}{\log\log d}$, we have

$$\sum_{p\leq x}\frac{\varphi(p-1)}{p-1}=\mathrm{Li}(x)\sum_{d=1}^{\infty}\frac{\mu(d)}{d\varphi(d)}+\mathrm{O}\left(\mathrm{Li}(x)\int_{(\log x)^A}^{\infty}\frac{\log\log t}{t^2}dt\right)+\mathrm{O}\left(\frac{x}{(\log x)^A}\right).$$

From here we deduce the desired result. □

Exercise 31. *Fill in the details in Theorem* 30*.*

Exercise 32. *Show that*
(i)

$$\sum_{d^2|n}\mu(d)=\begin{cases}1 & \text{if } n \text{ is squarefree,}\\ 0 & \text{if } n \text{ is not squarefree.}\end{cases}$$

(ii) (Knobloch-Mirsky)

$$\frac{1}{\pi(x)}\#\{p\leq x;\ p-1 \text{ is squarefree}\}\sim\prod_p\left(1-\frac{1}{p(p-1)}\right),$$

as $x\to\infty$. In other words, the natural density of primes p for which $p-1$ is squarefree is the Artin constant.

Exercise 33. *Derive the Knobloch-Mirsky's result by an application of Theorem* 29 *(Bombieri-Vinogradov).*

Let $\tau(n)$ be the number of divisors of n. If $n=p_1^{\alpha_1}...p_k^{\alpha_k}$, then

$$\tau(n)=(\alpha_1+1)...(\alpha_k+1).$$

It can be shown that $\tau(n) \ll_\epsilon n^\epsilon$ and

$$\sum_{n\le x} \tau(n) = x\log x + \mathrm{O}(x).$$

Thus, the average order of $\tau(n)$ is $\log n$. In 1930, Titchmarsh studied the behaviour of

$$\sum_{p\le x} \tau(p-\ell),$$

where ℓ is fixed. He conjectured an asymptotic formula for this sum and proved it under the assumption of GRH. Later in 1961, Linnik proved the asymptotic formula unconditionally using his disperssion method. The following unconditional proof is due to Rodriquez (1965) and, independently, Halberstam (1966). We state the theorem for $\ell = 1$. The proof for general ℓ is similar.

Theorem 34 (**Titchmarsh Divisor Problem).** *We have*

$$\sum_{p\le x} \tau(p-1) = \frac{\zeta(2)\zeta(3)}{\zeta(6)} x + \mathrm{O}\left(x \frac{\log\log x}{\log x}\right).$$

Proof. We start bmng the sum in terms of $\pi(x;m,1)$ as m varies. We have

$$\sum_{p\le x} \tau(p-1) = \sum_{p\le x} \sum_{m|p-1} 1 = \sum_{m\le x-1} \sum_{\substack{p\le x \\ p\equiv 1 \pmod m}} 1.$$

Thus,

$$\sum_{p\le x} \tau(p-1) = \sum_{m\le x-1} \pi(x;m,1).$$

Now by Dirichlet hyperbola method, we have

$$\sum_{p\le x} \tau(p-1) = \sum_{\substack{m,k \\ p-1=mk \\ p\le x}} 1 = \sum_{m\le\sqrt{x-1}} \sum_{\substack{\sqrt{x-1}<k\le \frac{x-1}{m} \\ km=p-1 \\ p\le x}} 1 + \sum_{k\le\sqrt{x-1}} \sum_{\substack{\sqrt{x-1}<m\le \frac{x-1}{k} \\ km=p-1 \\ p\le x}} 1 + \sum_{k\le\sqrt{x-1}} \sum_{\substack{m\le\sqrt{x-1} \\ km=p-1 \\ p\le x}} 1.$$

Since the first two sums are equal, we have the above

$$\begin{aligned} &= 2\sum_{m\le\sqrt{x-1}} \sum_{\substack{m\sqrt{x-1}+1<p\le x \\ p\equiv 1 \pmod m}} 1 + \sum_{m\le\sqrt{x-1}} \sum_{\substack{p\le m\sqrt{x-1}+1 \\ p\equiv\ 1 \pmod m}} 1. \\ &= \sum_{m\le\sqrt{x-1}} \left[2\left(\pi(x;m,1) - \pi(m\sqrt{x-1}+1;m,1)\right) + \pi(m\sqrt{x-1}+1;m,1)\right]. \end{aligned}$$

Thus,

$$\sum_{p\leq x}\tau(p-1)=2\sum_{m\leq\sqrt{x-1}}\pi(x;m,1)-\sum_{m\leq\sqrt{x-1}}\pi(m\sqrt{x-1}+1;m,1) \tag{5}$$

Now by Theorem 29, given $A=1$, there is $B>0$ such that

$$\sum_{m\leq\frac{\sqrt{x-1}}{(\log x)^B}}\left|\pi(x;m,1)-\frac{\mathrm{Li}(x)}{\varphi(m)}\right|\ll\frac{x}{\log x}. \tag{6}$$

By employing (6) in (5), we have

$$\begin{aligned}\sum_{p\leq x}\tau(p-1)= {} & 2\sum_{m\leq\frac{\sqrt{x-1}}{(\log x)^B}}\frac{\mathrm{Li}(x)}{\varphi(m)}+\mathrm{O}\left(\frac{x}{\log x}\right)+2\sum_{\frac{\sqrt{x-1}}{(\log x)^B}<m\leq\sqrt{x-1}}\pi(x;m,1)\\ &-\sum_{m\leq\sqrt{x-1}}\pi\left(m\sqrt{x-1}+1;m,1\right).\end{aligned}$$

Now by applying Theorem 26 in the last two sums, we get

$$\begin{aligned}\sum_{p\leq x}\tau(p-1)={} & 2\ \mathrm{Li}(x)\sum_{m\leq\frac{\sqrt{x-1}}{(\log x)^B}}\frac{1}{\varphi(m)}+\mathrm{O}\left(\frac{x}{\log x}\right)+\mathrm{O}\left(\frac{x}{\log x}\sum_{\frac{\sqrt{x-1}}{(\log x)^B}<m\leq\sqrt{x-1}}\frac{1}{\varphi(m)}\right)\\ &+\mathrm{O}\left(\sum_{m\leq\sqrt{x-1}}\frac{m\sqrt{x-1}+1}{\varphi(m)\log(\sqrt{x-1}+\frac{1}{m})}\right).\end{aligned}$$

The result follows from the above identity and the following exercise. □

Exercise 35. *For $\Re(s)>0$, show that*

$$\sum_{n=1}^{\infty}\frac{1}{\varphi(n)n^s}=\zeta(s+1)\prod_p\left(1+\frac{1}{p^{s+1}(p-1)}\right).$$

Conclude that the Dirichlet series has a simple pole of residue $\prod_p\left(1+\frac{1}{p(p-1)}\right)$ *at* $s=0$*. Use Perron's formula to deduce that*

$$\sum_{n\leq x}\frac{1}{\varphi(n)}\sim\prod_p\left(1+\frac{1}{p(p-1)}\right)\log x,$$

as $x\to\infty$*. Show that*

$$\prod_p\left(1+\frac{1}{p(p-1)}\right)=\frac{\zeta(2)\zeta(3)}{\zeta(6)}\approx 1.943596...$$

The above constant is called the Titchmarsh-Linnik constant. Next we describe another interpretation of the Titchmarsh divisor problem that can be generalized to other settings, such as a geometric setting involving elliptic curves. In order to describe our new interpretation, we first need a generalization of Dirichlet's theorem on primes in arithmetic progressions.

