MAT 415 Notes

Max Chien

Fall 2025

Contents

Introduction

Chapter 1

Preliminaries

1.1 Dirichlet's Theorem on Primes in Progression

Theorem 1.1: Dirichlet

Given $a, q \in \mathbb{N}$ with $(a, q) = 1$, there are infinitely many primes p such that $p \equiv a \pmod{q}$.

We begin by considering Euler's proof of the infinitude of primes. Recall that the zeta function,

$$\sum_{n=1}^{\infty} n^{-s}$$

converges absolutely for $s > 1$ (for now we will work with real s), and diverges for $n = 1$. Moreover, consider the product

$$\prod_p (1 - p^{-s})^{-1} = \prod_p \sum_{k=0}^{\infty} p^{-ks}$$

Since we still have absolute convergence, we may rearrange the generic terms in the product. Each such term is of the form $(p_1^{k_1} \cdots p_m^{k_m})^{-s}$, and by unique factorization thsi means the term n^{-s} shows up exactly once for each n. Hence

$$\prod_p (1 - p^{-s})^{-1} = \sum_{n=1}^{\infty} n^{-s}$$

for $\mathrm{Re}(s) > 1$. Taking $s \to 1$, the right hand side diverges so the left hand side does as well. Hence it is clear that there are infinitely many primes. So our goal will be to use a similar strategy which demonstrates that

$$\sum_{p \equiv a \pmod{m}} \frac{1}{p} = \infty$$

To do this, consider the ring $\mathbb{Z}/m\mathbb{Z}$, as well as its group of units $(\mathbb{Z}/m\mathbb{Z})^*$. Recall that the totient function is

$$\phi(m) = \left|(\mathbb{Z}/m\mathbb{Z})^*\right| = \#\left\{\text{numbers } \leq m \text{ rel. prime to } m\right\}$$

We will work with the space of functions $f : (\mathbb{Z}/m\mathbb{Z})^* \to \mathbb{C}$. The goal is to define a sense of Fourier expansion for this vector space. We define

$$e(z) \coloneqq e^{2\pi i z}$$

For $\mathbb{R}/\mathbb{Z}$, we can perform such an expansion by observing that the set of $e(mx)$ for $m \in \mathbb{Z}$ defines an orthonormal basis for $L^2(\mathbb{R}/\mathbb{Z} \to \mathbb{C})$. More generally, if G is a finite abelian group, then we denote by $\hat{G}$ the group of its characters; that is, homomorphisms $\chi : G \to \mathbb{C}^*$. Since every element in G has finite order, each character maps into the roots of unity.

Remark

We denote additive characters by ψ and multiplicative ones by χ.

Proposition 1.2

$G \cong \hat{G}$.

Proof. First suppose G is cyclic. Then we can assume we are working with $(\mathbb{Z}/r\mathbb{Z}, +)$. Any additive character is determined by $\psi(1)$, and $\psi(1)$ is necessarily an rth root of unity. So the characters are precisely those of the form

$$\psi_\nu(x) = e\left(\frac{\nu x}{r}\right)$$

for $\nu \in \mathbb{Z}/r\mathbb{Z}$. So clearly $\left|\hat{G}\right| = |G|$. Also, $\psi_\nu \psi_\mu = \psi_{\nu+\mu}$, so the map $\nu \mapsto \psi_\nu$ is an onto homomorphism from G to $\hat{G}$, hence an isomorphism.

TODO: in the general case, use the classification of finite groups, and apply this to $G = ((\mathbb{Z}/m\mathbb{Z})^*, \cdot)$. □

Note that this isomorphism is not canonical, however the isomorphism $G \cong \hat{\hat{G}}$ is.

