Some Interesting Topics in Number Theory

Vatsal Jha, Shubansu Katiyar, Amit Sawant,
Ronnie Sebastian, Neel Singh, Edwin Saji Uthuppan

October 25, 2022

In Fall 2018 I taught Basic Number Theory at IIT Bombay. The students in my class had some background in group theory and complex analysis, and more importantly were extremely enthusiastic. In view of this we decided to go beyond the prescribed syllabus and try to understand more advanced topics. The main references we used were

- A concise introduction to the theory of numbers, by Alan Baker
- A course in arithmetic, by J.-P. Serre
- https://web.math.pmf.unizg.hr/nastava/studnatj/Dirichlet_theorem.pdf
- http://www.math.mcgill.ca/darmon/courses/11-12/nt/notes/lecture3.pdf

There were several lectures by students; on the transcendence of e and π, Dirichlet Theorem on infinitely many primes in an arithmetic progression and the meromorphic continuation and functional equation of the Zeta function. The students also volunteered to write down notes for the material we covered and the first six chapters are a result of their efforts. These notes contain most of the material that we covered. The topics that we covered and are not present are the transcendence of e and π. The authors of the various chapters are

- Chapters 2 and 3 - Shubhansu Katiyar
- Chapter 4 - Amit Sawant
- Chapter 5 - Edwin Saji Uthuppan
- Chapter 6 - Neel Singh

A topic that I wanted to lecture on in the course, but could not, because of lack of expertise and time, is Hardy's Theorem, that the critical line contains infinitely many zeros of the Riemann Zeta function. In Summer 2019, Vatsal Jha, an undergraduate math student at IIT Dhanbad, visited me and we decided to go through the notes of Richard Chapling on Hardy's Theorem. Chapling's notes are available here

- http://people.ds.cam.ac.uk/rc476/complexanalysis/hardy'stheorem.pdf

The last chapter in these notes expands on Chapling's notes and gives more details.

I really enjoyed interacting with all the above students and I thank Amit, Edwin, Neel, Shubansu and Vatsal for the interest and enthusiasm that they showed.

The main result in section §7.1 was explained to me by R. Balasubramanian and I thank him for this. I also thank R. Raghunathan for some useful discussions.

If you find any errors or have any comments, please write to me at
ronnie@math.iitb.ac.in

Ronnie Sebastian

Contents

Chapter 1

Finite Abelian Groups

In this chapter we will collect some results on finite abelian groups. Some of these will be used in Chapter 5. Of course, many of the results below hold in greater generality, but we will limit ourselves to what we need. Throughout this chapter G will denote a finite abelian group. Let

$$\mathbb{C}^{\times} := \mathbb{C} \setminus \{0\}$$

and let

$$S^1 := \{z \in \mathbb{C} \mid |z| = 1\}.$$

1.1 Characters of finite abelian groups

Definition 1.1.1. *A character of a finite abelian group G is a group homomorphism $\chi : G \to S^1$.*

Remark 1.1.2. We could have defined characters as homomorphisms $\chi : G \to \mathbb{C}^{\times}$. Since G is a finite group, it easily follows that the image of χ lands in S^1.

Definition 1.1.3. *The group of characters of G is denoted $\hat{G}$.*

Proposition 1.1.4. *If G is a finite group then $\hat{G}$ is a finite group.*

Proof. Let the cardinality of G be n. Let χ be a character of G.

$$1 = |\chi(e)| = |\chi(g^n)| = |\chi(g)^n| = |\chi(g)|^n$$

It follows that the image of χ lands in the nth roots of unity, which is a set of size n. Since the set of maps from a finite set to a finite set is finite, it follows that $\hat{G}$ is finite. □

Consider the following multiplication on characters. Define

$$(\chi_1\chi_2)(g) := \chi_1(g)\chi_2(g)$$

One checks easily that this binary operation makes $\hat{G}$ into a finite abelian group. The identity element in this group is the character 1_G which sends $g \mapsto 1$ for every $g \in G$.

Proposition 1.1.5. *Let G_i be finite abelian groups and let χ_i be characters of G_i. Then*

$$(\chi_1, \chi_2) : G_1 \times G_2 \to S^1$$

given by $(g_1, g_2) \mapsto \chi_1(g_1)\chi_2(g_2)$ defines a character of the group $G_1 \times G_2$.

Proof. Left to the reader. □

Proposition 1.1.6. *Let $H \subset G$ be a subgroup of G. Any character of H can be extended to a character of G.*

Proof. Let χ be a character of H. Let $x \in G \backslash H$. Let K denote the subgroup of G generated by H and x. We will show that χ can be extended to K, and it follows inductively that χ can be extended to G.

Let a denote the smallest positive integer such that $x^a \in H$. Consider the following map, which is a group homomorphism since we are dealing with abelian groups.

$$\phi : H \times \langle x \rangle \to G \qquad\qquad (h, x^i) \mapsto hx^i$$

We first claim that the kernel of this map is generated by (x^a, x^{-a}). Let us assume that $(h, x^i) \mapsto e$. This means that $x^{-i} = h$ and so $x^{-i} \in H$. We also have $x^a \in H$. If $a \nmid i$ then let $0 < d = \gcd(a, i) < a$. Since there are integers x, y such that $ax + iy = d$, it follows that $x^d \in H$, contradicting the minimality of a. Thus, $i = la$ and so $(h, x^i) = (x^{-la}, x^{la})$ which proves the claim.

The image of ϕ is clearly K. We will define a group homomorphism

$$\psi : H \times \langle x \rangle \to \mathbb{C}^\times$$

which is χ on H, and check that it vanishes on Ker ϕ. Then clearly ψ descends to a homomorphism of K. Let d_x be the order of the element x in G. Then the cardinality of the group $\langle x \rangle$ is d_x. Since $x^{d_x} = e \in H$, it is easily checked as above that $a | d_x$. The order of x^a is d_x/a. This is an element of H. Thus,

$$\chi(x^a) = e^{\frac{2\pi il}{d_x/a}}$$

Check that $\chi_2(x) := e^{\frac{2\pi i l}{d_x}}$ defines a character of the cyclic group $\langle x \rangle$. Using Proposition 1.1.5 define a character ψ of $H \times \langle x \rangle$ by letting it to be χ on H and χ_2 on $\langle x \rangle$. It is easily checked that ψ vanishes on (x^a, x^{-a}). Thus, it descends to a character on K. This completes the proof of the proposition. □

1.2 Some exactness properties

Definition 1.2.1. *Suppose $f : A \to B$ is a homomorphism of abelian groups. Then there is a natural map $\hat{f} : \hat{B} \to \hat{A}$, given by $\chi \mapsto \chi \circ f$.*

Proposition 1.2.2. *The map $\hat{f}$ defined above is a homomorphism of abelian groups.*

Proof. Left to the reader. □

Definition 1.2.3. *Let A_i, $i \in \mathbb{Z}$, be abelian groups. Let $f_i : A_i \to A_{i+1}$ be homomorphisms of abelian groups. Consider the diagram*

$$\dots A_i \xrightarrow{f_i} A_{i+1} \xrightarrow{f_{i+1}} A_{i+2} \xrightarrow{f_{i+2}} \dots$$

1. *It is called a complex if $f_{i+1} \circ f_i = 0$, for all i.*
2. *A complex is called exact if $f_i(A_i) = \operatorname{Ker} f_{i+1}$ for all i.*
3. *An exact complex of the form*

   $$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$$

   is called a short exact sequence.

Proposition 1.2.4. *Suppose we are given a complex*

$$\dots A_i \xrightarrow{f_i} A_{i+1} \xrightarrow{f_{i+1}} A_{i+2} \xrightarrow{f_{i+2}} \dots \tag{1.2.5}$$

This gives rise to the complex

$$\dots \hat{A}_i \xleftarrow{\hat{f}_i} \hat{A}_{i+1} \xleftarrow{\hat{f}_{i+1}} \hat{A}_{i+2} \xleftarrow{\hat{f}_{i+2}} \dots \tag{1.2.6}$$

Proof. We only need to check that $\hat{f}_i \circ \hat{f}_{i+1} = 0$ for all i. This is an easy check which is left to the reader. □

Proposition 1.2.7. *Let*

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$$

be a short exact sequence. Then the complex

$$0 \to \hat{C} \xrightarrow{\hat{g}} \hat{B} \xrightarrow{\hat{f}} \hat{A} \to 0$$

is exact.

Proof. We need to check exactness at $\hat{C}, \hat{B}, \hat{A}$.

1. Exactness at $\hat{C}$. From the definition of exactness, we need to show that Ker $\hat{g} = \{1_C\}$. Let χ be a character of C such that $\hat{g}(\chi) = 1_B$. By the definition of $\hat{g}$, this means that $\chi \circ g = 1_B$. Since g is surjective, it follows that $\chi = 1_C$.

2. Exactness at $\hat{B}$. We need to show that if χ is a character of B such that $\hat{f}(\chi) = 1_A$ then there is a character ψ of C such that $\chi = \hat{g}(\psi)$. Since $\hat{f}(\chi) = \chi \circ f$ it follows that $\chi(f(A)) = 1$. Thus, χ factors through $\bar{\chi} : B/f(A) \to S^1$. As the sequence $0 \to A \to B \to C \to 0$ is short exact, it follows that g induces an isomorphism $\bar{g} : B/f(A) \to C$. Letting $\psi := \bar{\chi} \circ \bar{g}^{-1}$ it is easily seen that $\chi = \psi \circ g = \hat{g}(\psi)$.

3. Exactness at $\hat{A}$. We need to show that given a character χ of A, there is a character ψ of B such that $\chi = \psi \circ f$. By the exactness of the sequence we may view of f as identifying A as a subgroup of B. Now using Proposition 1.1.6, we see that the character χ may be extended to a character ψ of B. It follows that $\chi = \hat{f}(\psi)$.

□

1.3 Sums of characters

Proposition 1.3.1. *Let $n = \#(G)$ and let $\chi \in \hat{G}$. Then*

$$\sum_{x \in G} \chi(x) = \begin{cases} n & \text{if } \chi = 1_G \\ 0 & \text{if } \chi \neq 1_G \end{cases}$$

Proof. If $\chi = 1_G$ then $\chi(x) = 1 \ \forall \ x \in G$ and the first part follows. To prove the second part, choose $y \in G$ such that $\chi(y) \neq 1$. We have

$$\chi(y) \sum_{x \in G} \chi(x) = \sum_{x \in G} \chi(xy) = \sum_{x \in G} \chi(x)$$

Hence

$$(\chi(y)-1)\sum_{x\in G}\chi(x)=0$$

Since $\chi(y)\neq 1$ this implies $\sum_{x\in G}\chi x=0$. □

Corollary 1.3.2. *Let $x\in G$. Then*

$$\sum_{\chi\in\hat{G}}\chi(x)=\begin{cases}|\hat{G}| & \textit{if } x=1\\ 0 & \textit{if } x\neq 1\end{cases}$$

Proof. If $x=1$ then the first part follows. There is a natural map $G\to\hat{\hat{G}}$. This is given by $a\mapsto\Phi_a$. Let $\chi\in\hat{G}$, then

$$\Phi_a(\chi):=\chi(a).$$

For $x\in G$, there is a character χ_0 of G such that $\chi_0(x)\neq 1$. This is clear because we can first take a nontrivial character on the cyclic subgroup $\langle x\rangle$ and then extend it to G. Thus,

$$\begin{aligned}\sum_{\chi\in\hat{G}}\chi(x)&=\sum_{\chi\in\hat{G}}\Phi_x(\chi)\\ &=\sum_{\chi\in\hat{G}}\Phi_x(\chi\chi_0)\\ &=\Phi_x(\chi_0)\sum_{\chi\in\hat{G}}\Phi_x(\chi)\end{aligned}$$

This shows that

$$(\Phi_x(\chi_0)-1)\sum_{\chi\in\hat{G}}\Phi_x(\chi)=(\chi_0(x)-1)\sum_{\chi\in\hat{G}}\Phi_x(\chi)=0$$

Since $\chi_0(x)\neq 1$ we see that $\sum_{\chi\in\hat{G}}\chi(x)=0$. □

Chapter 2

Quadratic Residues

In this chapter we shall study the solutions of the equation $x^2 \equiv a \pmod{p}$, where p is a prime. The main result that we want to prove here is the law of quadratic reciprocity, which states the following.

Theorem (Theorem 2.3.1)**.** *Let p and q be odd primes. Then*

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

2.1 Legendre Symbol and Euler's Criterion

Definition 2.1.1. *Let $a \in (\mathbb{Z}/p\mathbb{Z})^*$.*

1. *Define $\left(\frac{a}{p}\right) = 1$ if $x^2 \equiv a \pmod{p}$ has a solution. In this case we say that a is a quadratic residue* mod *p.*
2. *Otherwise, define $\left(\frac{a}{p}\right) = -1$. In this case we say that a is a quadratic non-residue* mod *p.*

The following proposition follows from the definition.

Proposition 2.1.2. *Consider the map $\psi : (\mathbb{Z}/p\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*$ defined by $\psi(x) = x^2$. Then $\left(\frac{a}{p}\right) = 1$ if and only if a is in the image of ψ.*

Proposition 2.1.3. *Let $f(x) \in \mathbb{Z}/p\mathbb{Z}[x]$ be a polynomial of degree d. Then $f(x)$ has at most d distinct roots in $\mathbb{Z}/p\mathbb{Z}$.*

Proof. Note that $\mathbb{Z}/p\mathbb{Z}$ is a field. Let $a \in \mathbb{Z}/p\mathbb{Z}$ be a root of $f(x)$. Since $f(x)$ is a polynomial, for any $b \in \mathbb{Z}/p\mathbb{Z}$, writing $x = x-b+b$ and expanding, we get that

$$f(x) = (x-b)g_b(x) + f(b)$$

Here $g_b(x)$ is a polynomial which depends on b. Taking $b = a$ we get that $f(x) = (x-a)g_a(x)$. The proof follows by induction on the degree of polynomial $f(x)$. □

Proposition 2.1.4. *If p is an odd prime, then*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

Proof. Let us first suppose that $\left(\frac{a}{p}\right) = 1$. Then, by definition, there is an x such that $x^2 \equiv a \pmod{p}$. Raising both sides to an exponent of $\frac{p-1}{2}$, we get $x^{p-1} \equiv a^{\frac{p-1}{2}} \pmod{p}$. However, by Fermat's Theorem we know that $x^{p-1} \equiv 1 \mathrm{mod}\ p$. Thus,

$$a^{\frac{p-1}{2}} \equiv 1 \equiv \left(\frac{a}{p}\right) \pmod{p}.$$

Next let us assume that $\left(\frac{a}{p}\right) = -1$. We need to show $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. Consider the polynomial $f(x) = x^{\frac{p-1}{2}} - 1$. The elements of the set

$$S = \{1^2, 2^2, \cdots (\frac{p-1}{2})^2\}$$

are distinct roots of this polynomial. These are roots of this polynomial follows from Fermat's theorem. These are distinct as

$$a^2 \equiv b^2 \pmod{p} \implies a \equiv b \pmod{p} \text{ or } a \equiv -b \pmod{p}$$

which is not true for any $a, b \in \{1, 2, \cdots \frac{p-1}{2}\}$ with $a \neq b$. By proposition 2.1.3, the elements of S are exactly all the roots of $f(x)$ in $\mathbb{Z}/p\mathbb{Z}$, as $|S| = deg(f) = \frac{p-1}{2}$. In particular, if $a \notin S$ then a is not a root of f. Since a is a quadratic non-residue $(\mathrm{mod}\ p)$, $a \notin S$ and hence $f(a) = a^{\frac{p-1}{2}} - 1 \neq 0$.

By Fermat's theorem, $(a^{\frac{p-1}{2}})^2 \equiv 1 \pmod{p}$. Thus,

$$(a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \equiv 0 \bmod p$$

Since $a^{\frac{p-1}{2}} - 1 \neq 0$, we get $a^{\frac{p-1}{2}} + 1 \equiv 0 \bmod p$. Thus,

$$a^{\frac{p-1}{2}} \equiv -1 \equiv \left(\frac{a}{p}\right) \pmod{p}.$$

□

Corollary 2.1.5. *Legendre Symbol is multiplicative, that is,*

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$$

holds for all integers a, b not divisible by p.

We make some remarks about the Legendre symbol for composite numbers. Let n be an odd composite number. As before we may define the Legendre symbol as follows.

Definition 2.1.6. *Let $a \in (\mathbb{Z}/n\mathbb{Z})^*$.*

1. *Define $\left(\frac{a}{n}\right) = 1$ if $x^2 \equiv a \pmod{n}$ has a solution. In this case we say that a is a quadratic residue* mod n.
2. *Otherwise, define $\left(\frac{a}{n}\right) = -1$. In this case we say that a is a quadratic non-residue* mod n.

One may ask if the following holds

$$\left(\frac{a}{n}\right)\left(\frac{b}{n}\right) = \left(\frac{ab}{n}\right)? \tag{2.1.7}$$

We now address the above question. Let us write $n = \prod_{i=1}^{l} p_i^{r_i}$. We have the map $\psi : (\mathbb{Z}/n\mathbb{Z})^* \to (\mathbb{Z}/n\mathbb{Z})^*$ defined as $\psi(x) = x^2$. It is clear that $\left(\frac{a}{n}\right) = 1$ iff a is in the image of ψ. By the Chinese Remainder Theorem, there is a commutative square

$$\begin{tikzcd}
(\mathbb{Z}/n\mathbb{Z})^* \arrow[r, "\psi"] \arrow[d, "\theta", "\cong"'] & (\mathbb{Z}/n\mathbb{Z})^* \arrow[d, "\theta"', "\cong"] \\
\prod_{i=1}^{l}(\mathbb{Z}/p_i^{r_i}\mathbb{Z})^* \arrow[r, "\prod_{i=1}^{l}\psi_i"] & \prod_{i=1}^{l}(\mathbb{Z}/p_i^{r_i}\mathbb{Z})^*
\end{tikzcd}$$

The vertical arrows are $a \pmod{n} \mapsto (a \pmod{p_i^{r_i}})_i$. The lower horizontal arrow is given by $(x_1, \ldots, x_l) \mapsto (x_1^2, \ldots, x_l^2)$. The map ψ_i is simply the square map $(\mathbb{Z}/p_i^{r_i}\mathbb{Z})^* \to (\mathbb{Z}/p_i^{r_i}\mathbb{Z})^*$ given by $x \mapsto x^2$. As the vertical arrows are isomorphisms, it follows that $\left(\frac{a}{n}\right) = 1$ iff $\theta(a)$ is in the image of $\prod_{i=1}^{l} \psi_i$.

It is clear that $\mathrm{Image}(\prod_{i=1}^{l} \psi_i) = \prod_{i=1}^{l} \mathrm{Image}(\psi_i)$. As $\prod_{i=1}^{l}(\mathbb{Z}/p_i^{r_i}\mathbb{Z})^*$ is an abelian group it follows that every subgroup is normal, and so we have the group

$$\prod_{i=1}^{l}(\mathbb{Z}/p_i^{r_i}\mathbb{Z})^*/\prod_{i=1}^{l}\mathrm{Image}(\psi_i) = \prod_{i=1}^{l}(\mathbb{Z}/p_i^{r_i}\mathbb{Z})^*/\mathrm{Image}(\psi_i)\,.$$

As p_i is an odd prime, we know that $(\mathbb{Z}/p_i^{r_i}\mathbb{Z})^*$ is cyclic. Using this it easily follows that

$$(\mathbb{Z}/p_i^{r_i}\mathbb{Z})^*/\mathrm{Image}(\psi_i) = \mathbb{Z}/2\mathbb{Z}\,.$$

Thus, we get that

$$\prod_{i=1}^{l}(\mathbb{Z}/p_i^{r_i}\mathbb{Z})^*/\mathrm{Image}(\prod_{i=1}^{l}\psi_i) = (\mathbb{Z}/2\mathbb{Z})^l\,.$$

Consider the natural map

$$\prod_{i=1}^{l}(\mathbb{Z}/p_i^{r_i}\mathbb{Z})^* \xrightarrow{\Theta} \prod_{i=1}^{l}(\mathbb{Z}/p_i^{r_i}\mathbb{Z})^*/\mathrm{Image}(\prod_{i=1}^{l}\psi_i) = (\mathbb{Z}/2\mathbb{Z})^l\,.$$

It follows that $\left(\frac{a}{n}\right) = 1$ iff $\theta(a)$ is in the image of $\prod_{i=1}^{l}\psi_i$ iff $\Theta(\theta(a)) = 0$. Assume that $l > 1$. Let $a_1 \in (\mathbb{Z}/n\mathbb{Z})^*$ be such that $\Theta(\theta(a_1)) = (1, 0, 0, \ldots, 0)$ and let $a_2 \in (\mathbb{Z}/n\mathbb{Z})^*$ be such that $\Theta(\theta(a_2)) = (0, 1, 0, \ldots, 0)$. It follows that

$$\Theta(\theta(a_1a_2)) = \Theta(\theta(a_1)\theta(a_2)) = \Theta(\theta(a_1)) + \Theta(\theta(a_2)) = (1, 1, 0, \ldots, 0)\,.$$

This shows that

$$\left(\frac{a_1}{n}\right) = \left(\frac{a_2}{n}\right) = \left(\frac{a_1a_2}{n}\right) = -1\,.$$

Thus, if $l > 1$ then (2.1.7) may not be true. On the other hand if $l = 1$ then (2.1.7) is true.

2.2 Gauss' Lemma

Let p be an odd prime and let $r = \frac{p-1}{2}$. Represent residue classes in $\mathbb{Z}/p\mathbb{Z}$ by integers in the interval $[-r, r]$. Fix $a \in (\mathbb{Z}/p\mathbb{Z})^*$ and for

$$j \in T := \{1, 2, \cdots r\}$$

define x_j to be the unique residue class in $[-r, r]$ which is congruent to aj mod p. In other words, x_j is the unique integer in the interval $[-r, r]$ such that $aj \equiv x_j$ mod p. Notice that $x_j \neq 0$ as both a and j are nonzero residue classes in $(\mathbb{Z}/p\mathbb{Z})^*$.

Lemma 2.2.1. *(Gauss' Lemma) Let $l := \#\{j \in T \mid x_j < 0\}$. Then*

$$\left(\frac{a}{p}\right) = (-1)^l$$

Proof. We claim that the absolute values $|x_j|$ are distinct and take all integer values in the set $[1, r]$. For if $|x_j| = |x_k|$, then $aj = \pm ak$, that is, $a(j \pm k) \equiv 0 \pmod p$. This shows that $j \pm k \equiv 0 \pmod p$ as $p \nmid a$. Now this is not possible unless $j = k$, since $j, k \in \{1, 2, \cdots \frac{p-1}{2}\}$.

Now

$$\prod_{j \in T} aj \equiv a^{\frac{p-1}{2}} \prod_{j \in T} j \pmod p$$

and

$$\prod_{j \in T} aj \equiv \prod_{j \in T} x_j \equiv (-1)^l \prod_{j \in T} |x_j| \equiv (-1)^l \prod_{j \in T} j \pmod p$$

This shows that

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

□

As an application of the lemma, let us compute $\left(\frac{2}{p}\right)$ when p is an odd prime.

Corollary 2.2.2. *Let p be an odd prime. Then*

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

Proof. Look at the set $j \in \{1, 2, \cdots \frac{p-1}{2}\}$ and compute $2j \pmod p$. Recall that we need to find a representative x_j of $2j$ mod p in the set $[-r, r]$. Note that $x_j < 0$ if and only if $2j > \frac{p-1}{2}$, that is, $j > \lfloor \frac{p-1}{4} \rfloor$. So

$$l = \frac{p-1}{2} - \lfloor \frac{p-1}{4} \rfloor$$

Check that when $p \equiv \pm 1 \pmod 8$, $l \equiv 0 \equiv \frac{p^2-1}{8} \pmod 2$ and if $p \equiv \pm 3 \pmod 8$, $l \equiv 1 \equiv \frac{p^2-1}{8} \pmod 2$. In either case, $l \equiv \frac{p^2-1}{8} \pmod 2$ and hence,

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

□

2.3 Quadratic Reciprocity

In this section we will prove the quadratic reciprocity theorem.

Theorem 2.3.1 (Quadratic reciprocity)**.** *Let p and q be odd primes. Then*

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

Proof. Recall the number l and the notation in Lemma 2.2.1. We take the prime number in Lemma 2.2.1 to be q and we take a to be p. Then l is the cardinality of the set

$$l = \#\left\{j \in [-\frac{q-1}{2}, \frac{q-1}{2}] \,\middle|\, x_j < 0\right\}.$$

Notice that there is an equality of sets

$$\left\{j \in [-\frac{q-1}{2}, \frac{q-1}{2}] \,\middle|\, x_j < 0\right\} = \left\{1 \leqslant x \leqslant \frac{q-1}{2} \,\middle|\, \exists y \in \mathbb{Z}, -\frac{q-1}{2} \leqslant px - qy < 0\right\}.$$

Thus, we get $\left(\frac{p}{q}\right) = (-1)^l$, where

$$l = \#\left\{1 \leqslant x \leqslant \frac{q-1}{2} \,\middle|\, \exists y \in \mathbb{Z}, \qquad -\frac{q-1}{2} \leqslant px - qy < 0\right\}$$

We have the following equalities.

$$\begin{aligned} l =& \#\left\{1 \leqslant x \leqslant \frac{q-1}{2} \,\middle|\, \exists y \in \mathbb{Z}, \qquad -\frac{q-1}{2} \leqslant px - qy < 0\right\} \\ =& \#\left\{0 < x < \frac{q+1}{2} \,\middle|\, \exists y \in \mathbb{Z}, \qquad -\frac{q-1}{2} \leqslant px - qy < 0\right\} \\ =& \#\left\{0 < x < \frac{q+1}{2} \,\middle|\, \exists y \in \mathbb{Z}, \qquad -\frac{q}{2} < px - qy < 0\right\} \end{aligned} \tag{2.3.2}$$

The last equality is because $px - qy$ is an integer. Observe the following two.

1. If $px - qy < 0$ and $x > 0$ then $y > 0$.
2. If $px - qy \geqslant -\frac{q-1}{2}$ and $x \leqslant \frac{q-1}{2}$ then $y \leqslant (\frac{q-1}{2q})(p+1) < \frac{p+1}{2}$.

Using this we see that the sets in (2.3.2) are exactly those points $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ such that

1. $0 < x < \frac{q+1}{2}$
2. $0 < y < \frac{p+1}{2}$
3. $-\frac{q}{2} < px - qy < 0$

This is exactly the set of points in Region 1 in the diagram below with integer coordinates.

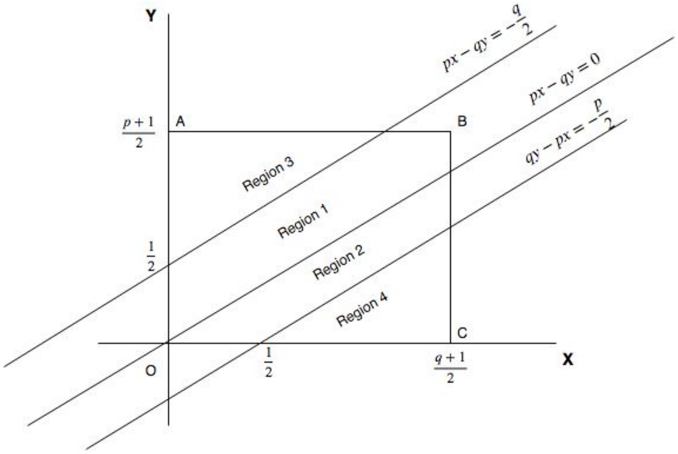


Figure 2.1: The rectangle OABC is divided into 4 regions by the lines $px - qy = -\frac{q}{2}$, $px - qy = 0$, and $qy - px = -\frac{p}{2}$

We analyse $\left(\frac{q}{p}\right)$ in a similar manner, however, we switch the roles of p and q and the variables x and y. We take the prime number in Lemma 2.2.1 to be p and we take a to be q. Then $\left(\frac{q}{p}\right) = (-1)^m$, where m is the cardinality of the set

$$m = \#\Big\{j \in [-\frac{p-1}{2}, \frac{p-1}{2}] \,\Big|\, x_j < 0\Big\}.$$

Notice that there is an equality of sets

$$\Big\{j \in [-\frac{p-1}{2}, \frac{p-1}{2}] \,\Big|\, x_j < 0\Big\} = \Big\{1 \leqslant y \leqslant \frac{p-1}{2} \,\Big|\, \exists x \in \mathbb{Z}, -\frac{p-1}{2} \leqslant qy - px < 0\Big\}.$$

Thus, we get $\left(\frac{q}{p}\right) = (-1)^m$, where

$$m = \#\Big\{1 \leqslant y \leqslant \frac{p-1}{2} \;\Big|\; \exists x \in \mathbb{Z}\,, \qquad -\frac{p-1}{2} \leqslant qy - px < 0\Big\}$$

We have the following equalities.

$$\begin{aligned} m =&\#\Big\{1 \leqslant y \leqslant \frac{p-1}{2} \;\Big|\; \exists x \in \mathbb{Z}\,, \qquad -\frac{p-1}{2} \leqslant qy - px < 0\Big\} \\ =&\#\Big\{0 < y < \frac{p+1}{2} \;\Big|\; \exists x \in \mathbb{Z}\,, \qquad -\frac{p-1}{2} \leqslant qy - px < 0\Big\} \\ =&\#\Big\{0 < y < \frac{p+1}{2} \;\Big|\; \exists y \in \mathbb{Z}\,, \qquad -\frac{p}{2} < qy - px < 0\Big\} \end{aligned} \tag{2.3.3}$$

The last equality is because $qy - px$ is an integer. Observe the following two.

1. If $qy - px < 0$ and $y > 0$ then $x > 0$.
2. If $qy - px \geqslant -\frac{p-1}{2}$ and $y \leqslant \frac{p-1}{2}$ then $x \leqslant (\frac{p-1}{2p})(q+1) < \frac{q+1}{2}$.

Using this we see that the sets in (2.3.3) are exactly those points $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ such that

1. $0 < x < \frac{q+1}{2}$
2. $0 < y < \frac{p+1}{2}$
3. $-\frac{p}{2} < qy - px < 0$

This is exactly the set of points in Region 2 in the diagram above with integer coordinates.

Observe that the transformation $x = \frac{q+1}{2} - x', y = \frac{p+1}{2} - y'$ gives a one-one correspondence between Region 3 and Region 4. Further, it takes points with integer coordinates to point with integer coordinates. Hence, number of points in Region 3 with integer coordinates, is the same as the number of points in Region 4 with integer coordinates.

The total number of points with integer coordinates strictly inside the rectangle OABC is $(\frac{p-1}{2})(\frac{q-1}{2})$. Let t_i denote the number of points with integer coordinates in Region i. Then

$$(\frac{p-1}{2})(\frac{q-1}{2}) = t_1 + t_2 + t_3 + t_4$$

Since $t_3 = t_4$, it follows that modulo 2,

$$(\frac{p-1}{2})(\frac{q-1}{2}) = t_1 + t_2 \qquad \text{mod } 2$$

Since $t_1 = l$ and $t_2 = m$ this proves that

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

□

The law of quadratic reciprocity is useful in the calculation of Legendre symbols. For example, we have:

$$\left(\frac{15}{71}\right) = \left(\frac{3}{71}\right)\left(\frac{5}{71}\right) = -\left(\frac{71}{3}\right)\left(\frac{71}{5}\right) = -\left(\frac{2}{3}\right)\left(\frac{1}{5}\right) = 1$$

Chapter 3

Quadratic Forms

One may ask what integers can be written as a sum of squares of two integers. Let $f(x, y) = x^2 + y^2$, then this question is same as asking when $f(x, y) = n$ has integer solutions. This naturally leads us to binary quadratic forms, which are a generalization of the function x^2+y^2. We will put an equivalence relation on the set of binary quadratic forms of discriminant $d < 0$ and prove that in each equivalence class there is a unique reduced binary quadratic form. The number of reduced binary quadratic forms of discriminant $d < 0$ is finite and is denoted by $h(d)$. This number, amazingly, coincides with the class number of $\mathbb{Q}(\sqrt{d})$ (the definition of class number is beyond the scope of this course). After this we will address the question of which integers can be represented by a given binary quadratic form. Finally, we prove Lagrange's Four Square Theorem, which states that

Theorem (Theorem 3.4.1)**.** *Every integer $n \geqslant 0$ is a sum of four squares.*

3.1 Binary Quadratic Forms

Definition 3.1.1. *A binary quadratic form is a function $f : \mathbb{Z}^2 \to \mathbb{Z}$ of the form $f(x, y) = ax^2 + bxy + cy^2$, where $a, b, c \in \mathbb{Z}$. By the discriminant of f, we mean the number $Disc(f) = b^2 - 4ac$, usually denoted by d.*

Note that

$$\begin{aligned} 4af(x, y) &= 4a^2x^2 + 4abxy + 4acy^2 \\ &= (2ax + by)^2 - dy^2 \end{aligned}$$

Thus, if $d < 0$, then $f(x, y)$ takes only positive values or only negative values according to whether a is positive or negative.