4 The Chebotarev Density Theorem

Recall that the Dirichlet theorem for primes in arithmetic progressions states that for $(a,m)=1$, the Dirichelt density of prime numbers p such that $p\equiv a \pmod{m}$ is $\frac{1}{\varphi(m)}$. We know that de la Vallee Poussin proved that in this statement the Dirichlet density can be replaced by the natural density. Thus,

$$\lim_{x\to\infty}\frac{\#\ \{p\leq x;\ p\equiv a \pmod{m}\}}{\#\{p\leq x\}}=\frac{1}{\varphi(m)}.$$

The Chebotarev theorem is a generalization of the above assertion. This theorem was first formulated by Frobenius as a conjecture and later in 1922 was proved by Chebotarev. This theorem also is closely related to a theorem of Frobenius regarding the composition types of a polynomial modulo primes p. Here, we describe Frobenius' theorem.

Let f be a polynomial with integer coefficients. Let G be the Galois group of f over $\mathbb{Q}$. Thus, each element of G can be considered as a permutation of the roots of f. For a prime p, we say that f has a *decomposition type* $(n_1,n_2,...,n_t)$ if f reduces to a product of irreducible polynomials of degree $n_1,n_2,...,n_t$ respectively. For example, let

$$f(x)=x^4+3x^2+7x+4.$$

Then the decomposition type mod 2 of f is $(1,3)$, since

$$f(x)=x(x^3+x+1) \pmod{2}.$$

Also the decomposition type mod 11 of f is $(2,2)$, as

$$f(x)=(x^2+5x-1)(x^2-5x-4) \pmod{11}.$$

The Frobenius' theorem states that the density of primes p with a certain type is equal to the proportion of elements of the Galois group of the polynomial with the same cycle pattern.

Theorem 36 (Frobenius). *Let $f\in\mathbb{Z}[x]$ and G be its Galois group. Then*

$$\lim_{x\to\infty}\frac{\#\ \{p\leq x;\ f \text{ has decomposition type } (n_1,n_2,...,n_t)\}}{\#\ \{p\leq x\}}$$
$$=\frac{\#\ \{\sigma\in G;\ \sigma \text{ has the cycle pattern } (n_1,n_2,...,n_t)\}}{|G|}.$$

As an application of this theorem, by considering $f(x)=x^m-1$, we can recover Dirichlet's theorem in certain cases (however not always). For example, for $m=12$, it can be shown that the decomposition type of $x^{12}-1$ depends only on the residue class of $p \mod 12$. More precisely,

$$\begin{aligned}
&p\equiv 1 \pmod{12} \text{ has decomposition type } (1,1,1,1,1,1,1,1,1,1,1,1),\\
&p\equiv 5 \pmod{12} \text{ has decomposition type } (1,1,1,1,2,2,2,2),\\
&p\equiv 7 \pmod{12} \text{ has decomposition type } (1,1,1,1,1,1,2,2,2),\\
&p\equiv 11 \pmod{12} \text{ has decomposition type } (1,1,2,2,2,2,2).
\end{aligned}$$

Thus in this case Frobenius' theorem recovers Dirichlet's theorem. However, this is not the case always. For example for $x^{10}-1$, we have

$$\begin{aligned}
&p \equiv 1 \pmod{10} \text{ has decomposition type } (1,1,1,1,1,1,1,1,1,1),\\
&p \equiv 3,7 \pmod{10} \text{ has decomposition type } (1,1,4,4),\\
&p \equiv 9 \pmod{10} \text{ has decomposition type } (1,1,2,2,2,2).
\end{aligned}$$

Frobenius conjectured that instead of decomposition type of elements of the Galois group of f, one can correspond to each prime a class of conjugacy elements of the Galois group in a way that one can recover Dirchlet's theorem in the case $f(x)=x^m-1$. We next describe this conjecture (which is now a theorem).

Let $K/\mathbb{Q}$ be a Galois extension of $\mathbb{Q}$ with $\mathrm{Gal}(K/\mathbb{Q})=G$. Note that if $\mathfrak{p}$ is a prime ideal of $\mathfrak{O}_K$, then so is $\sigma(\mathfrak{p})$ for any $\sigma \in G$. For each prime $p \in \mathbb{Z}$, we have

$$p\mathfrak{O}_K = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}.$$

By uniqueness of factorization, we deduce that G acts on the set of prime ideals $\mathfrak{p}_1,\dots,\mathfrak{p}_r$ that lie above a fixed prime ideal p.

Exercise 37. *Show that the action of the Galois group on the set of prime ideals lying above a fixed prime of $\mathbb{Z}$ is a transitive action.*

For a prime $\mathfrak{p}$ in $\mathfrak{O}_K$, the *decomposition group* of $\mathfrak{p}$, denoted $D_{\mathfrak{p}}$, is defined by

$$D_{\mathfrak{p}} = \{\sigma \in G \mid \sigma(\mathfrak{p}) = \mathfrak{p}\}.$$

Note that for each $\sigma \in D_{\mathfrak{p}}$ we can construct a $\mathbb{Z}/p\mathbb{Z}$ automorphism of $\mathfrak{O}_K/\mathfrak{p}$, because $\mathfrak{p}$ is invariant under all $\sigma \in D_{\mathfrak{p}}$. More precisely, we can consider the map

$$\phi : D_{\mathfrak{p}} \to \mathrm{Gal}(\mathfrak{O}_K/\mathfrak{p} : \mathbb{Z}/p\mathbb{Z})$$

$$\sigma \longmapsto \overline{\sigma}$$

where

$$\overline{\sigma} : \mathfrak{O}_K/\mathfrak{p} \to \mathfrak{O}_K/\mathfrak{p}$$

$$x + \mathfrak{p} \longmapsto \sigma(x) + \mathfrak{p}.$$

Exercise 38. *Show that ϕ is a well-defined surjective homomorphism.*

Let $I_{\mathfrak{p}} = \ker(\phi)$. Then $I_{\mathfrak{p}}$ is called the *inertia group* of $\mathfrak{p}$. We have

$$I_{\mathfrak{p}} = \{\sigma \in D_{\mathfrak{p}};\ \sigma(a) - a \in \mathfrak{p} \text{ for all } a \in \mathfrak{O}_K\}.$$

By the fundamental theorem of homomorphism, we have

$$D_{\mathfrak{p}}/I_{\mathfrak{p}} \cong \mathrm{Gal}(\mathfrak{O}_K/\mathfrak{p} : \mathbb{Z}/p\mathbb{Z}).$$

Now the finite field $\mathfrak{O}_K/\mathfrak{p}$ is a finite Galois extension of $\mathbb{Z}/p\mathbb{Z}$ and thus its Galois group is generated by the Frobenius automorphism $x \longmapsto x^p$. Since ϕ is surjective, the Frobenius automorphism can be lifted to an element $\sigma_{\mathfrak{p}}$ of $D_{\mathfrak{p}}$ which is well-defined mod $I_{\mathfrak{p}}$. We have

$$\sigma_{\mathfrak{p}}(x) \equiv x^p \pmod{\mathfrak{p}}, \text{ for all } x \in \mathfrak{O}_K.$$

We can show that for $\mathfrak{p}$ above an unramified p we have $I_{\mathfrak{p}} = \{1\}$. Thus if p is unramified, then for any $\mathfrak{p}$ above p there is a unique lifting of the Frobenius at p, which is denoted by $\sigma_{\mathfrak{p}}$.

Now suppose that $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are two primes above an unramified prime p. Then there exists $\eta \in \mathrm{Gal}(K/\mathbb{Q})$ such that $\eta\mathfrak{p}_1 = \mathfrak{p}_2$. Now if $\sigma_{\mathfrak{p}_1}$ is the lifting of the Frobenius at p corresponding to $\mathfrak{p}_1$ and $\sigma_{\mathfrak{p}_2}$ is the lifting corresponding to $\mathfrak{p}_2$, then

$$\sigma_{\mathfrak{p}_2} = \eta \circ \sigma_{\mathfrak{p}_1} \circ \eta^{-1}.$$

In other words any two liftings of the Frobenius at p are conjugate. Thus, we can consider the conjugacy class

$$\sigma_p = \{\sigma_{\mathfrak{p}};\ \mathfrak{p} \text{ lies above } p\}.$$

The conjugacy class σ_p is called the *Artin Symbol* (or the *Frobenius conjugacy class*) of p (or at p).