Suppose $\chi \in \hat{G}$, and $f : G \to \mathbb{C}$ is a function. Then we define the **Fourier transform** $\hat{f} : \hat{G} \to \mathbb{C}$ of f on G by

$$\hat{f}(\chi) = \sum_{g \in G} f(g)\chi(g)$$

Proposition 1.3

If χ_e denotes the trivial character which takes all elements to $1 \in \mathbb{C}$, then

$$\sum_{g \in G} \chi(g) = \begin{cases} |G|, & \chi = \chi_e \\ 0 \end{cases}$$

$$\sum_{\chi \in \hat{G}} \chi(g) = \begin{cases} \left|\hat{G}\right| = |G|, & g = e \\ 0 \end{cases}$$

Proof. For the first, the formula is obvious when $\chi = \chi_e$. Otherwise, there is an element a where $\chi(a) \neq 1$. But then

$$S = \sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(ag) = S = \chi(a)S$$

But $\chi(a) \neq 1$, so we must have $S = 0$. A similar proof holds for the second formula. □

Theorem 1.4: Fourier Inversion

For any $f : G \to \mathbb{C}$,

$$f(g) = \frac{1}{|G|} \sum_{\chi \in \hat{G}} \hat{f}(\chi)\overline{\chi(g)}$$

Proof.

$$\frac{1}{|G|} \sum_{\chi \in \hat{G}} \hat{f}(\chi)\overline{\chi(g)} = \frac{1}{|G|} \sum_{\chi \in \hat{G}} \sum_{h \in G} f(h)\chi(h)\overline{\chi(g)} = \frac{1}{|G|} \sum_{h \in G} f(h) \sum_{\chi \in G} \overline{\chi(g)}\chi(h)$$

□

Now, we want to calculate the transform of the indicator function I_a for some $a \in G$. Then by fourier inversion,

$$\hat{I}_a(\chi) = \sum_{g \in G} I_a(g)\chi(g) = \chi(a)$$

$$I_a(g) = \frac{1}{|G|} \sum_{\chi \in \hat{G}} \hat{I}_a(g)\overline{\chi(g)} = \frac{1}{|G|} \sum_{\chi \in \hat{G}} \chi(a)\overline{\chi(g)}$$

Definition 1.1

Let $m \in \mathbb{N}$ and $\chi \in \widehat{(\mathbb{Z}/m\mathbb{Z})^*}$. Then the **Dirichlet L-function** associated with χ is

the function $L(\cdot, \chi) : \mathbb{C} \to \mathbb{C}$, where

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

where we extend χ to the integers by defining

$$\chi(n) = \begin{cases} 0, & (n, m) > 1 \\ \chi(n \pmod m) & \end{cases}$$

Note that because $|\chi| \leq 1$, the series converges absolutely for $\mathrm{Re}(s) > 1$, and the Euler product is given by

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

because $\chi(mn) = \chi(m)\chi(n)$. Actually, we can make do with a slightly weaker assumption so an alternate form of the Euler product holds.

Definition 1.2

Let $f : \mathbb{N} \to \mathbb{C}$. Then f is called **multiplicative** if $f(1) = 1$ and $f(mn) = f(m)f(n)$ whenever $(m, n) = 1$. It is called **totally multiplicative** if $f(mn) = f(m)f(n)$ for all m, n.

For any multiplicative f,

$$\prod_p (1 + f(p)p^{-s} + f(p^2)p^{-2s} + \ldots) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}$$

Proposition 1.5

1. $L(s, \chi)$ converges absolutely on $\mathrm{Re}(s) > 1$, and is analytic there. If $\chi \neq \chi_0$ then it is analytic on $\mathrm{Re}(s) > 0$ as well, though it converges conditionally ($L(s, \chi_e)$ has a pole at 0).
2. $L(s, \chi)$ is nonzero on $\mathrm{Re}(s) > 1$.
3. $L(s, \chi_e) = \zeta(s) \prod_{q|m} (1 - q^{-s})$.

