Fourier Analysis and Number Theory Minicourse

Brandon Hanson

University of Maine, Orono

Spring 2024

Table of Contents

1

BASICS OF FOURIER ANALYSIS ON $\mathbb{Z}$

Fourier analysis is one of the basic tools for handling problems in analytic number theory. It comes in under various guises, depending on what sort of problem we are working on, but there is an appropriate sense in which the most famous function in analytic number theory, the Riemann zeta function

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

is a Fourier series. Fourier series are often useful as generating functions, and $\zeta(s)$ is no exception, but it is useful as a generating function for multiplicative problems. In this short course, we will devote our attention to additive problems, and to do this, we will replace the n^s term, which is an example of a *multiplicative character*, with an *additive character*

$$e(n\theta) = e^{2\pi i n\theta}.$$

This function is periodic in the sense that $e(n(\theta + t)) = e(n\theta)$ whenever $t \in \mathbb{Z}$. For this reason we will focus on $\theta \in \mathbb{R}/\mathbb{Z}$ which we identify with the interval $[0, 1)$.

Next, there is an issue of convergence, so we introduce a weight to go with each character, say $f(n)$. The result is a formal series

$$F(\theta) = \sum_{n \in \mathbb{Z}} f(n)e(n\theta).$$

The numbers $f(n)$, which could be any complex numbers for the time being, are called the Fourier coefficients of F and we denote them $f(n) = \widehat{F}(n)$.

Ultimately, we want to do analysis, and this means turning $F(\theta)$ into a function, which in turn requires some convergence. The easiest way to do that is to look at those F such that $\widehat{F}(n)$ is non-zero for only finitely many n. If the support of f is a set $A \subseteq \mathbb{Z}$, the resulting function can then be written

$$F(\theta) = \sum_{a \in A} f(a) e(a\theta)$$

and now this is called a *trigonometric polynomial*. The *degree* of the trigonometric polynomial is $\max_{a \in A} |a|$.

In this first chapter, we discuss the basic properties of Fourier series and trigonometric polynomials, especially those properties which are useful to number theorists. But we would be remiss to leave out some of the classical questions about convergence, and so these will be discussed as well.

1.1 Trigonometric Polynomials

First we need our cast of characters, the functions

$$\theta \mapsto e(n\theta)$$

where

$$e(n\theta) = e^{2\pi i n\theta} = \cos(2\pi n\theta) + i \sin(2\pi n\theta).$$

These functions are maps from $\mathbb{R}/\mathbb{Z}$ to $S^1 = \{z \in \mathbb{C} : |z| = 1\}$ with the property

$$e(n\theta)e(m\theta) = e((n+m)\theta)$$

This means the functions are characters in the sense of group theory – both as a function of $n \in \mathbb{Z}$ and as a function of $\theta \in \mathbb{R}/\mathbb{Z}$.

Lemma 1.1: Orthogonality relations

Let n be an integer. We have the formula

$$\int_0^1 e(n\theta)\, d\theta = \begin{cases} 1 & \text{if } n = 0, \\ 0 & \text{if } n \neq 0. \end{cases}$$

Proof. Use Euler's identity. □

These relations are one of the key ingredients for number theorists - we want to count solutions to equations involving integers, and we can detect solutions with this identity.

Proposition 1.1

Let

$$F(\theta) = \sum_{|n|\le N} a_n e(n\theta),\ G(\theta) = \sum_{|n|\le N} b_n e(n\theta)$$

be trigonometric polynomials, where the a_n and b_n are complex numbers. Then

Coefficient formula:

$$a_n = \int_0^1 F(\theta) e(-n\theta)\, d\theta,$$

Parseval's identity:

$$\sum_{|n|\le N} a_n \overline{b_n} = \int_0^1 F(\theta)\overline{G(\theta)}\, d\theta,$$

Plancherel's formula:

$$\sum_{|n|\le N} |a_n|^2 = \int_0^1 |F(\theta)|^2 d\theta.$$

Proof. For (1), the right hand side is

$$\int_0^1 \sum_{|m|\le N} a_m e(m\theta)\cdot e(-n\theta)\, d\theta = \sum_{|m|\le N} a_m \int_0^1 e((m-n)\theta)\, d\theta$$

and the integral on the right only survives when $n = m$.