Theorem 39 **(Chebotarev).** *Let $K/\mathbb{Q}$ be a finite Galois extension of $\mathbb{Q}$ with the Galois group G. Let $C \subseteq G$ be closed under conjugation. Then*

$$\lim_{x\to\infty} \frac{\#\ \{p \leq x;\ p \text{ is unramified and } \sigma_p \subseteq C\}}{\#\ \{p \leq x\}} = \frac{|C|}{|G|}.$$

In other words, Artin symbols are uniformly distributed in the conjugacy classes.

Definition 40. *A prime $p \in \mathbb{Z}$ is said to* split completely *in $\mathfrak{O}_K$ if*

$$p\mathfrak{O}_K = \mathfrak{p}_1\mathfrak{p}_2 ... \mathfrak{p}_n, \text{ where } n = [K : \mathbb{Q}].$$

The fundamental relation

$$n = \sum_{i=1}^{g} e_i f_i$$

implies that if p splits completely then $e_i = f_i = 1$, for all $1 \leq i \leq n$. From here we conclude that the *residue field extension* $(\mathfrak{O}_K/\mathfrak{p})/(\mathbb{Z}/p\mathbb{Z})$ is trivial, and thus $D_{\mathfrak{p}} = I_{\mathfrak{p}} = \{1\}$. We deduce that p splits completely in $\mathfrak{O}_K$ if and only if $\sigma_p = \{1\}$. Thus, the following holds.

Theorem 41. *The set of primes p which split completely in $\mathfrak{O}_K$ has density $\frac{1}{[K:\mathbb{Q}]}$.*

Note that for $K = \mathbb{Q}(\zeta_m)$, the above theorem can be deduced from the Frobenius theorem. In this case we have $\mathfrak{O}_K = \mathbb{Z}[\zeta_m]$, and so one can show that a prime p splits completely in $\mathfrak{O}_K$ if and only if the polynomial $x^m - 1$ splits over $\mathbb{Z}/p\mathbb{Z}$ as a product of linear irreducible polynomials. In other words in this case $x^m - 1$ has a decomposition type over $\mathbb{Z}/p\mathbb{Z}$ in the form $(1,1,...,1)$ with m ones. By the Frobenius theorem the density of such primes is $\frac{1}{\varphi(m)}$.

Now we describe σ_p in the cyclotomic field $\mathbb{Q}(\zeta_m)$. It is known that the only ramified primes p in $\mathbb{Q}(\zeta_m)$ are odd primes $p|m$ and also 2 if $m \equiv 0 \pmod 4$. Also

$$\mathrm{Gal}(\mathbb{Q}(\zeta_m) : \mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^{\times},$$

which is an Abelian group. Thus, for any unramified prime, we have that σ_p has only one element. On the other hand for a prime $\mathfrak{p}$ lying above p, we have

$$\sigma_{\mathfrak{p}}(x) \equiv x^p \pmod{\mathfrak{p}} \text{ for all } x \in \mathbb{Z}[\zeta_m].$$

Now assume that $p \neq 2$ is unramified. Then $(p,m) = 1$. For a prime $\mathfrak{p}$ lying above p, we have $\sigma_{\mathfrak{p}} : \zeta_m^a \longmapsto \zeta_m^p$, where $(a,m) = 1$. Thus,

$$\sigma_{\mathfrak{p}}(\zeta_m) = \zeta_m^a \equiv \zeta_m^p \pmod{\mathfrak{p}}.$$

Therefore, for $p \equiv a \pmod m$ we consider the automorphism $\eta_a : \zeta_m \longmapsto \zeta_m^a$ as the unique element of σ_p. In other words, primes $p \equiv a \pmod m$ can be identified by η_a which is an element of $\mathrm{Gal}(\mathbb{Q}(\zeta_m) : \mathbb{Q})$. Applying the Chebotarev theorem in this setting yeilds

$$\lim_{x\to\infty} \frac{\#\ \{p \leq x;\ p \equiv a \pmod m\}}{\#\ \{p \leq x\}} = \lim_{x\to\infty} \frac{\#\ \{p \leq x;\ \sigma_p = \{\eta_a : \zeta_m \longmapsto \zeta_m^a\}\}}{\#\ \{p \leq x\}} = \frac{1}{\varphi(m)}.$$

So we recover Dirichlet's theorem for primes in arithmetic progressions as a cyclotomic case of the Chebotarev density theorem.

Now in analogy with $\pi(x;m,a)$, we define for $C \subset G = \mathrm{Gal}(K/\mathbb{Q})$, which is closed under conjugation, the following prime counting function:

$$\Pi_C(x;K/\mathbb{Q}) := \#\{p \leq x;\ p \text{ is a prime of } \mathbb{Q} \text{ unramified in } K \text{ such that } \sigma_p \subset C\},$$

where σ_p is the Frobenius conjugacy class (Artin Symbol) corresponding to p in $\mathrm{Gal}(K/\mathbb{Q})$. Then the Chebotarev density theorem can be stated as

$$\prod_C(x;K/\mathbb{Q}) \sim \frac{|C|}{|G|}\mathrm{Li}(x), \text{ as } x \to \infty.$$

It is natural to ask whether theorems similar to Brun-Titchmarsh, Siegel-Walfisz, or Bombieri-Vinogradov theorem are known in this context. The versions of these theorems for $\Pi_C(x;K/\mathbb{Q})$ are known, although the results are much weaker than the cyclotomic case (the primes in arithmetic progressions case). One statement that holds with a quality similar to the cyclotomic case, is an effective version of the Chebotarev density theorem under the assumption of GRH. By the GRH (Generalized Riemann Hypothesis) we mean that the Dedekind zeta function $\zeta_K(s)$ does not have any zero in the half-plane $\Re(s) > 1/2$. The following theorem is due to Lagarias and Odlyzko, (with contribution from Serre).

Theorem 42 (Effective Chebotarev). *Let $K/\mathbb{Q}$ be a finite Galois extension with Galois group G. Let $C \subset G$ be closed under conjugation and assume the GRH for K. Then*

$$\Pi_C(x;K/\mathbb{Q}) = \frac{|C|}{|G|}\mathrm{Li}(x) + \mathrm{O}\left(|C|x^{\frac{1}{2}}\log\left(|G|\left(\prod_{p\in P(K/\mathbb{Q})} p\right)x\right)\right),$$

where $P(K/\mathbb{Q})$ is the set of rational primes that ramify in K and the constant appearing in the O-notation is absolute and effectively computable.

Exercise 43. *Let d be an integer that is not a perfect square. Prove that the density of the set of primes p such that $\left(\frac{d}{p}\right) = 1$ is $\frac{1}{2}$.*

Exercise 44. *If a natural number n is a square mod p for a set of primes p which has density bigger than $\frac{1}{2}$, show that n must be a square.*

Exercise 45. *Let q be prime. Show that the set of primes p for which $p \equiv 1 \pmod q$ and $2^{\frac{p-1}{q}} \equiv 1 \pmod p$ has density $\frac{1}{q(q-1)}$.*

5 Analytic Problems for Elliptic Curves

Recall that in the cyclotomic field $\mathbb{Q}(\zeta_m)$ a prime $p \neq 2$ splits completely if and only if $p \equiv 1 \pmod m$. We can also show that $p = 2$ splits completely in $\mathbb{Q}(\zeta_m)$ if and only if $m = 1, 2$. Now we reformulate the Titchmarsh divisor problem using the above splitting criterion. Let

$$\mathcal{C} = \{\mathbb{Q}(\zeta_m);\ m = 1, 2, ...\}$$

be the family of cyclotomic fields. For $p \neq 2$, let

$$\tau_{\mathcal{C}}(p) = \#\ \{m;\ p \text{ splits completely in } \mathbb{Q}(\zeta_m)\} = \tau(p-1).$$

Therefore, we can find the following formulation of the Titchmarsh divsor problem.