Proof. 1) Convergence is easy since $|\chi(n)| \leq 1$. If $\chi \neq \chi_e$,

$$\sum_{n=1}^{m} \chi(n) = 0$$

so

$$\left| \sum_{n=1}^{T} \right| \chi(n) \leq m$$

for any T. Then we employ summation by parts:

$$\sum_{n\leq T}\chi(n)n^{-s}=\sum_{n\leq T}\left(\sum_{\nu\leq n}\chi(\nu)\right)[n^{-s}-(n+1)^{-s}]=\sum_{n\leq T}\left(\sum_{\nu\leq n}\chi(\nu)\right)\frac{s}{n^{-(s+1)}}$$

Since the factor $\sum_{\nu\leq n}\chi(\nu)$ is bounded, this sum converges for $\mathrm{Re}(s)>0$.

2) For $\mathrm{Re}(s)>1$, the Euler product

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

converges. But no factor is zero, so the whole product is not either.

TODO: 3 □

For $\mathrm{Re}(s)>1$, we then have

$$\log L(s,\chi)=-\sum_p\log(1-\chi(p)p^{-s})=\sum_p\sum_{k=1}^{\infty}\frac{\chi(p^k)}{p^{ks}}=\sum_p\frac{\chi(p)}{p^s}+\sum_p\sum_{k=2}^{\infty}p^{-ks}\chi(p^k)$$

The second term is uniformly bounded on $\mathrm{Re}(s)\geq\sigma_0>1/2$. Therefore

$$\sum_{\chi\in\hat{G}}\chi(a)\log L(s,\overline{\chi})=|G|\sum_{p\equiv a(m)}p^{-s}+O_{m,\sigma_0}(1)$$

The notation O_{m,σ_0} means that the last quantity is uniformly bounded, but the constant depends on m,σ_0. Now we extract the trivial character as

$$|G|\sum_{p\equiv a(m)}p^{-s}=\log L(s,\chi_e)+\sum_{\chi\neq\chi_e}\chi(a)\log L(s,\overline{\chi})$$

Here we would like to take the limit $s\to 1^+$. However, in order to conclude divergence, we need to know that $L(1,\chi)\neq 0$ if $\chi\neq\chi_0$, so that the second term of the right hand side is finite.

Result (3) suggests that we should look at analytic continuations of $\zeta(s)$. Recall that

$$\zeta(s)=1+2^{-s}+3^{-s}+\ldots$$

Consider

$$A(s)\coloneqq 1-2^{-s}+3^{-s}-\ldots$$

Then

$$\zeta(s)-A(s)=2^{1-s}(1+2^{-s}+3^{-s}+\ldots)=2^{1-s}\zeta(s)$$

Thus

$$\zeta(s)=\left[1-2^{-(s-1)}\right]^{-1}A(s)$$

$A(s)$ is analytic for $\mathrm{Re}(s)>0$, and the factor in front only has a pole at $s=1$. Thus $\zeta(s)$ may be continued to $\mathrm{Re}(s)>0$ so that it has a simple pole at $s=1$ only.

Returning to the formula in terms of L-functions, we have

$$\log L(s, \chi_e) = \log \zeta(s) + O(1)$$

as $s \to 1$ for $s > 0 \in \mathbb{R}$. Since we know $s = 1$ is a simple pole, we can expand ζ about 1 as

$$\zeta(s) = A(s-1)^{-1} + B + C(s-1) + \dots$$

Then

$$\log \zeta(s) + O(1) = -\log(s-1) + O(1) \to \infty$$

Combining with oour previous work, we get

$$|G| \sum_{p \equiv a(m)} p^{-s} = \sum_{\chi \in \hat{G}} \chi(a) \log L(s, \overline{\chi}) + O(1) = -\log(s-1) + \sum_{\chi \neq \chi_e} \chi(a) \log L(s, \overline{\chi}) + O(1)$$

We still need to show that $L(1, \chi) \neq 0$ for $\chi \neq \chi_e$. Indeed, note that if $L(1, \chi) = 0$ then $L(1, \overline{\chi}) = 0$ as well. So if $\chi \neq \overline{\chi}$ and $L(1, \chi) = 0$, then we write

$$L(s, \chi) = A(s-1)^{\nu}$$

Here ν is the order of the zero at 1. Then $\overline{\chi}$ also has the same order zero.