Lemma 3.1.2. *If $d > 0$, then $f(x, y)$ takes both positive and negative values.*

Proof. First consider the case when $a = 0$. Then $f(x, y) = bxy + cy^2 = y(bx + cy)$. If we put $y = 1$, then it is clear that $f(x, 1)$ takes both positive and negative values.

Next assume that $a > 0$. Clearly, $f(1, 0) > 0$. Choose $y \gg 0$ so that $a - dy^2 < 0$. Now consider the integer by. By adding to by an appropriate multiple of $2a$, we can translate this integer into the set $[-a, a]$. That is, there is a unique integer x such that $|2ax - by| \leqslant a$. It is then clear that

$$4af(x, y) = (2ax + by)^2 - dy^2 \leqslant a^2 - dy^2 < 0\,.$$

As $a > 0$ it follows that $f(x, y) < 0$.

If $a < 0$ then we put $g(x, y) = -f(x, y)$. As the set of values taken by f and g are the same, and by the preceding argument $g(x, y)$ takes positive and negative values, it follows that $f(x, y)$ also takes positive and negative values. □

Definition 3.1.3. *Let f and g be binary quadratic forms. We say they are equivalent, written $f \sim g$ if there exists a linear isomorphism $U : \mathbb{Z}^2 \to \mathbb{Z}^2$ such that det$(U) = 1$ and $g = f \circ U$, i.e.,*

$$U = \begin{bmatrix} p & q \\ r & s \end{bmatrix} \in M_2(\mathbb{Z}) \quad \textit{where } ps - qr = 1$$

In the above, $M_2(\mathbb{Z})$ denotes 2×2 matrices with integer coefficients.

Remark 3.1.4. Equivalence of binary quadratic forms ($\sim$) is an equivalence relation. More precisely, this means the following three conditions are satisfied.

1. For every f we have $f \sim f$.
2. For any f, g if $f \sim g$ then $g \sim f$.
3. For any f, g, h if $f \sim g$ and $g \sim h$, then $f \sim h$.

Let us now make the following observation. Let $f(x, y) = ax^2 + bxy + cy^2$. Define a symmetric matrix

$$A_f := \left[\begin{array}{cc} a & b/2 \\ b/2 & c \end{array} \right]$$

Let

$$v := \left(\begin{array}{c} x \\ y \end{array} \right)$$

Then

$$f(x, y) = v^t A_f v. \tag{3.1.5}$$

Conversely, if A is a symmetric 2×2 matrix such that

$$f(x, y) = v^t A v$$

then we easily check that

1. $A_{11} = f(1, 0) = a$
2. $A_{22} = f(0, 1) = c$
3. $A_{11} + A_{12} + A_{21} + A_{22} = A_{11} + 2A_{12} + A_{22} = f(1, 1) = a + b + c$

This forces that $A_{12} = b/2$. Thus, the symmetric matrix A_f is the unique one which satisfies equation (3.1.5). Let us also note that

$$Disc(f) = -4det(A_f). \tag{3.1.6}$$

Now let us assume that $f \sim g$. Then there is $U \in M_2(\mathbb{Z})$ such that $g = f \circ U$. This shows that

$$g(x, y) = v^t U^t A_f U v.$$

By the uniqueness of the matrix A_g, we get that

$$A_g = U^t A_f U$$

This shows that

$$\begin{aligned} Disc(g) &= -4det(A_g) \\ &= -4det(U^t A_f U) \\ &= -4det(A_f) \\ &= Disc(f) \end{aligned}$$

Thus, we have proved the following proposition.

Proposition 3.1.7. *If $f \sim g$ then $Disc(f) = Disc(g)$.*

3.2 Reduction of Quadratic Forms

If f and g are equivalent binary quadratic forms, then we have seen that $Disc(f) = Disc(g)$. Fix an integer $d < 0$. Since $d < 0$, a quadratic form with discriminant d will take only positive values (if $a > 0$) or negative values (if $a < 0$). Consider the set $\mathfrak{B}$ of all binary quadratic forms with discriminant d and such that $a > 0$. Notice that if $f \sim g$ then the set of values they take is the same, thus, both of them take either positive or negative. The equivalence relation $\sim$ breaks the set $\mathfrak{B}$ into equivalence classes. We want to write down a unique representative in each equivalence class.

Throughout this section d is a fixed integer such that $d < 0$.

Definition 3.2.1. *A binary quadratic form $f(x, y) = ax^2 + bxy + cy^2$, with discriminant d and $a > 0$ is called reduced if*

$$-a < b \leqslant a < c \qquad \textit{or} \qquad 0 \leqslant b \leqslant a = c$$

Remark 3.2.2. Since $d < 0$, the case $a = 0$ cannot happen.

Remark 3.2.3. If $d < 0$ and $c \leqslant 0$, then as $a > 0$ we get $d = b^2 - 4ac \geqslant 0$, a contradiction. Thus, we have $c > 0$.

Consider the following three matrices.

$$U := \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \qquad\qquad V := \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

One checks easily that for any $k \in \mathbb{Z}$ we have

$$V^k = \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix}$$

Note that

$$f \circ U \begin{pmatrix} x \\ y \end{pmatrix} = cx^2 - bxy + ay^2. \tag{3.2.4}$$

That is, applying U interchanges a and c while reversing the sign of b. Also note

$$\begin{aligned} f \circ V^k \begin{pmatrix} x \\ y \end{pmatrix} &= a(x + ky)^2 + b(x + ky)y + cy^2 \\ &= ax^2 + (b + 2ak)xy + (ak^2 + bk + c)y^2 \end{aligned} \tag{3.2.5}$$

That is, applying V^k allows to increase or decrease the value of b without changing the value of a.

Theorem 3.2.6. *Let $f(x,y) = ax^2+bxy+cy^2$ be a binary quadratic form of discriminant d and $a > 0$. Then f is equivalent to a reduced binary quadratic form.*

Proof. We will prove the theorem by induction on a. The base case for the induction is $a = 1$. There is a unique $k \in \mathbb{Z}$ such that $b + 2k \in \{0, 1\}$. Thus,

$$f \circ V^k = x^2 + b'xy + c'y^2$$

Now by Remark 3.2.3 it follows that $c' > 0$ since $f \circ V^k$ has discriminant d and $a > 0$. Thus, it is clear that exactly one of the following two will hold

$$-1 < b' \leqslant 1 < c' \qquad \text{or} \qquad 0 \leqslant b' \leqslant 1 = c'.$$

This proves that $f \circ V^k$ is reduced and the base case for induction is done.

Let $f(x,y) = ax^2 + bxy + cy^2$ be a binary quadratic form with discriminant d and $a > 0$. Let us assume that the theorem has been proved for all binary quadratic forms $g(x,y) = a'x^2 + b'xy + c'y^2$ whose discriminant is d and $0 < a' < a$. We will now prove the theorem holds for $f(x,y)$.

1. If $a > c$, then let $f' = f \circ U$.

   $$f'(x,y) = cx^2 - bxy + ay^2$$

   Then $f \sim f'$. Since $c < a$, by induction hypothesis, $f' \sim g$ and g is reduced. By transitivity, $f \sim g$ and we are done.

2. Assume $a \leqslant c$. We can find a unique $k \in \mathbb{Z}$ such that $b+2ak \in (-a, a]$. Let $f' = f \circ V^k$, by equation (3.2.5)

   $$f'(x,y) = ax^2 + (b + 2ak)xy + c'y^2$$

   for some $c' \in \mathbb{Z}$. Again by Remark 3.2.3 $c' > 0$. We now have

   $$-a < b' \leqslant a.$$

   (a) If $a < c'$ then we have

   $$-a < b' \leqslant a < c'$$

   and so f' is reduced. Thus, f is equivalent to a reduced binary quadratic form.

(b) If $a = c'$ and $b' \geqslant 0$, then f' is reduced since $0 \leqslant b' \leqslant a = c'$ and so f is equivalent to a reduced binary quadratic form.

(c) If $a = c'$ and $b' < 0$, then

$$f' \circ U(x,y) = c'x^2 - b'xy + ay^2$$

and

$$0 \leqslant -b' \leqslant a = c'$$

Thus $f' \circ U$ is reduced and so f is equivalent to a reduced binary quadratic form.

(d) If $a > c'$, then by induction $f' \circ U(x,y) = c'x^2 - b'xy + ay^2$ is equivalent to a reduced binary quadratic form. Thus, f is also equivalent to a reduced binary quadratic form.

This completes the proof of the theorem. □

Proposition 3.2.7. *Let $d < 0$. There are only finitely many reduced quadratic forms with discriminant d and $a > 0$.*

Proof. Since f is reduced, $|b| \leqslant a \leqslant c$. Thus, $b^2 \leqslant ac$. Now

$$d = b^2 - 4ac \leqslant ac - 4ac = -3ac.$$

That is, $3ac \leqslant -d$. Thus, a and c are bounded. Since $|b| \leqslant a$, b is also bounded. Hence, there can be only finitely many reduced binary quadratic forms with discriminant d and $a > 0$. □

Definition 3.2.8. *Let S be the set*

$$S := \{(x,y) \in \mathbb{Z}^2 \setminus (0,0) \quad | \quad \gcd(x,y) = 1\}.$$

We emphasize that $(\pm 1, 0)$ and $(0, \pm 1) \in S$.

We claim that S is invariant under $SL_2(\mathbb{Z})$ (2×2 matrices with determinant 1). In other words, for any $U \in SL_2(\mathbb{Z})$, we have $U(S) = S$. Let $\begin{pmatrix} x \\ y \end{pmatrix} \in S$ and let $U \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x' \\ y' \end{pmatrix}$. Then

$$\begin{pmatrix} x \\ y \end{pmatrix} = U^{-1} \begin{pmatrix} x' \\ y' \end{pmatrix}$$

As $U^{-1} \in SL_2(\mathbb{Z})$, x and y are linear combinations of x' and y' with integer coefficients. Thus, $\gcd(x', y')$ divides both x and y. Since $\gcd(x, y) = 1$, we get $\gcd(x', y') = 1$ and $\begin{pmatrix} x' \\ y' \end{pmatrix} \in S$. We have thus proved that $U(S) \subset S$. On the other hand, $\begin{pmatrix} x \\ y \end{pmatrix} = U\left(U^{-1}\begin{pmatrix} x \\ y \end{pmatrix}\right)$ and by what we have just seen, $U^{-1}\begin{pmatrix} x \\ y \end{pmatrix} \in S$, since $U^{-1} \in SL_2(\mathbb{Z})$. Hence, $S \subset U(S)$. Combining, we get $S = U(S)$ as desired.

Proposition 3.2.9. *Let f and g be two quadratic forms such that $f \sim g$. Then $f(S) = g(S)$ and the cardinality of $(f|_S)^{-1}(x)$ is same as that of $(g|_S)^{-1}(x)$ $\forall x \in \mathbb{Z}$.*

Proof. We saw above that $U(S) = S$. Thus, $g(S) = g(U(S)) = g \circ U(S) = f(S)$. Restricting $f = g \circ U$ to S we get $g|_S = f|_S \circ U$. In terms of a commutative diagram, this is easily understood as the commutativity of

$$\begin{tikzcd}
S \arrow[r, "U"] \arrow[d] & S \arrow[d] \\
\mathbb{Z}^2 \arrow[r, "U"] \arrow[dr, "f"'] & \mathbb{Z}^2 \arrow[d, "g"] \\
& \mathbb{Z}
\end{tikzcd}$$

That $\#(f|_S)^{-1}(x) = \#(g|_S)^{-1}(x)$ for all $x \in \mathbb{Z}$ follows using $g|_S = f|_S \circ U$ and from the fact that U is a bijective map. □

Theorem 3.2.10. *Two reduced quadratic forms are not equivalent to each other.*

Proof. The key idea of the proof is to recover the coefficients of the reduced binary quadratic form from the values it takes on the set S.

Let $f(x, y) = ax^2 + bxy + cy^2$ be a reduced quadratic form. In particular, this means that $0 \leqslant |b| \leqslant a \leqslant c$. Using Remark 3.2.2 we see that $0 < a \leqslant c$. Let

$$S^o := \{\begin{pmatrix} x \\ y \end{pmatrix} \in S \mid x \neq 0,\ y \neq 0\}\,.$$

Let $\begin{pmatrix} x \\ y \end{pmatrix} \in S^o$. First assume that $|x| \geqslant |y|$. Note that as $0 \leqslant a \leqslant c$, we have $|ax^2 + cy^2| = ax^2 + cy^2$. We also have $c - |b| \geqslant a - |b| \geqslant 0$. Using these we get the following inequalities. Then,

$$\begin{aligned} |f(x,y)| = |ax^2 + bxy + cy^2| &\geqslant |ax^2 + cy^2| - |b||xy| \\ &\geqslant ax^2 - |b||x|^2 + cy^2 = (a - |b|)x^2 + cy^2 \\ &\geqslant a - |b| + c \end{aligned}$$

Similarly, if $|y| \geqslant |x|$ then we have

$$\begin{aligned} |f(x,y)| = |ax^2 + bxy + cy^2| &\geqslant |ax^2 + cy^2| - |b||xy| \\ &\geqslant ax^2 - |b||y|^2 + cy^2 = (a - |b|)x^2 + cy^2 \\ &\geqslant a - |b| + c \end{aligned}$$

Thus, if

$$\begin{pmatrix} x \\ y \end{pmatrix} \in S^o \quad \text{then} \quad |f(x,y)| \geqslant a - |b| + c. \tag{3.2.11}$$

We also note that

$$f(\pm 1, 0) = a \tag{3.2.12}$$

$$f(0, \pm 1) = c \tag{3.2.13}$$

Note that

$$S = S^o \sqcup \begin{pmatrix} \pm 1 \\ 0 \end{pmatrix} \sqcup \begin{pmatrix} 0 \\ \pm 1 \end{pmatrix}$$

and since f is reduced we have

$$a \leqslant c \leqslant (a - |b|) + c.$$

It is important to note that all these values are attained. In particular, the value $a - |b| + c$ is attained by f at one of $(1, 1)$ or $(1, -1)$.

Using the above and (3.2.11), it follows that the smallest integer in the set $f(S)$ is a. Thus, we can recover a from the set $f(S)$. The cardinality of the set $f(S)$ is infinite, as can be seen by looking at the values $f(x, 0)$ or $f(0, y)$. If we let

$$\alpha < \beta$$

be the two smallest integers which appear in $f(S)$, then we have just seen that $a = \alpha$.

Next we will consider several cases depending on the cardinality of the set $(f|_S)^{-1}(a)$. Note that

$$a = f(\pm 1, 0) \leqslant c = f(0, \pm 1) \leqslant a - |b| + c \leqslant \min_{s \in S^o} f(s)\,.$$

Thus, $(f|_S)^{-1}(a) \supset \{(\pm 1, 0)\}$ and so $\#(f|_S)^{-1}(a) \geqslant 2$. The only possible cases are $\#(f|_S)^{-1}(a) = 2$, $\#(f|_S)^{-1}(a) = 4$ and $\#(f|_S)^{-1}(a) > 4$.

1. If $\#(f|_S)^{-1}(a) = 2$. This can happen only

   $$(f|_S)^{-1}(a) = \{(\pm 1, 0)\}\,.$$

   Then it follows that $a < c$. Thus, it follows that c is the second smallest integer in the set $f(S)$, that is, $c = \beta$. Once we know a and c in terms of α, β, we also know $|b|$ since the discriminant is d.

2. If $\#(f|_S)^{-1}(a) = 4$. This can happen only

   $$(f|_S)^{-1}(a) = \{(\pm 1, 0), (0, \pm 1)\}\,.$$

   This forces that $a = c < a - |b| + c$. It follows that we can recover $a - |b| + c$ as the second smallest integer in the set $f(S)$, that is, $a - |b| + c = \beta$. Again, it follows that we can recover $a, |b|, c$ in terms of α, β.

3. $\#(f|_S)^{-1}(a) > 4$. This can happen only if an element of S^o maps to a. This forces $\alpha = a = c = a - |b| + c$, that is, $\alpha = a = |b| = c$. Thus, in this case too, we can recover $a, |b|, c$ in terms of α, β.

The above discussion shows that from the pair $(f(S), \#(f|_S)^{-1}(a))$ we can recover $a, |b|, c$.

Let $f(x, y) = ax^2 + bxy + cy^2$ and $g(x, y) = a'x^2 + b'xy + c'y^2$ be reduced binary quadratic forms such that $f \sim g$. By Proposition 3.2.9 and since the values taken by f and g on S are the same, it follows that $f(S) = g(S)$. In particular, the smallest elements in these sets are the same, and so $a = a'$. Again, by Proposition 3.2.9 it follows that

$$(f(S), \#(f|_S)^{-1}(a)) = (g(S), \#(g|_S)^{-1}(a'))\,.$$

It follows then that

$$a = a',\ |b| = |b'|,\ c = c'\,.$$

We claim that $b = b'$. If $b \neq b'$, then $b' = -b$ and we get $f(x, y) = ax^2 + bxy + cy^2$, $g(x, y) = ax^2 - bxy + cy^2$. If $a = c$, then $b \geqslant 0$ (as f is reduced) and $-b \geqslant 0$ (as g is reduced). So we get $b = 0 = -b = b'$, a contradiction. If $a < c$, then $b = a$ implies $-b = -a$, which is not possible as g being reduced implies

$$-a < -b \leqslant a < c\,.$$

Hence, if $a < c$ then $|b| < a < c$. This forces that

$$a = f(\pm 1, 0) < c = f(0, \pm 1) < a - |b| + c \leqslant \min_{s \in S^o} f(s)\,.$$

In particular, the above forces that

$$(f|_S)^{-1}(a) = \{(\pm 1, 0)\}\,, \quad (f|_S)^{-1}(c) = \{(0, \pm 1)\}\,.$$

Let $g = f \circ U$ where $U = \begin{bmatrix} p & q \\ r & s \end{bmatrix}$ with $ps - qr = 1$. Then $a = g\begin{pmatrix} 1 \\ 0 \end{pmatrix} = f\begin{pmatrix} p \\ r \end{pmatrix}$. The vector $\begin{pmatrix} p \\ r \end{pmatrix} \in S$ and as we saw above, the only choice for $\begin{pmatrix} p \\ r \end{pmatrix}$ is $\begin{pmatrix} \pm 1 \\ 0 \end{pmatrix}$. Similarly, $c = g\begin{pmatrix} 0 \\ 1 \end{pmatrix} = f\begin{pmatrix} q \\ s \end{pmatrix}$ and the only choice for $\begin{pmatrix} q \\ s \end{pmatrix}$ is $\begin{pmatrix} 0 \\ \pm 1 \end{pmatrix}$. Now, $\det(U) = 1$ implies $U = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ or $\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$. In either case, $g = f \circ U = f$, which shows that $b = b'$, a contradiction. This proves $b = b'$ and so $f = g$ as desired. □

The number of reduced quadratic forms of discriminant d with $a > 0$ is denoted by $h(d)$. Clearly, $h(d) = 0$ if $d \not\equiv 0$ or 1 (mod 4).

As an example, let us write down all reduced quadratic forms with discriminant -4. As $d = b^2 - 4ac = -4$ and $|b| \leqslant a \leqslant c$ implies $a = c = 1$, $b = 0$, that is, there is only one reduced quadratic form with discriminant -4. Hence, $h(-4) = 1$.

3.3 Representations by Binary Quadratic Forms

We say a number n is properly represented by f if there exists $\begin{pmatrix} x \\ y \end{pmatrix} \in S$ (see Definition 3.2.8) $f(x, y) = n$. Note that if n is representable by f and $f' \sim f$, then n is also representable by f' as f and f' take the same values on S.

Proposition 3.3.1. *n is properly representable by a quadratic form of discriminant d if and only if the quadratic congruence $x^2 \equiv d$ (mod $4n$) has a solution.*

Proof. Assume $x^2 \equiv d \pmod{4n}$ has a solution, say b. Then $b^2 - d = 4nc$ for some $c \in \mathbb{Z}$. Let $f(x,y) = nx^2 + bxy + cy^2$. Then $Disc(f) = d$ and $f(1,0) = n$. Hence, n is properly representable by f.

Conversely, suppose n is properly representable. Then there exists $\begin{pmatrix} p \\ r \end{pmatrix}$ such that $\gcd(p,r) = 1$ and $f(p,r) = n$ for some f with $Disc(f) = d$. Since $\gcd(p,r) = 1$, there exist $s, q \in \mathbb{Z}$ such that $ps - qr = 1$. Let $f' = f \circ U$, where

$$U := \begin{bmatrix} p & q \\ r & s \end{bmatrix} \in SL_2(\mathbb{Z})$$

Now $f' \begin{pmatrix} 1 \\ 0 \end{pmatrix} = f \begin{pmatrix} p \\ r \end{pmatrix} = n$. Thus, $f'(x,y) = nx^2 + bxy + cy^2$ for some $b, c \in \mathbb{Z}$. Since $f' \sim f$ we have $Disc(f') = Disc(f) = d$.

$$Disc(f') = b^2 - 4nc = d$$

Hence $x^2 \equiv d \pmod{4n}$ has a solution, namely b. □

Proposition 3.3.2. *Let $n = x^2 + y^2$. Let p be a prime which divides n and suppose $p \equiv 3$ (mod 4). Then an even power of p appears in prime factorization of n.*

Proof. We go modulo p. If p does not divide y, then $(xy^{-1})^2 \equiv -1$ (mod p). Raising both sides to the power $\frac{p-1}{2}$, $(xy^{-1})^{p-1} \equiv (-1)^{\frac{p-1}{2}} \equiv -1$ (mod p) as $p \equiv 3 \pmod 4$. By Fermat's Little Theorem we have

$$(xy^{-1})^{p-1} \equiv 1 \equiv -1 \pmod{p}.$$

This is not possible. Hence, $p|y$ and similarly, $p|x$.

Let $x = px',\ y = py'$. Then $p^2|n$ and

$$x'^2 + y'^2 = \frac{n}{p^2}.$$

If p does not divide $\frac{n}{p^2}$ then this shows that p occurs with an even power in the prime factorization of n. If p divides $\frac{n}{p^2}$ then we repeat the above process. Proceeding in this way we get that the power of p that appears in the prime factorization of n is even. □

Proposition 3.3.3. *Let p be a prime such that $p \equiv 1$ (mod 4). Then there exist $x, y \in \mathbb{Z}$ such that $x^2 + y^2 = p$.*

Proof. Note that $Disc(x^2 + y^2) = -4$ and we checked that $h(-4) = 1$, that is, there is only one reduced quadratic form of discriminant -4. So it is enough to show that there exists some binary quadratic form of discriminant -4 such that p is representable by f. Then it will follow that the unique reduced binary quadratic form in the equivalence class of f also takes the value p. But this reduced quadratic form is forced to be $x^2 + y^2$.

By Proposition 3.3.1, n is properly representable by such a binary quadratic form iff $x^2 \equiv -4 \pmod{4p}$ has a solution. As $p \equiv 1 \pmod 4$, $\left(\frac{-1}{p}\right) = 1$. Hence, there exists $\alpha \in \mathbb{Z}$, such that $\alpha^2 \equiv -1 \pmod p$. Clearly, 2α is a solution of the quadratic congruence $x^2 \equiv -4 \pmod{4p}$. Hence, proved. □

Proposition 3.3.4. *Let n be a positive integer. Then we can write n uniquely as $n = ml^2$, where m is a square free positive integer. Suppose every odd prime p which divides m is congruent to 1 mod 4. Then n can be written as a sum of two squares.*

Proof. The hypothesis can also be phrased as follows. If p is congruent to 3 mod 4 and p divides n, then an even power of p appears in the prime factorization of n.

We can write $n = m \times l^2$ such that m is square-free. By assumption, if p divides m, then $p \equiv 1 \pmod 4$ or $p = 2$. It is enough to show that m is a sum of squares as $x^2 + y^2 = m$ implies $(lx)^2 + (ly)^2 = n$. Consider the identity,

$$(x^2 + y^2)(x'^2 + y'^2) = (xx' - yy')^2 + (xy' + yx')^2$$

This implies that if a and b are sum of squares, then so is ab. We are done as by Proposition 3.3.3, any prime p of the form $p \equiv 1 \pmod 4$ is the sum of two squares and $2 = 1^2 + 1^2$. □

3.4 Lagrange's Four Square Theorem

Theorem 3.4.1 (Lagrange's Four Squares Theorem)**.** *Every $n \geqslant 0$ is a sum of four squares.*

Proof. Note that

$$\begin{aligned}(x^2 + y^2 + z^2 + w^2)(x'^2 + y'^2 + z'^2 + w'^2) = (xx' + yy' + zz' + ww')^2 + \\ (xy' - yx' + wz' - zw')^2 + (xz' - zx' + yw' - wy')^2 \\ + (xw' - wx' + zy' - yz')^2 \,.\end{aligned}$$

In view of this identity, it is enough to show that every prime is a sum of four squares. Observe that $2 = 1^2 + 1^2 + 0^2 + 0^2$.

Let p be an odd prime. Let $T := \{z \mid 0 \leqslant z \leqslant \frac{p-1}{2}\}$. Define

$$T_1 := \{z^2 \pmod p \mid z \in T\} \qquad T_2 := \{-1 - z^2 \pmod p \mid z \in T\}\,.$$

Observe that $\#T_1 = \#T_2 = \frac{p+1}{2}$ since $z_1^2 \equiv z_2^2 \pmod p$ or $-1 - z_1^2 \equiv -1 - z_2^2 \pmod p$ implies $z_1 \equiv z_2 \pmod p$ or $z_1 \equiv -z_2 \pmod p$ which forces $z_1 = z_2$ as $z_1, z_2 \in T$. Hence, there exists $x, y \in T$ such that $x^2 \equiv -1 - y^2 \pmod p$, that is, $x^2 + y^2 + 1 = l_1 p$ for some $l_1 \in \mathbb{Z}$. Note that

$$l_1 p = x^2 + y^2 + 1 < \frac{p^2}{2} + \frac{p^2}{2} + 1 < p^2\,.$$

This implies $0 < l < p$. Let l be the smallest positive integer such that $lp = x^2 + y^2 + z^2 + w^2$ for some $x, y, z, w \in \mathbb{Z}$. We just proved that $l < p$. We will show that $l = 1$. If possible let $l > 1$.

Claim: l is odd.
If l is even, then either 0, 2 or 4 of x, y, z, w are odd. Without loss of generality, we may assume that $x \pm y$ and $z \pm w$ are even. Then

$$\frac{l}{2}p = \frac{(x+y)^2}{4} + \frac{(x-y)^2}{4} + \frac{(z+w)^2}{4} + \frac{(z-w)^2}{4} = \frac{x^2 + y^2 + z^2 + w^2}{2}\,.$$

contradicting the minimality of l. This proves the claim.

The integers $s' \in [-\frac{l-1}{2}, \frac{l-1}{2}]$ form a full set of residues modulo l. Let $x' \in [-\frac{l-1}{2}, \frac{l-1}{2}]$ be such that $x \equiv x' \pmod l$. Define y', z' and w' in a similar way. Then

$$x'^2 + y'^2 + z'^2 + w'^2 \equiv x^2 + y^2 + z^2 + w^2 \equiv 0 \pmod l,$$

that is, $x'^2 + y'^2 + z'^2 + w'^2 = kl$ for some $k \in \mathbb{Z}$. Clearly that $k > 0$. Note that

$$kl < \frac{l^2}{4} + \frac{l^2}{4} + \frac{l^2}{4} + \frac{l^2}{4} = l^2\,,$$

that is, $k < l$. Then

$$\begin{aligned}(kl)(lp) &= (x^2 + y^2 + z^2 + w^2)(x'^2 + y'^2 + z'^2 + w'^2)\\ &= (xx' + yy' + zz' + ww')^2 + (xy' - yx' + wz' - zw')^2\\ &\quad + (xz' - zx' + yw' - wy')^2 + (xw' - wx' + zy' - yz')^2\end{aligned} \tag{3.4.2}$$

Consider $xx' + yy' + zz' + ww'$. Going modulo l,

$$xx' + yy' + zz' + ww' \equiv x^2 + y^2 + z^2 + w^2 \equiv 0 \bmod l$$

Hence, l divides $(xx' + yy' + zz' + ww')$. Similarly check that l divides $(xy' - yx' + wz' - zw')$, $(xz' - zx' + yw' - wy')$ and $(xw' - wx' + zy' - yz')$. Let

$$\begin{aligned}(xx' + yy' + zz' + ww') =& \alpha_1 l,\\ (xy' - yx' + wz' - zw') =& \alpha_2 l,\\ (xz' - zx' + yw' - wy') =& \alpha_3 l,\\ (xw' - wx' + zy' - yz') =& \alpha_4 l\end{aligned}$$

Then 3.4.2 becomes

$$kpl^2 = (\alpha_1 l)^2 + (\alpha_2 l)^2 + (\alpha_3 l)^2 + (\alpha_4 l)^2 \tag{3.4.3}$$

which implies $kp = \alpha_1^2 + \alpha_2^2 + \alpha_3^2 + \alpha_4^2$. This contradicts the minimality of l. Hence, $l = 1$, completing the proof. □

Chapter 4

Continued Fractions

4.1 Dirichlet's Theorem on approximations

Proposition 4.1.1. *Let $\theta \in \mathbb{R}$ and let q be a positive integer. Then $\exists p \in \mathbb{Z}$ such that $\left|\theta - \frac{p}{q}\right| \leqslant \frac{1}{q}$*

Proof. We can write

$$\mathbb{R} = \bigcup_{k \in \mathbb{Z}} \left[\frac{k}{q}, \frac{k+1}{q}\right].$$

Since θ is in one of these intervals, the proposition is clear. □

Theorem 4.1.2 (Dirichlet)**.** *Let $Q > 1$ be an integer. Given any $\theta \in \mathbb{R}$, we can find $p, q \in \mathbb{Z}$ such that $0 < q < Q$ and*

$$\left|\theta - \frac{p}{q}\right| \leqslant \frac{1}{qQ}$$

Proof. Consider the intervals $\left[0, \frac{1}{Q}\right], \left[\frac{1}{Q}, \frac{2}{Q}\right] \dots \left[\frac{Q-1}{Q}, 1\right]$. These are Q intervals and each of these has width $\frac{1}{Q}$. For an real number α, let $\{\alpha\}$ denote the fractional part, that is, $\{\alpha\} := \alpha - \lfloor \alpha \rfloor$. Clearly $0 \leqslant \{\alpha\} < 1$. Consider the set

$$S = \{0, \{\theta\}, \{2\theta\} \dots \{(Q-1)\theta\}, 1\}$$

S has $Q + 1$ elements (note that some of these may be equal), so by the pigeon-hole principle, at least two of these belong to the same interval. Clearly 0 and 1 cannot be in the same interval. Thus, either $\{i\theta\}$ and 1 are in the same interval, or $\{i_1\theta\}$ and $\{i_2\theta\}$ are in the same interval. We know that $\{i\theta\} = i\theta - p$, for some $p \in \mathbb{Z}$. In the first case we get

$$|(i\theta - p) - 1| \leqslant \frac{1}{Q} \qquad\qquad 0 < i < Q\,.$$

In the second case we get

$$|(i_1\theta - p_1) - (i_2\theta - p_2)| \leqslant \frac{1}{Q} \qquad\qquad i_1 \neq i_2.$$

Letting $q = i$ or $|i_1 - i_2|$, it is clear that $0 < q < Q$ and that

$$\left|\theta - \frac{p}{q}\right| \leqslant \frac{1}{qQ}$$

This completes the proof of the theorem. □

Proposition 4.1.3. *If $\theta \in \mathbb{Q}$ then there exist only finitely many pairs $p, q \in \mathbb{Z}$ with $q > 0$ and such that*

$$0 < \left|\theta - \frac{p}{q}\right| \leqslant \frac{1}{q^2} \tag{4.1.4}$$

Proof. Let $\theta = \frac{a}{b}$ with $b > 0$. Let $p, q \in \mathbb{Z}$ with $q > 0$ be such that

$$0 < \left|\frac{a}{b} - \frac{p}{q}\right| \leqslant \frac{1}{q^2}\,.$$

Then (since $1 \leqslant |aq - bp|$ as all of them are integers)

$$\frac{1}{bq} \leqslant \frac{|aq - bp|}{bq} \leqslant \frac{1}{q^2}$$

Thus, $q \leqslant b$ and so there are only finitely many choices for q. For a fixed q there can be only finitely many $p \in \mathbb{Z}$ such that

$$\frac{a}{b} \in \left[\frac{p}{q} - \frac{1}{q^2}, \frac{p}{q} + \frac{1}{q^2}\right]\,.$$

Thus, the number of pairs for which the condition holds is finite. □

Proposition 4.1.5. *Let $\theta \in \mathbb{R} \setminus \mathbb{Q}$, then there are infinitely many pairs $p, q \in \mathbb{Z}$ with $q > 0$ such that equation* (4.1.4) *holds.*

Proof. Fix any $Q_1 > 1$ and find, using Theorem 4.1.2, $\frac{p_1}{q_1}, 0 < q_1 < Q_1$ such that

$$\left|\theta - \frac{p_1}{q_1}\right| \leqslant \frac{1}{q_1 Q_1} < \frac{1}{q_1^2}$$

Since θ is irrational, $\theta - \frac{p_1}{q_1} \neq 0$. Thus, $\exists Q_2 > 0$ such that

$$0 < \frac{1}{Q_2} < \left|\theta - \frac{p_1}{q_1}\right| < \frac{1}{q_1^2}$$

Applying Theorem 4.1.2 to Q_2, we get $\frac{p_2}{q_2}$ such that

$$\left|\theta - \frac{p_2}{q_2}\right| \leqslant \frac{1}{q_2 Q_2} < \frac{1}{q_2^2}$$

We also have

$$\left|\theta - \frac{p_2}{q_2}\right| \leqslant \frac{1}{q_2 Q_2} \leqslant \frac{1}{Q_2} < \left|\theta - \frac{p_1}{q_1}\right|$$

Since the inequality is strict, we get $\frac{p_2}{q_2} \neq \frac{p_1}{q_1}$. Proceeding in this manner, we get a sequence of distinct rational numbers $\frac{p_n}{q_n}$ which satisfy the condition

$$\left|\theta - \frac{p}{q}\right| < \frac{1}{q^2} \tag{4.1.6}$$

□

4.2 Continued fractions

Let θ be an irrational number. We saw that there is an infinite sequence of rational numbers $\frac{p}{q}$ which satisfy equation (4.1.6). Now we will explain a construction which produces such a sequence of rationals for a given θ.