Titchmarsh Divsor Problem (New Version). Study the asymptotic behaviour of

$$\sum_{2<p\leq x} \tau_{\mathcal{C}}(p),$$

as $x \to \infty$.

The above formulation allows us to formulate a non-cyclotomic version of the Titchmarsh divisor problem. Observe that the m-th roots of unity can be constructed as the kernel of the map

$$\lambda_m : \mathbb{C}^\times \to \mathbb{C}^\times$$

$$z \longmapsto z^m.$$

Note that $\ker(\lambda_m)$ is the collection of the m-th roots of unity, or equivalently $\ker(\lambda_m)$ consists of complex numbers of multiplicative order dividing m. Having this in mind we describe an analogous situation arising from the theory of elliptic curves. Let

$$E : y^2 = x^3 + ax + b, \text{ where } a, b \in \mathbb{Z},$$

be a cubic curve. We assume that the polynomial $x^3 + ax + b$ has distinct roots in $\mathbb{C}$ and thus the cubic curve is non-singular (an elliptic curve). Let $\mathcal{O}$ denote the point at ∞. It is known that

$$E(\mathbb{C}) = \left\{(x, y) \in \mathbb{C} \times \mathbb{C};\ y^2 = x^3 + ax + b\right\} \cup \{\mathcal{O}\}$$

forms an abelian group with $\mathcal{O}$ as its identity element. We denote the group operation with $+$, thus if $P, Q \in E(\mathbb{C})$ then $P + Q \in E(\mathbb{C})$. For any positive integer m, we define a map

$$\lambda_m : E(\mathbb{C}) \to E(\mathbb{C})$$

$$P \longmapsto mP = P + P + ... + P \ (m\text{-times}).$$

We denote the kernel of λ_m by $E[m]$. Thus,

$$E[m] = \ker(\lambda_m) = \{P \in E(\mathbb{C});\ mP = \mathcal{O}\}.$$

The group $E[m]$ is the set of points of order dividing m. It is called the *m-torsion subgroup* of $E(\mathbb{C})$. It has m^2 elements. Let

$$E[m] = \left\{(x_1, y_1), ..., (x_{m^2-1}, y_{m^2-1}), \mathcal{O}\right\}.$$

Let

$$\mathbb{Q}(E[m]) = \mathbb{Q}(x_1, y_1, ..., x_{m^2-1}, y_{m^2-1})$$

be the field obtained by joining the coordinates of the m-torsion points of E to $\mathbb{Q}$.

Theorem 46. *The field of $\mathbb{Q}(E[m])$ is a finite Galois extension of $\mathbb{Q}$ which contains the m-th cyclotomic field; that is,*

$$\mathbb{Q}(\zeta_m) \subseteq \mathbb{Q}(E[m]).$$

Proof. Let $\sigma : \mathbb{Q}(E[m]) \to \mathbb{C}$ be an embedding (field homomorphism). Let $P \in E[m]$. Then we have

$$\mathcal{O} = \sigma(\mathcal{O}) = \sigma(mP) = m\sigma(P).$$

Therefore, $\sigma(P) \in E[m]$. This shows that $\sigma(\mathbb{Q}(E[m])) \subseteq \mathbb{Q}(E[m])$. In fact, $\sigma(\mathbb{Q}(E[m])) = \mathbb{Q}(E[m])$ (why?). Thus every embedding of $\mathbb{Q}(E[m])$ to $\mathbb{C}$ in fact is an embedding to $\mathbb{Q}(E[m])$. Therefore $\mathbb{Q}(E[m])$ is a Galois extension of $\mathbb{Q}$. Moreover, any element of the Galois group can be considered as a permutation of the m^2 points in $E[m]$. This shows that the coordinates of m-torsion points are algebraic (otherwise the Galois group was infinite). Since an extension formed by adjoining finitely many algebraic numbers to $\mathbb{Q}$ is finite, $\mathbb{Q}(E[m])$ is a finite extension of $\mathbb{Q}$. Finally the fact that $\mathbb{Q}(\zeta_m) \subset \mathbb{Q}(E[m])$ is a consequence of the Weil pairing. □

For an example illustrating the above theorem we can consider the elliptic curve

$$E : y^2 = x^3 + x.$$

Then we have

$$\mathbb{Q}(E[3]) = \mathbb{Q}\left(i, \frac{\sqrt[4]{8\sqrt{3}-12}}{9}\right) \supset \mathbb{Q}(\zeta_3) \supset \mathbb{Q}$$

and

$$\mathbb{Q}(E[4]) = \mathbb{Q}(i, \sqrt{2}) \supset \mathbb{Q}(\zeta_4) \supset \mathbb{Q}.$$

We are ready to state a non-cyclotomic analouge of the Titchmarsh divisor problem. We consider the following family of fields

$$\mathcal{E} = \left\{\mathbb{Q}(E[m]);\ m \in \mathbb{N}\right\}.$$

For $p \neq 2$ we define the *elliptic divisor function* by

$$\tau_{\mathcal{E}}(p) = \#\ \left\{m \in \mathbb{N};\ p \text{ splits completely in } \mathbb{Q}(E[m])\right\}.$$

Note that $\tau_{\mathcal{E}}(p)$ is well-defined, since if p splits completely in $\mathbb{Q}(E[m])$, then it splits in $\mathbb{Q}(\zeta_m)$ and thus $p \equiv 1 \pmod{m}$. In other words, only divsors of $p-1$ can contribute to $\tau_{\mathcal{E}}(p)$ and so $\tau_{\mathcal{E}}(p) < \infty$.

Elliptic Titchmarsh Divisor Problem. Study the asymptotic behaviour of

$$\sum_{2<p\leq x} \tau_{\mathcal{E}}(p),$$

as $x \to \infty$.

We can easily formulate a conjecture on this problem. Note that

$$\begin{aligned}\sum_{2<p\leq x} \tau_{\mathcal{E}}(p) &= \sum_{2<p\leq x} \#\ \left\{m \in \mathbb{N};\ p \text{ splits completely in } \mathbb{Q}(E[m])\right\}\\ &= \sum_{m\leq x-1} \pi_{\mathcal{E}}(x;m),\end{aligned}$$

where

$$\pi_{\mathcal{E}}(x;m) = \ \#\ \left\{2 < p \leq x;\ p \text{ splits completely in } \mathbb{Q}(E[m])\right\}.$$

From the Chebotarev density theorem, we know that

$$\pi_{\mathcal{E}}(x;m) \sim \frac{1}{|G_m|}\ \mathrm{Li}(x),\ \text{ as } x \to \infty,$$

where $G_m = \mathrm{Gal}(\mathbb{Q}(E[m]):\mathbb{Q})$. Therefore,

$$\begin{aligned}\sum_{2<p\leq x} \tau_{\mathcal{E}}(p) &= \sum_{m\leq x-1} \pi_{\mathcal{E}}(x;m)\\ &\approx \sum_{m\leq x-1} \frac{1}{|G_m|}\ \mathrm{Li}(x)\\ &\approx \left(\sum_{m=1}^{\infty} \frac{1}{|G_m|}\right)\frac{x}{\log x},\end{aligned}$$

as $x\to\infty$. So the behaviour of $\tau_{\mathcal{E}}(p)$ on average over primes is different from the behaviour of $\tau(p-1)$ on average over primes. This is expected as $\tau_{\mathcal{E}}(p)$ is a smaller function when compared to $\tau(p-1)$.

There are important theorems regarding the size of G_m. These theorems show that the size of G_m intimately depends on the size of the endomorphism ring of E. For any $m\in\mathbb{Z}$ the map $P\longmapsto mP$, where P is a point of E, is an endomorphism of E. Thus the ring of endomorphisms of E at least contains $\mathbb{Z}$. Now if $\mathrm{End}(E)\supsetneqq\mathbb{Z}$ we say that E has *complex multiplication*, otherwise if $\mathrm{End}(E)=\mathbb{Z}$, we say that E does not have complex multiplication. The following two theorems state that $|G_m|\approx m^2$ if E has complex multiplication and $|G_m|\approx m^4$ if E does not have complex multiplication.