Let us briefly assume that $a = 1$, so that we are looking for primes which have remainder 1 mod m. Then $\chi(1) = 1$ for all χ, which simplifies to

$$|G| \sum_{p \equiv 1(m)} p^{-s} = -\log(s-1) + \sum_{\chi \neq \chi_0} \log L(s, \overline{\chi}) + O(1)$$

In this case, if $\chi \neq \overline{\chi}$ and $L(s, \chi)$ vanishes with order ν at 1, then the sum at least contains the term

$$2\nu \log(s-1)$$

On the right hand side the term $-\log(s-1)$ tends to $+\infty$, but the terms in the sum may only diverge to $-\infty$ (since they can only have zeroes, not poles). Indeed, if $\nu \geq 1$ for at least one nonreal, nontrivial character, then the RHS tends to $-\infty$, but the left hand side is nonnegative. Thus no such character vanishes at $s = 1$. Note that this is the case regardless of a; we simply use $a = 1$ in order to generate a contradiction.

So we have reduced to

$$|G| \sum_{p \equiv a(m)} p^{-s} = -\log(s-1) + \sum_{\chi = \chi \neq \chi_e} \chi(a) \log L(s, \overline{\chi}) + O(1)$$

and merely need to show that $L(1, \chi) \neq 0$ for real characters $\chi = \overline{\chi}, \chi \neq \chi_e$. We form the function

$$F(s) = \prod_{\chi \in \hat{G}} L(s, \chi)$$

This function is analytic on $\mathrm{Re}(s) > 1$. On $\mathrm{Re}(s) > 0$, it is analytic except possibly at $s = 1$. Here, if $L(s, \chi) \neq 0$ for $\chi \neq \chi_e$, then there is a simple pole. Otherwise, $F(1)$ is finite. Since F is a product of Dirichlet series, we can write

$$F(s) = \sum_{n=1}^{\infty} a_n n^{-s}$$

Proposition 1.6

$a_n \geq 0$ for all n. Moreover, $n \mapsto a_n$ is multiplicative (but not necessarily totally multiplicative).

Note that this is because $F(s)$ shows up as the **Dedekind zeta function** $\zeta_K(s)$ of a number field K, but we don't need that for this proof, since we compute the coefficients directly.

Proof. Write

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s} = \prod_p (1 + a_p p^{-s} + a_{p^2} p^{-2s} + \ldots) \prod_{\chi \in \hat{G}} (1 - \chi(p) p^{-s})^{-1}$$

For $(p, m) = 1$,

$$\prod_{\chi \in \hat{G}} (1 - \chi(p) p^{-s})^{-1} = (1 - (p^{-s})^{f(p)})^{-g(p)}$$

where $f(p)$ is the order of p in $(\mathbb{Z}/p\mathbb{Z})^*$ and

$$g(p) = \frac{\phi(m)}{f(p)}$$

and expanding this gives a series with nonnegative coefficients by the binomial theorem. □

Recall that for a power series

$$\sum_{n=0}^{\infty} c_n z^n$$

with $c_n \geq 0$, there is a pole at $z = \rho_0$, where ρ_0 is the radius of convergence.

Definition 1.3

For a Dirichlet series

$$\sum_{n=1}^{\infty} \frac{a_n}{n^{-s}}$$

the **abscissa of absolute convergence** is

$$\sigma_0 = \inf \left\{ \sigma \in \mathbb{R} : \sum_{n=1}^{\infty} \left| \frac{a_n}{n^{-s}} \right| < \infty (\mathrm{Re}(s) > \sigma) \right\}$$

Lemma 1.7

Let

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

with $a_n \geq 0$, and let $\sigma = \rho_0$ be the abscissa of absolute convergence. If f is analytic for $\mathrm{Re}(s) > \rho$ then $\rho_0 \leq \rho$.