For (2), we have

$$\overline{G(\theta)} = \sum_{|m|\le N} \overline{b_m} e(-m\theta)$$

so that

$$\int_0^1 F(\theta)\overline{G(\theta)}\, d\theta = \int_0^1 \sum_{n,m} a_n \overline{b_m} e((n-m)\theta)\, d\theta = \sum_{n,m} a_n \overline{b_m} \int_0^1 e((n-m)\theta)\, d\theta,$$

and again the only terms of the sum which survive orthogonality are those where $n = m$, so we get

$$\sum_{n,m} a_n \overline{b_m} \int_0^1 e((n-m)\theta)\, d\theta = \sum_{|n|\le N} a_n \overline{b_n}.$$

For (3), we apply (2) with $a_n = b_n$, then $G(\theta) = F(\theta)$ and

$$\int_0^1 |F(\theta)|^2 d\theta = \int_0^1 F(\theta)\overline{G(\theta)}\, d\theta = \sum_{|n|\le N} a_n \overline{b_n} = \sum_{|n|\le N} |a_n|^2.$$

□

From part (1), we can recover the coefficients a_n from the function $F(\theta)$. We sometimes write

$$a_n = \widehat{F}(n)$$

to show this dependence ($\widehat{F}(n)$ is the n'th Fourier coefficient of F).

Lemma 1.2: Convolution to product

Let

$$F(\theta) = \sum_{|n|\leq N} a_n e(n\theta),\ G(\theta) = \sum_{|n|\leq N} b_n e(n\theta)$$

be trigonometric polynomials, where the a_n and b_n are complex numbers. Then

$$\widehat{F\cdot G}(l) = \sum_{n+m=l} a_n b_m,$$

and if

$$H(\theta) = \int_0^1 F(\tau)G(\theta-\tau)d\tau$$

then

$$H(\theta) = \sum_{|n|\leq N} a_n b_n e(n\theta).$$

Proof. For the first claim

$$F(\theta)G(\theta) = \sum_{|n|,|m|\leq N} a_n b_m e((n+m)\theta)$$

so that grouping terms according to $n+m$ we get

$$F(\theta)G(\theta) = \sum_l \left(\sum_{n+m=l} a_n b_m\right) e(l\theta),$$

which means that the coefficient of $e(l\theta)$ is

$$\left(\sum_{n+m=l} a_n b_m\right),$$

which is precisely the statement we want.

For the second claim,

$$\begin{aligned} H(\theta) &= \int_0^1 \sum_n a_n e(n\tau) \sum_m b_m e(m(\tau-\theta))d\tau \\ &= \sum_{n,m} a_n b_m e(m\theta) \int_0^1 e((n-m)\tau)d\tau \\ &= \sum_n a_n b_n e(n\theta) \end{aligned}$$

by orthogonality. □

The notation

$$H(\theta) = \int_0^1 F(\tau)G(\theta-\tau)d\tau$$

can be thought of as a restricted double integral

$$H(\theta) = \int_{\tau+\sigma=\theta} F(\tau)G(\sigma)d\tau d\sigma$$

and we often denote this as $(F * G)(\theta)$. Changing the integral to a sum, and τ, σ and θ to n and m and l, we get

$$\sum_{n+m=l} a_n b_m = \sum_{n+m=l} \widehat{F}(n)\widehat{G}(m)$$

which we denote $(\widehat{F} * \widehat{G})(l)$. The operation $*$ is called convolution, but these are separated instances of it. Indeed, one is happening to functions on $\mathbb{Z}$ and the other to functions on $\mathbb{R}/\mathbb{Z}$.