Theorem 47 (**Deuring**). *If E has complex multiplcation and $\mathrm{End}(E)\cong\mathfrak{O}_K$, where K is an imaginary quadratic field, then for $m\geq 3$, we have $|G_m| = 2|\widetilde{G}_m|$. Here $\widetilde{G}_m$ is a subgroup of bounded index of $(\mathfrak{O}_K/m\mathfrak{O}_K)^\times$. By a subgroup of bounded index we mean that there exists a number $i(E)$, depending only on E, such that*

$$\left[(\mathfrak{O}_K/m\mathfrak{O}_K)^\times : \widetilde{G}_m\right] \leq i(E).$$

Note that

$$\left|(\mathfrak{O}_K/m\mathfrak{O}_K)^\times\right| = m^2\prod_{\mathfrak{p}|\langle m\rangle}\left(1-\frac{1}{\mathrm{N}\mathfrak{p}}\right).$$

Theorem 48 (**Serre**). *If E is an elliptic curve without complex multiplication, then there exists a constant $i(E)$, depending only on E, such that*

$$[\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) : G_m] \leq i(E),$$

where

$$\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) = \left\{\begin{pmatrix} a & b\\ c & d\end{pmatrix};\ a,b,c,d\in\mathbb{Z}/m\mathbb{Z} \text{ and } ad-bc\not\equiv 0 \pmod{m}\right\}.$$

Note that

$$|\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})| = m^2\varphi(m)^2\prod_{p|m}\left(1+\frac{1}{p}\right).$$

We now provide another description of $\tau_{\mathcal{E}}(p)$. In order to do this we need some facts on reduction mod p of elliptic curves. Let $E: y^2 = x^3+ax+b$ be an elliptic curve defined over $\mathbb{Z}$. We call a prime p a good prime, if p does not divide $\Delta = 4a^3 + 27b^2$. For a prime p, E_p is the elliptic curve over $\mathbb{F}_p$ (the finite field of p elements). By Mordell's theorem, we know that $E(\mathbb{Q})$ is a finitely generated group. Thus,

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{tor}}.$$

The following assertion provides a desciption of $E_p(\mathbb{F}_p)$.

Proposition 49. *There are two positive integers $i(p)$ and $e(p)$ such that*

$$E_p(\mathbb{F}_p) \cong (\mathbb{Z}/i(p)\mathbb{Z}) \oplus (\mathbb{Z}/e(p)\mathbb{Z}),$$

and $i(p) \mid e(p)$. Moreover, $i(p) \leq \sqrt{p} + 1$.

Proof. Since $E_p(\mathbb{F}_p)$ is an abelain group, it has a finite exponent. Let $e(p)$ be the the exponent of $E_p(\mathbb{F}_p)$. So $e(p)$ is the maximum order of elements of $E_p(\mathbb{F}_p)$. Since elements of $E_p(\mathbb{F}_p)$ are torsion points and $E_p(\mathbb{F}_p)$ has exponet $e(p)$, we conclude that

$$E_p(\mathbb{F}_p) \subseteq E_p[e(p)] \subseteq \mathbb{Z}/e(p)\mathbb{Z} \oplus \mathbb{Z}/e(p)\mathbb{Z}.$$

Thus, there exists $i(p)$ such that $i(p) \mid e(p)$ and

$$E_p(\mathbb{F}_p) \cong (\mathbb{Z}/i(p)\mathbb{Z}) \oplus (\mathbb{Z}/e(p)\mathbb{Z}).$$

(Note that since $(\mathbb{Z}/i(p)\mathbb{Z}) \oplus (\mathbb{Z}/i(p)\mathbb{Z}) \cong E_p[i(p)]$, we have $(p, i(p)) = 1$.) Moreover,

$$n_p(E) = p + 1 - a_p(E) = i(p)^2 e'(p),$$

where $e(p) = i(p)e'(p)$. Thus,

$$i(p)^2 e'(p) \leq p + 1 + 2\sqrt{p} = (\sqrt{p} + 1)^2.$$

Here we use the fact that from Hasse's bound we know that

$$|a_p(E)| \leq 2\sqrt{p}.$$

From the above we conclude that $i(p) \leq \sqrt{p} + 1$.

□

In the above proposition $e(p)$ is the exponent of $E_p(\mathbb{F}_p)$ and $i(p)$ is the index of the maximal cyclic subgroup of $E_p(\mathbb{F}_p)$.

We can describe $i(p)$ as the index of the maximal subgroup of $E_p(\mathbb{F}_p)$. The following proposition establishes a close link between primes that split completely in $\mathbb{Q}(E[m])$ and $i(p)$.

Proposition 50. *Let p be an odd prime of good reduction. Then p splits completely in $\mathbb{Q}(E[m])$ if and only if $m \mid i(p)$.*

Proof. Assume that $m \mid i(p)$. Then $E_p[m] \subseteq E_p(\mathbb{F}_p)$. Note that in this case $E_p[m] \cong (\mathbb{Z}/m\mathbb{Z}) \oplus (\mathbb{Z}/m\mathbb{Z})$ and thus $p \nmid m$. From the theory of elliptic curves we know that if $p \nmid m\Delta_E$ (where Δ_E is the discriminant of E) then p is unramified in $\mathbb{Q}(E[m])$. Now assume that $\mathfrak{p}$ is a prime lying above p in $K = \mathbb{Q}(E[m])$. Then $\mathfrak{O}_K/\mathfrak{p} \cong \mathbb{Z}/p\mathbb{Z}(E_p[m])$ (why?). Since $E_p[m]$ is defined over $\mathbb{Z}/p\mathbb{Z}$, we have $\mathbb{Z}/p\mathbb{Z}(E_p[m]) = \mathbb{Z}/p\mathbb{Z}$. Thus, the residue field extension is trivial and so $\sigma_{\mathfrak{p}} = 1$. Thus, $\sigma_p = \{1\}$ and p splits completely in K.

Conversely, suppose that p splits completely in K. Then p splits completely in $\mathbb{Q}(\zeta_m)$ and so $p \nmid m$. Again in this case $\mathfrak{O}_K/\mathfrak{p} \cong \mathbb{Z}/p\mathbb{Z}(E_p[m])$ (why?), for any prime $\mathfrak{p}$ above p. Since p splits completely, then $\sigma_{\mathfrak{p}} = 1$. Thus, $x^p \equiv x \pmod{\mathfrak{p}}$ for all $x \in \mathfrak{O}_K$. This implies that the Galois group of the residue field extension is trivial and thus $\mathbb{Z}/p\mathbb{Z}(E_p[m]) = \mathbb{Z}/p\mathbb{Z}$. Thus, $E_p[m] \subseteq E_p(\mathbb{F}_p)$, and so $m \mid i(p)$. □

Note that in the above proof we used $\mathbb{Z}/p\mathbb{Z}$ and $\mathbb{F}_p$ as two different notations for the finite field of p elements. Our next goal is a conditional (under the assumption of GRH) asymptotic formula for

$$\sum_{2<p\leq x} \tau_{\mathcal{E}}(p).$$

In order to do this we need to establish a Brun-Titchmarsh type inequality for the prime counting function $\pi_{\mathcal{E}}(x;m)$.

Proposition 51 (Cojocaru-Ram Murty). *We have*

$$\pi_{\mathcal{E}}(x;m) \ll \frac{x^{3/2}}{m^3}.$$

Proof. Let $p \neq 2$ be a good prime that splits completely in $E_m = \mathbb{Q}(E[m])$. Then p splits completely in $\mathbb{Q}(\zeta_m)$ and thus $p \equiv 1 \pmod{m}$. On the other hand by Proposition 50, we have

$$m^2 \mid \# E_p(\mathbb{F}_p) = p + 1 - a_p.$$

Since $p \equiv 1 \pmod{m}$, this implies that

$$a_p \equiv 2 \pmod{m}.$$

Since $|a_p| \leq 2\sqrt{p}$, we conclude that

$$\pi_{\mathcal{E}}(x;m) \quad \leq \sum_{\substack{|c|\leq 2\sqrt{x} \\ c\equiv 2 \pmod{m}}} \pi(x;m^2,c-1), \tag{7}$$

where

$$\pi(x;m^2,c-1) = \# \left\{p \leq x;\ p \equiv c-1 \pmod{m^2}\right\}.$$

Applying the trivial bound

$$\pi(x;m^2,c-1) \ll \frac{x}{m^2}$$

in (7) yields the result. □

We are now ready to conditionally prove an elliptic version of the Titchmarsh divisor problem.