In other words, the above lemma says that the first pole of a Dirichlet series with nonnegative coefficients is on the real axis.

Now suppose that F has no pole at $s = 1$. Then our Dirichlet series representation of F must converge absolutely for $\mathrm{Re}(s) > 0$. Now note that

$$(1 - p^{f(p)s})^{-g(p)} \geq 1 + p^{-\phi(m)s} + p^{-2\phi(m)s} + \dots$$

So

$$\sum_{n=1}^{\infty} a_n n^{-s} \geq \sum_{n=1}^{\infty} n^{-\phi(m)s}$$

for $s > 0$. But taking $s = 1/\phi(m) > 0$, F must diverge, which is a contradiction. This concludes the proof of Dirichlet's theorem.

The proof of Dirichlet's theorem made use of the fact that $\zeta(1) \neq 0$. In fact a stronger theorem is true, which uses the results on nonnegative coefficient Dirichlet series we derived.

Theorem 1.8

$\zeta(s) \neq 0$ for $\mathrm{Re}(s) = 1$.

Proof. For $\nu \in \mathbb{C}$ we define

$$\sigma_\nu(n) = \sum_{d|n} d^\nu$$

For $t_0 = \mathrm{Im}(s) \neq 0$ (we showed this for $t_0 = 0$ already) we also define

$$F(s) = \sum_{n=1}^{\infty} \frac{[\sigma_{it_0}(n)]^2}{n^s}$$

This is equal to

$$\frac{\zeta^2(s)\zeta(s + it_0)\zeta(s - it_0)}{\zeta(2s)}$$

But since this is a Dirichlet series with positive coefficients, we just need to show that there is no pole at $s = 1$. Suppose for contradiction that there is a zero at $\zeta(1 + it_0)$. Then there is also a zero at $\zeta(1 - it_0)$, which cancels with the order 2 pole for $\zeta^2(s)$. Moreover, since ζ only has poles at $s = 0, 1$, and it is nonzero for $\mathrm{Re}(s) > 1$, this represents the series for all $\mathrm{Re}(s) > 1/2$. At $s = 1/2$ the denominator forces $F(1/2) = 0$. But by inspection it is plainly untrue that $F(1/2) = 0$. □

1.2 Class Number Field

Consider $\mathbb{F}$ a finite field. Then $(\mathbb{F}, +)$ and $(\mathbb{F}^*, \cdot)$ are finite abelian groups, so we may consider their dual groups. Since both structures are in place, we may think about the additive properties of multiplicative characters, or multiplicative properties of additive characters.

Definition 1.4

Given $\psi \in \widehat{(\mathbb{F}, +)}, \chi \in \widehat{(\mathbb{F}^*, \cdot)}$, the **Gauss sum** of ψ, χ is

$$G(\psi, \chi) = \sum_{a \in \mathbb{F}^*} \psi(a)\chi(a) = \hat{\chi}(\psi) = \hat{\psi}(\chi)$$

Example 1.1

Let $\mathbb{F} = \mathbb{R}$. Then the additive characters are those of the form

$$\psi(x) = e(\alpha x)$$

for $\alpha \in \mathbb{C}$, and the multiplicative characters are

$$\chi(a) = a^s |a|$$

for $s \in \mathbb{C}, a \in \mathbb{R}^*$. Since $\mathbb{R}^*$ is infinite, we will need to convert our sum to an integral over an appropriate measure. If we try to assign a "translation invariant" measure to a group, we will need to look at the measure

$$\frac{\mathrm{d}a}{a}$$

which is called the **Haar measure**. So the Gauss sum becomes

$$G(\alpha, s) = \int_0^\infty e^{\alpha x} x^s \frac{\mathrm{d}x}{x}$$

which is the Gamma function.