Continued fraction expansion of θ: Let $\theta = \theta_0 \in \mathbb{R}$. Define the continued fraction expansion of θ as follows.

- Define $a_0 \in \mathbb{Z}$ to be the unique integer which satisfies $0 \leqslant \theta_0 - a_0 < 1$
- if $\theta_0 - a_0 = 0$ then the continued fraction expansion of θ is $[a_0]$.
- if $0 < \theta_0 - a_0 < 1$, define $\theta_1 = \frac{1}{\theta_0 - a_0}$. Thus, $\theta_1 > 1$.
- For $i \geqslant 1$ and $\theta_{i-1} - a_{i-1} \neq 0$

- Define $a_i \in \mathbb{Z}_{\geqslant 1}$ to be the unique integer which satisfies $0 \leqslant \theta_i - a_i < 1$
- if $\theta_i - a_i = 0$ then the continued fraction expansion of θ is $[a_0, a_1, \ldots, a_i]$.
- if $0 < \theta_i - a_i < 1$, define $\theta_{i+1} = \frac{1}{\theta_i - a_i}$.

Here are two examples.

1. Consider $\theta = \frac{15}{8}$.

$$\begin{aligned} \frac{15}{8} &= 1 + \frac{7}{8} \\ &= 1 + \frac{1}{1 + \frac{1}{7}} \end{aligned}$$

Thus $\theta = 1.875 = [1, 1, 7] = 1 + \frac{1}{1+\frac{1}{7}}$

2. For $\theta = \sqrt{2}$. Note that

$$\sqrt{2} + 1 = 2 + \frac{1}{\sqrt{2}+1}$$

Thus, we get

$$\begin{aligned} \sqrt{2} &= 1 + \sqrt{2} - 1 \\ &= 1 + \frac{1}{\sqrt{2}+1} \\ &= 1 + \frac{1}{2 + \frac{1}{\sqrt{2}+1}} \\ &= 1 + \frac{1}{2 + \frac{1}{2+\frac{1}{\sqrt{2}+1}}} \end{aligned}$$

Thus, we get $\sqrt{2} = [1, 2, 2, 2, \ldots]$.

Proposition 4.2.1. *If the algorithm for obtaining the continued fraction expansion for θ stops in finitely many steps, then $\theta \in \mathbb{Q}$.*

Proof. Clearly we have

$$\begin{aligned}\theta = \theta_0 &= a_0 + \frac{1}{\theta_1} \\ &= a_0 + \frac{1}{a_1 + \frac{1}{\theta_2}} \\ &= \cdots\end{aligned}$$

As this process stops in finitely many steps, we get that θ is rational. □

Proposition 4.2.2. *If $\theta \in \mathbb{Q}$, then the continued fraction expansion of θ is finite.*

Proof. Let $\theta = \frac{p}{q}$. The proof is by induction on q. If $q = 1$, the process stops at a_0. Assume $q > 1$, then a_0 is such that $0 < \frac{p}{q} - a_0 < 1$. Thus, $0 < p - qa_0 < q$. As $\theta_1 = \frac{1}{\frac{p}{q} - a_0} = \frac{q}{p - a_0 q}$, by induction hypothesis, the continued fraction expression for θ_1 is finite. Hence the same holds for θ.

We have used the following, which is clear. If the continued fraction expansion of θ_1 is $[b_0, b_1, \ldots]$, then the continued fraction expansion of θ is $[a_0, b_0, b_1, \ldots]$. □

Definition 4.2.3 (Convergents)**.** *Let $\theta = [a_0, a_1, \ldots] \in \mathbb{R} \setminus \mathbb{Q}$. For $n \geqslant 0$, define $p_0 = a_0$, $q_0 = 1$, $p_1 = a_0 a_1 + 1$ and $q_1 = a_1$. Inductively define integers*

$$p_n := a_n p_{n-1} + p_{n-2}\,, \quad q_n := a_n q_{n-1} + q_{n-2}\,.$$

Proposition 4.2.4. $\frac{p_n}{q_n} = [a_0, a_1, \ldots, a_n]$.

Proof. To indicate the dependence of θ on a_i, p_i, q_i, we shall use the notation $a_i(\theta)$, $p_i(\theta)$ and $q_i(\theta)$. Recall $\theta_1 = [a_1, a_2, \ldots] \in \mathbb{R} \setminus \mathbb{Q}$.

We claim that for all $n \geqslant 1$

$$q_n(\theta) = p_{n-1}(\theta_1)\,.$$

If $n = 1$ then we have using definitions that $q_1(\theta) = a_1 = p_0(\theta_1)$. If $n = 2$ then we have $q_2(\theta) = a_2 a_1 + 1$. On the other hand

$$p_1(\theta_1) = a_0(\theta_1) a_1(\theta_1) + 1 = a_1 a_2 + 1\,.$$

This shows that $p_1(\theta_1) = q_2(\theta)$. Let $n \geqslant 3$. Using the definition of $q_n(\theta)$ and induction we get

$$\begin{aligned} q_n(\theta) &= a_n q_{n-1}(\theta) + q_{n-2}(\theta) \\ &= a_{n-1}(\theta_1) p_{n-2}(\theta_1) + p_{n-3}(\theta_1) \\ &= p_{n-1}(\theta_1)\,. \end{aligned}$$

This proves the claim.

In the same way let us show that for $n \geqslant 1$

$$p_n(\theta) = a_0 q_n(\theta) + q_{n-1}(\theta_1)\,.$$

Using definitions one checks that this is true for $n = 1$. When $n = 2$, one checks that

$$\begin{aligned} p_2(\theta) &= a_0 a_1 a_2 + a_2 + a_0 \\ &= a_0(a_1 a_2 + 1) + a_2 \\ &= a_0 q_2(\theta) + q_1(\theta_1) \end{aligned}$$

This proves the claim when $n = 2$. Assume that $n \geqslant 3$. Using induction and definitions we easily see

$$\begin{aligned} a_0 q_n(\theta) + q_{n-1}(\theta_1) &= a_0(a_n q_{n-1}(\theta) + q_{n-2}(\theta)) + a_{n-1}(\theta_1) q_{n-2}(\theta_1) + q_{n-3}(\theta_1) \\ &= a_n(a_0 q_{n-1}(\theta) + q_{n-2}(\theta_1)) + a_0 q_{n-2}(\theta) + q_{n-3}(\theta_1) \\ &= a_n p_{n-1}(\theta) + p_{n-2}(\theta) \\ &= p_n(\theta)\,. \end{aligned}$$

This proves the claim.

To prove the Proposition we need to show that

$$\frac{p_n(\theta)}{q_n(\theta)} = a_0 + \frac{1}{[a_1, \ldots, a_n]}\,.$$

But showing this is equivalent to showing that

$$\frac{p_n(\theta) - a_0 q_n(\theta)}{q_n(\theta)} = \frac{q_{n-1}(\theta_1)}{p_{n-1}(\theta_1)}\,.$$

But this is clear in view of the above two claims. This completes the proof of the Proposition. □

Remark 4.2.5. Suppose we are given a sequence of real numbers a_i for $0 \leqslant i \leqslant n+1$ such that $a_i > 0$ for $i > 0$. Then we may define a sequence of real numbers as follows. For $0 \leqslant i \leqslant n+1$, define $p_0 = a_0$, $q_0 = 1$, $p_1 = a_0 a_1 + 1$ and $q_1 = a_1$. Inductively real numbers

$$p_i := a_i p_{i-1} + p_{i-2}\,, \quad q_i := a_i q_{i-1} + q_{i-2}\,.$$

The proof of the previous proposition shows that

$$\frac{p_i}{q_i} = [a_0, a_1, \ldots, a_i]\,.$$

Proposition 4.2.6. *$\gcd(p_n, q_n) = 1$.*

Proof. Since

$$\begin{aligned} p_n &= a_n p_{n-1} + p_{n-2} \\ q_n &= a_n q_{n-1} + q_{n-2} \\ \therefore \qquad p_n q_{n-1} - q_n p_{n-1} &= p_{n-2} q_{n-1} - q_{n-2} p_{n-1} \end{aligned}$$

Thus, we have

$$|p_n q_{n-1} - q_n p_{n-1}| = |p_{n-1} q_{n-2} - q_{n-1} p_{n-2}| = \cdots = |p_1 q_0 - q_1 p_0|$$

$$|p_1 q_0 - q_1 p_0| = |(a_0 a_1 + 1) - a_1 a_0| = 1$$

$$\therefore \quad |p_n q_{n-1} - q_n p_{n-1}| = 1 \tag{4.2.7}$$

Hence, we can find integers $r, s \in \mathbb{Z}$ such that, $rp_n + sq_n = 1$. Thus, $\gcd(p_n, q_n) = 1$. □

Corollary 4.2.8. *$\lim_{n\to\infty} \left|\frac{p_n}{q_n} - \frac{p_{n+1}}{q_{n+1}}\right| = 0$.*

Proof. Recall from (4.2.7) that we have $|p_n q_{n+1} - q_n p_{n+1}| = 1$. Thus,

$$\left|\frac{p_n}{q_n} - \frac{p_{n+1}}{q_{n+1}}\right| = \frac{1}{q_n q_{n+1}}$$

Since $q_0 = 1$, $q_1 = a_1 \geqslant 1$, and $q_n = a_n q_{n-1} + q_{n-2}$, where $a_n \geqslant 1$, we see that q_i is a strictly increasing sequence for $i \geqslant 1$. This proves the corollary. □

Corollary 4.2.9. *$\frac{p_n}{q_n} \to \theta$.*

Proof. Notice that, if $0 < \gamma < \beta$, then

$$[\alpha, \beta] = \alpha + \frac{1}{\beta} < \alpha + \frac{1}{\gamma} = [\alpha, \gamma]$$

Now

$$[a_n, a_{n+1}, a_{n+2}] = a_n + \frac{1}{a_{n+1} + \frac{1}{a_{n+2}}} > a_n.$$

Using this for $\alpha = a_{n-1}$, $\beta = [a_n, a_{n+1}, a_{n+2}]$, and $\gamma = a_n$

$$[a_{n-1}, a_n, a_{n+1}, a_{n+2}] < [a_{n-1}, a_n]$$

In the same manner

$$[a_{n-2}, a_{n-1}, a_n, a_{n+1}, a_{n+2}] > [a_{n-2}, a_{n-1}, a_n] \quad \ldots$$

If n is even, $n = 2k$

$$[a_0, a_1, \ldots a_{2k+2}] > [a_0, a_1, \ldots a_{2k}]$$

This shows that

$$\frac{p_{2k+2}}{q_{2k+2}} > \frac{p_{2k}}{q_{2k}}.$$

That is the sequence $\frac{p_{2k}}{q_{2k}}$ is an increasing sequence.

If n is odd, $n = 2k + 1$

$$[a_1, a_2, \ldots a_{2k+1}] > [a_1, a_2, \ldots a_{2k-1}]$$
$$[a_0, a_1, \ldots a_{2k+1}] < [a_0, a_1, \ldots a_{2k-1}]$$

Thus,

$$\frac{p_{2k+1}}{q_{2k+1}} < \frac{p_{2k-1}}{q_{2k-1}}.$$

That is, the sequence $\frac{p_{2k+1}}{q_{2k+1}}$ is a decreasing sequence.

Consider $\theta = [a_0, a_1, \ldots a_n, \theta_{n+1}]$

$$[a_n, \theta_{n+1}] = a_n + \frac{1}{\theta_{n+1}} > a_n$$
$$\implies [a_{n-1}, a_n, \theta_{n+1}] < [a_{n-1}, a_n]$$
$$\implies [a_{n-3}, a_{n-2}, a_{n-1}, a_n, \theta_{n+1}] < [a_{n-2}, a_{n-1}, a_n, \theta_{n+1}] \quad \text{and so on}$$

Thus, $[a_0, a_1, \dots a_n, \theta_{n+1}] < [a_0, a_1, \dots a_n]$ implies $\theta < \frac{p_n}{q_n}$ for odd n. Similarly, $\theta > \frac{p_n}{q_n}$ for even n. The sequence $\frac{p_{2k}}{q_{2k}}$ is an increasing sequence bounded above by θ, the sequence $\frac{p_{2k-1}}{q_{2k-1}}$ is a decreasing sequence bounded below by θ. Using the previous corollary it follows easily that $\frac{p_n}{q_n} \to \theta$. □

Corollary 4.2.10. $\left|\theta - \frac{p_n}{q_n}\right| < \frac{1}{q_n^2}$.

Proof. We know, from the proof of the previous corollary, that $\frac{p_n}{q_n} < \theta < \frac{p_{n+1}}{q_{n+1}}$ or $\frac{p_{n+1}}{q_{n+1}} < \theta < \frac{p_n}{q_n}$, depending on the parity of n.

$$\begin{aligned}\left|\theta - \frac{p_n}{q_n}\right| &< \left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right| \\ &= \frac{1}{q_n q_{n+1}} \qquad (|p_{n+1}q_n - p_n q_{n+1}| = 1) \\ &< \frac{1}{q_n^2} \qquad (q_{n+1} > q_n \text{ for } n \geqslant 2)\end{aligned}$$

□

Corollary 4.2.11. *For any n, either $\left|\theta - \frac{p_n}{q_n}\right| \leqslant \frac{1}{2q_n^2}$ or $\left|\theta - \frac{p_{n+1}}{q_{n+1}}\right| \leqslant \frac{1}{2q_{n+1}^2}$.*

Proof. Assume that $\left|\theta - \frac{p_i}{q_i}\right| > \frac{1}{2q_i^2}$ for $i = n, n+1$. Since θ lies between $\frac{p_n}{q_n}$ and $\frac{p_{n+1}}{q_{n+1}}$ we get

$$\left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right| > \frac{1}{2}\left(\frac{1}{q_n^2} + \frac{1}{q_{n+1}^2}\right) \geqslant \frac{1}{2} \cdot \frac{2}{q_n q_{n+1}}$$

Thus,

$$\left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right| > \frac{1}{q_n q_{n+1}}$$

which is a contradiction. □

Corollary 4.2.12. *Given $\theta \in \mathbb{R}\backslash\mathbb{Q}$, there is an infinite sequence of rationals $\frac{p_n}{q_n}$ such that, $\left|\theta - \frac{p_n}{q_n}\right| < \frac{1}{2q_n^2}$.*

Next we prove a very surprising result.

Theorem 4.2.13. *If $\left|\theta - \frac{p}{q}\right| < \frac{1}{2q^2}$ then $\frac{p}{q} = \frac{p_n}{q_n}$ for some n.*

Proof. First, we show that $|q_n\theta - p_n| > |q_{n+1}\theta - p_{n+1}|$. Recall by definition of θ_{n+1} we have $\theta = [a_0, a_1, \dots, a_n, \theta_{n+1}]$. As in Remark 4.2.5 we define p_i and q_i, and we have

$$\begin{aligned} p_{n+1} &= \theta_{n+1}p_n + p_{n-1}\,, \\ q_{n+1} &= \theta_{n+1}q_n + q_{n-1}\,, \end{aligned}$$

such that $\frac{p_{n+1}}{q_{n+1}} = [a_0, \dots, a_n, \theta_{n+1}]$. Thus,

$$\theta = \frac{p_{n+1}}{q_{n+1}} = \frac{\theta_{n+1}p_n + p_{n-1}}{\theta_{n+1}q_n + q_{n-1}}\,.$$

Using this we get

$$\begin{aligned} \theta\theta_{n+1}q_n + \theta q_{n-1} &= \theta_{n+1}p_n - p_{n-1} \\ \implies |\theta q_{n-1} - p_{n-1}| &= \theta_{n+1}|\theta q_n - p_n| \end{aligned}$$

Since $\theta_{n+1} > 1$, we have $|\theta q_{n-1} - p_{n-1}| > |\theta q_n - p_n|$.

Now let $0 < q < q_{n+1}$. For any $p \in \mathbb{Z}$ we will show that $|q\theta - p| \geqslant |q_n\theta - p_n|$. Since $p_nq_{n+1} + p_{n+1}q_n = \pm 1$, we can solve the system

$$\begin{bmatrix} p_n & p_{n+1} \\ q_n & q_{n+1} \end{bmatrix} \begin{bmatrix} u \\ v \end{bmatrix} = \begin{bmatrix} p \\ q \end{bmatrix}$$

for $u, v \in \mathbb{Z}$. Take the equation $q_nu + q_{n+1}v = q$. If $u = 0$, then $q_{n+1}v = q$, which contradicts our assumption that $q < q_{n+1}$. Thus, $u \neq 0$. If $v = 0$, then $p = up_n$, $q = uq_n$. Thus, $|q\theta - p| = |u||q_n\theta - p_n| \geqslant |q_n\theta - p_n|$ and we are done. If $v \neq 0$, then u and v have opposite signs, or else we will get $q > q_{n+1}$. Thus,

$$\begin{aligned} |q\theta - p| &= |(q_nu + q_{n+1}v)\theta - (p_nu + p_{n+1}v)| \\ &= |u(q_n\theta - p_n) + v(q_{n+1}\theta - p_{n+1})| \end{aligned}$$

We already know (see the proof of Corollary 4.2.9) that $q_n\theta - p_n$ and $q_{n+1}\theta - p_{n+1}$ have opposite signs. Thus, $u(q_n\theta - p_n)$ and $v(q_{n+1}\theta - p_{n+1})$ have the same sign. Thus,

$$|q\theta - p| \geqslant |u(q_n\theta - p_n)| \geqslant |q_n\theta - p_n|.$$

Now we come to proving our theorem. Let n be such that $q_n \leqslant q < q_{n+1}$.

$$\begin{aligned}\left|\frac{p}{q} - \frac{p_n}{q_n}\right| &\leqslant \left|\frac{p}{q} - \theta\right| + \left|\theta - \frac{p_n}{q_n}\right| \\ &= \frac{|p - q\theta|}{q} + \frac{|p_n - q_n\theta|}{q_n} \\ &\leqslant |p - q\theta|\Big(\frac{1}{q} + \frac{1}{q_n}\Big) \\ &< \frac{1}{2q}\Big(\frac{1}{q} + \frac{1}{q_n}\Big) \\ &< \frac{1}{2q} \cdot \frac{2}{q_n} \qquad \text{(Since } q > q_n\text{)}\end{aligned}$$

Thus, we arrive at the result,

$$\frac{1}{qq_n} \cdot |pq_n - p_nq| < \frac{1}{qq_n}$$

which implies that $|pq_n - p_nq| < 1$. Since $|pq_n - p_nq|$ is an integer, it has to be zero which implies $\frac{p}{q} = \frac{p_n}{q_n}$. □

Proposition 4.2.14. *Given any θ, there is an infinite sequence of rationals such that $\left|\theta - \frac{p}{q}\right| < \frac{1}{\sqrt{5}q^2}$.*

Proof. We will show that, for any $n > 2$, there is an $i \in \{n, n+1, n+2\}$ such that

$$\left|\theta - \frac{p_i}{q_i}\right| < \frac{1}{\sqrt{5}q_i^2}$$

where $\frac{p_i}{q_i}$ are the convergents in the continued fraction expansion of θ.

Assume $\left|\theta - \frac{p_i}{q_i}\right| \geqslant \frac{1}{\sqrt{5}q_i^2}$ for all $i \in \{n, n+1, n+2\}$. Recall that

$$|p_{n+1}q_n - p_nq_{n+1}| = 1.$$

We have

$$\begin{aligned}\frac{1}{q_nq_{n+1}} = \left|\frac{p_n}{q_n} - \frac{p_{n+1}}{q_{n+1}}\right| &= \left|\frac{p_n}{q_n} - \theta\right| + \left|\theta - \frac{p_{n+1}}{q_{n+1}}\right| \\ &\geqslant \frac{1}{\sqrt{5}}\left(\frac{1}{q_n^2} + \frac{1}{q_{n+1}^2}\right)\end{aligned}$$

This shows that

$$\sqrt{5} \geqslant \left(\frac{q_{n+1}}{q_n} + \frac{q_n}{q_{n+1}}\right).$$

Let $\lambda = \frac{q_{n+1}}{q_n}$. Thus, $\sqrt{5} \geqslant \lambda + \frac{1}{\lambda}$. Similarly, for $\nu = \frac{q_{n+2}}{q_{n+1}}$, $\sqrt{5} \geqslant \nu + \frac{1}{\nu}$. Simplifying the equation, (and using that λ, ν are rational)

$$\lambda^2 - \sqrt{5}\lambda + 1 \leqslant 0 \implies \frac{\sqrt{5}-1}{2} < \lambda < \frac{\sqrt{5}+1}{2}$$

$$\nu^2 - \sqrt{5}\nu + 1 \leqslant 0 \implies \frac{\sqrt{5}-1}{2} < \nu < \frac{\sqrt{5}+1}{2}$$

We know that $q_{n+2} = a_{n+2}q_{n+1} + q_n$. Dividing by q_{n+1} we get

$$\nu = a_{n+2} + \frac{1}{\lambda} \geqslant 1 + \frac{1}{\lambda}$$

$$\lambda < \frac{\sqrt{5}+1}{2} \implies \frac{1}{\lambda} > \frac{\sqrt{5}-1}{2}$$

$$\therefore \nu > 1 + \frac{1}{\lambda} = \frac{\sqrt{5}+1}{2}$$

which is a contradiction. □

Corollary 4.2.15. *For $c = \sqrt{5}$, there are infinitely many rationals for any θ such that $\left|\theta - \frac{p}{q}\right| < \frac{1}{cq^2}$.*

Proposition 4.2.16. *$c = \sqrt{5}$ is the best possible bound.*

Proof. We show that there is at least one $\theta \in \mathbb{R}$ for which there is no better bound. Consider $\theta = \frac{\sqrt{5}+1}{2}$, then

$$\theta = 1 + \cfrac{1}{1 + \frac{1}{1+\cdots}}$$

$$\theta = [1, 1, 1 \ldots] = [1, \theta] = [1, 1, \theta] = \ldots$$

One checks easily that for this θ, the convergents satisfy

$$q_n = p_{n-1} \tag{4.2.17}$$

Assume there is a $c > \sqrt{5}$ such that there are infinitely many rationals $\frac{p}{q}$ for which

$$\left|\theta - \frac{p}{q}\right| < \frac{1}{cq^2}.$$

Since $c > 2$, it follows from Theorem 4.2.13 that these rationals are forced to be the convergents. From Remark 4.2.5 it follows that

$$\theta = \frac{p_{n+1}}{q_{n+1}} = \frac{\theta_{n+1}p_n + p_{n-1}}{\theta_{n+1}q_n + q_{n-1}}.$$

This shows (as $\theta_{n+1} = \theta$)

$$\left|\theta - \frac{p_n}{q_n}\right| = \left|\frac{\theta p_n + p_{n-1}}{\theta q_n + q_{n-1}} - \frac{p_n}{q_n}\right| = \frac{1}{q_n(\theta q_n + q_{n-1})}$$

Thus,

$$\frac{1}{cq_n^2} > \left|\theta - \frac{p_n}{q_n}\right| = \frac{1}{q_n(\theta q_n + q_{n-1})}$$

Now using equation (4.2.17) we get

$$c < \theta + \frac{q_{n-1}}{q_n} < \theta + \frac{q_{n-1}}{p_{n-1}}.$$

Taking limit $n \to \infty$ we get

$$c \leqslant \theta + \frac{1}{\theta} = \frac{\sqrt{5}+1}{2} + \frac{\sqrt{5}-1}{2} = \sqrt{5}$$

which is a contradiction. □

4.3 Quadratic irrationals

Let θ be irrational. Then we will say that the continued fraction expansion of θ is periodic, if there are integers $l \geqslant 0, m > 0$ such that if $\theta = [a_0, a_1, \ldots]$ then $a_i = a_{i+m}$ for all $i \geqslant l$. We will denote this by

$$\theta = [a_0, a_1, \ldots, a_{l-1}, \overline{a_l, a_{l+1}, \ldots, a_{l+m-1}}]$$

Theorem 4.3.1. *For any $\theta \in \mathbb{R} \setminus \mathbb{Q}$, the continued fraction expansion of θ is periodic if and only if θ satisfies a quadratic polynomial $\in \mathbb{Q}[x]$*

Proof. Let $\theta \in \mathbb{R} \setminus \mathbb{Q}$ be such that

$$\theta = [a_0, a_1 \ldots a_{l-1}, \overline{a_l, a_{l+1} \ldots a_{l+m-1}}]$$

for some $l \geqslant 0, m > 0$. We will show that θ satisfies a quadratic polynomial over $\mathbb{Q}$. Let

$$\phi = [\overline{a_l, a_{l+1} \ldots a_{l+m-1}}] = [a_l, a_{l+1} \ldots a_{l+m-1}, \phi]$$

If $\frac{p_m}{q_m}$ denotes the convergents of ϕ, then by Remark 4.2.5 we have

$$\phi = \frac{p_m}{q_m} = \frac{\phi p_{m-1} + p_{m-2}}{\phi q_{m-1} + q_{m-2}}$$

It is clear that ϕ satisfies the polynomial

$$X^2 q_{m-1} + X(q_{m-2} - p_{m-1}) - p_{m-2} = 0.$$

Clearly, the subset of $\mathbb{R}$ consisting of elements of the type $a + b\phi$, where $a, b \in \mathbb{Q}$, forms a $\mathbb{Q}$ vector space, call it $F \subset \mathbb{R}$. Since ϕ satisfies a polynomial of degree 2 with coefficients in $\mathbb{Q}$, it is easily checked that the product of two elements of F is in F.

We will now show that if $a+b\phi \in F$ and $a+b\phi \neq 0$ then the real number $\frac{1}{a+b\phi} \in F$. Let $\alpha := a+b\phi$. Since $\alpha \in F$ F is a vector space over $\mathbb{Q}$ of rank 2, we see that $1, \alpha, \alpha^2$ cannot be linearly independent over $\mathbb{Q}$. Thus, α satisfies an equation of the type

$$l\alpha^2 + m\alpha + n = 0.$$

If $l = 0$, then $\alpha \in \mathbb{Q}$ and so clearly $\frac{1}{\alpha} \in \mathbb{Q} \subset F$. So let us assume that $l \neq 0$. If $n = 0$, then we get $\alpha(l\alpha + m) = 0$. Since $\alpha \neq 0$ this shows again that $\alpha \in \mathbb{Q}$. Thus, assume that $l \neq 0, n \neq 0$. In this case we get

$$\frac{1}{\alpha} = \frac{l\alpha + m}{-n} \in F$$

which proves our assertion.

Recall that we wanted to prove that θ satisfies a quadratic polynomial with coefficients in $\mathbb{Q}$. Since

$$\theta = [a_0, a_1, \ldots, a_{l-1}, \phi]$$

it is clear from Remark 4.2.5 that

$$\theta = \frac{a + b\phi}{c + d\phi} = (a + b\phi)\frac{1}{c + d\phi} \in F$$

As $\theta \in F$, we see that $1, \theta, \theta^2$ cannot be linearly independent, and so it follows that θ satisfies a quadratic polynomial with coefficients in $\mathbb{Q}$.

Next we show that if θ is quadratic over $\mathbb{Q}$, then the continued fraction expansion of θ is periodic. Assume θ satisfies $ax^2 + bx + c = 0$. Consider the quadratic form

$$f(X) = X^{\intercal} \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} X = X^{\intercal} A_f X$$

Define $f_n = f \circ U_n$, where $U_n = \begin{bmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{bmatrix}$. Here $\frac{p_n}{q_n}$ are the convergents to θ. Recall $p_n q_{n-1} - q_n p_{n-1} = \pm 1 = \det(U_n)$. It is clear that the discriminant of f (see 3.1.1 and 3.1.6) is equal to the discriminant of f_n. Write

$$f_n \begin{pmatrix} x \\ y \end{pmatrix} = \alpha_n x^2 + \beta_n xy + \gamma_n y^2$$

Then

$$\beta_n^2 - 4\alpha_n \gamma_n = b^2 - 4ac.$$

Since ax^2+bx+c has a real solution which is not rational, we have $b^2-4ac > 0$. Writing $\theta = [a_0, a_1, \dots a_n, \theta_{n+1}]$, we get

$$\theta = \frac{p_n \theta_{n+1} + p_{n-1}}{q_n \theta_{n+1} + q_{n-1}}.$$

$$\begin{aligned} f_n \begin{pmatrix} \theta_{n+1} \\ 1 \end{pmatrix} &= f \circ \begin{bmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{bmatrix} \begin{bmatrix} \theta_{n+1} \\ 1 \end{bmatrix} \\ &= f \begin{pmatrix} p_n \theta_{n+1} + p_{n-1} \\ q_n \theta_{n+1} + q_{n-1} \end{pmatrix} \\ &= f \begin{pmatrix} \frac{p_n \theta_{n+1} + p_{n-1}}{q_n \theta_{n+1} + q_{n-1}} \\ 1 \end{pmatrix} (q_n \theta_{n+1} + q_{n-1})^2 \\ &= f \begin{pmatrix} \theta \\ 1 \end{pmatrix} (q_n \theta_{n+1} + q_{n-1})^2 \\ &= (a\theta^2 + b\theta + c)(q_n \theta_{n+1} + q_{n-1})^2 \\ &= 0 \end{aligned}$$

Note that

$$\begin{aligned} \alpha_n = f_n \begin{pmatrix} 1 \\ 0 \end{pmatrix} &= f \begin{pmatrix} p_n \\ q_n \end{pmatrix} = q_n^2 f \begin{pmatrix} \frac{p_n}{q_n} \\ 1 \end{pmatrix} \\ \frac{\alpha_n}{q_n^2} &= f \begin{pmatrix} \frac{p_n}{q_n} \\ 1 \end{pmatrix} = f \begin{pmatrix} \frac{p_n}{q_n} \\ 1 \end{pmatrix} - f \begin{pmatrix} \theta \\ 1 \end{pmatrix} \qquad \text{(Since f}(\theta) = 0) \\ &= a\left(\frac{p_n^2}{q_n^2} - \theta^2\right) + b\left(\frac{p_n}{q_n} - \theta\right) \end{aligned}$$

From which we get

$$\begin{aligned}\left|\frac{\alpha_n}{q_n^2}\right| &\leqslant |a|\left|\frac{p_n}{q_n}-\theta\right|\left|\frac{p_n}{q_n}+\theta\right| + |b|\left|\frac{p_n}{q_n}-\theta\right| \\ &\leqslant \frac{|a|}{q_n^2}\left|\frac{p_n}{q_n}+\theta\right| + \frac{|b|}{q_n^2} \qquad \text{Corollary 4.2.10}\end{aligned}$$

This implies that

$$|\alpha_n| \leqslant |a|\left|\frac{p_n}{q_n}+\theta\right| + |b|.$$

Thus, α_n are bounded. Similarly,

$$\gamma_n = f_n\begin{pmatrix}0\\1\end{pmatrix} = f\begin{pmatrix}p_{n-1}\\q_{n-1}\end{pmatrix} = \alpha_{n-1}$$

Thus, γ_n is also bounded.

$$\beta_n^2 = disc(f_n) + 4\alpha_n\gamma_n \implies |\beta_n|^2 \leqslant disc(f_n) + 4|\alpha_n||\gamma_n|$$

which implies that β_n are bounded. Thus, there are only finitely many possibilities for f_n. Let us call this set $g_1, g_2, \ldots, g_l$. Each θ_n is a root of g_i for some i. This shows that $\theta_n = \theta_{n+l}$ for some n and $l \geqslant 1$.