Theorem 52 (Akbary-Ghioca). *Under the assumption of GRH for the Dedekind zeta function of* $\mathbb{Q}(E[m])$*, we have*

$$\sum_{p\leq x}\tau(i(p))=\left(\sum_{m=1}^{\infty}\frac{1}{[\mathbb{Q}(E[m]):\mathbb{Q}]}\right)\operatorname{Li}(x)+\mathrm{O}\left(x^{\frac{5}{6}}(\log x)^{\frac{2}{3}}\right).$$

Proof. From Proposition 50, we have

$$\sum_{2<p\leq x}\tau(i(p))=\sum_{m\leq\sqrt{x}+1}\Pi_{\mathcal{E}}(x;m,1).$$

Note that from Proposition 49, we know that $i(p)\leq\sqrt{p}+1$. Thus if $m\mid i(p)$, where $p\leq x$, we get $m\leq\sqrt{x}+1$. We break this interval to two ranges. In the first range we apply Theorem 42 and in the second range we apply Proposition 51. We have

$$\begin{aligned}\sum_{m<2\sqrt{x}+1}\pi_{\mathcal{E}}(x;m)&=\sum_{m\leq\frac{x^{1/3}}{(\log x)^{1/3}}}\pi_{\mathcal{E}}(x;m)+\sum_{\frac{x^{1/3}}{(\log x)^{1/3}}<m\leq\sqrt{x}+1}\pi_{\mathcal{E}}(x;m)\\&=\sum_{m\leq\frac{x^{1/3}}{(\log x)^{1/3}}}\left(\frac{1}{[\mathbb{Q}(E[m]):\mathbb{Q}]}\operatorname{Li}(x)+\mathrm{O}\left(x^{1/2}\log(mx)\right)\right)\\&\qquad+\sum_{\frac{x^{1/3}}{(\log x)^{1/3}}<m\leq\sqrt{x}+1}\frac{x^{3/2}}{m^{3}}.\end{aligned}$$

Simplifying the above will give the result. □

6 Suggestions for Further Readings

Knobloch-Mirsky's problem can be re-interpreted as a problem on the asymptotic density of primes that do not split completely in any cyclotomic field $\mathbb{Q}(\zeta_{m^2})$ with $m>1$. One can replace the family $\{\mathbb{Q}(\zeta_{m^2});\ m>1\}$ with other families. Serre's cyclicity problem is an instance of this problem for the family of division fields $\{\mathbb{Q}(E[m]);\ m>1\}$.

Serre's Cyclicity Problem. Study the asymptotic behaviour of

$$\#\{p\leq x;\ E_p(\mathbb{F}_p)\text{ is cyclic}\}.$$

This is equivalent to the study of

$$\#\{p\leq x;\ i(p)=1\}$$

or equivalently

$$\#\{p \leq x;\ p \text{ never splits completely in } \mathbb{Q}(E[m]) \text{ for any } m > 1\}.$$

Similarly given a non-square integer a, one can ask about the asymptotic density of primes p for which a is a primitive root mod p.

Artin's Primitive Root Problem. Study the asyptotic behaviour of

$$\#\{p \leq x;\ a \text{ is a primitive root mod } p\}.$$

One can show that this is equivalent to the study of

$$\#\{p \leq x;\ p \text{ never splits completely in } \mathbb{Q}(\zeta_m, a^{1/m}) \text{ for and } m > 1\}.$$

So Artin's primitive root problem is related to studying splitting of primes in Kummerian fields $\mathbb{Q}(\zeta_m, a^{1/m})$.

In the other direction Titchmarsh divisor problem and its elliptic and Kummerian analogues are related to the study of the asymptotics for primes that split completely in certain family of extensions of $\mathbb{Q}$.

$\mathbb{Q}(\zeta_m)$	$\mathbb{Q}(E[m])$	$\mathbb{Q}\left(\zeta_m, a^{\frac{1}{m}}\right)$
Knobloch-Mirsky's Problem	Serre's Cyclicity Problem	Artin's Primitive Root Problem
Titchmarsh Divisor Problem	Elliptic Divisor Problem	Kummerian Divisor Problem

For basic algebraic and analytic number theory see [11] and [12]. References [3], [7], and [9] include a wide variety of analytic problems in number fields and elliptic curves. For Mirsky's problem see [8]. For the results on Serre's cyclicity problem see [2], [4], and [10]. For a conditional proof of Artin's primitive root problem see [6]. For elliptic and Kummerian variants of the Titchmarsh divisor problem see [1] and [5].

7 Solutions

Solution 1. The answer to the first question is no. For the second question the answer is yes. Note that

$$x^{-\epsilon} = e^{-\epsilon \log x} \text{ and } (\log x)^{\alpha} = e^{\alpha \log\log x}.$$

Solution 3.

(i) This is a consequence of the unique factorization property of integers (the fundamental theorem of arithmetic).

(ii) This follows from (i) and the fact that $(1 - \frac{1}{p^s})^{-1} \neq 0$ for $\Re(s) > 1$.

(iii) By applying Theorem 2, for $\Re(s) > 1$, we have

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = s \int_1^{\infty} \frac{[x]}{x^{s+1}}\, dx$$

$$= s \int_1^{\infty} \frac{x - \{x\}}{x^{s+1}}\, dx$$

$$= \frac{s}{s-1} - \int_1^{\infty} \frac{\{x\}}{x^{s+1}}\, dx.$$

The result follows since, for $\Re(s) > 0$,

$$\left| \int_1^{\infty} \frac{\{x\}}{x^{s+1}} \right| \le \int_1^{\infty} \frac{dx}{x^{s+1}} < \infty.$$

(iv) Multiplying the two sides of the expression for $\zeta(s)$ in (iii) by $(s-1)$ and sending $s \to 1$ gives the result.

Solution 6. The proof is similar to the proof for $\zeta(s)$.

Solution 8. We divide such lattice points into the following two sets:

$$B_1(x) = \Big\{(a,b) \neq (0,0);\ a,b \ge 0 \text{ and } (a+1)^2 + (b+1)^2 \le x\Big\}$$

$$B_2(x) = \Big\{(a,b) \neq (0,0);\ a,b \ge 0,\ a^2 + b^2 \le x, \text{ and } (a,b) \notin B_1(x)\Big\}.$$

It is clear from our choice of the above sets that

$$\#\ B_1(x)\ \le\ \frac{\pi}{4} x \le \#B_1(x)\ +\ \#B_2(x) = A(x). \tag{8}$$

Now, if $(a,b) \in B_2(x)$ then $\left(\sqrt{x} - \sqrt{2}\right)^2 \le a^2 + b^2 \le (\sqrt{x})^2$. Thus, we have

$$\#\ B_2(x)\ \le\ \pi(x) - \pi\left(\sqrt{x} - \sqrt{2}\right)^2 = \mathrm{O}\left(\sqrt{x}\right).$$

Therefore, from (8), we have

$$0\ \le A(x) - \frac{\pi}{4}\ x\ \le\ \#\ B_2(x)\ \le\ c\sqrt{x},$$

for some $c > 0$. This gives the desired result.