Over finite field $\mathbb{F}_p$, $p > 2$, then there is an additive group isomorphism $\mathbb{F}_p \to \hat{\mathbb{F}_p}$ given by

$$a \mapsto \psi_a(x) = e\left(\frac{ax}{p}\right)$$

Note that the choice of pth root of unity implicit in this statement shows why the isomorphism is noncanonical. So then for $b \in \mathbb{Z}/p\mathbb{Z}$ and $\chi \in \widehat{(\mathbb{Z}/p\mathbb{Z})^*}$, the Gauss sum is given by

$$\tau(b, \chi) = \sum_{a=1}^{p-1} \chi(a) e\left(\frac{ab}{p}\right)$$

Proposition 1.9

For $\chi \in \widehat{(\mathbb{Z}/p\mathbb{Z})^*}$,

- $\tau(a,\chi) = \overline{\chi(a)}\tau(1,\chi)$,
- For $\tau(\chi) \coloneqq \tau(1,\chi)$, $|\tau(\chi)|^2 = p$.

- *Proof.* If $a \neq 1$, then writing $ca = w$,

$$\tau(a,\chi) = \sum_{c=1}^{p-1} \chi(c) e\left(\frac{ca}{p}\right) = \sum_{c=1}^{p-1} \chi(wa^{-1}) e\left(\frac{w}{p}\right) = \overline{\chi(a)}\tau(1,\chi) \qquad \square$$

We have

$$|\tau(\chi)|^2 = \sum_{a\in\mathbb{F}^*} \chi(a)\psi(a)\overline{\sum_{b\in\mathbb{F}^*} \chi(b)\psi(b)}$$
$$= \sum_{a,b\in\mathbb{F}^*} \chi(a)\overline{\chi(b)}\psi(a)\overline{\psi(b)} = \sum_{a,b} \chi(ab^{-1})\psi(a-b)$$

Set $ab^{-1} = w$. Then this becomes

$$\sum_{b,w} \chi(w)\psi(b(w-1))$$

If $w = 1$, then each term is 1 and the sum over b is $p-1$. If $w \neq 1$, then the sum over b is

$$\sum_{b\in\mathbb{F}^*} \psi(b(w-1)) = \underbrace{\sum_{b\in\mathbb{F}} \psi(b(w-1))}_{=0} - \psi(0) = -1$$

So the sum is now

$$-\sum_{w\in\mathbb{F}^*} \chi(w)$$

Definition 1.5

Let $p > 2$. Then define the Legendre symbol as

$$\chi(n) = \left(\frac{n}{p}\right) = \begin{cases} 1, & n = x^2, x \in \mathbb{F}_p \\ -1 \end{cases}$$

This is a real multiplicative character of $\mathbb{F}_p$.

Proposition 1.10

If χ is the Legendre symbol for $\mathbb{F}_p$, $p > 2$,

$$\tau(x)^2 = \begin{cases} p, & p \equiv 1 \pmod 4 \\ -p, & p \equiv 3 \pmod 4 \end{cases}$$

Proof. We write out the Gauss sum:

$$\tau(\chi) = \sum_{n=1}^{p-1} \left(\frac{n}{p}\right) e\left(\frac{n}{p}\right) = \sum_{n=1}^{p-1} \left[\left(\frac{n}{p}\right) + 1\right] e\left(\frac{n}{p}\right) - \underbrace{\sum_{n=1}^{p-1} e\left(\frac{n}{p}\right)}_{=-1}$$

$$= \sum_{n=0}^{p-1} e\left(\frac{n}{p}\right) \left[\begin{cases} 2, & n = x^2 \\ 0 \end{cases}\right]$$