Now let us look at the continued fraction expansion of θ. It looks like

$$\begin{aligned}\theta &= [a_0, a_1, \ldots, a_{n-1}, \theta_n] \\ &= [a_0, a_1, \ldots, a_{n-1}, a_n, \theta_{n+1}] \\ &= [a_0, a_1, \ldots, a_{n-1}, a_n, \ldots, a_{n+l-1}, \theta_{n+l}] \\ &= [a_0, a_1, \ldots, a_{n-1}, a_n, \ldots, a_{n+l-1}, \theta_n] \\ &= [a_0, a_1, \ldots, a_{n-1}, a_n, \ldots, a_{n+l-1}, a_n, \theta_{n+1}] \\ &= [a_0, a_1, \ldots, a_{n-1}, \overline{a_n, \ldots, a_{n+l-1}}]\end{aligned}$$

This proves that the continued fraction expansion of θ is periodic. This completes the proof of the theorem. □

Corollary 4.3.2. *Let θ be a quadratic irrational. Then there is a constant $c > 0$ (depending on θ) such that for all rational we have*

$$\left|\theta - \frac{p}{q}\right| > \frac{1}{cq^2}$$

Proof. Since θ is irrational, it is not an integer. Thus, there is an $l > 0$ such that

$$|\theta - p| > \frac{1}{l}$$

Thus, if $q = 1$, then

$$\left|\theta - \frac{p}{q}\right| > \frac{1}{lq^2}.$$

So let us assume that $q > 1$. By Theorem 4.2.13, we know that if

$$\left|\theta - \frac{p}{q}\right| < \frac{1}{3q^2}$$

then $\frac{p}{q} = \frac{p_n}{q_n}$ for some convergent. Since $q > 1$, we have $n > 0$, or else, $q = q_n = q_0 = 1$. By Remark 4.2.5 we know

$$\theta = \frac{\theta_{n+1}p_n + p_{n-1}}{\theta_{n+1}q_n + q_{n-1}}$$

One checks easily that

$$\left|\theta - \frac{p_n}{q_n}\right| = \frac{1}{q_n(\theta_{n+1}q_n + q_{n-1})}$$

Since the continued fraction expansion of θ is periodic, we see that there is an M such that $\theta_{n+1} < M$ for all n. Thus,

$$\theta_{n+1}q_n + q_{n-1} < Mq_n + q_{n-1}$$

which implies that

$$\left|\theta - \frac{p_n}{q_n}\right| = \frac{1}{q_n(\theta_{n+1}q_n + q_{n-1})} > \frac{1}{q_n(Mq_n + q_{n-1})} \geqslant \frac{1}{q_n^2(M+1)}$$

Thus, we have proved that if $q > 1$ and $\left|\theta - \frac{p}{q}\right| < \frac{1}{3q^2}$ then

$$\left|\theta - \frac{p}{q}\right| > \frac{1}{q^2(M+1)}.$$

Thus, if $q > 1$ then either

$$\left|\theta - \frac{p}{q}\right| \geqslant \frac{1}{3q^2} > \frac{1}{4q^2}$$

or

$$\left|\theta - \frac{p}{q}\right| > \frac{1}{q^2(M+1)}.$$

Taking $c = \max\{4, l, M+1\}$ we get that for all rationals

$$\left|\theta - \frac{p}{q}\right| > \frac{1}{cq^2}$$

This proves the corollary. □

4.4 Liouville's Theorem

In this section we generalize Corollary 4.3.2.

Theorem 4.4.1 (Liouville's Theorem)**.** *Let $\alpha \in \mathbb{R}\setminus\mathbb{Q}$ and let α be algebraic satisfying a polynomial of degree n. Then there exists a constant $c > 0$ dependent on α ($c = c(\alpha)$) such that $\left|\alpha - \frac{p}{q}\right| > \frac{1}{cq^n} \quad \forall p, q \in \mathbb{Z}, q \neq 0$.*

Proof. We have already proved the theorem in the case $n = 2$ (see Corollary 4.3.2. We know that for algebraic α, there is a polynomial $P(x) \in \mathbb{Q}[x]$ which is irreducible, of degree n and $P(\alpha) = 0$, and this is the polynomial of least degree. Clearing denominators we get $P(x) \in \mathbb{Z}[x]$ of degree n such that $P(\alpha) = 0$. By the Mean Value Theorem, we have,

$$\left|P(\alpha) - P\left(\frac{p}{q}\right)\right| = \left|\alpha - \frac{p}{q}\right| \cdot \left|P'(\xi)\right|$$

for some ξ lying between α and $\frac{p}{q}$. Since $P(x)$ is irreducible over $\mathbb{Q}$, we have $P\left(\frac{p}{q}\right) \neq 0$. Thus,

$$\left|P\left(\frac{p}{q}\right)\right| = \left|\alpha - \frac{p}{q}\right| \cdot \left|P'(\xi)\right|$$

Since

$$P\left(\frac{p}{q}\right) = a_n\frac{p^n}{q^n} + a_{n-1}\frac{p^{n-1}q}{q^n} + a_{n-2}\frac{p^{n-2}q^2}{q^n} \cdots + a_0$$

we get

$$\left|P\left(\frac{p}{q}\right)\right| \geqslant \frac{1}{q^n}$$

$$\left|\alpha - \frac{p}{q}\right| \geqslant \frac{1}{q^n P'(\xi)}$$

If $\left|\alpha - \frac{p}{q}\right| \geqslant 1$, then $\left|\alpha - \frac{p}{q}\right| > \frac{1}{2q^n}$. So assume $\left|\alpha - \frac{p}{q}\right| < 1$. Since ξ lies between α and $\frac{p}{q}$ we get $|\xi| < |\alpha| + 1$.

$$\left|P'(\xi)\right| \leqslant \sum_{i=0}^{n} \left|ia_i\xi^{i-1}\right| \leqslant \sum_{i=0}^{n} i|a_i|(|\alpha|+1)^{i-1}$$

Define

$$M := \sum_{i=0}^{n} i|a_i|(|\alpha|+1)^{i-1}$$

Then we have just seen that

$$\left|P'(\xi)\right| \leqslant M$$

Choose $c = \max(M+1, 2)$ to satisfy the condition $\left|\alpha - \frac{p}{q}\right| \geqslant \frac{1}{cq^n}$. This proves the theorem. □

Corollary 4.4.2. *Let α be such that there is an infinite sequence of distinct rationals p_n/q_n satisfying $\left|\alpha - \frac{p_n}{q_n}\right| < \frac{c}{q_n^{\omega_n}}$ and $\omega_n \to \infty$. Then α is transcendental.*

Proof. For any $c > 0$, there are only finitely many numbers with $q = 1$ and $\left|\alpha - \frac{p}{q}\right| < c$. Thus, we can discard those $\frac{p_n}{q_n}$ for which $q_n = 1$, there are only finitely many such. From now on we assume $q_n \geqslant 2$. If α were algebraic with degree m, we can find a bound $c(\alpha)$ such that

$$\frac{1}{c(\alpha)q_n^m} < \left|\alpha - \frac{p_n}{q_n}\right| < \frac{c}{q_n^{\omega_n}} \quad \forall n$$

Thus, $q_n^{\omega_n - m} < c.c(\alpha)$. But as $\omega_n \to \infty, q_n^{\omega_n - m} \to \infty$. We reach a contradiction, and hence α is not algebraic. □

Chapter 5

Dirichlet's Theorem

The main aim of this chapter is to prove Dirichlet's Theorem which states that there are infinitely many primes in an arithmetic progression.

We will assume the Dominated Convergence Theorem and Cauchy's integral formula as black boxes. In the first section we will prove (the extremely useful) Theorem 5.1.5 on convergence of sequences of holomorphic functions. In the second section we discuss Dirichlet series. There are two important and interesting results in this section. The first says if a Dirichlet series converges at $z = z_0$, then it converges and defines a holomorphic function in the right half place $\mathrm{Re}(z) > \mathrm{Re}(z_0)$. The second says that if a Dirichlet series f converges at $z = z_0$ and if there is a holomorphic function g in a small neighborhood around z_0, which agrees with f at points where they both converge, then there is $\epsilon > 0$ such the Dirichlet series f converges on $\mathrm{Re}(z) > \mathrm{Re}(z_0) - \epsilon$. This is a crucial input in the proof of Dirichlet's Theorem. The rest of the chapter is devoted to the proof of Dirichlet's Theorem. The idea of the proof involves some notation and has been explained in Remark 5.7.5.

5.1 Preliminaries

Theorem 5.1.1 (Dominated Convergence Theorem)**.** *Let X be a "measure space". Let f_n be a sequence of functions on X. Suppose $f_n \to f$. Suppose there is a function g such that $|f_n| \leqslant g$ and $\int_X g(x)d\mu < \infty$. Then*

$$\mathrm{lim}_n \int_X f_n(x)d\mu = \int_X \mathrm{lim}_n f_n(x)d\mu = \int_X f(x)d\mu\,.$$

We shall use the above theorem without proof.

Corollary 5.1.2. *Assume that X is metric space with a measure such that the volume is finite. Let f_n be a sequence of continuous functions such that $f_n \to f$ uniformly. Then f is continuous and*

$$\lim_n \int_X f_n(x) d\mu = \int_X f(x) d\mu \,.$$

Proof. First we shall show that $f(x)$ is continuous. Let $x_k \in X$ be a sequence converging to x_0. We have

$$f(x_k) - f(x_0) = (f(x_k) - f_n(x_k)) - (f(x_0) - f_n(x_0)) - (f_n(x_0) - f_n(x_k)) \,.$$

Now from the uniform convergence of $f_n \to f$, there is n_0, such that for all $n \geqslant n_0$

$$|f_n(x) - f(x)| < \epsilon/3 \qquad \forall x \in X \,.$$

In particular it holds for all x_k and x_0. Since f_n is continuous, we have

$$|(f_n(x) - f_n(x_k))| < \epsilon/3 \qquad \forall k > k_0 \,.$$

Therefore we have

$$\begin{aligned} |f(x_k) - f(x_0)| &= |(f(x_k) - f_n(x_k)) - (f(x_0) - f_n(x_0)) - (f_n(x_0) - f_n(x_k))| \\ &\leqslant |(f(x_k) - f_n(x_k))| + |(f(x_0) - f_n(x_0))| + |(f_n(x_0) - f_n(x_k))| \\ &< \epsilon/3 + \epsilon/3 + \epsilon/3 \\ &= \epsilon \qquad \forall k > k_0 \,. \end{aligned}$$

This proves that f is continuous.

We have

$$|f_n(x) - f(x)| < 1 \; \forall x \in X \text{ and } n > N_0 \,.$$

because of uniform convergence of f_n. Since X is compact and f is continuous, $|f|$ attains a maximum on X. Let this maximum be M. Then

$$|f_n(x)| - |f(x)| \leqslant |f_n(x) - f(x)| < 1$$

$$\Rightarrow \; |f_n(x)| < M + 1 \,.$$

Now apply DCT(5.1.1) on f_n with the bounding function $g(x) \equiv M+1$. □

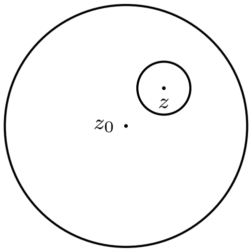
Lemma 5.1.3. *Let f be a continuous function on a domain $U \subset \mathbb{C}$. Let $z_0 \in U$ and let $r > 0$ such that $\{z \mid |z - z_0| \leqslant r\} \subset U$. Consider the following function on the open set $B(z_0, r) := \{z \mid |z - z_0| < r\}$,*

$$g(z) := \int_{|w-z_0|=r} \frac{f(w)}{w-z} dw \,.$$

This function is holomorphic and its derivative is given by

$$g'(z) := \int_{|w-z_0|=r} \frac{f(w)}{(w-z)^2} dw \,.$$

Proof. Let $z \in B(z_0, r)$. There is $r' > 0$ such that $B(z, r') \subset B(z_0, r)$.



Let $h_n \in \mathbb{C}$ be a sequence converging to zero. Ignoring the first few terms, we may assume that $|h_n| < r'$. Therefore, whatever follows is well defined. Now we have

$$\begin{aligned} \frac{g(z+h_n) - g(z)}{h_n} &= \frac{1}{h_n} \left(\int_{|w-z_0|=r} \frac{f(w)}{w-(z+h_n)} dw - \int_{|w-z_0|=r} \frac{f(w)}{w-z} dw \right) \\ &= \int_{|w-z_0|=r} \frac{f(w)}{(w-z-h_n)(w-z)} dw \,. \end{aligned}$$

We have

$$\begin{aligned} |w-z| &= |w - z_0 + z_0 - z| \\ &\geqslant |w-z_0| - |z_0 - z| \\ &= r - |z_0 - z| > 0 \,. \end{aligned}$$

We have

$$\begin{aligned} |w - z - h_n| &\geqslant |w-z| - |h_n| \\ &\geqslant r - |z_0 - z| - r' \,. \end{aligned}$$

If r' is chosen sufficiently small, then the above quantity is positive. Thus, there is a constant $m > 0$, which is independent of n, such that

$$|w - z - h_n|, |w - z| > m.$$

Since f is continuous and $|w - z_0| = r$ is compact, we have

$$|f(x)| \leqslant M, \qquad \forall x \in |w - z_0| = r,$$

which implies,

$$\left| \frac{f(w)}{(w - z - h_n)(w - z)} \right| < \frac{M}{m^2}\,.$$

Now using DCT for the sequence of functions

$$\alpha_n(w) = \frac{f(w)}{(w - z - h_n)(w - z)} \ \forall \ n > N_0\,.$$

We get

$$\begin{aligned} g'(z) &= \lim_n \frac{g(z + h_n) - g(z)}{h_n} \\ &= \lim_n \int_{|w - z_0| = r} \frac{f(w)}{(w - z - h_n)(w - z)} dw \\ &= \int_{|w - z_0| = r} \lim_n \frac{f(w)}{(w - z - h_n)(w - z)} dw \\ &= \int_{|w - z_0| = r} \frac{f(w)}{(w - z)^2} dw\,. \end{aligned}$$

This completes the proof of the Lemma. □

Theorem 5.1.4 (Cauchy's integral formula)**.** *Let $U \subset \mathbb{C}$ be an open subset. Let $f : U \to \mathbb{C}$ be a function which is holomorphic on U. Let $z_0 \in U$ and let $r > 0$ such that $B(z_0, r) := \{|z - z_0| \leqslant r\} \subset U$. Then for every z such that $|z - z_0| < r$, we have*

$$f(z) = \frac{1}{2\pi i} \int_{|w - z_0| = r} \frac{f(w)}{w - z} dw\,.$$

We shall use the above theorem without proof.

Theorem 5.1.5. *Let f_n be a sequence of holomorphic functions on $U \subset \mathbb{C}$. Assume that $f_n \to f$ uniformly on every compact subset $C \subset U$. Then f is holomorphic and the derivatives f_n' converge uniformly on all compact subsets to the derivative f'.*

Proof. Fix a point $z_0 \in U$. There is $R > 0$ such that $\{z \mid |z - z_0| \leqslant R\} \subset U$ as U is open. Let $0 < r < R$. We will show that f is holomorphic in $B(z_0, r) := \{z \mid |z - z_0| < r\}$, thereby making it holomorphic at z_0.

Choose an r_1 such that $r < r_1 < R$. Using Cauchy's integral formula, we have, for $z \in B(z_0, r)$,

$$f_n(z) = \frac{1}{2\pi i} \int_{|w-z_0|=r_1} \frac{f_n(w)}{w-z} dw\,.$$

Now

$$\begin{aligned} f(z) &= \lim_n f_n(z) \\ &= \lim_n \frac{1}{2\pi i} \int_{|w-z_0|=r_1} \frac{f_n(w)}{w-z} dw\,. \end{aligned}$$

To take the limit inside, we have to show that $\frac{f_n(w)}{w-z}$ converges to $\frac{f(w)}{w-z}$ uniformly on the compact set $X = \{w \in \mathbb{C} \mid |w - z_0| = r_1\}$. To this end, we have to find an $N \in \mathbb{N}$, such that

$$\left| \frac{f_n(w)}{w-z} - \frac{f(w)}{w-z} \right| < \epsilon \qquad \forall\, n > N \qquad \forall w \in X\,.$$

We know that $f_n \to f$ uniformly on every compact subset of U, in particular on X . Therefore there exists $N_0 \in \mathbb{N}$ such that for all $w \in X$

$$|f_n(w) - f(w)| < (r_1 - r)\epsilon \;\forall\, n > N_0\,.$$

It is easily seen that

$$|w - z| \geqslant r_1 - r > 0$$

and therefore

$$\frac{1}{|w-z|} \leqslant \frac{1}{r_1 - r}\,.$$

Multiplying this with the above equation gives

$$\left| \frac{f_n(w)}{w-z} - \frac{f(w)}{w-z} \right| < \epsilon \qquad \forall\, n > N \qquad \forall w \in X\,.$$

Now, using 5.1.2, we get

$$f(z) = \frac{1}{2\pi i} \int_{|w-z_0|=r_1} \lim_n \frac{f_n(w)}{w-z} dw\,.$$

Therefore we have

$$f(z) = \frac{1}{2\pi i}\int_{|w-z_0|=r_1} \frac{f(w)}{w-z}dw\,.$$

Since $f_n \to f$ uniformly on compact sets, the function f is continuous on $\{z \mid |z-z_0| \leqslant R\}$. Now apply 5.1.3 taking $U = B(z_0, R)$. Therefore, we have that the RHS is holomorphic. Hence $f(z)$ is holomorphic on $B(z_0, r)$.

We shall now prove the second part of the theorem. By 5.1.3, we have (for the same point z_0 and the same points and regions considered earlier)

$$f_n'(z) = \frac{1}{2\pi i}\int_{|w-z_0|=r_1} \frac{f_n(w)}{(w-z)^2}dw$$

and

$$f'(z) = \frac{1}{2\pi i}\int_{|w-z_0|=r_1} \frac{f(w)}{(w-z)^2}dw$$

for $|z-z_0| \leqslant r$. For $z \in |z-z_0| \leqslant r$ we have that

$$\frac{1}{|w-z|^2} \leqslant \frac{1}{(r_1-r)^2}\,.$$

Also for a suitable N,

$$|f_n(w) - f(w)| < (r_1-r)^2\epsilon \;\forall\; n > N\,.$$

Hence,

$$\left|\frac{f_n(w)}{(w-z)^2} - \frac{f(w)}{(w-z)^2}\right| < \epsilon \qquad \forall\; n > N,$$

for $|w-z_0| = r_1$ and $|z-z_0| \leqslant r$. Therefore,

$$\begin{aligned}\left|f_n'(z) - f'(z)\right| &= \left|\int_{|w-z_0|=r_1} \frac{f_n(w)-f(w)}{(w-z)^2}dw\right| \\ &\leqslant \int_{|w-z_0|=r_1} \frac{|f_n(w)-f(w)|}{(|w-z|)^2}dw \\ &\leqslant 2\pi r_1\epsilon,\end{aligned}$$

for all $|z-z_0| \leqslant r$ and therefore $f_n'(z) \to f(z)$ uniformly on this set.

We have proved that for every $z_0 \in U$, there is an $r > 0$ such that $\{z \mid |z-z_0| \leqslant r\} \subset U$, and on this subset the functions $f_n' \to f'$ uniformly.

Consider any compact subset $K \subset U$. Apply the preceding discussion for each $z \in K$. Then there are finitely many $z_i \in K$ such that the closures

$$\overline{B(z_i, r_i)} := \{z \mid |z-z_i| \leqslant r_i\}$$

cover K and on each of these $f_n' \to f'$ uniformly. It easily follows that $f_n' \to f'$ uniformly on K. □

5.2 Dirichlet Series

Let λ_n be an increasing sequence of real numbers tending to $+\infty$. For the sake of simplicity we suppose that the $\lambda_n \geqslant 0$. The reader will quickly realize that this is not necessary for the questions we are going to consider.

The Dirichlet series with exponents λ_n is a series of the form

$$\sum_{n\geqslant 1} a_n e^{-\lambda_n z} \ (a_n \in \mathbb{C}, z \in \mathbb{C}) .$$

Lemma 5.2.1. *Abel's Lemma Let a_n and b_n be two sequences. Put*

$$A_{m,p} = \sum_{n=m}^{p} a_n \quad \text{and} \quad S_{m,m'} = \sum_{n=m}^{m'} a_n b_n .$$

The we have

$$S_{m,m'} = \sum_{n=m}^{m'-1} A_{m,n}(b_n - b_{n+1}) + A_{m,m'} b_{m'} .$$

Proof. We can see that

$$a_n = A_{m,n} - A_{m,n-1} .$$

This will work for $n = m$ as well if we consider $A_{m,m-1} = 0$. Substituting this in the expression for $S_{m,m'}$,

$$\begin{aligned} S_{m,m'} &= \sum_{n=m}^{m'} (A_{m,n} - A_{m,n-1}) b_n = \sum_{n=m}^{m'} A_{m,n} b_n - \sum_{n=m}^{m'} A_{m,n-1} b_n \\ &= \sum_{n=m}^{m'} A_{m,n} b_n - \sum_{k=m-1}^{m'-1} A_{m,k} b_{k+1} = \sum_{n=m}^{m'} A_{m,n} b_n - \sum_{n=m-1}^{m'-1} A_{m,n} b_{n+1} \\ &= \sum_{n=m}^{m'-1} A_{m,n}(b_n - b_{n+1}) + A_{m,m'} b_{m'} - A_{m,m-1} b_m \\ &= \sum_{n=m}^{m'-1} A_{m,n}(b_n - b_{n+1}) + A_{m,m'} b_{m'} \qquad \because A_{m,m-1} = 0 . \end{aligned}$$

□

Lemma 5.2.2. *Let α, β be two real numbers with $0 < \alpha \leqslant \beta$. Let $z = x + iy$ with $x, y \in \mathbb{R}$ and $x > 0$. Then*

$$|e^{-\alpha z} - e^{-\beta z}| \leqslant \left|\frac{z}{x}\right| (e^{-\alpha x} - e^{-\beta x}) .$$

Proof. First observe that if $\alpha = \beta$ then equality holds. So we shall assume $\alpha < \beta$. We observe that

$$e^{-\alpha z} - e^{-\beta z} = z \int_{\alpha}^{\beta} e^{-tz} dt .$$

Hence,

$$\begin{aligned} |e^{-\alpha z} - e^{-\beta z}| &= \left| z \int_{\alpha}^{\beta} e^{-tz} dt \right| \\ &\leqslant |z| \int_{\alpha}^{\beta} |e^{-tz}| dt \\ &= |z| \int_{\alpha}^{\beta} e^{-tx} dt \\ &= \left|\frac{z}{x}\right| (e^{-\alpha x} - e^{-\beta x}) . \end{aligned}$$

□

Definition 5.2.3. *Let f_n be a sequence of functions and $A \subset \mathbb{C}$. Suppose for every $\epsilon > 0$ there exist an N (which depends on ϵ) such that*

$$|f_n(x) - f_m(x)| < \epsilon \qquad \forall\ x \in A \text{ and } n, m > N .$$

Then such a sequence is called Uniformly Cauchy on A.

Lemma 5.2.4. *A sequence is uniformly Cauchy on A iff it is uniformly convergent on A.*

Proof. First assume the sequence of functions f_n is uniformly convergent to f on A. Then we have

$$|f_n(x) - f(x)| < \frac{\epsilon}{2} \qquad\qquad \forall x \in A \text{ and } n > N .$$

Therefore, we have for $n, m > N$,

$$\begin{aligned} |f_n(x) - f_m(x)| &\leqslant |f_n(x) - f(x)| + |f(x) - f_m(x)| \\ &= \frac{\epsilon}{2} + \frac{\epsilon}{2} \\ &= \epsilon \qquad\qquad \forall x \in A \text{ and } n, m > N . \end{aligned}$$

This proves that f_n's are uniformly Cauchy on A.

Now let us assume that f_n is uniformly Cauchy on A. Choose an $x \in A$. The sequence of complex numbers $f_n(x)$ is convergent as it is Cauchy. Let $f_n(x) \to y$. Define a function f such that $f(x) = y$. As the sequence is uniformly Cauchy, there exists N_0 such that $|f_n(x) - f_m(x)| < \frac{\epsilon}{2}$ $\forall$ $x \in A$ and $n, m > N_0$. Choose an $x \in A$. Then

$$\begin{aligned} |f_n(x) - f(x)| &\leqslant |f_n(x) - f_m(x)| + |f_m(x) - f(x)| \\ &< \frac{\epsilon}{2} + |f_m(x) - f(x)|\,. \end{aligned}$$

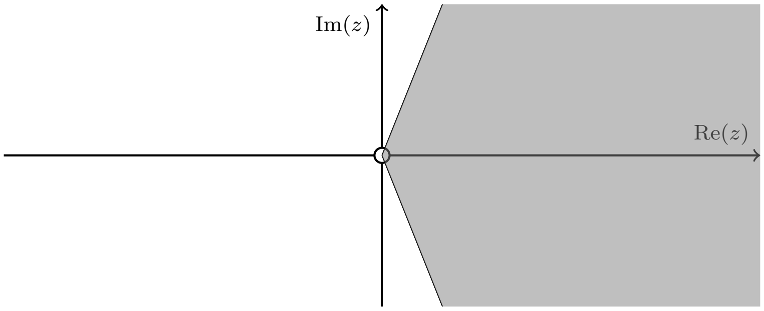
Since $f_m(x)$ is pointwise convergent to $f(x)$, keeping n fixed and letting $m \to \infty$ we have

$$|f_n(x_i) - f(x_i)| \leqslant \epsilon\,.$$

This proves that $f_n \to f$ uniformly on A. □

Proposition 5.2.5. *If the series $f(z) = \sum_{n\geqslant 1} a_n e^{-\lambda_n z}$ converges for $z = 0$, it converges uniformly in every domain of the form*

$$\{z \mid x := \mathrm{Re}(z) > 0, \left|\frac{z}{x}\right| \leqslant k < \infty\}\,.$$



Proof. We have that $f(0) = \sum_{n\geqslant 1} a_n$ converges and we have to show that $f(z)$ converges uniformly for $\mathrm{Re}(z) > 0$ and $\left|\frac{z}{x}\right| \leqslant k$. Let $z = x + iy$, where $x > 0$ and $y \in \mathbb{R}$. Let $B_{m,m'} = \sum_{n=m}^{m'} a_n$ and $S_{m,m'} = \sum_{n=m}^{m'} a_n e^{-\lambda_n z}$. From Abel's lemma(5.2.1), we obtain

$$S_{m,m'} = \sum_{n=m}^{m'-1} B_{m,n}(e^{-\lambda_n z} - e^{-\lambda_{n+1} z}) + B_{m,m'} e^{-\lambda_{m'} z}\,.$$

Now we have

$$\begin{aligned}|S_{m,m'}| &\leqslant \sum_{n=m}^{m'-1} |B_{m,n}(e^{-\lambda_n z} - e^{-\lambda_{n+1} z})| + |B_{m,m'} e^{-\lambda_{m'} z}| \\ &\leqslant \sum_{n=m}^{m'-1} |B_{m,n}| \left|\frac{z}{x}\right| (e^{-\lambda_n x} - e^{-\lambda_{n+1} x}) + |B_{m,m'}| e^{-\lambda_{m'} x}\end{aligned}$$

(from 5.2.2, along with $\lambda_n \leqslant \lambda_{n+1}$ and $x > 0$)

$$< \sum_{n=m}^{m'-1} |B_{m,n}| \left|\frac{z}{x}\right| (e^{-\lambda_n x} - e^{-\lambda_{n+1} x}) + |B_{m,m'}|$$

(because $e^{-\lambda_{m'} x} < 1$ as $\lambda_{m'} x > 0$).

We shall consider the region $\left|\frac{z}{x}\right| \leqslant k$. Since $\sum_{n\geqslant 1} a_n$ is convergent, there exists N such that $|B_{m,m'}| < \frac{\epsilon}{k+1}$ $\forall\ m, m' > N$. Therefore we have,

$$\begin{aligned}|S_{m,m'}| &< \frac{\epsilon}{k+1}\left(\sum_{n=m}^{m'-1} (e^{-\lambda_n x} - e^{-\lambda_{n+1} x}) k + 1\right) \\ &= \frac{\epsilon}{k+1}\left((e^{-\lambda_m x} - e^{-\lambda_{m'} x}) k + 1\right) .\end{aligned}$$

As $m < m'$ and λ_n is an increasing sequence, we have that $0 \leqslant e^{-\lambda_m x} - e^{-\lambda_{m'} x} \leqslant 1$. Therefore, for $m, m' > N$,

$$|S_{m,m'}| < \frac{\epsilon}{k+1}(k+1) = \epsilon .$$

Thus, we have shown that the $S_m(z) = \sum_{n=1}^{m} a_n e^{-\lambda_n z}$ is uniformly Cauchy on $\mathrm{Re}(z) > 0, \left|\frac{z}{x}\right| \leqslant k$. Thus it is uniformly convergent on this set by Lemma 5.2.4. □

Translating the above by z_0, the following corollary is clear.

Corollary 5.2.6. *If the series $f(z) = \sum_{n\geqslant 1} a_n e^{-\lambda_n z}$ converges for $z = z_0$, it converges uniformly in every domain of the form*

$$\{z \mid \mathrm{Re}(z - z_0) > 0, \left|\frac{z - z_0}{\mathrm{Re}(z - z_0)}\right| \leqslant k < \infty\} .$$

Theorem 5.2.7. *If $f(z) = \sum_{n\geqslant 1} a_n e^{-\lambda_n z}$ converges for $z = z_0$, it converges for $\mathrm{Re}(z) > \mathrm{Re}(z_0)$ and the function thus defined is holomorphic.*

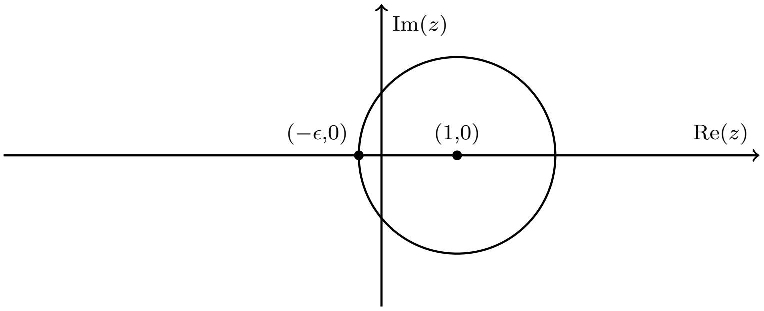
Proof. Let $C \subset \{z \mid \mathrm{Re}(z - z_0) > 0\}$ be a compact subset. Then clearly there is a $k > 0$ such that C is contained in the set

$$\{z \mid \mathrm{Re}(z - z_0) > 0, \left|\frac{z - z_0}{\mathrm{Re}(z - z_0)}\right| \leqslant k < \infty\}\,.$$

Since the series converges uniformly on this set, it converges uniformly on C. Now apply Theorem 5.1.5. □

Corollary 5.2.8. *The set of points of convergence of the series $f(z) = \sum_{n\geqslant 1} a_n e^{-\lambda_n z}$ contains a maximal open half plane, where we also consider $\emptyset$ and $\mathbb{C}$ as open half planes.*

Theorem 5.2.9. *Let $f(z) = \sum_{n\geqslant 1} a_n e^{-\lambda_n z}$ be a Dirichlet series with a_n real and non-negative. Suppose that f converges for $\mathrm{Re}(z) > \rho$ with $\rho \in \mathbb{R}$ and that the function f can be extended analytically to a function holomorphic in a neighborhood of the point $z = \rho$. Then $\exists \epsilon > 0$ such that f converges for $\mathrm{Re}(z) > \rho - \epsilon$ and is holomorphic in this domain.*



Proof. We shall consider $g(z) = f(z + \rho) = \sum_{n\geqslant 1} b_n e^{-\lambda_n z}$ where $b_n = a_n e^{-\lambda_n \rho}$. Therefore we have that $g(z)$ converges for $\mathrm{Re}(z) > 0$ and it extends analytically to a holomorphic fucntion in the neighborhood of $z = 0$. Hence $\exists \epsilon > 0$ such that the Taylor series of g around 1 converges in the disc

$$\{z \mid |z - 1| \leqslant 1 + \epsilon\}\,.$$

We apply 5.1.5 to the holomorphic functions $g_m(z) = \sum_{n=1}^{m} b_n e^{-\lambda_n z}$ in the region $\mathrm{Re}(z) > 0$. We see that the p^{th} derivative of g is given by the following expression in $\mathrm{Re}(z) > 0$

$$g^{(p)}(z) = \sum_{n\geqslant 1} b_n (-\lambda_n)^p e^{-\lambda_n z}\,.$$

From which we have

$$g^{(p)}(1) = (-1)^p \sum_{n \geqslant 1} \lambda_n^p b_n e^{-\lambda_n} \,.$$

The Taylor series of g around 1 is given by

$$g(z) = \sum_{p=0}^{\infty} \frac{1}{p!}(z-1)^p g^{(p)}(1) \,.$$

This takes the following value at $z = -\epsilon$ (which is within the region of convergence of the Taylor series).

$$g(-\epsilon) = \sum_{p=0}^{\infty} \frac{1}{p!}(1+\epsilon)^p (-1)^p g^{(p)}(1) \,.$$

But $(-1)^p g^{(p)}(1) = \sum_n \lambda_n^p b_n e^{-\lambda_n}$ is a convergent series with positive terms. Hence the double sum below makes sense, converges and is equal to $g(-\epsilon)$ and so is any rearrangement because of absolute convergence.

$$g(-\epsilon) = \sum_{p,n} b_n \frac{1}{p!}(1+\epsilon)^p \lambda_n^p e^{-\lambda_n} \,.$$

Rearranging terms one obtains,

$$\begin{aligned} g(-\epsilon) &= \sum_n b_n e^{-\lambda_n} \sum_{p=0}^{\infty} \frac{1}{p!}(1+\epsilon)^p \lambda_n^p \\ &= \sum_n b_n e^{-\lambda_n} e^{\lambda_n(1+\epsilon)} \\ &= \sum_n b_n e^{\lambda_n \epsilon} \,. \end{aligned}$$

This shows that the Dirichlet series $\sum_n b_n e^{-\lambda_n z}$ converges for $z = -\epsilon$ and thus also for $\mathrm{Re}(z) > -\epsilon$ from 5.2.5. Thus, $\sum_n a_n e^{-\lambda_n z}$ converges on $\mathrm{Re}(z) > \rho - \epsilon$. Finally apply 5.2.7. □

We are particularly interested in the case $\lambda_n = \log n$. In this case the corresponding series becomes

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

Proposition 5.2.10. *If the a_n are bounded, then the Dirichlet series $f(s) = \sum_{n\geqslant 1}\frac{a_n}{n^s}$ converges absolutely for* $\mathrm{Re}(s) > 1$ *and is holomorphic in this region.*

Proof. Let $|a_n| < M$. Therefore,

$$\begin{aligned}\sum_{n=1}^{\infty}\left|\frac{a_n}{n^s}\right| &< M\sum_{n=1}^{\infty}\left|\frac{1}{n^s}\right|\\ &= \sum_{n=1}^{\infty}\frac{1}{n^{\mathrm{Re}(s)}}\,.\end{aligned}$$

The RHS is convergent for $\mathrm{Re}(s) > 1$. Therefore the series is absolutely convergent for $\mathrm{Re}(s) > 1$ and is holomorphic in this region using 5.2.7. □

Proposition 5.2.11. *If the partial sums $A_{m,p} = \sum_m^p a_n$ are bounded, then the Dirichlet series $f(s) = \sum_{n\geqslant 1}\frac{a_n}{n^s}$ converges (not necessarily absolute) and is holomorphic in the region* $\mathrm{Re}(s) > 0$.