Let A be a set of integers. Define the *sumset* of A to be

$$A + A = \{a_1 + a_2 : a_1, a_2 \in A\}.$$

Next let

$$F_A(\theta) = \sum_{a\in A} e(a\theta).$$

Thus

$$\widehat{F_A}(n) = \mathbf{1}_A(n) = \begin{cases} 1 & \text{if } n \in A \\ 0 & \text{if } n \notin A. \end{cases}$$

Moreover,

$$\widehat{F_A \cdot F_A}(l) = \mathbf{1}_A * \mathbf{1}_A(l) = \sum_{n+m=l} \mathbf{1}_A(n)\mathbf{1}_A(m)$$

which, in other words, is the number of ways of writing l as a sum of two elements of A. From this we see that the support of $\mathbf{1}_A * \mathbf{1}_A$ is $A + A$.

Exercise. *Show that if*

$$F(\theta) = \sum_{\substack{p\le N \\ p \text{ prime}}} e(p\theta)$$

then the number T_N of twin prime pairs $(p, p+2)$ with $p \le N$ is given by the formula

$$T_N = \int_0^1 |F(\theta)|^2 e(-2\theta)d\theta.$$

Thus, the twin prime conjecture is equivalent to showing the integral on the right tends to infinity with N. Notice that by Plancherel's formula,

$$\int_0^1 |F(\theta)|^2 d\theta = \sum_{p\le N} 1$$

is just the number of primes up to N, which does tend to infinity. All one needs to do to establish the twin prime conjecture is deal with the exponential $e(-2\theta)$...

We close this section with two important (families of) trigonometric polynomials that are fundamental to the subject. They the *Dirichlet kernel*

$$D_N(\theta) = \sum_{|n|\le N} e(n\theta)$$

and the *Fejér kernel*

$$K_N(\theta) = \sum_{|n|\le N} \left(1 - \frac{|n|}{N+1}\right) e(n\theta).$$

Exercise. *Show that* $D_N(\theta) = \sin(\pi(N+1)\theta)/\sin(\pi\theta)$ *for* $\theta \neq 0$ *and*

$$K_N(\theta) = \frac{1}{N+1} \frac{(\sin(\pi(N+1)\theta))^2}{(\sin(\pi\theta))^2}.$$

Lemma 1.3

The function K_N is called a good kernel. It has the following properties.

Positivity:

$$K_N(\theta) \ge 0,$$

Unit mass:

$$\int_0^1 K_N(\theta)\, d\theta = 1,$$

Zero detector: for any $t > 0$,

$$\int_t^{1-t} K_N(\theta) \to 0$$

as $N \to \infty$.

Proof. (1) follows from the preceding exercise. For (2), we have

$$\int_0^1 K_N(\theta)\, d\theta = \sum_{|n|\le N} \left(1 - \frac{|n|}{N+1}\right) \int_0^1 e(n\theta)\, d\theta = 1.$$

For (3), we have

$$\lim_{N\to\infty} \int_t^{1-t} K_N(\theta)\, d\theta = \lim_{N\to\infty} \frac{1}{N+1} \int_t^{1-t} \frac{(\sin(\pi(N+1)))^2}{(\sin(\pi\theta))^2}\, d\theta = 0$$

since the integrand in the middle is bounded. □

1.2 Pointwise convergence

We now begin an investigation as to what happens when a trigonometric polynomial is replaced by a trigonometric series. This brings about all sorts of questions involving convergence. Three particular questions are listed below.

1. What does converge mean?
2. If F is a function, does it have a convergent Fourier series?
3. If $f : \mathbb{Z} \to \mathbb{C}$ is a function, does the series

$$\sum_{n\in\mathbb{Z}} f(n)e(n\theta)$$

converge?

Definition 1.1: Pointwise convergence

We say the Fourier series

$$\sum_{n\in\mathbb{Z}} f(n)e(n\theta)$$

converges pointwise at θ if the sequence

$$\lim_{N\to\infty} \sum_{|n|\leq N} f(n)e(n\theta)$$

converges.