Solution 10. We consider cases. If p is ramified then $p \mid d_K$, thus $\left(\frac{d_K}{p}\right) = 0$ and $a_p = 1 = 1 + \left(\frac{d_K}{p}\right)$. If p splits, then either p is odd or $p = 2$ and $d_K \equiv -1 \pmod 8$. In both these cases, $\left(\frac{d_K}{p}\right) = 1$. Thus, $a_p = 2 = 1 + \left(\frac{d_K}{p}\right)$. If p is inert then either p is odd and $\left(\frac{d_K}{p}\right) = -1$, or $p = 2$ and $d_K \equiv -3 \pmod 8$ (thus $\left(\frac{d_K}{p}\right) = -1$). Therefore, $a_p = 0 = 1 + \left(\frac{d_K}{p}\right)$.

Solution 13. The solution is identical to the proof of Theorem 7, considering the asymptotic formula given in Theorem 12.

Solution 24.

(i) From the definition of Dirichlet density we conclude the existence of a δ such that if $1 < s < 1 + \delta$ then

$$\sum_{n \in S} \frac{1}{n^s} > \frac{\alpha}{2} \log \zeta(s).$$

Sending $s \to 1^+$, we have $\sum_{n \in S} \frac{1}{n} = \infty$, which implies that S is infinite.

(ii) From the identity (3) we have

$$\frac{1}{\varphi(m)} \sum_{\chi \ (\mathrm{mod}\ m)} \overline{\chi}(a) \frac{\log L(s,\chi)}{\log \zeta(s)} = \frac{1}{\log \zeta(s)} \sum_{p \equiv a \ (\mathrm{mod}\ m)} \frac{1}{p^s} + \frac{1}{\log \zeta(s)} \sum_{\substack{p, n \geq 2 \\ p^n \equiv a \ (\mathrm{mod}\ m)}} \frac{1}{np^{ns}}.$$

Now sending $s \to 1^+$ in the left-hand side results in $\frac{1}{\varphi(m)}$ (why?). Thus,

$$\lim_{s \to 1^+} \frac{\sum_{p \equiv a \ (\mathrm{mod}\ m)} \frac{1}{p^s}}{\log \zeta(s)} = \frac{1}{\varphi(m)}.$$

Solution 32. (*ii*) By part (*i*), the quantity to estimate is

$$\sum_{p \leq x} \sum_{d^2 | p-1} \mu(d).$$

This can be done in a manner similar to Theorem 30. We have

$$\sum_{p \leq x} \sum_{d^2 | p-1} \mu(d) = \sum_{d \leq \sqrt{x-1}} \mu(d) \pi(x; d^2, 1).$$

The latter is equal to

$$\sum_{d \leq (\log x)^A} \mu(d) \left(\frac{\mathrm{Li}(x)}{\varphi(d^2)} + \mathrm{O}(xe^{-B\sqrt{\log x}}) \right) + \mathrm{O}\left(\sum_{d > (\log x)^A} \frac{x}{d^2} \right).$$

Now observing that $\varphi(d^2) = d\varphi(d)$ and following steps similar to Theorem 30 yield the result.

Solution 37. Suppose that the action is not transitive. Thus, there are two prime ideals $\mathfrak{p}_1$ and $\mathfrak{p}_2$ above a prime p such that

$$\mathfrak{p}_2 \neq \sigma\mathfrak{p}_1 \text{ for all } \sigma \in \mathrm{Gal}(K/\mathbb{Q}) = G.$$

Since $\mathfrak{p}_2$ and $\sigma\mathfrak{p}_1$ (for all $\sigma \in G$) are prime (and thus maximal) ideals, we know, by the Chinese remainder theorem, that there is an $x \in \mathfrak{O}_K$ such that

$$\begin{cases} x \equiv 0 \pmod{\mathfrak{p}_2}, \\ x \equiv 1 \pmod{\sigma\mathfrak{p}_1}, \text{ for all } \sigma \in G. \end{cases}$$

Now since $x \in \mathfrak{p}_2$, then $\mathrm{N}(x) \in \langle p \rangle = \mathfrak{p}_1 \cap \mathbb{Z}$. Therefore, $\mathrm{N}(x) \in \mathfrak{p}_1$. Since $\mathfrak{p}_1$ is a prime ideal, then there exists $\sigma \in G$ such that $\sigma(x) \in \mathfrak{p}_1$ and thus $x \equiv 0 \pmod{\sigma^{-1}\mathfrak{p}_1}$. This is a contradiction with our assumption that $x \equiv 1 \pmod{\sigma^{-1}\mathfrak{p}_1}$. Thus, there is $\sigma \in G$ such that $\mathfrak{p}_2 = \sigma\mathfrak{p}_1$.

Solution 43. Let d_0 be the square-free part of d. Then the density in question is the same as the density of primes p such that $\left(\frac{d_0}{p}\right) = 1$. An odd prime with $\left(\frac{d_0}{p}\right) = 1$ is an unramified prime which splits completely in $\mathbb{Q}(\sqrt{d_0})$. For such primes p the corresponding $\sigma_p = \{1\}$. By the Chebotarev density theorem the density of such primes is $\frac{1}{2}$.

Solution 44. Suppose that n is not a square. Then $\mathbb{Q}(\sqrt{n})$ is a quadratic field. By Exercise 43, the set of primes p for which $\left(\frac{n}{p}\right) = 1$ has density $\frac{1}{2}$. This is a contradiction. Thus, n must be a perfect square.

Solution 45. We aim at proving that a prime p satisfies the conditions $p \equiv 1 \pmod{q}$ and $2^{\frac{p-1}{q}} \equiv 1 \pmod{p}$ if and only if p splits completely in the Kummerian field $K = \mathbb{Q}(\zeta_q, 2^{\frac{1}{q}})$. Then the result follows from the fact that K is a Galois extension of degree $q(q-1)$ of $\mathbb{Q}$ by an application of the Chebotarev density theorem.

Now suppose that p splits completely in K then $(p, 2q) = 1$. Let $\mathfrak{p}$ be a prime lying above p. Then the lifting $\sigma_{\mathfrak{p}}$ satisifies

$$\sigma_{\mathfrak{p}}(x) \equiv x^p \pmod{\mathfrak{p}} \text{ for all } x \in \mathfrak{O}_K.$$

On the other hand $\sigma_{\mathfrak{p}}(x) \in \mathrm{Gal}(K/\mathbb{Q})$, thus $\sigma_{\mathfrak{p}}(\zeta_q) = \zeta_q^a$, where $(a, q) = 1$ and $\sigma_{\mathfrak{p}}(2^{\frac{1}{q}}) = 2^{\frac{1}{q}}$ for $i = 0, 1, ..., q-1$. Since p splits completely, then $\sigma_{\mathfrak{p}}(x) = x$, and thus

$$\sigma_{\mathfrak{p}}(\zeta_q) = \zeta_q \equiv {\zeta_q}^p \pmod{\mathfrak{p}}$$

and

$$\sigma_{\mathfrak{p}}(2^{\frac{1}{q}}) = 2^{\frac{1}{q}} \equiv 2^{\frac{p}{q}} \pmod{\mathfrak{p}}.$$

Since the above relations hold for any prime above p, we conclude that $\zeta_q = {\zeta_q}^p$ and $2^{\frac{p-1}{q}} \equiv 1 \pmod{p}$. Thus, $p \equiv 1 \pmod{q}$ and $2^{\frac{p-1}{q}} \equiv 1 \pmod{p}$.

Conversely, suppose that $p \equiv 1 \pmod{q}$ and $2^{\frac{p-1}{q}} \equiv 1 \pmod{p}$. Then $(p, 2q) = 1$. Moreover for any prime lying above p, like $\mathfrak{p}$, we have

$$\zeta_q{}^p \equiv \zeta_q \pmod{\mathfrak{p}} \text{ and } 2^{\frac{p}{q}} \equiv 2^{\frac{1}{q}} \pmod{\mathfrak{p}}.$$

Thus, $\sigma_{\mathfrak{p}} = 1$ for any prime lying above p and thus $\sigma_p = \{1\}$. In other words, p splits completely in K.