Proof. Let $|A_{m,p}| \leqslant M$. Let $S_{m,m'} = \sum_{n=m}^{m'}\frac{a_n}{n^s}$. Now by applying Abel's lemma(5.2.1) we get,

$$\begin{aligned}|S_{m,m'}| &= \left|\sum_{n=m}^{m'-1} A_{m,n}\left(\frac{1}{n^s} - \frac{1}{(n+1)^s}\right) + A_{m,m'}\frac{1}{(m')^s}\right|\\ &\leqslant \sum_{n=m}^{m'-1}\left|A_{m,n}\left(\frac{1}{n^s} - \frac{1}{(n+1)^s}\right)\right| + \left|A_{m,m'}\frac{1}{(m')^s}\right|\\ &\leqslant M\sum_{n=m}^{m'-1}\left|\left(\frac{1}{n^s} - \frac{1}{(n+1)^s}\right)\right| + \left|\frac{1}{(m')^s}\right|\,.\end{aligned}$$

What we did above is valid for all s. We shall evaluate the RHS for $s = r > 0$.

$$M\sum_{n=m}^{m'-1}\left|\left(\frac{1}{n^r} - \frac{1}{(n+1)^r}\right)\right| + \left|\frac{1}{(m')^r}\right| = M\frac{1}{m^r},$$

because for $r > 0$, $\frac{1}{n^r} - \frac{1}{(n+1)^r} > 0$.

Denote by $S_m(r) = \sum_{n=1}^{m}\frac{a_n}{n^r}$. The above shows that this is a Cauchy sequence and so it converges. It follows from 5.2.7 that the Dirichlet series converges on $\mathrm{Re}(s) > r$ and is holomorphic. Since this happens for every $r > 0$, the same conclusion follows in the region $\mathrm{Re}(s) > 0$. □

5.3 Riemann Zeta Function

Theorem 5.3.1. *The Riemann Zeta function is*

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

$\zeta(s)$ is holomorphic in $\mathrm{Re}(s) > 1$ *and has a meromorphic extension to* $\mathrm{Re}(s) > 0$*, which is holomorphic everywhere except a simple pole at $s = 1$.*

Proof. By Proposition 5.2.10 this function is holomorphic in the region $\mathrm{Re}(z) > 1$. Let

$$F(s) := \sum_{n\geqslant 1} \frac{(-1)^{n+1}}{n^s}\,. \tag{5.3.2}$$

Then $F(s)$ is a Dirichlet series which converges in the region Re(s) > 0 by Proposition 5.2.11. We have

$$\zeta(s) + F(s) = \sum_{n\geqslant 1} \frac{2}{(2n)^s} = \frac{1}{2^{s-1}} \sum_{n\geqslant 1} \frac{1}{n^s} = \frac{1}{2^{s-1}}\zeta(s)\,.$$

Thus, we get

$$\zeta(s) = \frac{-F(s)}{\left(1 - \dfrac{1}{2^{s-1}}\right)} = \frac{-2^{s-1}F(s)}{2^{s-1}-1}\,. \tag{5.3.3}$$

The only possible poles of the RHS in the region Re(s) > 0 occur when $2^{s-1} = 1$. Set $\omega = e^{2\pi i/3}$ and consider the functions

$$F_1(s) = \sum_{n\geqslant 1} \frac{\omega^n}{n^s},$$
$$F_2(s) = \sum_{n\geqslant 1} \frac{\omega^{2n}}{n^s}\,.$$

Then $F_i(s)$ is a Dirichlet series which converges in the region Re(s) > 0 by Proposition 5.2.11. We have

$$\zeta(s) + F_1(s) + F_2(s) = \sum_{n\geqslant 1} \frac{3}{(3n)^s} = \frac{1}{3^{s-1}} \sum_{n\geqslant 1} \frac{1}{n^s} = \frac{1}{3^{s-1}}\zeta(s)\,.$$

Thus, we get

$$\zeta(s) = \frac{-F_1(s) - F_2(s)}{\left(1 - \dfrac{1}{3^{s-1}}\right)} = \frac{-3^{s-1}(F_1(s) + F_2(s))}{3^{s-1} - 1}\,. \tag{5.3.4}$$

The only possible poles of the RHS in the region Re(s) >0 occur when $3^{s-1} = 1$. Combining this with the above, we see that if s is such that Re(s) >0 and is a pole for $\zeta(s)$, then

$$2^{s-1} = 3^{s-1} = 1\,.$$

Taking log we get

$$(s-1)\log 2 = (s-1)\log 3$$

which is possible only if $s = 1$. At $s = 1$ the series $F(s)$ converges (since it is holomorphic at $s = 1$) to a positive quantity since

$$F(1) = \left(1 - \frac{1}{2}\right) + \left(\frac{1}{3} - \frac{1}{4}\right) + \cdots\,.$$

Thus, at $s = 1$ the Zeta function has a simple pole because $2^{s-1} - 1$ has a simple zero at $s = 1$. □

5.4 Euler product

The Riemann Zeta function has an Euler product

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \,\text{is prime}} \frac{1}{1 - \frac{1}{p^s}}\,.$$

Formally, as an algebraic series, it is clear that

$$\begin{aligned}\zeta(s) &= \sum_{n=1}^{\infty} \frac{1}{n^s} \\ &= \prod_{p \text{ is prime}} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \frac{1}{p^{3s}} + \cdots\right) \\ &= \prod_{p \text{ is prime}} \frac{1}{1 - p^{-s}}\,.\end{aligned}$$

Consider the series of functions for $N \geqslant 2$,

$$f_N(s) = \prod_{p \leqslant N} \frac{1}{1 - p^{-s}}\,.$$

It is easily checked that on any right half plane Re(s) $\geqslant$ m > 1 the functions $f_N(s) \to \zeta(s)$ uniformly. Thus, we have an equality of holomorphic functions on Re(s) > 1,

$$\zeta(s) = \prod_{p \text{ is prime}} \frac{1}{1-p^{-s}}\,.$$

where the RHS is the limit of the functions $f_N(s)$. This is referred to as the Euler product of the Zeta function.

5.5 Dirichlet Characters

We will look at characters of the finite abelian group $(\mathbb{Z}/m\mathbb{Z})^\times$ whose order is $\phi(m)$. All that was discussed in 1.1 applies to these characters. These characters are functions from $(\mathbb{Z}/m\mathbb{Z})^\times$ to $S^1 \subset \mathbb{C}$. For our purposes, we have to extend the definition of these functions to $\mathbb{Z}$. This will be achieved as described below. Let

$$\chi : (\mathbb{Z}/m\mathbb{Z})^\times \to S^1$$

be a character. Then define $\tilde{\chi} : \mathbb{Z} \to \mathbb{C}^\times$ as

$$\tilde{\chi}(x) = \begin{cases} \chi(a \bmod m) & \text{if } \gcd(a,m) = 1 \\ 0 & \text{otherwise} \end{cases}$$

We shall refer to such characters $\tilde{\chi}$ that are extended to all of $\mathbb{Z}$ as **Dirichlet characters**, where the original group $(\mathbb{Z}/m\mathbb{Z})^\times$ is clear from context or is specified. The set of functions obtained from characters of $(\mathbb{Z}/m\mathbb{Z})^\times$ will be denoted, by abuse of notation, $\widehat{(\mathbb{Z}/m\mathbb{Z})}^\times$.

The Dirichlet character which is the extension of the trivial character of $(\mathbb{Z}/mZ)^\times$ will be denoted by 1. We emphasize that on an integer a which is coprime to m, this character takes the value 1, and on an integer which is not coprime to m this character takes the value 0.

Proposition 5.5.1. *Let χ be a Dirichlet character on $(\mathbb{Z}/m\mathbb{Z})^\times$. Let A be a set of m integers such that modulo m it becomes the set $\{0, 1, \ldots m-1\}$. Then*

$$\sum_{x \in A} \chi(x) = \begin{cases} \phi(m) & \text{if } \chi = 1 \\ 0 & \text{if } \chi \neq 1 \end{cases}$$

Proof.

$$\sum_{x \in A} \chi(x) = \sum_{x \in A \text{ and } \gcd(x,m)=1} \chi(x) = \sum_{x \in (\mathbb{Z}/m\mathbb{Z})^\times} \chi(x)$$

which gives the desired result from 1.3.1. The first equality follows beacuse $\chi(x) = 0$ for x not coprime to m. □

Proposition 5.5.2. *Let $x \in (\mathbb{Z}/m\mathbb{Z})^\times$. Then*

$$\sum_{\chi \in \widehat{(\mathbb{Z}/m\mathbb{Z})^\times}} \chi(x) = \begin{cases} \phi(m) & \text{if } x \equiv 1 \pmod{m} \\ 0 & \text{otherwise} \end{cases}$$

Proof. There are three mutually exclusive cases for x:

- $x \equiv 1 \pmod{m}$. (This implies that $\gcd(x, m) = 1$)
- $x \not\equiv 1 \pmod{m}$ and $\gcd(x, m) = 1$.
- $x \not\equiv 1 \pmod{m}$ and $\gcd(x, m) \neq 1$.

In the first case, we have the first part of 1.3.2. In the second case, we have the second part of 1.3.2. In the third case, we have by definition $\chi(x) = 0 \;\forall\; \chi \in \widehat{(\mathbb{Z}/m\mathbb{Z})^\times}$. □

5.6 Dirichlet L-series

In this section and the following sections whenever we refer to a Dirichlet character, it will be one that is extended from a character of $(\mathbb{Z}/N\mathbb{Z})^\times$.

Definition 5.6.1. *Let χ be a Dirichlet character. Then the Dirichlet L-series corresponding to χ is*

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

In the same way that $\zeta(s)$ has an Euler product, see 5.4, it follows that $L(\chi, s)$ also has an Euler product.

$$\begin{aligned} L(\chi, s) &= \prod_{p \text{ is prime}} \frac{1}{1 - \chi(p)p^{-s}} \\ &= \prod_{p \nmid N} \frac{1}{1 - \chi(p)p^{-s}}, \qquad \text{since } \chi(p) = 0 \text{ if } p|N\,. \end{aligned}$$

Proposition 5.6.2. *$L(\chi, s)$ is absolutely convergent and holomorphic on* $\mathrm{Re}(s) > 1$.

Proof. $|\chi(n)| = 1$. Therefore the coefficients in $L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ are bounded. Hence from 5.2.10 we have that $L(\chi, s)$ is convergent on $\mathrm{Re}(s) > 1$. □

Proposition 5.6.3. *For $\chi \neq 1$, $L(\chi, s)$ is convergent and holomorphic on* $\mathrm{Re}(s) > 0$*.*

Proof. The partial sums of coefficients are $A_{m,p} = \sum_{n=m}^{p} \chi(n)$. Every N consecutive integers form a set of the form A as described in 5.5.1. Therefore in considering $A_{m,p}$, we only have to consider cases where $p - m < N$, since from 5.5.1 $A_{m',p'} = 0$ if $p' - m' = kN$ with $k \in \mathbb{Z}$. Therefore, for $p - m < N$

$$|A_{m,p}| \leqslant \sum_{n=m}^{p} |\chi(n)| \leqslant N \,.$$

Hence from 5.2.11 we have shown the statement of the theorem. □

Proposition 5.6.4. *For $\chi = 1$, one has*

$$L(1, s) = F(s)\zeta(s) with\ F(s) = \prod_{p|N} \left(1 - p^{-s}\right) \,.$$

In particular, $L(1, s)$ is holomorphic on $\{\mathrm{Re}(s) > 0\} \backslash \{1\}$ and it has a simple pole at $s = 1$.

Proof.

$$\begin{aligned} L(1, s) &= \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} \\ &= \prod_{p \nmid N} \frac{1}{\left(1 - \frac{1}{p^s}\right)} \\ &= \prod_{p|N} \left(1 - p^{-s}\right) \prod_{\text{all } p} \frac{1}{(1 - p^{-s})} \\ &= F(s)\zeta(s) \,. \end{aligned}$$

The meromorphicity with simple pole at $s = 1$ is clear from 5.3.1 and the fact that $\prod_{p|N} (1 - p^{-s})$ is not zero on $\mathrm{Re}(s) > 0$. This is because $p^s \neq 1$ on this set. □

5.7 Dirichlet's Theorem on primes in arithmetic progression

Theorem 5.7.1. *Let $a, N \in \mathbb{Z}_{>0}$ be such that* $\gcd(a, N) = 1$*. Then there are infinitely many prime numbers p such that $p \equiv a$* $\text{mod}N$

We need some notation before we can explain the strategy of proof.

Definition 5.7.2. *Define*

$$l_1(\chi, s) := \sum_p \frac{\chi(p)}{p^s}\,.$$

The above definition is motivated by the following observation. Fix a class $a \in (\mathbb{Z}/N\mathbb{Z})^\times$.

$$\begin{aligned}
\sum_\chi \chi^{-1}(a) l_1(\chi, s) &= \sum_\chi \sum_p \frac{\chi^{-1}(a)\chi(p)}{p^s} \\
&= \sum_p \sum_\chi \frac{\chi^{-1}(a)\chi(p)}{p^s} \\
&= \sum_p \sum_\chi \frac{\chi(b)\chi(p)}{p^s} && ba \equiv 1 \text{ mod}N \\
&= \sum_p \frac{1}{p^s} \sum_\chi \chi(bp) \\
&= \sum_{bp \equiv 1 \text{ mod}N} \frac{\phi(N)}{p^s}, && \because 5.5.2\,.
\end{aligned}$$

Thus, we conclude,

$$\sum_{p \equiv a \text{ mod}N} \frac{1}{p^s} = \frac{1}{\phi(N)} \sum_\chi \chi^{-1}(a) l_1(\chi, s)\,. \tag{5.7.3}$$

where ϕ is the Euler totient function.

Proposition 5.7.4. *$l_1(\chi, s)$ is a Dirichlet series that is absolutely convergent and holomorphic on* $\text{Re}(s) > 1$*.*

Proof. From its definition we can see that since $|\chi(n)| = 1$ (and hence bounded), we can use 5.2.10 and the theorem follows. □

Remark 5.7.5. The strategy of proof will be to show that $\sum_{p\equiv a \bmod N} \frac{1}{p}$ is a diverging sum. For this it suffices to show that the Dirichlet series $(p > 0)$

$$\sum_{p\equiv a \bmod N} \frac{1}{p^s},$$

which is absolutely convergent and holomorphic on the right half plane $\mathrm{Re}(s) > 1$, see Proposition 5.2.10, diverges as $s \to 1$. This Dirichlet series is exactly the LHS of (5.7.3). To show that it diverges as $s \to 1$, it suffices to show that in the RHS, when $\chi \neq 1$, each $l_1(\chi, s)$ is holomorphic in a neighborhood of $s = 1$ (in particular, it converges at $s = 1$) and when $\chi = 1$, the series $l_1(1, s)$ diverges as $s \to 1$. The problem of showing that when $\chi \neq 1$, each $l_1(\chi, s)$ is holomorphic at $s = 1$, will be reduced to showing that when $\chi \neq 1$, each $L(\chi, s)$ is nonzero at $s = 1$. The other part of showing that when $\chi = 1$, the series $l_1(1, s)$ diverges, follows without much difficulty, and is proved in Corollary 5.7.12.

Definition 5.7.6. *Define*

$$l(\chi, s) := \sum_p \sum_{n\geqslant 1} \frac{\chi(p^n)/n}{p^{ns}}.$$

Proposition 5.7.7. *$l(\chi, s)$ is a Dirichlet series of the form $\sum_{m\geqslant 1} \frac{a_m}{m^s}$*

$$a_m = \begin{cases} \chi(p^n)/n & \text{if } m = p^n \text{ for some prime } p \text{ and } n \in \mathbb{N} \\ 0 & \text{otherwise} \end{cases}$$

It is absolutely convergent and holomorphic on $\mathrm{Re}(s) > 1$.

Proof. It is clear that a_m is bounded and now use 5.2.10 to see absolute convergence and holomorphy. □

Proposition 5.7.8. *In the right half plane* $\mathrm{Re}(s) > 1$, *we have*

$$e^{l(\chi,s)} = L(\chi, s).$$

Proof. Consider the following formal algebraic calculations. Since χ is multiplicative, as an algebraic equality of series, we have

$$L(\chi, s) = \sum_{n\geqslant 1} \frac{\chi(n)}{n^s} = \prod_p \frac{1}{1 - \frac{\chi(p)}{p^s}}.$$

Taking log on both sides we get

$$\begin{aligned}\log L(\chi,s) &= -\sum_p \log\left(1-\frac{\chi(p)}{p^s}\right)\\ &= \sum_p \sum_{n=1}^{\infty} \frac{\left(\frac{\chi(p)}{p^s}\right)^n}{n}\\ &= \sum_p \sum_{n\geqslant 1} \frac{\chi(p^n)/n}{p^{ns}} = l(\chi,s)\,.\end{aligned}$$

Now let $s_0 \in$ Re(s) > 1. Then the series $l(\chi, s_0)$ is absolutely convergent. In view of this, the value $e^{l(\chi,s_0)}$ can be obtained after any rearrangement. After formally rearranging the series, we see that this is exactly $L(\chi, s_0)$. Thus, both functions agree on Re(s) > 1. □

Definition 5.7.9. *Define*

$$R(\chi,s) \coloneqq l(\chi,s) - l_1(\chi,s) = \sum_p \sum_{n\geqslant 2} \frac{\chi(p^n)/n}{p^{ns}}\,.$$

Proposition 5.7.10. *$R(\chi, s)$ is a Dirichlet series that is absolutely convergent and holomorphic in the region* $\mathrm{Re}(s) > 1/2$.

Proof. Let $\mathrm{Re}(s) = x > 1/2$.

$$\begin{aligned}\sum_p \sum_{n\geqslant 2} \left|\frac{\chi(p^n)/n}{p^{ns}}\right| &\leqslant \sum_{n\geqslant 2} \sum_p \frac{1}{np^{nx}}\\ &\leqslant \sum_p \sum_{n\geqslant 2} \frac{1}{p^{nx}} = \sum_p \frac{1}{p^x(p^x-1)}\\ &= \frac{1}{2^x(2^x-1)} + \frac{1}{3^x(3^x-1)} + \sum_{p\geqslant 5} \frac{2}{p^{2x}}\\ &\leqslant \frac{1}{2^x(2^x-1)} + \frac{1}{3^x(3^x-1)} + \sum_{n\geqslant 5} \frac{2}{n^{2x}}\,.\end{aligned}$$

The last sum is convergent when $x > 1/2$. Now apply 5.2.7. □

Corollary 5.7.11. *$l_1(\chi, s)$ diverges at $s = 1$ iff $l(\chi, s)$ diverges at $s = 1$.*

Corollary 5.7.12. *$l_1(1, s)$ diverges at $s = 1$.*

Proof. Let $s > 1$ be real. If we let $s \to 1$ then it is clear that $l(1, s)$ diverges, since $\sum_p \frac{1}{p}$ diverges. Now apply the previous corollary. □

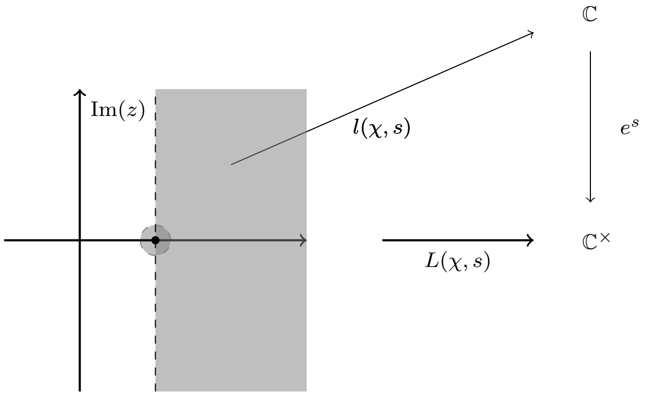
Next we want to show that if $\chi \neq 1$, then $l(\chi, s)$ converges at $s = 1$. In view of the above corollary, it follows that $l_1(\chi, s)$ converges at $s = 1$. We will reduce this to a question about $L(\chi, s)$ as follows.

Proposition 5.7.13. *If $\chi \neq 1$ and $L(\chi, s) \neq 0$, then $l(\chi, s)$ converges at $s = 1$.*

Proof. We have the following commutative diagram by Proposition 5.7.8.

(5.7.14)
$$\begin{tikzcd}
 & \mathbb{C} \arrow[d, "e^s"] \\
\{\text{Re(s)} > 1\} \arrow[ur, dashed, "l(\chi,s)"] \arrow[r, "L(\chi,s)"'] & \mathbb{C}^*
\end{tikzcd}$$

We already know, from Proposition 5.6.3, that for $\chi \neq 1$ the Dirichlet series $L(\chi, s)$ is convergent on $\text{Re(s)} > 0$. Let us assume that $L(\chi, 1) = c_0 \neq 0$. Then there is a small open subset $B(1, \epsilon)$ around 1 such that $L(\chi, s) \neq 0$ for $s \in B(1, \epsilon)$. Let V be a small open set around c_0 which is evenly covered for the covering map $s \mapsto e^s$. We may choose ϵ small enough so that the image of $B(1, \epsilon)$ lands in V. Now we can extend $l(\chi, s)$ to the open subset $B(1, \epsilon)$.



This shows that $l(\chi, s)$ is defined and holomorphic in a small neighborhood around $s = 1$, which proves the Proposition. □

Definition 5.7.15. *The Dedekind Zeta function is defined as*

$$\zeta_N(s) = \prod_\chi L(\chi, s)\,.$$

Proposition 5.7.16. *We have*

$$\zeta_N(s) = \prod_{p \nmid N} \frac{1}{\left(1 - \frac{1}{p^{f(p)s}}\right)^{g(p)}},$$

where $f(p)$ is the order of p in $(\mathbb{Z}/N\mathbb{Z})^\times$ and $g(p) = \frac{\phi(N)}{f(p)}$.

Proof. We require $p \nmid N$ for $f(p)$ to make sense. Let $\mu_{f(p)}$ be the group $f(p)^{\text{th}}$ roots of unity. Then we have the polynomial identity

$$\prod_{w \in \mu_{f(p)}} (1 - wx) \ = 1 - x^{f(p)}\,.$$

For a prime $p \nmid N$ consider the cyclic subgroup $\langle p \rangle \subset (\mathbb{Z}/N\mathbb{Z})^\times$. Let us denote this subgroup by H_p. Then

$$\begin{aligned} \zeta_N(s) &= \prod_{\chi \in \widehat{(\mathbb{Z}/N\mathbb{Z})}^\times} L(\chi, s) \\ &= \prod_{\chi \in \widehat{(\mathbb{Z}/N\mathbb{Z})}^\times} \prod_{p \nmid N} \frac{1}{1 - \chi(p)p^{-s}} = \prod_{p \nmid N} \prod_{\chi \in \widehat{(\mathbb{Z}/N\mathbb{Z})}^\times} \frac{1}{1 - \chi(p)p^{-s}} \\ &= \prod_{p \nmid N} \prod_{\chi \in \widehat{(\mathbb{Z}/N\mathbb{Z})}^\times} \frac{1}{1 - (\chi|_{H_p})(p)p^{-s}}\,. \end{aligned}$$

For a character χ of $(\mathbb{Z}/N\mathbb{Z})^\times$ its restriction to H_p is completely determined by its value on p, since H_p is the cyclic subgroup generated by p. Consider the short exact sequence

$$0 \to H_p \to (\mathbb{Z}/N\mathbb{Z})^\times \to Q_p \to 0\,.$$

From Proposition 1.2.7 it follows that the dual sequence

$$0 \to \hat{Q}_p \to \widehat{(\mathbb{Z}/N\mathbb{Z})}^\times \to \hat{H}_p \to 0$$

is exact. For every $\psi \in \hat{H}_p$ there are exactly $\left|\hat{Q}_p\right|$ many characters $\chi \in \widehat{(\mathbb{Z}/N\mathbb{Z})}^\times$ whose restriction to H_p is equal to ψ. Thus,

$$\prod_{p \nmid N} \prod_{\chi \in \widehat{(\mathbb{Z}/N\mathbb{Z})}^\times} \frac{1}{1 - (\chi|_{H_p})(p)p^{-s}} = \prod_{p \nmid N} \prod_{\psi \in \hat{H}_p} \left(\frac{1}{1 - \psi(p)p^{-s}}\right)^{|\hat{Q}_p|}.$$

Now note that H_p is a cyclic group of order $f(p)$. Thus, it is easily seen that

$$\prod_{\psi\in\hat{H}_p}\Big(\frac{1}{1-\psi(p)p^{-s}}\Big)=\frac{1}{1-p^{-f(p)s}}\,.$$

Also it is clear that $\left|\hat{Q}_p\right|=g(p)$. Putting these together we get that

$$\begin{aligned}\zeta_N(s)&=\prod_{\chi\in\widehat{(\mathbb{Z}/N\mathbb{Z})^\times}}L(\chi,s)\\&=\prod_{p\nmid N}\prod_{\chi\in\widehat{(\mathbb{Z}/N\mathbb{Z})^\times}}\frac{1}{1-(\chi|_{H_p})(p)p^{-s}}\\&=\prod_{p\nmid N}\prod_{\psi\in\hat{H}_p}\Big(\frac{1}{1-\psi(p)p^{-s}}\Big)^{|\hat{Q}_p|}\\&=\prod_{p\nmid N}\Big(\frac{1}{1-p^{-f(p)s}}\Big)^{g(p)}\,.\end{aligned}$$

This completes the proof. □

Corollary 5.7.17. *The Dedekind Zeta function ζ_N is a Dirichlet series with non-negative integral coefficients, converging absolutely in the half-plane* $\mathrm{Re}(s)>1$.

Proof. It is clear that a product of two Dirichlet series is again a Dirichlet series. ζ_N is a product of fintiely many functions which have Dirichlet series representations on $\mathrm{Re}(s)>1$. We also know that each of the Dirichlet series is absolutely convergent on $\mathrm{Re}(s)>1$ (by 5.6.2) and hence the product series will also be absolutely convergent on $\mathrm{Re}(s)>1$.

We know from 5.7.16 that

$$\zeta_N(s)=\prod_{p\nmid N}\frac{1}{\Big(1-\frac{1}{p^{f(p)s}}\Big)^{g(p)}}\,.$$

We can expand the factor in the Euler product as

$$\frac{1}{\Big(1-\frac{1}{p^{f(p)s}}\Big)^{g(p)}}=\Bigg(1+\frac{1}{p^{f(p)s}}+\frac{1}{p^{2f(p)s}+\dots}\Bigg)^{g(p)}\,.$$

We can expand out the RHS and it will only contain positive terms. When we multiply these factors over p, we clearly obtain a Dirichlet series with non-negative terms. □

Proposition 5.7.18. *If $\chi \neq 1$ then $L(\chi, 1) \neq 0$.*

Proof. Let us assume that there is $\chi \neq 1$ for which $L(\chi, 1) = 0$. Note that $L(1, s)$ is holomorphic on $\{\mathrm{Re(s)} > 0\} \setminus \{1\}$ and has a simple pole at $s = 1$, see 5.6.4. We also know, from Proposition 5.6.3 that when $\chi \neq 1$ the series $L(\chi, s)$ is holomorphic on $\mathrm{Re(s)} > 0$. Thus, it is clear that $\zeta_N(s)$, which is a holomorphic function on $\mathrm{Re(s)} > 1$ can be extended to a meromorphic function on $\mathrm{Re(s)} > 0$ which has at worst a simple pole at $s = 1$.

If $L(\chi, 1) = 0$ for some $\chi \neq 1$, then this zero will cancel the simple pole of $L(1, s)$ and we get the function $\zeta_N(s)$ is holomorphic in the region $\mathrm{Re(s)} > 0$. By Theorem 5.2.9 the Dirichlet series defining $\zeta_N(s)$ converges in a right half plane $\mathrm{Re}(s) > 1 - \rho$ for some $\rho > 0$. We claim that this Dirichlet series converges in the region $\mathrm{Re}(s) > 0$. If not, let

$$0 < \epsilon = \inf\{t \in (0, 1) \mid \text{The Dirichlet series converges in } \mathrm{Re}(s) > t\}.$$

Since $\zeta_N(s)$ is holomorphic in the region $\mathrm{Re(s)} > 0$, it is holomorphic in a neighborhood of ϵ, and so it follows from Theorem 5.2.9 that this series will converge in $\mathrm{Re}(s) > \epsilon - \delta$ for some $\delta > 0$, which is a contradiction. This proves the claim.

Let $s > 0$. From the definition

$$\zeta_N(s) = \prod_{p \nmid N} \frac{1}{\left(1 - \frac{1}{p^{f(p)s}}\right)^{g(p)}}.$$

We can expand the factor in the Euler product as

$$\frac{1}{\left(1 - \frac{1}{p^{f(p)s}}\right)^{g(p)}} = \left(1 + \frac{1}{p^{f(p)s}} + \frac{1}{p^{2f(p)s} + \dots}\right)^{g(p)}.$$

Now by ignoring cross terms as we raise the factor to $g(p)$, we obtain (as all the terms in the factor are positive)

$$\begin{aligned}\frac{1}{\left(1 - \frac{1}{p^{f(p)s}}\right)^{g(p)}} &\geqslant \left(1 + \frac{1}{p^{g(p)f(p)s}} + \frac{1}{p^{2g(p)f(p)s} + \dots}\right) \\ &= \left(1 + \frac{1}{p^{\phi(N)s}} + \frac{1}{p^{2\phi(N)s} + \dots}\right).\end{aligned}$$

Multiplying this over all $p \nmid N$, we obtain

$$\prod_{p \nmid N} \frac{1}{\left(1 - \frac{1}{p^{f(p)s}}\right)^{g(p)}} \geqslant \sum_{\gcd(n,N)=1} \frac{1}{n^{\phi(N)s}}.$$

Evaluating at $s = 1/\phi(N)$, we obtain

$$\zeta_N\Big(\frac{1}{\phi(N)}\Big) \geqslant \sum_{\gcd(n,N)=1} \frac{1}{n}\,.$$

But

$$\sum_{\gcd(n,N)=1} \frac{1}{n} \geqslant \sum_{k=1}^{\infty} \frac{1}{Nk+1}$$

and the RHS diverges. Therefore we obtain that $\zeta_N(s)$ has a pole at $s = 1/\phi(N)$ which is clearly a contradiction. □

Theorem 5.7.19. $\sum_{p\equiv a \mod N} \frac{1}{p}$ *is infinite.*

Proof. Recall equation (5.7.3) that

$$\sum_{p\equiv a \mod N} \frac{1}{p^s} = \frac{1}{\phi(N)} \sum_{\chi} \chi^{-1}(a) l_1(\chi, s)\,.$$

By Corollary 5.7.12 we know that $l_1(1, s)$ diverges as $s \to 1$. From Proposition 5.7.18 and Proposition 5.7.13 it follows that for $\chi \neq 1$ the series $l(\chi, s)$ converges at $s = 1$. Now it follows from Corollary 5.7.11 that for $\chi \neq 1$ the series $l_1(\chi, s)$ converges at $s = 1$. Taking limit in equation (5.7.3) as $s \to 1$ from the right, we see that the LHS tends to infinity at $s = 1$. This proves the theorem. □

Chapter 6

The Zeta function

In this chapter we prove two important and interesting results. It is easy to see that the Gamma function has a meromorphic continuation to the entire plane. Our first important result is that the Gamma function has no zeros on the complex plane. The idea of the proof is the following. First show that the function $\sin(\pi z)\Gamma(z)\Gamma(1-z)$ is periodic with period 1. Therefore, it descends as a function on the cylinder $\mathbb{C}/\mathbb{Z}$. Now show that along the ends of the cylinder this function has a limit, thereby, showing that this defines a holomorphic function on the Riemann sphere, and so is a constant. The first two sections are a discussion of the Gamma function.