The Legendre symbol factor turns this sum into twice the sum over the quadratic residues, and since half the numbers are quadratic residues, we can double count by simply summing:

$$\tau(\chi) = \sum_{n=0}^{p-1} e\left(\frac{n^2}{p}\right)$$

□

Theorem 1.11: Gauss

- Let p be an odd prime. Then

$$\sum_{n=0}^{p-1} e\left(\frac{n^2}{p}\right) = \begin{cases} p \equiv 1 \pmod 4 \\ p \equiv 3 \pmod 4 \end{cases}$$

- If p, q are odd primes,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$$

For instance, a consequence of this is that if $p \equiv q \equiv 1 \pmod 4$, then p has a square root mod q if and only if q has a square root mod p. To prove this theorem, we will introduce Poisson summation.

Typically, we are looking at $\mathbb{R}$ and the subgroup $\mathbb{Z}$, so that we want to consider the quotient $\mathbb{R}/\mathbb{Z} = [0, 1)$. We will consider $S(\mathbb{R})$, the **Schwartz space** of functions which are smooth and for which all derivatives decay at ∞ faster than $|x|^{-A}$.

Definition 1.6

Let $f \in S(\mathbb{R})$. Then define the **Fourier transform** of f to be $\hat{f} : \mathbb{R} \to \mathbb{C}$ given by

$$\hat{f}(\xi) = \int_{-\infty}^{\infty} f(x)e(-x\xi)\,\mathrm{d}x$$

Proposition 1.12

$\hat{f} \in S(\mathbb{R})$.

Proof. To see that $\hat{f}$ is bounded, integrate by parts, which brings a factor of $\frac{1}{\xi}$. The boundary terms vanish because of the decay condition, and repeatedly differentiating gives decay for derivatives. □

Theorem 1.13: Poisson Summation

For $f \in S(\mathbb{R})$,

$$\sum_{n\in\mathbb{Z}} f(n) = \sum_{m\in\mathbb{Z}} \hat{f}(m)$$

Proof. Define

$$F(x) = \sum_{n\in\mathbb{Z}} f(x+n)$$

The sum converges absolutely because of the decay of f, so F is smooth and has period 1. Thus we can expand it as a Fourier series:

$$F(z) = \sum_{m\in\mathbb{Z}} \hat{F}(m)e(mx)$$

where

$$\hat{F}(m) = \int_0^1 F(x)e(-mx)\,\mathrm{d}x = \int_0^1 e(-mx)\sum_{k\in\mathbb{Z}} f(x+k)\,\mathrm{d}x = \int_{-\infty}^{\infty} f(x)e(-mx)\,\mathrm{d}x = \hat{f}(m)$$

So

$$F(x) = \sum_{m\in\mathbb{Z}} \hat{f}(m)e(-mx)\,\mathrm{d}x$$

Substitute $x = 0$:

$$\sum_{n\in\mathbb{Z}} f(n) = \sum_{m\in\mathbb{Z}} \hat{f}(m)$$

□

The following proof instead uses the functional analysis fact that an operator's trace is invariant under change of basis.

Alternate Proof of Poisson Summation. Let $K(x,y) : S \times S \to \mathbb{C}$, and define the operator T_K on $L^2(S)$ by

$$T_K f(x) = \int_0^1 K(x,y) f(y)\,\mathrm{d}y$$

If K is continuous, then T_K is a compact operator. In this case we define

$$\mathrm{tr}(T_K) = \int_0^1 K(x,x)\,\mathrm{d}x$$

If $\phi_1, \phi_2, \ldots$ are an orthonormal eigenbasis for $L^2(S)$ and T_K, we can also compoute the trace by diagonalization as

$$\mathrm{tr}(T_K) = \sum_j \lambda_j$$

Now, to prove Poisson summation, let $f \in S(\mathbb{R})$, and define

$$K_f(x,y) \sum_{m \in \mathbb{Z}} f(x - y + m)$$

□

Definitions