References

[1] Amir Akbary and Dragos Ghioca, *A geometric variant of Titchmarsh divisor problem*, Int. J. Number Theory **8** (2012), no. 1, 53–69, DOI 10.1142/S1793042112500030. MR2887882

[2] Amir Akbary and V. Kumar Murty, *An analogue of the Siegel-Walfisz theorem for the cyclicity of CM elliptic curves mod p*, Indian J. Pure Appl. Math. **41** (2010), no. 1, 25–37, DOI 10.1007/s13226-010-0002-4. MR2650098

[3] Alina Carmen Cojocaru, *Questions about the reductions modulo primes of an elliptic curve*, Number theory, CRM Proc. Lecture Notes, vol. 36, Amer. Math. Soc., Providence, RI, 2004, pp. 61–79. MR2076566

[4] Alina Carmen Cojocaru and M. Ram Murty, *Cyclicity of elliptic curves modulo p and elliptic curve analogues of Linnik's problem*, Math. Ann. **330** (2004), no. 3, 601–625, DOI 10.1007/s00208-004-0562-x. MR2099195

[5] Adam Tyler Felix and M. Ram Murty, *A problem of Fomenko's related to Artin's conjecture*, Int. J. Number Theory **8** (2012), no. 7, 1687–1723, DOI 10.1142/S1793042112500984. MR2968946

[6] Christopher Hooley, *On Artin's conjecture*, J. Reine Angew. Math. **225** (1967), 209–220, DOI 10.1515/crll.1967.225.209. MR0207630

[7] E. Kowalski, *Analytic problems for elliptic curves*, J. Ramanujan Math. Soc. **21** (2006), no. 1, 19–114. MR2226355

[8] L. Mirsky, *The number of representations of an integer as the sum of a prime and a k-free integer*, Amer. Math. Monthly **56** (1949), 17–19, DOI 10.2307/2305811. MR0028335

[9] Pieter Moree, *Artin's primitive root conjecture—a survey*, Integers **12** (2012), no. 6, 1305–1416, DOI 10.1515/integers-2012-0043. MR3011564

[10] M. Ram Murty, *On Artin's conjecture*, J. Number Theory **16** (1983), no. 2, 147–168, DOI 10.1016/0022-314X(83)90039-2. MR698163

[11] M. Ram Murty and J. Esmonde, *Problems in algebraic number theory, second edition*, Springer, 2005.

[12] M. Ram Murty, *Problems in analytic number theory, second edition*, Springer, 2008.

A Appendix

A.1 Tutorial Wedensday July 5

Problem 1. Let $F = \mathbb{Q}(\alpha)$, where $\alpha^3 = -\alpha - 1$. Compute disc $\mathbb{Q}(\alpha)$ and determine the prime ideal decomposition of $(2), (3), (5), (7), (11), (13), (17), (19), (23), (29)$ and (31).

Problem 2. If $f(n)$ is multiplicative and $f(p^m) \to 0$ as $p^m \to \infty$, then $f(n) \to 0$ as $n \to \infty$.

Problem 3. Let $\tau(n)$ be the number of divisors of n, then show that:

(i) $\tau(n) \leq 2\sqrt{n}$.

(ii) $\tau(n) \ll_{\varepsilon} n^{\varepsilon}$.

Problem 4. Let $\tau_k(n)$ be the number of representations of n as a product of k factors. Then

$$\tau_k(n) \ll_{\varepsilon,k} n^{\varepsilon}.$$

Problem 5. Let K be an algebraic number field of degree N. Let

$$F(a) = \#\{\text{ideals } I \subset \mathfrak{O}_K;\ \mathrm{N}(I) = a\}.$$

Then prove that $F(a) \leq \tau_N(a)$.

A.2 Tutorial Saturday July 8

Problem 1. Show that

$$\sum_{d^2|n} \mu(d) = \begin{cases} 1 & \text{if } n \text{ is square-free,} \\ 0 & \text{otherwise.} \end{cases}$$

Problem 2. Let $q_k(n) = 1$ if n is the k-th power-free and zero otherwise. Show that

$$\sum_{n \leq x} q_k(n) = c_k x + \mathrm{O}(x^{1/k}),$$

where

$$c_k = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^k}.$$

Problem 3. Let $K = \mathbb{Q}(\sqrt{D})$, where D is square-free and let p be a prime. Show that if $p|d_k$ then $p\mathfrak{O}_K = \mathfrak{p}^2$. Also if $p \nmid d_k$, we have the following cases:
If p is odd, then

$$p\mathfrak{O}_K = \begin{cases} \mathfrak{p}_1\mathfrak{p}_2 & \text{if} \left(\frac{d_k}{p}\right) = 1, \\ \mathfrak{p} & \text{if} \left(\frac{d_k}{p}\right) = -1, \end{cases}$$

and if $p = 2$, then

$$2\mathfrak{O}_K = \begin{cases} \mathfrak{p}_1\mathfrak{p}_2 & \text{if } d_k \equiv 1 \pmod{8}, \\ \mathfrak{p} & \text{if } d_k \equiv 5 \pmod{8}. \end{cases}$$

Problem 4. Let $A(x)$ be the number of the non-zero lattice points (a,b) that lie within the first quadrant inside the disk

$$a^2 + b^2 \leq (\sqrt{x})^2.$$

Show that

$$A(x) = \frac{\pi}{4}x + \mathrm{O}(\sqrt{x}).$$

Problem 5. For $\Re(s) > 1$, and $K = \mathbb{Q}(i)$, show that

$$\zeta_{\mathbb{Q}(i)}(s) = \zeta(s) \left(\sum_{\substack{n=1, \\ n \text{ odd}}}^{\infty} \frac{(\frac{-1}{n})}{n^s} \right). \tag{9}$$

Show that

$$\sum_{4k+1 \le n \le 4k+4} \left(\frac{-4}{n} \right) = 0,$$

and thus (9) gives an analytic continuation of $\zeta_{\mathbb{Q}(i)}(s)$ to $\Re(s) > 0$. Conclude that

$$\pi = 4\left(1 + \frac{(\frac{-1}{3})}{3} + \frac{(\frac{-1}{5})}{5} + \frac{(\frac{-1}{7})}{7} + \cdots \right).$$

A.3 Tutorial Tuesday July 11

Problem 1. Let $K = \mathbb{Q}(\sqrt{d})$ and a_n denote the number of ideals of $\mathfrak{O}_K$ with norm n. Show that $a_p = 1 + \left(\frac{d_k}{p}\right)$ and $a_{p^n} = \sum_{k=0}^{n} \left(\frac{d_k}{p^k}\right)$.

Problem 2. Let $(a, m) = 1$. Prove that the Dirichelt density of primes congruent to a mod m is $1/\varphi(m)$.

Problem 3. Prove that

$$\lim_{x \to \infty} \frac{\#\{p \le x;\ p-1 \text{ is square free}\}}{\#\{p \le x\}} = \prod_p \left(1 - \frac{1}{p(p-1)} \right).$$

Problem 4. For $\Re(s) > 0$, show that

$$\sum_{n=1}^{\infty} \frac{1}{\phi(n) n^s} = \zeta(s+1) \prod_p \left(1 + \frac{1}{p^{s+1}(p-1)} \right).$$

Use this to deduce that $\sum_{n \le x} \frac{1}{\varphi(n)} \sim \prod_p \left(1 + \frac{1}{p(p-1)}\right) \log x$, as $x \to \infty$. Show that

$$\prod_p \left(1 + \frac{1}{p(p-1)} \right) = \frac{\zeta(2)\zeta(3)}{\zeta(6)} \approx 1.943596\cdots$$

Problem 5. Show that the action of the Galois group on the set of prime ideals lying above a fixed prime of $\mathbb{Z}$ is a transitive action.

Problem 6. Let d be an integer that is not a perfect square. Prove that the density of the set of primes p such that $\left(\frac{d}{p}\right) = 1$ is $\frac{1}{2}$.

Problem 7. If a natural number n is a square mod p for a set of primes p which has density bigger that $\frac{1}{2}$, show that n must be a square.