Our second important result, which is a lot harder to prove than the first one, is that the Zeta function satisfies a certain functional equation. This functional equation enables us to meromorphically extend the Zeta function to the entire complex plane. The functional equation involves the Gamma function and that is why the Gamma function also appears in this chapter. The key step in the proof is to write an integral representation for the Zeta function in terms of the Jacobi Theta function and then use the functional equation for the Jacobi Theta function.

6.1 Gamma function

Definition 6.1.1 (Gamma Function)**.**

$$\Gamma(z) = \int_0^\infty t^{z-1}e^{-t}\,dt \qquad \textit{for } z \in \mathbb{C} \textit{ and } \mathrm{Re(z)} > 2$$

Proposition 6.1.2. *The Gamma function is holomorphic in the region* $\mathrm{Re(z)} > 2$*.*

Proof. To show differentiability we need to prove the following limit exists and is finite for all z such that $Re(z) > 2$

$$\lim_{h\to 0}\frac{\Gamma(z+h)-\Gamma(z)}{h}$$

Now

$$\lim_{h\to 0}\frac{\Gamma(z+h)-\Gamma(z)}{h} = \lim_{h\to 0}\int_0^\infty e^{-t}t^{z-1}\left(\frac{t^h-1}{h}\right)dt$$

We will use 5.1.1 to prove that the limit and the integral commute in this case and then the limit can be taken inside and evaluated. Consider some sequence h_n of complex numbers such that $h_n \to 0$ as $n \to \infty$ and let

$$\begin{aligned} f_n(t) &= e^{-t}t^{z-1}\left(\frac{t^{h_n}-1}{h_n}\right) \qquad Re(z) > 2 \text{ and } t \in (0,\infty) \\ |f_n(t)| &= e^{-t}t^{x-1}\left|\frac{t^{h_n}-1}{h_n}\right| \qquad z = x+iy \end{aligned} \tag{6.1.3}$$

We have

$$\begin{aligned} \left|\frac{t^{h_n}-1}{h_n}\right| = \left|\frac{e^{h_n\log t}-1}{h_n}\right| &= \left|\frac{1+\frac{h_n\log t}{1!}+\frac{(h_n\log t)^2}{2!}+\cdots-1}{h_n}\right| \\ &\leqslant |\log t|\Big(\frac{1}{1!}+\left|\frac{h_n\log t}{2!}\right|+\left|\frac{(h_n\log t)^2}{3!}\right|+\cdots\Big) \\ &\leqslant |\log t|\Big(\frac{1}{1!}+\left|\frac{h_n\log t}{1!}\right|+\left|\frac{(h_n\log t)^2}{2!}\right|+\cdots\Big) \\ &= |\log t|e^{|h_n\log t|} \end{aligned}$$

Since $h_n \to 0$ we get $|h_n| < 1/2$ for $n > N_0$. Thus,

$$\frac{t^{h_n}-1}{h_n} \leqslant |\log(t)|e^{\frac{|\log t|}{2}} \quad \forall n > N_0 \tag{6.1.4}$$

Define the function $g : (0,\infty) \to \mathbb{R}$ as,

$$g(t) = e^{-t}t^{x-1}|\log t|e^{\frac{|\log t|}{2}}$$

Clearly

$$|f_n(t)| \leqslant g(t) \quad \forall\, n > N_0$$

Now

$$\begin{aligned}\int_0^\infty g(t)\,dt &= \int_0^1 e^{-t}t^{x-1}|\log t|e^{\frac{|\log t|}{2}}\,dt + \int_1^\infty e^{-t}t^{x-1}|\log t|e^{\frac{|\log t|}{2}}\,dt\\ &= -\int_0^1 e^{-t}t^{x-3/2}\log t\,dt + \int_1^\infty e^{-t}t^{x-1/2}\log t\,dt\end{aligned}$$

Note that $\mathrm{Re}(z) = x > 2$. The first integral is finite because the integrand is bounded in $(0,1]$. For the second integral, since $\log t < e^{t/2}$, we get

$$e^{-t}t^{x-1/2}\log t < e^{-t/2}t^{x-1/2}$$

and so

$$\int_1^\infty e^{-t}t^{x-1/2}\log t\,dt < \int_1^\infty e^{-t/2}t^{x-1/2}\,dt < \infty$$

Hence,

$$\int_0^\infty g(t)\,dt < \infty$$

Then using 5.1.1

$$\lim_{n\to\infty}\int_0^\infty e^{-t}t^{z-1}\left(\frac{t^{h_n}-1}{h_n}\right)dt = \int_0^\infty e^{-t}t^{z-1}\lim_{n\to\infty}\frac{t^{h_n}-1}{h_n}$$

Since this is true for any such sequence h_n,

$$\begin{aligned}\therefore\ \Gamma'(z) &= \lim_{h\to 0}\int_0^\infty e^{-t}t^{z-1}\left(\frac{t^h-1}{h}\right)dt\\ &= \int_0^\infty e^{-t}t^{z-1}\lim_{h\to 0}\frac{t^h-1}{h}\\ &= \int_0^\infty e^{-t}t^{z-1}\log t\end{aligned}$$

which is finite for $Re(z) > 2$. This proves the proposition. □

Proposition 6.1.5. *Gamma function satisfies the following functional equation*

$$\Gamma(z+1) = z\Gamma(z)$$

Proof.

$$\Gamma(z+1) = \int_0^\infty e^{-t} t^z \, dt$$

(using integration by parts)

$$\begin{aligned} &= -t^z e^{-t}\Big|_0^\infty + \int_0^\infty z t^{z-1} e^{-t} \, dt \\ &= z\Gamma(z) \end{aligned}$$

□

Theorem 6.1.6. *Gamma function extends to a meromorphic function on the complex plane, which is holomorphic except with simple poles at*

$$0, -1, -2, -3, \cdots$$

Proof. For an integer $n \geqslant 0$ define a function $\Gamma_n(z)$ in the region $\mathrm{Re}(z) > -n$ by

$$\Gamma_n(z) := \frac{\Gamma(z+n+2)}{z(z+1)\cdots(z+n+1)}$$

From the functional equation 6.1.5 it is clear that for $\mathrm{Re}(z) > 2$

$$\Gamma_n(z) = \Gamma(z).$$

Further, $\Gamma_n(z)$ is holomorphic at all points in its domain except for z in

$$\{0, -1, -2, ..., -n+1\},$$

where it has simple poles. Hence, $\Gamma_n(z)$ meromorphically extends $\Gamma(z)$ to the right half plane $\mathrm{Re}(z) > -n$. Taking limit $n \to \infty$ we get a meromorphic function which is defined on the entire plane, it extends the Gamma function, and is holomorphic everywhere except on the set $\{0, -1, -2, \ldots\}$ where it has simple poles. □

6.2 Nonvanishing of $\Gamma(z)$

In this section we will show that the Gamma function has no zeros.

Lemma 6.2.1. *Let $y_0 > 0$. Then there is M (which depends on y_0) such that the following holds. Let $z = x + iy$ with $|y| > y_0 > 0$ and $x \in [0,1]$. Then $|\Gamma(z)| < M$.*

Proof. Using the functional equation 6.1.5

$$\Gamma(z) = \frac{\Gamma(z+3)}{z(z+1)(z+2)}$$

Since $\mathrm{Re}(z) = x \geqslant 0$, we get $\mathrm{Re}(z+3) = x+3 \geqslant 3$, and so we may compute $\Gamma(z+3)$ using its integral representation.

$$|\Gamma(z+3)| \leqslant \int_0^\infty |e^{-t}t^{z+3}|\,dt = \int_0^\infty e^{-t}t^{x+3}\,dt = \Gamma(x+3)$$

Since $x+3 \in [3,4]$ and the Gamma function is continuous, it follows that the above is bounded by M'. Next we have

$$\left|\frac{1}{z(z+1)(z+2)}\right| < \frac{1}{|y|^3} < \frac{1}{y_0^3}$$

Thus

$$|\Gamma(z)| = \left|\frac{\Gamma(z+3)}{z(z+1)(z+2)}\right| < \frac{M'}{y_0^3} = M$$

This proves the lemma. □

Proposition 6.2.2. *Define $G(z) := \sin(\pi z)\Gamma(z)\Gamma(1-z)$. Then $G(z)$ is a periodic function with period 1 and it is holomorphic everywhere.*

Proof. It is clear that $\Gamma(z)\Gamma(1-z)$ has simple poles at integers. Since $\sin(\pi z)$ has simple zeros at the integers, it follows that the function $G(z)$ has no poles.

$$\begin{aligned} G(z+1) &= \sin(\pi(z+1))\Gamma(z+1)\Gamma(-z) \\ &= (-\sin(\pi z))\left(\frac{\Gamma(z)}{z}\right)(-z\Gamma(1-z)) \\ &= \sin(\pi z)\Gamma(z)\Gamma(1-z) \\ &= G(z) \end{aligned}$$

This proves the proposition. □

Since $G : \mathbb{C} \to \mathbb{C}$ has period 1, it descends to a function $\tilde{G}$ on $\mathbb{C}^\times$, that is, there is a commutative diagram

$$\begin{tikzcd} \mathbb{C} \arrow[rr, "G"] \arrow[dr, "e^{2\pi i z}"'] & & \mathbb{C} \\ & \mathbb{C}^\times \arrow[ur, "\tilde{G}"'] & \end{tikzcd}$$

How to define $\tilde{G}$ is clear. For any $s \in \mathbb{C}^\times$ let z be any element of $\mathbb{C}$ such that $e^{2\pi i z} = s$. Define

$$\tilde{G}(s) = G(z).$$

This is well defined since if z' is another element such that $e^{2\pi i z'} = s$, then $z - z' \in \mathbb{Z}$ and G is periodic with period 1. The map $z \mapsto \exp(z) = e^{2\pi i z}$ is a holomorphic covering map. Given an point $s \in \mathbb{C}^\times$, and $z \in \mathbb{C}$ such that $\exp(z) = s$, there are small neighborhoods $V \subset \mathbb{C}^\times$ around s and $U \subset \mathbb{C}$ around z such that

1. The inverse image of V breaks into a disjoint union
$$\exp^{-1}(V) = \bigsqcup_{n \in \mathbb{Z}} U + n = \bigsqcup_{n \in \mathbb{Z}} \{x + n \mid x \in U\}$$
2. For each $n \in \mathbb{Z}$, $\exp : U + n \to V$ is a bijection whose inverse is holomorphic

Because of the above, it follows that the local properties of G descend to $\tilde{G}$, in particular, $\tilde{G}$ is a holomorphic function.

Theorem 6.2.3 (Liouville's theorem)**.** *Let $f : \mathbb{C} \to \mathbb{C}$ be a bounded holomorphic function. Then f is constant.*

We will use this theorem to show that $G(z)$ is a constant function.

Theorem 6.2.4. *$G(z)$ is a constant function.*

Proof. First we will prove that $\tilde{G}(t)$ can be extended to a holomorphic function on $\mathbb{C}$. Under the map $z \mapsto e^{2\pi i z}$, the strip $0 \leqslant \mathrm{Re}(z) \leqslant 1$ maps surjectively onto $\mathbb{C}^\times$. Thus, for $t \in \mathbb{C}^\times$, we may choose z in this strip such that $t = e^{2\pi i z}$.

$$t\tilde{G}(t) = e^{2\pi i z} G(z) = e^{2\pi i z} \Gamma(z)\Gamma(1-z) \sin \pi z$$

If $z = x + iy$ then

$$\begin{aligned} |t\tilde{G}(t)| &= e^{-2\pi y} |\Gamma(z)\Gamma(1-z) \sin \pi z| \\ &= e^{-2\pi y} |\Gamma(z)\Gamma(1-z)| \left| \frac{e^{i\pi z} - e^{-i\pi z}}{2i} \right| \\ &\leqslant e^{-2\pi y} \left(\frac{|e^{i\pi z}| + |e^{-i\pi z}|}{2} \right) |\Gamma(z)\Gamma(1-z)| \\ &\leqslant \left(\frac{|e^{-3\pi y}| + |e^{-\pi y}|}{2} \right) |\Gamma(z)\Gamma(1-z)| \end{aligned}$$

If $|t|$ is small, then $y \gg 0$. Then by Lemma 6.2.1 $|\Gamma(z)\Gamma(1-z)|$ is bounded and the exponential terms tend to 0 as $y \to \infty$. Therefore we have

$$t\tilde{G}(t) \to 0 \quad \text{as} \qquad t \to 0$$

Since $t\tilde{G}(t)$ is holomorphic for $t \in \mathbb{C}^*$, this shows that it has a removable singularity at $t = 0$. Thus, defining $t\tilde{G}(t) = 0$ at $t = 0$ makes it holomorphic everywhere. We will write the analytic series of $t\tilde{G}(t)$ at $t = 0$.

$$t\tilde{G}(t) = a_0 + a_1 t + a_2 t^2 + \dots$$

Since $a_0 = 0$ we have

$$t\tilde{G}(t) = a_1 t + a_2 t^2 + a_3 t^3 + \dots$$

which implies

$$\tilde{G}(t) = a_1 + a_2 t + a_3 t^2 + \dots$$

Thus, $\tilde{G}(t)$ is holomorphic on $\mathbb{C}$.

Next we will prove $\tilde{G}(t)$ is bounded as $|t| \to \infty$. First define a function $H : \mathbb{C}^* \to \mathbb{C}^*$ by

$$H(z) = \tilde{G}(\frac{1}{z})$$

Since $\tilde{G}(z)$ and $\frac{1}{z}$ are holomorphic on $\mathbb{C}^*$, $H(z)$ is holomorphic on $\mathbb{C}^*$. For $t = \frac{1}{s} = e^{2\pi i z}$ consider

$$\begin{aligned}
|sH(s)| &= \left|\frac{\tilde{G}(1/s)}{1/s}\right| = \left|\frac{\tilde{G}(t)}{t}\right| = \left|e^{-2\pi i z} G(z)\right| \\
&= e^{2\pi y} |\Gamma(z)\Gamma(1-z) \sin \pi z| \\
&= e^{2\pi y} \left|\frac{e^{i\pi z} - e^{-i\pi z}}{2i}\right| |\Gamma(z)\Gamma(1-z)| \\
&\leqslant e^{2\pi y} \left(\frac{|e^{i\pi z}| + |e^{-i\pi z}|}{2}\right) |\Gamma(z)\Gamma(1-z)| \\
&\leqslant \left(\frac{|e^{\pi y}| + |e^{3\pi y}|}{2}\right) |\Gamma(z)\Gamma(1-z)|
\end{aligned}$$

As before, for any s, we may choose $z = x + iy$ such that $0 \leqslant x \leqslant 1$ and $1/s = e^{2\pi i z}$. Now $|s| \to 0$ iff $|t| \to \infty$ iff $y \to -\infty$. Clearly $|sH(s)| \to 0$ since the gamma function part is bounded. Now using the same reasoning as before we have

$$H(s) = b_1 + b_2 s + b_3 s^2 + \dots$$

which implies $H(s)$ is bounded as $s \to 0$ which proves that $\tilde{G}(t)$ is bounded as $|t| \to \infty$.

Thus, $\tilde{G}(t)$ is a holomorphic function on all of $\mathbb{C}$ which is bounded for $|t| \gg 0$. Therefore, by Liouville's theorem $\tilde{G}(t)$ is constant. This in turn implies $G(z)$ is constant, that is,

$$\Gamma(z)\Gamma(1-z)\sin \pi z = C$$

Evaluating at $z = \frac{1}{2}$, we get $C = \pi$. □

Theorem 6.2.5. *The function $\Gamma(z)$ has no zeros.*

Proof. If $\Gamma(z_0) = 0$, then since

$$\Gamma(z)\Gamma(1-z)\sin \pi z = \pi$$

it follows that $\Gamma(1-z)\sin(\pi z)$ has a pole at z_0. Since $\sin(\pi z)$ is entire, it has no poles. Thus, $\Gamma(1-z)$ has a pole at z_0. But we know that the poles of $\Gamma(1-z)$ are exactly at the positive integers. This forces that $z_0 \in \{1, 2, 3 \ldots\}$, which is a contradiction since $\Gamma(n) = n!$ for $n \in \mathbb{Z}_{>0}$. □

6.3 Fourier Series

The main result in this section is that if we take a "nice" periodic function on $\mathbb{R}$, then its Fourier series converges to itself pointwise .

Definition 6.3.1 (Fourier series)**.** *Let $f : \mathbb{R} \to \mathbb{C}$ be a periodic function with period* 1*. We define the n^{th} Fourier coefficient of f as*

$$a_n := \int_0^1 f(x)e^{-2\pi i n x}\, dx\,. \tag{6.3.2}$$

Then the Fourier series of f is a function $S(f) : \mathbb{R} \to \mathbb{C}$ defined as

$$S(f)(x) := \sum_{n=-\infty}^{\infty} a_n e^{2\pi i n x}\,.$$

We will use the following theorem without proof.

Theorem 6.3.3. *Let $f : \mathbb{R} \to \mathbb{C}$ be a periodic function with period 1. Assume that $f|_{[0,1]} \in L^2([0,1])$. Then the Fourier series $S(f)$ is defined almost everywhere, $S(f)|_{[0,1]} \in L^2([0,1])$ and $f|_{[0,1]} = S(f)|_{[0,1]}$ in $L^2([0,1])$*

Theorem 6.3.4. *If $f : \mathbb{R} \to \mathbb{C}$ is periodic with period 1 and $f^{(2)}$ is continuous then $f(x) = S(f)(x)$ pointwise.*

Proof. If we can show that $S(f)$ is continuous, then since both are periodic of period 1 and are equal in $L^2([0,1])$ it will follow that $f = S(f)$. Note that

$$d(f(x)e^{-2\pi inx}) = f'(x)e^{-2\pi inx}\,dx - 2\pi in f(x)e^{-2\pi inx}\,dx\,.$$

Since $f(x)$ has period 1, integrating both sides from 0 to 1 we get

$$\frac{1}{2\pi in}\int_0^1 f'(x)e^{-2\pi inx}\,dx = \int_0^1 f(x)e^{-2\pi inx}\,dx\,.$$

Again integrating by parts we get

$$-\frac{1}{4\pi^2n^2}\int_0^1 f^{(2)}(x)e^{-2\pi inx}\,dx = \int_0^1 f(x)e^{-2\pi inx}\,dx\,.$$

If $f^{(2)}$ is continuous then $f^{(2)}(x)$ is bounded by some $M > 0$ and

$$\left|\int_0^1 f^{(2)}(x)e^{-2\pi inx}\,dx\right| \leqslant \int_0^1 \left|f^{(2)}(x)e^{-2\pi inx}\right|\,dx \leqslant M\,.$$

Therefore

$$\begin{aligned}\sum_{n=-\infty}^{\infty}|a_n| &= \sum_{n=-\infty}^{\infty}\left|\int_0^1 f(x)e^{-2\pi inx}\,dx\right| \\ &= \sum_{n=-\infty}^{\infty}\frac{1}{4\pi^2n^2}\left|\int_0^1 f^{(2)}(x)e^{-2\pi inx}\,dx\right| \leqslant \sum_{n=-\infty}^{\infty}\frac{M}{4\pi^2n^2} < \infty\,.\end{aligned}$$

For fixed $x \in [0,1]$ and $h \in \mathbb{R}$ define functions $g_h : \mathbb{Z} \to \mathbb{C}$ by

$$g_h(n) := a_n e^{-2\pi in(x+h)}\,. \tag{6.3.5}$$

For every h we have

$$\int_{\mathbb{Z}}|g_h(n)| = \int_{\mathbb{Z}}|a_n| = \sum_{n=-\infty}^{\infty}|a_n| < \infty\,.$$

Thus, can apply 5.1.1 and exchange the integral and the limit. We get

$$\begin{aligned}\lim_{h\to 0}\sum_{n=-\infty}^{\infty} a_n e^{-2\pi i n(x+h)} &= \lim_{h\to 0}\int_{\mathbb{Z}} g_h(n)\\ &= \int_{\mathbb{Z}} \lim_{h\to 0} g_h(n)\\ &= \sum_{-\infty}^{\infty} \lim_{h\to 0} a_n e^{-2\pi i n(x+h)}\\ &= \sum_{-\infty}^{\infty} a_n e^{-2\pi i n(x)}\,.\end{aligned}$$

Thus, we have proved that $\lim_{h\to 0} S(f)(x+h) = S(f)(x)$ and so $S(f)$ is continuous. □

6.4 Jacobi's Theta function

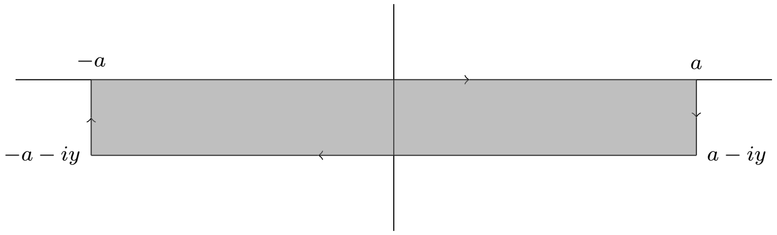
Lemma 6.4.1. *For any $z \in \mathbb{C}$*

$$\int_{\mathbb{R}} e^{-\pi(u+z)^2}\, du = 1\,.$$

Proof. If $z = x + iy$, then substituting $u' = u + x$ then we get

$$\int_{\mathbb{R}} e^{-\pi(u+z)^2}\, du = \int_{\mathbb{R}} e^{-\pi(u'+iy)^2}\, du'\,.$$

Thus, we need to evaluate $\int_{\mathbb{R}} e^{-\pi(u+iy)^2}\, du$. Consider the integral of $g(u) = e^{-\pi(u+iy)^2}$ over rectangular contour C_a shown in the figure.



Since $g(u)$ is a holomorphic function of u, $\int_{C_a} e^{-\pi(u+iy)^2}\, du = 0$. We break this integral into a sum of integrals over the following paths.

1. Let P_1 be the path from $-a$ to a.

2. Let P_2 be the path from a to $a - iy$.

3. Let P_3 be the path from $a - iy$ to $-a - iy$.

4. Let P_4 be the path from $-a - iy$ to $-a$.

Let us first look at the second integral. The path here is given by $\gamma(t) = a - it$, where t varies from 0 to y. Thus, using the definition of path integral

$$\begin{aligned}\left|\int_{P_2} e^{-\pi(u+iy)^2}\,du\right| &= \left|\int_0^y e^{-\pi(a-it+iy)^2}\,dt\right| \\ &\leqslant e^{-\pi a^2}\int_0^y e^{\pi(y-t)^2}\,dt\,.\end{aligned}$$

The integral in the RHS is bounded. Therefore, taking limit $a \to \infty$ we get

$$\lim_{a\to\infty}\int_{P_2} e^{-\pi(u+iy)^2}\,du = 0\,.$$

Similarly we can show the fourth integral also tends to 0 as $a \to \infty$. So we find that

$$0 = \lim_{a\to\infty}\int_{C_a} e^{-\pi(u+iy)^2}\,du = \lim_{a\to\infty}\int_{P_1} e^{-\pi(u+iy)^2}\,du + \lim_{a\to\infty}\int_{P_3} e^{-\pi(u+iy)^2}\,du\,.$$

In P_1 the path $\gamma(t)$ is given by $\gamma(t) = t$, where where t varies from $-a$ to a. By definition

$$\lim_{a\to\infty}\int_{P_1} e^{-\pi(u+iy)^2}\,du = \lim_{a\to\infty}\int_{-a}^{a} e^{-\pi(t+iy)^2}\,dt\,.$$

In P_3 the path $\gamma(t)$ is given by $\gamma(t) = t - iy$, where t varies from a to $-a$. By definition

$$\lim_{a\to\infty}\int_{P_3} e^{-\pi(u+iy)^2}\,du = \lim_{a\to\infty}\int_{a}^{-a} e^{-\pi t^2}\,dt\,.$$

Thus, since the sum of the two integrals is 0, it follows that

$$\int_{\mathbb{R}} e^{-\pi(t+iy)^2}\,dt = \int_{\mathbb{R}} e^{-\pi t^2}\,dt = 1\,.$$

□

Definition 6.4.2 (Jacobi's theta function)**.** *Define for $Re(z) > 0$*

$$\theta(z) := 1 + 2\sum_{m\geqslant 1} e^{-\pi m^2 z}\,. \tag{6.4.3}$$

Proposition 6.4.4. *$\theta(z)$ is holomorphic in the region $Re(z) > 0$.*

Proof. If $x = \mathrm{Re}(z) > \delta > 0$ then

$$\begin{aligned}\sum_{k}^{\infty}\left|e^{-\pi m^2 z}\right| &\leqslant \sum_{m=k}^{\infty} e^{-\pi m^2 x} < \sum_{m=k}^{\infty} e^{-\pi m x}\\ &< \sum_{m=k}^{\infty} e^{-\pi m\delta} = \frac{e^{-\pi k\delta}}{1-e^{-\pi\delta}}\,.\end{aligned}$$

By choosing k large we can make this as small as we like. Thus, the functions

$$f_k(z) := \sum_{m=1}^{k} e^{-\pi m^2 z}$$

converge uniformly in every right half plane $\mathrm{Re}(z) > \delta > 0$. By Theorem 5.1.5 it follows that $\theta(z)$ is holomorphic in the region $\mathrm{Re}(z) > 0$. □

Definition 6.4.5. *For $t \in \mathbb{R}$, $t > 0$ define*

$$f_t(z) := e^{-\pi z^2 t},$$

$$F_t(z) := \sum_{n\in\mathbb{Z}} f_t(z+n)\,.$$

Remark 6.4.6. $F_t(0) = \theta(t)$

Proposition 6.4.7. *The function $F_t(z)$ is holomorphic on $\mathbb{C}$.*

Proof. We have

$$\begin{aligned}F_t(z) &= \sum_{n\in\mathbb{Z}} e^{-\pi(z+n)^2 t}\\ &= e^{-\pi z^2 t} + \sum_{n=1}^{\infty} e^{-\pi(z+n)^2 t} + \sum_{n=1}^{\infty} e^{-\pi(z-n)^2 t}\,.\end{aligned}$$

The first term is holomorphic on $\mathbb{C}$. We will show that the two series are holomorphic at any arbitrary point $z = z_0$. Consider the first series $\sum_{n=1}^{\infty} e^{-\pi(z+n)^2 t}$. Define

$$f_k(z) := \sum_{m=1}^{k} e^{-\pi(z+n)^2 t}\,.$$

Let $x = \mathrm{Re}(z) > \delta > -\infty$. Choose $k \gg 0$ so that $\delta + k > 1$. Then

$$x + n > \delta + n > 1, \qquad (x+n)^2 > (\delta+n)^2 > \delta + n > 1$$

for all $n \geqslant k$. Using this we get

$$\begin{aligned} \sum_{n=k}^{\infty} \left| e^{-\pi(z+n)^2 t} \right| &= \sum_{n=k}^{\infty} e^{-\pi t((x+n)^2 - y^2)} \\ &= e^{\pi y^2 t} \sum_{n=k}^{\infty} e^{-\pi t(x+n)^2} \\ &< e^{\pi y^2 t} \sum_{n=k}^{\infty} e^{-\pi t(\delta+n)} = \frac{e^{\pi y^2 t} e^{-\pi t(\delta+k)}}{1 - e^{-\pi t}}\,. \end{aligned} \tag{6.4.8}$$

By choosing k large we can make this as small as we like. Thus, the functions

$$f_k(z) = \sum_{n=1}^{k} e^{-\pi(z+n)^2 t}$$

converge uniformly in every right half plane $\mathrm{Re}(z) > \delta$. By Theorem 5.1.5 it follows that $\sum_{n=1}^{\infty} e^{-\pi(z+n)^2 t}$ is holomorphic on $\mathbb{C}$. Similarly, we can show that the second series is also holomorphic on all of $\mathbb{C}$. This completes the proof. □

Theorem 6.4.9 (Functional equation)**.** *For* $\mathrm{Re}(z) > 0$

$$\theta(z) = \frac{\theta(1/z)}{\sqrt{z}}\,.$$

Proof. Consider the function $F_t(x)$ (see Definition 6.4.5) with domain restricted to the real line. Note that it is periodic with period 1. Since $F_t(z)$

is holomorphic, $F_t^{(2)}(x)$ is continuous, which implies its fourier series converges to itself pointwise.

$$\begin{aligned}\theta(t) = F_t(0) = S(F_t)(0) &= \sum_{n\in\mathbb{Z}}\left(\int_0^1 F_t(s)e^{-2\pi ins}\,ds)\right)\\ &= \sum_{n\in\mathbb{Z}}\left(\int_0^1 \sum_{m\in\mathbb{Z}} f_t(s+m)e^{-2\pi ins}\,ds)\right)\\ &= \sum_{n\in\mathbb{Z}}\left(\int_0^1 \lim_{l\to\infty}\sum_{|m|<l} f_t(s+m)e^{-2\pi ins}\,ds)\right)\,.\end{aligned}$$

On the interval $s\in[0,1]$ consider the functions

$$h_l(s) = \sum_{m\geqslant l} f_t(s+m)e^{-2\pi ins} + \sum_{m\leqslant -l} f_t(s+m)e^{-2\pi ins}\,.$$

That $h_l(s)$ converges uniformly as $l\to\infty$ has already been proved in Proposition 6.4.7. In fact, the uniform convergence of the first series follows from equation (6.4.8) since $|f_t(s+m)| = \left|f_t(s+m)e^{2\pi ins}\right|$. The uniform convergence of the second series may be deduced in the same way. Thus, we may apply Corollary 5.1.2. Taking the limit outside we get

$$\begin{aligned}\theta(t) &= \sum_{n\in\mathbb{Z}}\lim_{l\to\infty}\int_0^1 \sum_{|m|<l} f_t(s+m)e^{-2\pi ins}\,ds)\\ &= \sum_{n\in\mathbb{Z}}\sum_{m\in\mathbb{Z}}\int_0^1 f_t(s+m)e^{-2\pi ins}\,ds)\\ &= \sum_{n\in\mathbb{Z}}\sum_{m\in\mathbb{Z}}\int_m^{1+m} f_t(u)e^{-i2\pi in(u-m)}\,du\\ &= \sum_{n\in\mathbb{Z}}\int_{-\infty}^{\infty} f_t(u)e^{-2\pi inu}\,du = \sum_{n\in\mathbb{Z}}\int_{\mathbb{R}} e^{-\pi u^2t-2\pi inu}\,du\,.\end{aligned}$$

Substituting $u\sqrt{t}=s$ we get

$$\begin{aligned}\theta(t) &= \sum_{n\in\mathbb{Z}}\frac{1}{\sqrt{t}}\int_{\mathbb{R}} e^{-\pi s^2-i2\pi n\frac{s}{\sqrt{t}}}\,ds = \sum_{n\in\mathbb{Z}}\frac{1}{\sqrt{t}}\int_{\mathbb{R}} e^{-\pi(s+i\frac{n}{\sqrt{t}})^2-\pi\frac{n^2}{t}}\,ds\\ &= \sum_{n\in\mathbb{Z}}\frac{e^{-\pi\frac{n^2}{t}}}{\sqrt{t}}\int_{\mathbb{R}} e^{-\pi(s+i\frac{n}{\sqrt{t}})^2}\,ds\,.\end{aligned}$$

From the lemma 6.4.1, we know the integral evaluates to 1. So we get

$$\theta(t) = \sum_{n\in\mathbb{Z}} \frac{e^{-\pi\frac{n^2}{t}}}{\sqrt{t}} = \frac{\theta(1/t)}{\sqrt{t}}\,.$$

Note that both functions are holomorphic on $\mathrm{Re}(z) > 0$ and they agree on the positive real line. Thus, they agree everywhere, that is,

$$\theta(z) = \frac{\theta(1/z)}{\sqrt{z}}\,.$$

This completes the proof of the Theorem. □

6.5 Functional equation

Definition 6.5.1. *For* $\mathrm{Re}(s) > 0$ *define*

$$\xi(s) := \frac{s(s-1)}{2}\pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})\zeta(s)\,.$$

This defines a holomorphic function in the region Re(s) > 0. This is because $(s-1)\zeta(s)$ is holomorphic in the region Re(s) > 0, see Theorem 5.3.1, and all the other factors are holomorphic in the region Re(s) > 0. Define $\omega : \mathbb{R}_{>0} \to \mathbb{R}_{>0}$ by

$$\omega(u) := (\theta(u) - 1)/2 = \sum_{n\geqslant 1} e^{-\pi n^2 u}\,.$$

We will need the following lemma in the proof of the functional equation.

Lemma 6.5.2. *The integral*

$$f(s) := \int_1^\infty \omega(u)u^s\,du$$

converges for all $s \in \mathbb{C}$ *and defines a function which is holomorphic everywhere.*

Proof. Let us first prove that the integral converges. Let $s = x + iy$. Then

$$|f(s)| \leqslant \int_1^\infty \sum_{n\geqslant 1} e^{-\pi n^2 u} u^x\,du$$

Now note that $u^x e^{-\pi n^2 u} \leqslant u^x e^{-\pi n u}$. Taking sum over n we get

$$\begin{aligned}\sum_{n\geqslant 1} e^{-\pi n^2 u} u^x \leqslant \sum_{n\geqslant 1} e^{-\pi n u} u^x &= \frac{u^x}{e^{\pi u}-1}\\ &< u^x e^{-\pi u/2} \qquad (\text{since } u \geqslant 1)\,.\end{aligned}$$

Integrating we get

$$|f(s)| < \int_1^\infty u^x e^{-\pi u/2}\, du < \infty\,.$$

Now we prove that $f(s)$ is holomorphic.

$$\left|\frac{f(s+h)-f(s)}{h}\right| \leqslant \int_1^\infty \omega(u) u^x \left|\frac{u^h-1}{h}\right| du\,.$$

Recall the estimate proved in equation (6.1.4), if $|h| < 1/2$ then

$$\left|\frac{u^h-1}{h}\right| \leqslant \log(u) u^{1/2} < u^{3/2} \qquad (\text{since } u \geqslant 1)\,.$$

Thus,

$$\omega(u) u^x \left|\frac{u^h-1}{h}\right| \leqslant \omega(u) u^{x+3/2}\,.$$

But since

$$\int_1^\infty \omega(u) u^{x+3/2}\, du = f(x+3/2) < \infty,$$

we can apply 5.1.1 to see that the limit

$$\lim_{h\to 0} \frac{f(s+h)-f(s)}{h}$$

exists. This proves that $f(s)$ is holomorphic everywhere. □

Theorem 6.5.3 (Functional equation)**.** *For* $0 < \mathrm{Re}(s) < 1$,

$$\xi(1-s) = \xi(s)\,.$$

Proof. The strategy is to write $\xi(s)$ in terms of the Jacobi Theta function and then use the functional equation 6.4.9. We claim that for $\mathrm{Re}(s) > 4$

$$\pi^{\frac{-s}{2}} \Gamma(\frac{s}{2}) \zeta(s) = \int_0^\infty \omega(u) u^{\frac{s}{2}-1}\, du\,. \tag{6.5.4}$$

By definition, for $\mathrm{Re}(s) > 4$

$$\Gamma(\frac{s}{2}) = \int_0^\infty e^{-t} t^{\frac{s}{2}-1}\, dt\,.$$

Substituting $t = \pi n^2 u$

$$\begin{aligned}\Gamma(\frac{s}{2}) &= \int_0^\infty e^{-\pi n^2 u} \pi^{\frac{s}{2}} n^s u^{\frac{s}{2}-1}\, du \\ \pi^{\frac{-s}{2}} \frac{\Gamma(\frac{s}{2})}{n^s} &= \int_0^\infty e^{-\pi n^2 u} u^{\frac{s}{2}-1}\, du\,.\end{aligned}$$

Summing over n from 1 to infinity, we get

$$\begin{aligned}\pi^{\frac{-s}{2}} \Gamma(\frac{s}{2}) \zeta(s) &= \sum_{n=1}^\infty \int_0^\infty e^{-\pi n^2 u} u^{\frac{s}{2}-1}\, du \\ &= \lim_{k\to\infty} \int_0^\infty \sum_{n=1}^k e^{-\pi n^2 u} u^{\frac{s}{2}-1}\, du\,.\end{aligned} \tag{6.5.5}$$

We will use 5.1.1 to take the limit inside. Let $s = x + iy$ and define

$$h_k(u,s) = \sum_{n=1}^k e^{-\pi n^2 u} u^{\frac{s}{2}-1}\,.$$

Next we find a suitable bound for $h_k(u,s)$.

$$\begin{aligned}|h_k(u,s)| &\leqslant \sum_{n=1}^k \left| e^{-\pi n^2 u} u^{\frac{s}{2}-1} \right| \\ &= \sum_{n=1}^k e^{-\pi n^2 u} u^{\frac{x}{2}-1} = \frac{u^{\frac{x}{2}-1}}{e^{\pi u} - 1}\,.\end{aligned}$$

Since $x > 4$ we have $\lim_{u\to 0} \frac{u^{\frac{x}{2}-1}}{e^{\pi u}-1} = 0$. Using this it is easily checked that

$$\int_0^\infty \frac{u^{\frac{x}{2}-1}}{e^{\pi u} - 1}\, du < \infty\,.$$

Applying 5.1.1 to (6.5.5), we get

$$\pi^{\frac{-s}{2}} \Gamma(\frac{s}{2}) \zeta(s) = \int_0^\infty \sum_{n=1}^\infty e^{-\pi n^2 u} u^{\frac{s}{2}-1}\, du = \int_0^\infty \omega(u) u^{\frac{s}{2}-1}\, du\,.$$

This proves the claim in (6.5.4).

We break the above integral into 2 parts, from 0 to 1 and from 1 to ∞. In the first part make the substitution $u = \frac{1}{v}$ to get

$$\pi^{\frac{-s}{2}}\Gamma(\frac{s}{2})\zeta(s) = \int_1^\infty \omega(\frac{1}{v})v^{-\frac{s}{2}-1}\,dv + \int_1^\infty \omega(v)v^{\frac{s}{2}-1}\,dv\,.$$

We know that

$$\begin{aligned}\omega(\frac{1}{v}) &= \frac{1}{2}(\theta(\frac{1}{v}) - 1) = \frac{1}{2}(\sqrt{v}\theta(v) - 1)\\ &= \frac{1}{2}(\sqrt{v}(2\omega(v) + 1) - 1)\\ &= \sqrt{v}\omega(v) + \frac{\sqrt{v}}{2} - \frac{1}{2}\,.\end{aligned}$$

Therefore

$$\begin{aligned}\pi^{\frac{-s}{2}}\Gamma(\frac{s}{2})\zeta(s) &= \int_1^\infty (\sqrt{v}\omega(v) + \frac{\sqrt{v}}{2} - \frac{1}{2})v^{-\frac{s}{2}-1}\,dv + \int_1^\infty \omega(v)v^{\frac{s}{2}-1}\,dv\\ &= \int_1^\infty \frac{1}{2}(v^{-\frac{s+1}{2}} - v^{-\frac{s}{2}-1})\,dv + \int_1^\infty \omega(v)(v^{-\frac{s+1}{2}} + v^{\frac{s}{2}-1})\,dv\\ &= \frac{1}{s(s-1)} + \int_1^\infty \omega(v)(v^{-\frac{s+1}{2}} + v^{\frac{s}{2}-1})\,dv\,.\end{aligned}$$

So finally we have

$$\begin{aligned}\xi(s) &= \frac{s(s-1)}{2}\pi^{\frac{-s}{2}}\Gamma(\frac{s}{2})\zeta(s)\\ &= \frac{1}{2} + \frac{s(s-1)}{2}\int_1^\infty \omega(v)(v^{-\frac{s+1}{2}} + v^{\frac{s}{2}-1})\,dv\,.\end{aligned} \tag{6.5.6}$$

Let

$$I(s) = \int_1^\infty \omega(v)(v^{-\frac{s+1}{2}} + v^{\frac{s}{2}-1})\,dv,$$

then we have proved that

$$\xi(s) = \frac{1}{2} + \frac{s(s-1)}{2}I(s)\,.$$

Assume for a moment that $I(s)$ is analytic on $\mathbb{C}$. Putting $1-s$ in place of s and observing that $I(s) = I(1-s)$ gives the required functional equation. Thus, it only remains to prove that $I(s)$ is holomorphic on $\mathbb{C}$. But this is clear from Lemma 6.5.2. □

Corollary 6.5.7. *The function $\xi(s)$ extends to a holomorphic function on all of $\mathbb{C}$.*

Proof. It is clear from Theorem 6.1.6 and Theorem 5.3.1 that $\xi(s)$ is holomorphic in $\mathrm{Re}(s) > 0$. Thus, the function $\xi(1-s)$ is holomorphic in the region $\mathrm{Re}(s) < 1$. Since $\xi(s) = \xi(1-s)$ in the region $0 < \mathrm{Re}(s) < 1$, it follows that $\xi(s)$ extends to give a holomorphic function on $\mathbb{C}$. □

Corollary 6.5.8. *The function $\zeta(s)$ extends to a meromorphic function on $\mathbb{C}$ which is holomorphic everywhere except $s = 1$. At $s = 1$ it has a simple pole. It has simple zeros for $s \in \{-2, -4, -6, \ldots\}$.*

Proof. We have

$$\zeta(s) = \frac{2\pi^{s/2}\xi(s)}{(s-1)} \frac{1}{s\Gamma(s/2)} \,.$$

Clearly the numerator is holomorphic on $\mathbb{C}$. Since the Gamma function has no zeros, it follows that $1/\Gamma(s/2)$ is holomorphic on all of $\mathbb{C}$. At $s = 0$, the denominator $s\Gamma(s/2)$ is nonzero. Thus, $\zeta(s)$ has only one pole, which is at $s = 1$.

The function $1/s\Gamma(s/2)$ has simple zeros at the negative even integers. From this the assertion on the zeros of $\zeta(s)$ is clear. □

6.6 Non-vanishing of $\zeta(s)$ for $s \in (0,1)$

In this section we prove that $\zeta(s)$ does not vanish in the interval $(0,1)$. We already saw in Theorem 5.3.1 that the Zeta function has meromorphic extension to the region $\mathrm{Re}(s) > 0$ which is holomorphic everywhere except for a simple pole at $s = 1$. Recall

$$F(s) := \sum_{n \geqslant 1} \frac{(-1)^{n+1}}{n^s}. \tag{6.6.1}$$

Then $F(s)$ is a Dirichlet series which converges in the region Re(s) > 0 (see Proposition 5.2.11).

Proposition 6.6.2. $\zeta(s)$ *does not vanish in the interval* $(0, \infty)$.

Proof. Note

$$F(s) = \Big(1 - \frac{1}{2^s}\Big) + \Big(\frac{1}{3^s} - \frac{1}{4^s}\Big) + \cdots \,.$$

If $s > 0$, then $F(s)$ being a sum of positive quantities is positive and converges to a finite real number since $F(s)$ is holomorphic. The function

$2^{s-1}-1$ has no poles when $s>0$. Now equation (5.3.3) shows that the zeta function does not vanish on the interval $(0,\infty)$. □

Recall the function $\xi(s)$, which was defined as

$$\xi(s)=s(s-1)\pi^{-s/2}\Gamma\Big(\frac{s}{2}\Big)\zeta(s).$$

We proved that ξ extends to the entire plane and satisfies the functional equation

$$\xi(s)=\xi(1-s). \tag{6.6.3}$$

Since $\zeta(s)$ has been extended to the region Re(s) >0 we may use the above to define $\zeta(s)$ in the region Re(s) <1 by

$$\zeta(s)=\frac{\pi^{(s-1)/2}\Gamma\Big(\dfrac{1-s}{2}\Big)\zeta(1-s)}{\pi^{-s/2}\Gamma\Big(\dfrac{s}{2}\Big)} \qquad \mathrm{Re(s)}<1\,. \tag{6.6.4}$$

Proposition 6.6.5. *For $s\in\mathbb{R}$, $\zeta(s)=0$ iff $s\in\{\dots,-6,-4,-2\}$ (the negative even integers). At these points the zeros are simple zeros.*

Proof. Equation (6.6.3) is equivalent to

$$\pi^{-s/2}\Gamma\Big(\frac{s}{2}\Big)\zeta(s)=\pi^{(s-1)/2}\Gamma\Big(\frac{1-s}{2}\Big)\zeta(1-s)\,. \tag{6.6.6}$$

Recall that the Gamma function is holomorphic except simple poles at $\{\dots,-3,-2,-1,0\}$. Putting $s=0$ into equation (6.6.4) shows that the zeta function is holomorphic at $s=0$ and $\zeta(0)\neq 0$.

Next let us assume that $s_0\in\{\dots,-6,-4,-2\}$. Then $1-s_0>1$ and so the RHS of equation (6.6.6) is holomorphic and non-vanishing. In the LHS, however, the gamma factor has a simple pole. Thus, the Zeta function has to have a simple zero at s_0.

Finally suppose that $s_0\notin\{\dots,-6,-4,-2\}$ and $\zeta(s_0)=0$. By Proposition 6.6.2, and since $\zeta(0)\neq 0$, we get $s_0<0$. It follows that $1-s_0>1$ and so the RHS of equation (6.6.6) does not vanish. Since the gamma factor in the LHS does not have a pole, $\zeta(s_0)\neq 0$, which is a contradiction. Thus, $\zeta(s_0)\neq 0$. □

We record the conclusion of the above propositions in the following corollary.

Corollary 6.6.7. *For $s\in\mathbb{R}$, $\zeta(s)$ has simple zeros at $s\in\{\dots,-6,-4,-2\}$, a simple pole at $s=1$, and at all other points it is holomorphic and non-vanishing.*

Chapter 7

Zeros of the Zeta function

In this chapter we will prove Hardy's Theorem, which states that the Zeta function has infinitely many zeros on the critical line.

We sketch the main steps in the proof for the benefit of the reader.
Step 1. The starting point is the following equality which Hardy and Littlewood, in their long paper with a long title, "Contributions to the Theory of the Riemann Zeta Function and the Theory of the Distribution of Primes.", attribute to Cahen and Mellin, see equation (I.II) on page 2 of their article. For Re(y) > 0,

$$\frac{1}{2\pi i}\int_{k-i\infty}^{k+i\infty}\Gamma(u)y^{-u}du = e^{-y}.$$

This identity is first proved when $y \in \mathbb{R}_{>0}$, which is easy. Then using Stirling's approximation, it is proved that for $y \in \{\mathrm{Re(y)} > 0\}$ the LHS is a holomorphic function. The identity follows.
Step 2. Using this (and the familiar trick) we get

$$1 + 2\sum_{n=1}^{\infty} e^{-n^2 y} = 1 + \frac{1}{i\pi}\int_{2-i\infty}^{2+i\infty}\Gamma(u)y^{-u}\zeta(2u)du.$$

After this we shift the line of integration to Re(u) = 1/4 to get

$$1 + 2\sum_{n=1}^{\infty} e^{-n^2 y} = 1 + \sqrt{\frac{\pi}{y}} + \frac{1}{i\pi}\int_{1/4-i\infty}^{1/4+i\infty}\Gamma(u)y^{-u}\zeta(2u)du.$$

To shift the line of integration to Re(u) = 1/4, we will need an estimate on the Zeta function. The main result of section §7.1, which we will use to shift the line of integration, is Corollary 7.1.8.

Step 3. From this we derive the equation

$$e^{ia/2}\theta(e^{2ia}) = \cos\frac{a}{2} + \frac{1}{\pi}\int_0^\infty \Xi(\frac{t}{2})\cosh at\,dt,$$

where θ is Jacobi's Theta function and the function

$$\Xi(t) := \pi^{-(\frac{1}{4}+it)}\Gamma(\frac{1}{4}+it)\zeta(\frac{1}{2}+2it).$$

The above function has the same set of zeros as that of the Zeta function. There is one more ingredient we need, all derivatives of the LHS vanish when $a \to \pi/4$.
Step 4. Now we assume that $\Xi(t)$ has only finitely many zeros and obtain a contradiction.

7.1 An integral representation for $\zeta(s)$

For $a \geqslant 0$ and Re(s) > 1 consider the function

$$\zeta_1(s,a) = \sum_{n=1}^{\infty}\frac{1}{(n+a)^s}\,.$$

Consider functions

$$(7.1.1)\qquad f_k(s,a) = \sum_{n=1}^{k}\frac{1}{(n+a)^s}\,.$$

If $l > k$, then

$$(7.1.2)\qquad \begin{aligned} |f_l(s,a) - f_k(s,a)| &\leqslant \sum_{k+1}^{l}\frac{1}{(n+a)^x} \qquad s = x+iy \\ &< \sum_{k+1}^{\infty}\frac{1}{(n+a)^x} \leqslant \sum_{k+1}^{\infty}\frac{1}{n^x}\,. \end{aligned}$$

The above shows that this is a sequence of functions which is uniformly Cauchy in the set Re(s) $\geqslant \delta > 1$ (the bound is also independent of a). From Theorem 5.1.5 it follows that the limit of $f_k(s,a)$, which is $\zeta_1(s,a)$, is holomorphic in the region Re(s) > 1.

Proposition 7.1.3. *Let X be a measure space with finite measure, for example, a compact measure space. Let $U \subset \mathbb{C}$ be an open set. Suppose we are given a sequence of measurable functions $f_k(s,x)$ on $U \times X$ with the following properties*

1. *For $x \in X$ the function $s \mapsto f_k(s,x)$ is holomorphic in s.*

2. *Given any compact subset $K \subset U$ and $\epsilon > 0$, there is an integer $N(K,\epsilon)$ such that for all $k,l \geqslant N(K,\epsilon)$ we have $|f_k(s,x) - f_l(s,x)| < \epsilon$, for all $s \in K$ and $x \in X$.*

3. *The functions*
$$g_k(s) := \int_X f_k(s,x)dx$$
are holomorphic on U.

Then g_k are uniformly Cauchy on compact sets in U and so they converge to a holomorphic function on U.

Proof. The proof is straightforward. Fix $K \subset U$ and let $s \in K$. If $k,l \geqslant N(K,\epsilon)$ then

$$|g_k(s) - g_l(s)| \leqslant \int_X |f_k(s,x) - f_l(s,x)| < \epsilon \mathrm{Vol}(K)\,.$$

□

Corollary 7.1.4. *The function*

$$s \mapsto \int_0^1 \int_0^u \zeta_1(s, a+v)dvdu$$

is holomorphic on Re(s) > 1.

Proof. Let $X := \{(u,v) \mid 0 \leqslant u \leqslant 1,\ 0 \leqslant v \leqslant u\}$. Define

$$f_k(s,u,v) := \sum_{n=1}^{k} \frac{1}{(n+v)^s}\,.$$

It is a simple application of Theorem 5.1.1 to check that $g_k(s) = \int_X f_k(s,x)dx$ is holomorphic on $\mathbb{C}$. Let $U = \{\mathrm{Re(s)} > 1\}$. Use (7.1.2) and Proposition 7.1.3 to conclude the proof of the corollary. □

Theorem 7.1.5. *For $a \geqslant 0$ and* Re(s) > 1 *we have*

$$\zeta_1(s,a) = \frac{(1+a)^{-s+1}}{s-1} + s\int_0^1 \Big(\int_0^u \zeta_1(s+1, a+v)dv \Big) du\,.$$

Proof. For $a \geqslant 0$ and Re(s) > 1 consider the function

$$\int_1^\infty \frac{du}{(u+a)^s} = \frac{(1+a)^{-s+1}}{s-1}\,.$$

We have

$$\begin{aligned}
\zeta_1(s,a) &= \sum_{n=1}^\infty \frac{1}{(n+a)^s} - \int_1^\infty \frac{du}{(u+a)^s} + \int_1^\infty \frac{du}{(u+a)^s} \\
&= \sum_{n=1}^\infty \frac{1}{(n+a)^s} - \sum_{n=1}^\infty \int_n^{n+1} \frac{du}{(u+a)^s} + \frac{(1+a)^{-s+1}}{s-1} \\
&= \sum_{n=1}^\infty \int_0^1 \left(\frac{1}{(n+a)^s} - \frac{1}{(u+n+a)^s} \right) du + \frac{(1+a)^{-s+1}}{s-1} \\
&= \sum_{n=1}^\infty \int_0^1 \int_0^u \frac{s}{(v+n+a)^{s+1}} dvdu + \frac{(1+a)^{-s+1}}{s-1}\,.
\end{aligned}$$

Next we want to interchange the sum and the integral. Let Re(s) $\geqslant \delta > 0$ and let $f_{k,s}(u,v) := \sum_{n=1}^k \frac{s}{(v+n+a)^{s+1}}$. Then

$$\begin{aligned}
|f_{k,s}(u,v)| &\leqslant \sum_{n=1}^\infty \frac{|s|}{(v+n+a)^{x+1}} \qquad s = x+iy \\
&\leqslant \sum_{n=1}^\infty \frac{|s|}{n^{x+1}} \leqslant \sum_{n=1}^\infty \frac{|s|}{n^{\delta+1}}\,.
\end{aligned}$$

Let X be the measure space $\{(u,v) \mid 0 \leqslant u \leqslant 1,\ 0 \leqslant v \leqslant u\}$. On this measure space, whose measure is finite, we have functions $f_{k,s}$ which are bounded above by a constant. Thus, applying Theorem 5.1.1 we get

$$\lim_k \int_X f_{k,s} = \int_X \lim_k f_{k,s} = \int_X \sum_{n=1}^\infty \frac{s}{(v+n+a)^{s+1}} dvdu\,.$$

This shows

$$\begin{aligned}\zeta_1(s,a) &= \sum_{n=1}^{\infty}\int_0^1\int_0^u \frac{s}{(v+n+a)^{s+1}}dvdu + \frac{(1+a)^{-s+1}}{s-1}\\ &= \int_0^1\int_0^u\sum_{n=1}^{\infty}\frac{s}{(v+n+a)^{s+1}}dvdu + \frac{(1+a)^{-s+1}}{s-1}\\ &= \frac{(1+a)^{-s+1}}{s-1} + \int_0^1 s\Big(\int_0^u \zeta_1(s+1,a+v)dv\Big)du\,.\end{aligned}$$

This completes the proof of the theorem. □

If we put $a = 0$ we get the following corollary.

Corollary 7.1.6. *For* Re(s) > 0

$$\zeta(s) - \frac{1}{s-1} = s\int_0^1\Big(\int_0^u \zeta_1(s+1,v)dv\Big)du\,.$$

Proof. From the preceding theorem, the corollary holds for Re(s) > 1. Now note, using Corollary 7.1.4, the RHS makes sense for Re(s) > 0 and is holomorphic in this region. □

We will use this corollary to get an estimate for the Zeta function.

$$\zeta_1(s+1,v) = \sum_{n=1}^{\infty}\frac{1}{(n+v)^{s+1}}\,.$$

Thus, if Re(s) $> 1/5$, then we get

$$|\zeta_1(s+1,v)| \leqslant \sum_{n=1}^{\infty}\frac{1}{(n+v)^{x+1}} \leqslant \sum_{n=1}^{\infty}\frac{1}{n^{6/5}}\,. \tag{7.1.7}$$

Corollary 7.1.8. *If* Re(s) $> 1/5$*, then there is a* $c > 0$ *such that*

$$|\zeta(s)| \leqslant \frac{1}{|s-1|} + c|s|\,. \tag{7.1.9}$$

7.2 Cahen-Mellin integral for $y \in \mathbb{R}_{>0}$

In this section we will prove that for $y, k \in \mathbb{R}_{>0}$ we have

$$\frac{1}{2\pi i}\int_{k-i\infty}^{k+i\infty}\Gamma(u)y^{-u}du = e^{-y}.$$

For $\sigma \in \mathbb{R}$ we will denote by $[\sigma]$ the greatest integer $\leqslant \sigma$.

Lemma 7.2.1. *If $u = \sigma + it$ where $\sigma := \mathrm{Re}(u)$ and $t := \mathrm{Im}(u)$. Assume that $\sigma \notin \mathbb{Z}_{\leqslant 0}$. Then*

$$|\Gamma(u)| \leqslant |\Gamma(\sigma)| \,.$$

Proof. We divide the proof into two cases.

First consider the case $\sigma > 0$.

$$\begin{aligned} |\Gamma(u)| &= \left| \int_0^\infty x^{u-1} e^{-x} dx \right| \\ &\leqslant \int_0^\infty \left| x^{u-1} e^{-x} dx \right| \\ &= \int_0^\infty x^{\sigma-1} e^{-x} dx \\ &= \Gamma(\sigma) = |\Gamma(\sigma)| \,. \end{aligned}$$

Next consider the case $\sigma \leqslant 0$ and $\sigma \notin \mathbb{Z}$.

$$|\Gamma(u)| = \left| \frac{\Gamma(u - [\sigma])}{\prod_{j=0}^{j=-[\sigma]-1} (u+j)} \right| \,.$$

Using the previous case we get.

$$\begin{aligned} |\Gamma(u)| &\leqslant \frac{|\Gamma(\sigma - [\sigma])|}{\prod_{j=0}^{j=-[\sigma]-1} |(u+j)|} \\ &\leqslant \frac{|\Gamma(\sigma - [\sigma])|}{\prod_{j=0}^{j=-[\sigma]-1} |(\sigma+j)|} \\ &= |\Gamma(\sigma)| \,. \end{aligned}$$

This completes the proof of the Lemma. □

Lemma 7.2.2. *Let $k \in \mathbb{R}_{>0}$. The integral*

$$\int_{k-i\infty}^{k+i\infty} \Gamma(u) y^{-u} du$$

converges for $y \in \mathbb{R}_{>0}$.

Proof.

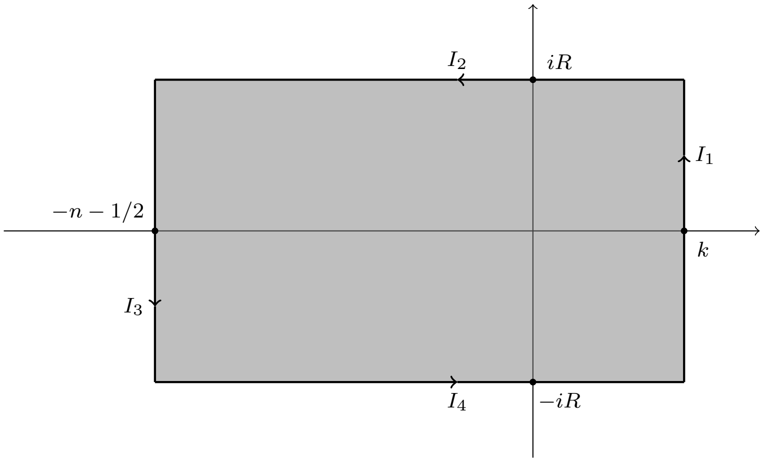
$$\int_{k-i\infty}^{k+i\infty} \left| \Gamma(u) y^{-u} du \right| = \int_{-\infty}^{\infty} \left| \frac{\Gamma(k+2+it) y^{-k-it}}{(k+it)(k+1+it)} \right| dt \,.$$

Using Lemma 7.2.1.

$$\begin{aligned}\int_{k-i\infty}^{k+i\infty} \left|\Gamma(u)y^{-u}du\right| &\leqslant \Gamma(k+2)y^{-k}\int_{-\infty}^{\infty}\frac{dt}{k^2+t^2}\\ &= \frac{\pi}{k}\Gamma(k+2)y^{-k}.\end{aligned}$$

□

Now consider the contour given below.



Fix a $y \in \mathbb{R}_{>0}$. We will integrate the meromorphic function $\Gamma(u)y^{-u}$ on the above contour. The poles of this function in the shaded region are exactly at the points $\{0, -1, \dots, -n\}$. By the Residue Theorem we have

(7.2.3)
$$\int_{I_1}\Gamma(u)y^{-u} + \int_{I_2}\Gamma(u)y^{-u} + \int_{I_3}\Gamma(u)y^{-u} + \int_{I_4}\Gamma(u)y^{-u} = 2\pi i\sum_{j=0}^{n}\frac{(-1)^j y^j}{j!}.$$

Next we will estimate the integrals on I_2, I_3 and I_4. We begin by estimating the integral on I_3.

Lemma 7.2.4. *For $n \in \mathbb{Z}_{>0}$ we have*

$$|\Gamma(-n-1/2)| \leqslant \frac{2\sqrt{\pi}}{n!}.$$

Proof. Using the functional equation for the Gamma function we get

$$\begin{aligned}|\Gamma(-n-1/2)| &= \left|\frac{\Gamma(1/2)}{\prod_{j=0}^{n}(j+1/2)}\right| \\ &\leqslant \frac{2\sqrt{\pi}}{n!}.\end{aligned} \tag{7.2.5}$$

This proves the Lemma. □

Lemma 7.2.6. *Let $y \in \mathbb{R}_{>0}$. Then*

$$\left|\int_{I_3} \Gamma(u)y^{-u}du\right| \leqslant \frac{2\pi^{3/2}y^{n+1/2}}{(n-1)!}\,.$$

Proof.

$$\begin{aligned}
\left|\int_{I_3} \Gamma(u)y^{-u}du\right| &\leqslant \int_{-n-1/2-iR}^{-n-1/2+iR} \left|\Gamma(u)y^{-u}\right|du \\
&\leqslant \int_{-\infty}^{\infty} \left|\Gamma(-n-1/2+it)y^{n+1/2-it}\right|dt \\
&= \int_{-\infty}^{\infty} \left|\frac{\Gamma(-n+3/2+it)y^{n+1/2-it}}{(-n-1/2+it)(-n+1/2+it)}\right| dt \\
&\leqslant \left|\Gamma(-n+3/2)y^{n+1/2}\int_{-\infty}^{\infty}\frac{1}{(n-1/2)^2+t^2}dt\right| \\
&= \left|\frac{\Gamma(-n+3/2)y^{n+1/2}\pi}{(n-1/2)}\right| \\
&= |\Gamma(-n+1/2)|y^{n+1/2}\pi\,.
\end{aligned}$$

Now applying Lemma 7.2.4 we see that

$$|\Gamma(-n+1/2)| \leqslant \frac{2\sqrt{\pi}}{(n-1)!}\,.$$

Using this we get

$$\begin{aligned}
\left|\int_{I_3} \Gamma(u)y^{-u}du\right| &\leqslant |\pi\Gamma(-n+1/2)|y^{n+1/2} \\
&\leqslant \frac{2\pi^{3/2}y^{n+1/2}}{(n-1)!}\,.
\end{aligned}$$

This completes the proof of the Lemma. □

Next we estimate the integral on I_4.

Lemma 7.2.7. *For $y \in \mathbb{R}_{>0}$ there exist constants M (independent of R, n, y) and M' (which depends only on y) such that*

$$\left|\int_{I_4} \Gamma(u)y^{-u}du\right| \leqslant \frac{M}{R}\left|\frac{1-(R/y)^{-n-1/2}}{\log R - \log y}\right| + \frac{2M'}{R}.$$

Proof. We break the integral on I_4 into two parts.

$$\begin{aligned}\int_{I_4} \Gamma(u) y^{-u} du &= \int_{-n-1/2-iR}^{k-iR} \Gamma(u) y^{-u} du \\ &= \int_{-n-1/2}^{0} \Gamma(\sigma - iR) y^{-\sigma} d\sigma + \int_{0}^{k} \Gamma(\sigma - iR) y^{-\sigma} d\sigma \,.\end{aligned}$$

Let us estimate the above two integrals. First we will be showing that

$$\left| \int_{-n-1/2}^{0} \Gamma(\sigma - iR) y^{-\sigma} d\sigma \right| \leqslant \frac{M}{R} \left| \frac{1 - (R/y)^{-n-1/2}}{\log R - \log y} \right| .$$

Recall that for $\sigma \in \mathbb{R}$ we denote by $[\sigma]$ the greatest integer $\leqslant \sigma$.

$$\begin{aligned}\left| \int_{-n-1/2}^{0} \Gamma(\sigma - iR) y^{-\sigma} d\sigma \right| &= \left| \int_{-n-1/2}^{0} \frac{\Gamma(\sigma - [\sigma] + 1 - iR)}{\prod_{j=0}^{j=-[\sigma]} (\sigma - iR + j)} y^{-\sigma} d\sigma \right| \\ &\leqslant \int_{-n-1/2}^{0} \left| \frac{\Gamma(\sigma - [\sigma] + 1 - iR)}{\prod_{j=0}^{j=-[\sigma]} (\sigma - iR + j)} y^{-\sigma} \right| d\sigma \\ &\leqslant \int_{-n-1/2}^{0} \frac{\Gamma(\sigma - [\sigma] + 1)}{\left| \prod_{j=0}^{j=-[\sigma]} (\sigma - iR + j) \right|} y^{-\sigma} d\sigma \\ &\leqslant \int_{-n-1/2}^{0} \frac{\Gamma(\sigma - [\sigma] + 1)}{R^{-\sigma-1}} y^{-\sigma} d\sigma \\ &\leqslant \frac{M}{R} \left| \frac{1 - (R/y)^{-n-1/2}}{\log R - \log y} \right| .\end{aligned}$$

In the above

$$M := \sup_{t \in [1,2]} \Gamma(t).$$

Next we show that the integral

$$\left| \int_{0}^{2} \Gamma(\sigma - iR) y^{-\sigma} d\sigma \right| \leqslant \frac{2M^{'}}{R} \,.$$

$$\begin{aligned}
\left|\int_0^k \Gamma(\sigma - iR)y^{-\sigma}d\sigma\right| &= \left|\int_0^k \frac{\Gamma(\sigma+1-iR)}{(\sigma+iR)}y^{-\sigma}du\right| \\
&\leqslant \int_0^k \left|\frac{\Gamma(\sigma+1-iR)}{\sigma+iR}y^{-\sigma}\right|d\sigma \\
&\leqslant \int_0^k \frac{|\Gamma(\sigma+1-iR)|}{R}y^{-\sigma}d\sigma \\
&\leqslant \int_0^k \frac{\Gamma(\sigma+1)}{R}y^{-\sigma}d\sigma \\
&\leqslant \frac{2M'}{R}\,.
\end{aligned}$$

In the above

$$M' := \sup_{t\in[0,k]} \Gamma(t+1)y^{-t}.$$

Having obtained the estimates for both the integrals we can now say

$$\begin{aligned}
\left|\int_{I_4} \Gamma(u)y^{-u}du\right| &= \left|\int_{-n-1/2}^0 \Gamma(\sigma - iR)y^{-\sigma}d\sigma + \int_0^k \Gamma(\sigma - iR)y^{-\sigma}d\sigma\right| \\
&\leqslant \left|\int_{-n-1/2}^0 \Gamma(\sigma - iR)y^{-\sigma}d\sigma\right| + \left|\int_0^k \Gamma(\sigma - iR)y^{-\sigma}d\sigma\right| \\
&\leqslant \frac{M}{R}\left|\frac{1-(R/y)^{-n-1/2}}{\log R - \log y}\right| + \frac{2M'}{R}\,.
\end{aligned}$$

This completes the proof of the Lemma. □

Lemma 7.2.8. *For $y \in \mathbb{R}_{>0}$ there exist constants M and M' defined as in the preceding lemma such that the following inequality holds*

$$\left|\int_{I_2} \Gamma(u)y^{-u}du\right| \leqslant \frac{M}{R}\left|\frac{1-(R/y)^{-n-1/2}}{\log R - \log y}\right| + \frac{2M'}{R}\,.$$

Proof. Same as previous lemma. □

Theorem 7.2.9. *Let $y, k \in \mathbb{R}_{>0}$. Then*

$$\frac{1}{2\pi i}\int_{k-i\infty}^{k+i\infty} \Gamma(u)y^{-u}du = e^{-y}.$$

Proof. Fix $y \in \mathbb{R}_{>0}$ and $n \in \mathbb{Z}_{>0}$. In view of the above Lemmas we see that the limits

$$\lim_{R\to\infty} \int_{I_2} \Gamma(u) y^{-u} du = \lim_{R\to\infty} \int_{I_4} \Gamma(u) y^{-u} du = 0$$

and

$$\left| \lim_{R\to\infty} \int_{I_3} \Gamma(u) y^{-u} du \right| \leqslant \frac{2\pi^{3/2} y^{n+1/2}}{(n-1)!}.$$

Now first taking limit $R \to \infty$ and then taking limit $n \to \infty$ in equation (7.2.3) we get

$$\frac{1}{2\pi i} \int_{k-i\infty}^{k+i\infty} \Gamma(u) y^{-u} du = e^{-y}.$$

□

7.3 Logarithm and Stirling's approximation

Define log : $\{\mathrm{Re(s)} > 0\} \to \mathbb{C}$ as follows. By $\log(s)$ we will mean the unique complex number such that

1. $e^{\log(s)} = s$

2. $-\pi/2 < \mathrm{Im}(\log(s)) < \pi/2$.

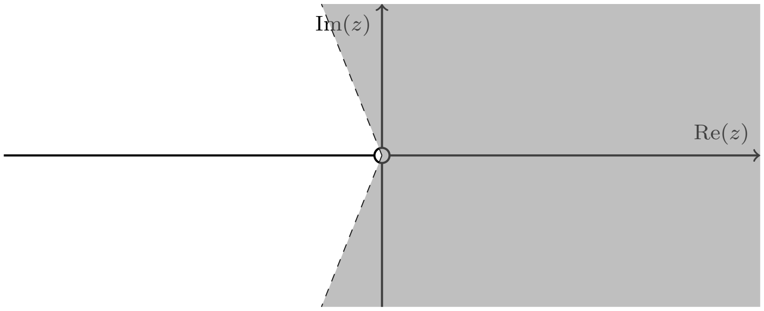
Here Im denotes the imaginary part of a complex number.

Using the lifting theorem for covering spaces, for any continuous function $f : \{\mathrm{Re(s)} > 0\} \to \mathbb{C}^*$, there is a lift G_f which makes the following diagram commute

(7.3.1)

$$\begin{tikzcd}
 & \mathbb{C} \arrow[d, "e^s"] \\
\{\mathrm{Re(s)} > 0\} \arrow[ur, dashed, "G_f"] \arrow[r, "f"'] & \mathbb{C}^*
\end{tikzcd}$$

The lift is not unique. However, if H_f is another lift, then $G_f(s) - H_f(s) = 2\pi i l$ for some $l \in \mathbb{Z}$. For example, if we take f to be the inclusion, then one choice for G is the function log defined above. We can define log in a slightly bigger region, which we will need.



Theorem 7.3.2 (Stirling's approximation)**.** *For* Re(s) > 0

$$\Gamma(s) = \exp\left\{ s\log(s/e) - \frac{1}{2}\log(s/2\pi) + \log\left(1 + O\Big(\frac{1}{s}\Big)\right)\right\}.$$

Corollary 7.3.3. *There is a constant C_0 such that for* Re(s) > 0

$$|\Gamma(s)| \leqslant \left|\exp\left\{ s\log(s/e) - \frac{1}{2}\log(s/2\pi)\right\}\right|\left|1 + \frac{C_0}{|s|}\right|$$

7.4 Cahen-Mellin integral for $y \in \{\mathrm{Re(s)} > 0\}$

In this section we will use Stirling's approximation to show that the integral

$$\int_{k-i\infty}^{k+i\infty} \Gamma(u) y^{-u} du$$

converges for $k \in \mathbb{R}_{>0}$ and $y \in \{\mathrm{Re(s)} > 0\}$ and in fact defines a holomorphic function in this region.

Lemma 7.4.1 (Estimate on $|\Gamma(u)|$)**.** *Fix $k \in \mathbb{R}_{>0}$ and let $u = k + it$. Then for $|t| > 2k$ we have*

$$|\Gamma(u)| \leqslant \exp\left\{ -\frac{|t|\pi}{2} + O(\log|t|)\right\}.$$

Proof. Since $\overline{\Gamma(u)} = \Gamma(\overline{u})$, it suffice to consider the case when $t > 0$. Let $u = k + it$ and assume that $t > 2k$. Then

$$\begin{aligned}(u - \frac{1}{2})\log(u) &= (k - \frac{1}{2} + it)\log(k + it)\\ &= (k - \frac{1}{2} + it)\Big[\log(it) + \log\Big(1 + \frac{k}{it}\Big)\Big]\\ &= (k - \frac{1}{2} + it)\Big[\frac{i\pi}{2} + \log t + \log\Big(1 + \frac{k}{it}\Big)\Big]\end{aligned}$$

Letting $\alpha := \log(1 + k/it)$ we get

$$= -\frac{t\pi}{2} + (k - \frac{1}{2})(\log t + \mathrm{Re}(\alpha)) - t\mathrm{Im}(\alpha) + i(*)\,.$$

Then

$$\begin{aligned} u\log(u/e) - \frac{1}{2}\log(u/2\pi) &= (u - \frac{1}{2})\log(u) - u + \frac{1}{2}\log(2\pi) \\ &= -\frac{t\pi}{2} + (k - \frac{1}{2})(\log t + \mathrm{Re}(\alpha)) - t\mathrm{Im}(\alpha) + \\ &\qquad - k + \frac{1}{2}\log(2\pi) + i(*)\,. \end{aligned}$$

Since $|t| > 2k$, then using the series expansion of $\log(1+z)$ we conclude that

$$|\alpha| = |\log(1 + k/it)| \leqslant \frac{2k}{t}\,.$$

If a, b are real numbers, then we have $a + b \leqslant a + |b|$. In view of this we get that

$$\mathrm{Re}\Big\{u\log(u/e) - \frac{1}{2}\log(u/2\pi)\Big\} \leqslant -\frac{t\pi}{2} + \left|k - \frac{1}{2}\right|(|\log t| + \frac{2k}{t}) + k + \frac{1}{2}\log(2\pi)\,.$$

Using Corollary 7.3.3 we get that

$$|\Gamma(u)| \leqslant \exp\left\{-\frac{t\pi}{2} + \left|k - \frac{1}{2}\right|(|\log t| + \frac{2k}{t}) + k\right\}\left|1 + \frac{C_0}{|u|}\right|\sqrt{2\pi} \tag{7.4.2}$$

From this the lemma follows. □

Lemma 7.4.3. *Let $y = re^{i\theta}$ with $-\pi/2 < \theta < \pi/2$ and $k \in \mathbb{R}_{>0}$. Then the integral*

$$\int_k^{k+i\infty} \Gamma(u) y^{-u} du$$

converges.

Proof. By Lemma 7.4.1, after choosing $T \gg 0$, we have

$$\int_{k+iT}^{k+i\infty} \left|\Gamma(u)y^{-u}du\right| \leqslant \int_T^\infty C' \exp\{(-\pi/2 + \theta)t + O(\log t)\}\,dt\,.$$

Since $-\pi/2 + \theta < 0$, after choosing $T \gg 0$, we may assume that

$$(-\pi/2 + \theta)t + O(\log t) \leqslant (-\pi/2 + \theta)t/2$$

for $t \geqslant T$. Then we get

$$\int_{k+iT}^{k+i\infty} \left|\Gamma(u) y^{-u} du\right| \leqslant \int_{T}^{\infty} C' \exp\left\{(-\pi/2+\theta)t/2\right\} dt \,.$$

This proves that the above integral converges. The integral over $[0,T]$ is finite since we are integrating a continuous function over a compact set. Putting these integrals together proves the Lemma. □

Lemma 7.4.4. *Let $y = re^{i\theta}$ with $-\pi/2 < \theta < \pi/2$ and $k \in \mathbb{R}_{>0}$. Then the integral*

$$\int_{k-i\infty}^{k} \Gamma(u) y^{-u} du$$

converges.

Proof. By Lemma 7.4.1, after choosing $T \ll 0$, we have

$$\int_{k-i\infty}^{k+iT} \left|\Gamma(u) y^{-u} du\right| \leqslant \int_{-\infty}^{T} C' \exp\left\{(\pi/2+\theta)t + O(\log|t|)\right\} dt \,.$$

Since $0 < \pi/2 + \theta$, after choosing $T \ll 0$, we may assume that

$$(\pi/2+\theta)t + O(\log|t|) \leqslant (\pi/2+\theta)t/2$$

for $t \leqslant T$. Then we get

$$\int_{k-i\infty}^{k+iT} \left|\Gamma(u) y^{-u} du\right| \leqslant \int_{-\infty}^{T} C' \exp\left\{(\pi/2+\theta)t/2\right\} dt \,.$$

This integral is finite.

The integral over $[T,0]$ is finite since we are integrating a continuous function over a compact set. Putting these integrals together proves the Lemma. □

Corollary 7.4.5. *Let* $\mathrm{Re(y)} > 0$ *and $k \in \mathbb{R}_{>0}$. Then the integral*

$$\int_{k-i\infty}^{k+i\infty} \Gamma(u) y^{-u} du$$

converges.

Theorem 7.4.6. *The function*

$$y \mapsto \int_{k-i\infty}^{k+i\infty} \Gamma(u) y^{-u} du,$$

which is defined for $\mathrm{Re(y)} > 0$*, is holomorphic.*

Proof. It suffices to show that the two integrals

$$\int_k^{k+i\infty} \Gamma(u) y^{-u} du \qquad \text{and} \qquad \int_{k-i\infty}^{k} \Gamma(u) y^{-u} du$$

define holomorphic functions in the variable y. Let $y_n \to y$ be a sequence and consider

$$\begin{aligned}\left|\frac{y^{-u} - y_n^{-u}}{y - y_n}\right| &= \left|\frac{y^{-u}}{y}\left(\frac{1-(y_n/y)^{-u}}{1-y_n/y}\right)\right| \\ &= \left|\frac{y^{-u}}{y}\left(\frac{1-e^{-u\log(y_n/y)}}{1-y_n/y}\right)\right| .\end{aligned}$$

Using the same step as in (6.1.3) we get

$$\leqslant \left|\frac{y^{-u}}{y}\right|\left|\frac{u\log(y_n/y)}{1-y_n/y}\right| e^{|u\log(y_n/y)|} .$$

Note that

$$\lim_{n\to\infty}\left|\frac{\log(y_n/y)}{1-y_n/y}\right| = 1$$

and so for $n \gg 0$ this quantity is bounded. Thus, we get

$$\begin{aligned}\left|\Gamma(u)\frac{y^{-u} - y_n^{-u}}{y - y_n}\right| &\leqslant C\left|\Gamma(u)\frac{y^{-u}u}{y} e^{|u\log(y_n/y)|}\right| \\ &= C'\left|\Gamma(u+1)y^{-u}e^{|u\log(y_n/y)|}\right| .\end{aligned} \tag{7.4.7}$$

Let $y = re^{i\theta}$ where $-\pi/2 < \theta < \pi/2$. By Lemma 7.4.1, for $t \gg 0$ we have

$$\left|\Gamma(u+1)y^{-u}\right| \leqslant C'' \exp\left\{(-\pi/2+\theta)t + O(\log t)\right\} .$$

We can find $T \gg 0$ such that

$$(-\pi/2+\theta)t + O(\log t) \leqslant (-\pi/2+\theta)t/2$$

for $t \geqslant T$. Let $\delta > 0$ be such that $-\pi/2 + \theta + \delta < 0$. Then by choosing $n \gg 0$ and $t \gg 0$ we may assume that $|u\log(y_n/y)| < t\delta/2$. Putting these together we get, for $n \gg 0$,

$$\left|\Gamma(u+1)y^{-u}e^{|u\log(y_n/y)|}\right| \leqslant C''' \exp\{(-\pi/2+\theta+\delta)t/2\}.$$

This proves that for $n \gg 0$

$$\left|\Gamma(u)\frac{y^{-u}-y_n^{-u}}{y-y_n}\right| \leqslant C''' \exp\{(-\pi/2+\theta+\delta)t/2\}.$$

As the function on the right is integrable, we see that the limit

$$\lim_{n\to\infty}\int_k^{k+i\infty}\left|\Gamma(u)\frac{y^{-u}-y_n^{-u}}{y-y_n}du\right|$$

exists. This shows that

$$\int_k^{k+i\infty}\Gamma(u)y^{-u}du$$

is a holomorphic function in y. The second integral is treated in the same way and this case is left to the reader. □

Corollary 7.4.8. *Let* Re(y) > 0 *and* $k \in \mathbb{R}_{>0}$. *Then*

$$\frac{1}{2\pi i}\int_{k-i\infty}^{k+i\infty}\Gamma(u)y^{-u}du = e^{-y}.$$

Proof. Follows from Theorem 7.2.9 and Theorem 7.4.6. □

This completes **Step 1** in the introduction.

7.5 Hardy's Theorem

Proposition 7.5.1. *Let* Re(y) > 0 *and* $k > 1/2$. *Then*

$$1+2\sum_{n=1}^{\infty}e^{-n^2y} = 1+\frac{1}{i\pi}\int_{k-i\infty}^{k+i\infty}\Gamma(u)y^{-u}\zeta(2u)du\,.$$

Proof. Using

$$\frac{1}{2\pi i}\int_{k-i\infty}^{k+i\infty}\Gamma(u)y^{-u}du = e^{-y}$$

we can say that for a finite $N \in \mathbb{N}$ the following holds

$$\begin{aligned}\frac{1}{2\pi i}\int_{k-i\infty}^{k+i\infty}\Gamma(u)y^{-u}\sum_{n=1}^{N}\frac{1}{n^{2u}}du &= \frac{1}{2\pi i}\sum_{n=1}^{N}\int_{k-i\infty}^{k+i\infty}\Gamma(u)\frac{y^{-u}}{n^{2u}}du\\ &= \sum_{n=1}^{N}e^{-n^2y}\,.\end{aligned}$$

Now having shown the equivalence for a finite N we need to prove this for $N \to \infty$ or in other words

$$\frac{1}{2\pi i} \lim_{N\to\infty} \int_{k-i\infty}^{k+i\infty} \Gamma(u) y^{-u} \sum_{n=1}^{N} \frac{1}{n^{2u}} du = \frac{1}{2\pi i} \int_{k-i\infty}^{k+i\infty} \Gamma(u) y^{-u} \lim_{N\to\infty} \sum_{n=1}^{N} \frac{1}{n^{2u}} du\,.$$

To justify this exchange of the lim and integral we will be showing that the sequence of functions $\{f_N\}$ defined as

$$f_N(u) := \Gamma(u) y^{-u} \sum_{n=1}^{N} \frac{1}{n^{2u}}$$

is bounded above by an integrable function. If $\mathrm{Re}(u) = k > 1/2 + \delta$ then it is clear that

$$|f_N(u)| \leqslant \left|\Gamma(u) y^{-u}\right| \sum_{n=1}^{\infty} \frac{1}{n^{1+2\delta}} = C(\delta) \left|\Gamma(u) y^{-u}\right|.$$

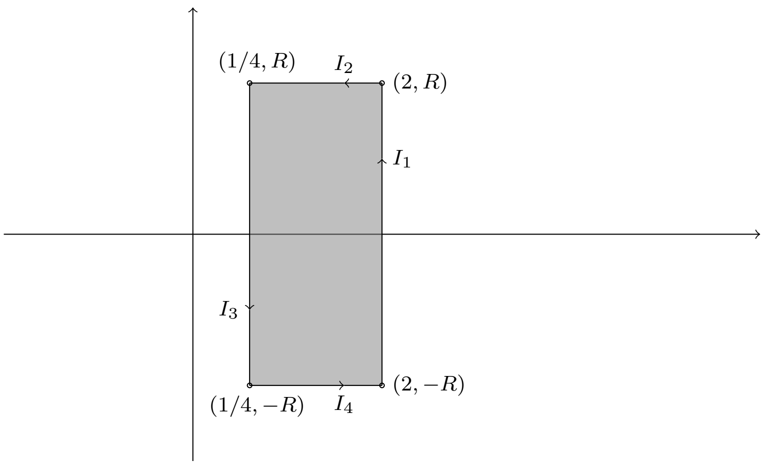
We have already seen that the integral $\int_{k-i\infty}^{k+i\infty} |\Gamma(u) y^{-u}| du < \infty$. Now applying Theorem 5.1.1 it follows that we can exchange the integral and the sum. This proves the Proposition. □

Corollary 7.5.2. *Taking $k = 2$ in the above Proposition we get*

$$1 + 2\sum_{n=1}^{\infty} e^{-n^2 y} = 1 + \frac{1}{i\pi} \int_{2-i\infty}^{2+i\infty} \Gamma(u) y^{-u} \zeta(2u) du.$$

Next we want to shift the line of integration to $k = 1/4$. Note that the proof of the above Proposition will not work since we cannot use the series for the Riemann Zeta function.

For a fixed y such that Re(y) > 0, we will be taking the integral of $\Gamma(u) y^{-u} \zeta(2u)$ along the following contour. The function $\Gamma(u) y^{-u} \zeta(2u)$ has a simple pole at $u = 1/2$ and is holomorphic elsewhere in this contour.



Therefore, by the Residue Theorem

$$\frac{1}{2\pi i}\Big(\int_{I_1}\Gamma(u)y^{-u}\zeta(2u)\,du+\int_{I_2}\Gamma(u)y^{-u}\zeta(2u)\,du+ \int_{I_3}\Gamma(u)y^{-u}\zeta(2u)\,du+\int_{I_4}\Gamma(u)y^{-u}\zeta(2u)\,du\Big)=\frac{1}{2}\sqrt{\frac{\pi}{y}}\,. \tag{7.5.3}$$

1. The integral over I_1 converges as $R\to\infty$; this follows from the proof of Proposition 7.5.1.

2. Now consider the integral of the function $\Gamma(u)y^{-u}\zeta(2u)$ taken along the path I_3. On this path $u = 1/4 + it$. By Corollary 7.1.8

$$|\zeta(1/2+2it)|\leqslant\frac{1}{|-1/2+2it|}+c|1/2+2it|=\exp\{O(\log|t|)\}\,.$$

   Proceeding as in Lemmas 7.4.3 and 7.4.4 we see that the integral converges on I_3.

3. Next we estimate the integral on I_2. Let $y = re^{i\theta}$ where $-\pi/2 < \theta < \pi/2$, let $\sigma\in[1/4, 2]$ and let $R \gg 0$. By Theorem 7.3.2, equation (7.4.2) and Corollary 7.1.8 we see that there is a constant C such that

   (7.5.4)
$$\big|\Gamma(\sigma+iR)y^{-\sigma-iR}\zeta(2\sigma+2iR)\big|\leqslant Ce^{R(-\pi/2+\theta)}R^3\Big(\frac{1}{R}+2cR\Big)\,.$$

   From the above inequality it is clear that

$$\lim_{R\to\infty}\int_{I_2}\Gamma(u)y^{-u}\zeta(2u)\,du\to 0.$$

4. The same estimate for the integral over I_4 is proved in the same way.

Thus, taking limit $R \to \infty$ in equation (7.5.3) and using Corollary 7.5.2 we get

$$1 + 2\sum_{n=1}^{\infty} e^{-n^2 y} = 1 + \sqrt{\frac{\pi}{y}} + \frac{1}{i\pi}\int_{1/4-i\infty}^{1/4+i\infty} \Gamma(u) y^{-u}\zeta(2u)du. \tag{7.5.5}$$

This completes **Step 2** in the introduction.

We have the functional equation, see Theorem 6.5.3,

$$\begin{aligned}\Xi(t) := \pi^{-(\frac{1}{4}+it)}\Gamma(\frac{1}{4}+it)\zeta(\frac{1}{2}+2it) &\overset{\text{fe}}{=} \pi^{-(\frac{1}{4}-it)}\Gamma(\frac{1}{4}-it)\zeta(\frac{1}{2}-2it)\\ &= \Xi(-t).\end{aligned} \tag{7.5.6}$$

Next we substitute $y = \pi e^{2ia}$, where $|a| < \pi/4$. Using the above functional equation, the integral in the RHS of (7.5.5) becomes

$$\begin{aligned}\int_{1/4-i\infty}^{1/4+i\infty} \Gamma(u)y^{-u}\zeta(2u)du &= 2ie^{-ia/2}\int_0^{\infty} \Xi(t)\cosh 2at\,dt\\ &= ie^{-ia/2}\int_0^{\infty}\Xi(\frac{t}{2})\cosh at\,dt\,.\end{aligned}$$

Substituting the above into equation (7.5.5), we get

$$e^{ia/2}\theta(e^{2ia}) = \cos\frac{a}{2} + \frac{1}{\pi}\int_0^{\infty}\Xi(\frac{t}{2})\cosh at\,dt, \tag{7.5.7}$$

where θ is Jacobi's Theta function, recall Definition 6.4.3.

Lemma 7.5.8. *Let $a_m := \pi(2m+1)^2/4$ and $k \in \mathbb{Z}_{\geqslant 0}$. Then the sequence of functions*

$$f_n(\delta) = \sum_{m=0}^{n} a_m^k e^{-a_m/\delta}$$

converges uniformly in the region

$$\{\delta = re^{i\alpha} \mid 0 < r < 1,\ -\pi/4 < \alpha < 0\}.$$

Proof. We see that

$$\operatorname{Re}(-a_m/\delta) = \frac{-a_m\cos\alpha}{r} \leqslant \frac{-a_m}{2r}. \tag{7.5.9}$$

Choose $n \gg 0$ so that

$$k \log a_m \leqslant \frac{a_m}{4} < \frac{a_m}{4r} \qquad \forall m \geqslant n.$$

It follows that

$$\left| a_m^k e^{-a_m/\delta} \right| < e^{-a_m/4r} < e^{-\pi m/4r} \qquad \forall m \geqslant n,$$

and so we get

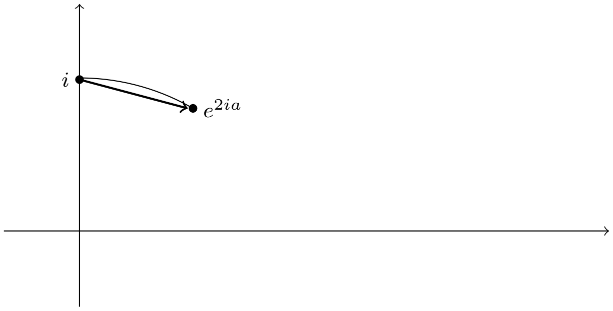
$$\sum_{m \geqslant n} \left| a_m^k e^{-a_m/\delta} \right| \leqslant \frac{e^{-\pi n/4r}}{1 - e^{-\pi/4r}} < \frac{e^{-\pi n/4r}}{1 - e^{-\pi/4}} < \frac{e^{-\pi n/4}}{1 - e^{-\pi/4}}. \tag{7.5.10}$$

We see that by choosing $n \gg 0$ we can make this as small as we want to. This shows that the $f_n \to f$ uniformly in the given region. □

Lemma 7.5.11. *Let $|a| < \pi/4$. For all integers $k \geqslant 0$ we have*

$$\lim_{a \to \pi/4} \theta^{(k)}(e^{2ia}) = 0.$$

Proof. Let $\delta := e^{2ia} - i$. We have that as $a \to \pi/4$, the argument of δ satisfies $-\pi/4 < \mathrm{Arg}(\delta) < 0$, see the following diagram.



Because of this, to prove the Lemma, it suffice to show that as $\delta \to 0$ in the region $-\pi/4 < \mathrm{Arg}(\delta) < 0$, the limit

$$\lim_{\delta \to 0} \theta^{(k)}(i + \delta) = 0,$$

for every $k \geqslant 0$. Using the definition of θ we get

$$\begin{aligned} \theta(e^{2ia}) = \theta(i + \delta) &= 1 + 2 \sum_{m \geqslant 1} e^{-\pi m^2 (i+\delta)} \\ &= 1 + 2 \sum_{m \geqslant 1} (-1)^m e^{-\pi m^2 \delta}. \end{aligned}$$

This shows that

$$\begin{aligned}\theta(i+\delta)+\theta(\delta) &= \Big(1+2\sum_{m\geqslant 1}(-1)^m e^{-\pi m^2\delta}\Big)+\Big(1+2\sum_{m\geqslant 1}e^{-\pi m^2\delta}\Big)\\ &= 2\theta(4\delta)\,.\end{aligned}$$

Now using the functional equation, Theorem 6.4.9, for the Jacobi theta function we get

$$\begin{aligned}\theta(i+\delta) &= \delta^{-1/2}\Big(\theta(\frac{1}{4\delta})-\theta(\frac{1}{\delta})\Big)\\ &= \delta^{-1/2}\sum_{m\geqslant 0}e^{-\pi(2m+1)^2/4\delta}\,.\end{aligned} \tag{7.5.12}$$

If we can differentiate under the summation, then it is clear that for every $k \geqslant 0$ we have

$$\theta^{(k)}(i+\delta)=\pm\delta^*\sum_{m\geqslant 0}e^{-a_m/\delta}\pm\delta^*\sum_{m\geqslant 0}a_m e^{-a_m/\delta}+\ldots+\pm\delta^*\sum_{m\geqslant 0}a_m^k e^{-a_m/\delta},$$

where $* \in \mathbb{Z}_{<0}+1/2$ (obviously different occurrences can take different values). That we can differentiate under the summation follows from Lemma 7.5.8 and Theorem 5.1.5. To prove the Lemma it suffices to show that

$$\lim_{\delta\to 0}\delta^*\sum_{m\geqslant 0}a_m^k e^{-a_m/\delta}=0.$$

This follows from equations (7.5.9) and (7.5.10), since by choosing $n \gg 0$ which works for all $j \in \{0,1,\ldots,k\}$, (recall $\delta = re^{i\alpha}$ and $* \in \mathbb{Z}_{<0}+1/2$)

$$\begin{aligned}\Big|\delta^*\sum_{m\geqslant 0}a_m^j e^{-a_m/\delta}\Big| &\leqslant \Big|\delta^*\sum_{m=0}^{n}a_m^j e^{-a_m/\delta}\Big|+\Big|\delta^*\sum_{m\geqslant n}a_m^j e^{-a_m/\delta}\Big|\\ &\leqslant \Big(r^*\sum_{m=0}^{n}a_m^j e^{-a_m/2r}\Big)+\frac{r^* e^{-\pi n/4r}}{1-e^{-\pi/4}}.\end{aligned}$$

From this the assertion follows by taking limit $r \to 0$. □

This completes **Step 3** in the introduction.

Now we return to equation (7.5.7). It is easily checked, using Lemma 7.4.1 and Corollary 7.1.8, by proceeding as in the proof of Theorem 7.4.6, that the integral in the RHS of (7.5.7) can be differentiated with respect to a

under the integral sign. Differentiating both sides of equation (7.5.7) $2n$ times with respect to a, taking limit $a \to \pi/4$ and using Lemma 7.5.11, we see that

$$0 = \frac{(-1)^n}{2^{2n}} \cos\frac{\pi}{8} + \lim_{a\to\pi/4} \frac{1}{\pi} \int_0^\infty t^{2n} \Xi(\frac{t}{2}) \cosh at \, dt, \tag{7.5.13}$$

Theorem 7.5.14 (Hardy's Theorem)**.** *The function $\zeta(1/2+it)$ vanishes for infinitely many values of $t \in \mathbb{R}$.*

Proof. Observe from the definition (7.5.6) of the function $\Xi(t)$ that

1. $\overline{\Xi(t)} = \Xi(-t) = \Xi(t)$,
2. The nonvanishing of the Gamma function, see Theorem 6.2.5, shows that the zeros of $\Xi(t)$ vanishes iff $\zeta(1/2 + 2it)$ vanishes.

It suffices to show that $\Xi(t)$ vanishes for infinitely many values of $t \in \mathbb{R}$. Let us assume that $\Xi(t)$ has only finitely many zeros. Then there is $T > 0$ such that $\Xi(t) \neq 0$ for all $t \geqslant T$.

Assume that $\Xi(t) > 0$ for $t \geqslant T$. Let m be the least value taken by $\Xi(t/2)\cosh at$ in the compact set $(t, a) \in [2T, 2T + 1] \times [\pi/8, \pi/4]$. Since $\cosh at$ does not vanish, it follows that $m > 0$. We get

$$\begin{aligned} \int_T^\infty t^{2n}\Xi(\frac{t}{2}) \cosh at\,dt &\geqslant \int_{2T}^{2T+1} t^{2n}\Xi(\frac{t}{2}) \cosh at\,dt, \\ &\geqslant m \int_{2T}^{2T+1} t^{2n} dt > m(2T)^{2n}. \end{aligned} \tag{7.5.15}$$

Since $\cosh t$ is an increasing function for $t \geqslant 0$ we get $\cosh at \leqslant \cosh \pi t/4$, say for $\pi/8 \leqslant a \leqslant \pi/4$. Let K denote the maximum of the function $|\Xi(t/2)\cosh \pi t/4|$ in the compact set $t \in [0, T]$. We get

$$\begin{aligned} \left|\int_0^T t^{2n}\Xi(\frac{t}{2}) \cosh at\,dt\right| &\leqslant \int_0^T t^{2n} \left|\Xi(\frac{t}{2})\right| |\cosh at|\,dt \\ &\leqslant \int_0^T t^{2n} \left|\Xi(\frac{t}{2})\right| |\cosh \pi t/4|\,dt \\ &\leqslant K \int_0^T t^{2n} dt = \frac{KT^{2n+1}}{2n+1}. \end{aligned} \tag{7.5.16}$$

Let

$$A := \lim_{a\to\pi/4} \int_0^T t^{2n}\Xi(\frac{t}{2}) \cosh at\,dt\,, \qquad B := \lim_{a\to\pi/4} \int_T^\infty t^{2n}\Xi(\frac{t}{2}) \cosh at\,dt.$$

From (7.5.15) and (7.5.16) we see that

$$|A| \leqslant \frac{KT^{2n+1}}{2n+1}, \qquad\qquad B \geqslant m(2T)^{2n}.$$

Choose n even and very large so that

$$\frac{KT}{2n+1} < 2^{2n}m. \tag{7.5.17}$$

We write equation (7.5.13) as

$$A + B = \frac{(-1)^{n+1}\pi}{2^{2n}} \cos\frac{\pi}{8} < 0.$$

But this is a contradiction to (7.5.17) since

$$0 < -\frac{KT^{2n+1}}{2n+1} + m(2T)^{2n} \leqslant A + B < 0.$$

If $\Xi(t) < 0$ for $t \geqslant T$ then write (7.5.13) as

$$\frac{(-1)^n}{2^{2n}} \cos\frac{\pi}{8} = \lim_{a\to\pi/4} \frac{1}{\pi}\int_0^\infty t^{2n}\Big(-\Xi(\frac{t}{2})\Big)\cosh at\,dt,$$

Let m be the least value taken by $-\Xi(t/2)\cosh at$ in the compact set $(t,a) \in [2T, 2T+1] \times [\pi/8, \pi/4]$. Defining A and B as above, with Ξ replaced by $-\Xi$, we get the same relations

$$|A| \leqslant \frac{KT^{2n+1}}{2n+1}, \qquad\qquad B \geqslant m(2T)^{2n}.$$

Choose n odd and very large so that

$$\frac{KT}{2n+1} < 2^{2n}m.$$

We write equation (7.5.13) as

$$A + B = \frac{(-1)^{n}\pi}{2^{2n}} \cos\frac{\pi}{8} < 0.$$

But this is a contradiction to (7.5.17) since

$$0 < -\frac{KT^{2n+1}}{2n+1} + m(2T)^{2n} \leqslant A + B < 0.$$

This completes the proof of Hardy's theorem. □