Remark. *The definition of convergence is a two-sided one as each new value of N introduces the terms $f(-N)e(-N\theta)$ and $f(N)e(N\theta)$. This introduces a fair bit of subtlety into questions of convergence.*

Exercise. *Show that if a Fouries series converges to a function $F(\theta)$ for each θ, then it is periodic: for any $t \in \mathbb{Z}$, we have $F(\theta + t) = F(\theta)$.*

So far we have defined the Fourier coefficients of F when F is a trigonometric polynomial. Such F are continuous (on the compact set $[0,1]$) and so belong to $L^1([0,1])$. In fact the definition of Fourier coefficients extend to all of $L^1([0,1])$:

$$\widehat{F}(n) = \int_0^1 F(\theta)e(-N\theta)d\theta.$$

In the same way we extend the notion of convolution to $L^1([0,1])$

$$(F * G)(\theta) = \int_0^1 F(\tau)G(\theta - \tau)d\tau$$

and we have

$$\widehat{F * G}(n) = \widehat{F}(n)\widehat{G}(n).$$

With this in mind, we write

$$S_N(F)(\theta) = \sum_{|n|\leq N} \widehat{F}(n)e(n\theta),$$

and $S_N(F)$ is called the N'th partial sum of F.

Lemma 1.4

If $F \in L^1([0,1])$, and if $K(\theta) = \sum_{|n|\le N} a_n e(n\theta)$ is any trigonometric polynomial, we have

$$(F * K)(\theta) = \sum_{|n|\le N} a_n \widehat{F}(n) e(n\theta).$$

In particular $S_N(F) = F * D_N$ where K_N is the Dirichlet kernel.

Proof. By definition, we have

$$(F * K)(\theta) = \int_0^1 F(\tau) \sum_{|n|\le N} a_n e(n(\theta-\tau))\, d\tau$$
$$= \sum_{|n|\le N} a_n e(n\theta) \int_0^1 F(\tau) e(-n\tau)\, d\tau = \sum_{|n|\le N} a_n \widehat{F}(n) e(n\theta).$$

□

Theorem 1.1: Fejér's Theorem

If $F \in L^1([0,1])$ then

$$\lim_{N\to\infty} (F * K_N)(\theta) = \lim_{h\to 0} \frac{f(\theta+h) + f(\theta-h)}{2},$$

provided the right hand side exists. Here K_N is the Fejér kernel of degree N. In particular, if F is continuous at θ then

$$(F * K_N)(\theta) \to F(\theta).$$

Proof. By replacing $F(t)$ with $F(t-\theta)$ we can take $\theta = 0$. The limit in question is

$$\int_0^1 F(\tau) K_N(-\tau)\, d\tau = \int_0^t F(\tau) K_N(-\tau)\, d\tau + \int_{1-t}^1 F(\tau) K_N(-\tau)\, d\tau + \int_t^{1-t} F(\tau) K_N(-\tau)\, d\tau.$$

Taking t so small that $|F(\tau) - F(0)| < \varepsilon$ for $0 < \tau < t$ and $1-t < \tau < 1$, the first two integrals can be approximated as

$$\int_0^t F(\tau) K_N(-\tau)\, d\tau + \int_{1-t}^1 F(\tau) K_N(-\tau)\, d\tau$$
$$= F(0)\left(\int_0^t K_N(-\tau)\, d\tau + \int_{1-t}^1 K_N(-\tau)\, d\tau\right) + O\left(\varepsilon \int_0^1 K_N(\tau)\, d\tau\right)$$
$$= F(0)\left(\int_0^t K_N(-\tau)\, d\tau + \int_{1-t}^1 K_N(-\tau)\, d\tau\right) + O(\varepsilon),$$

having used that K_N is positive and integrates to 1. Moreover,

$$\int_0^t K_N(-\tau)\, d\tau + \int_{1-t}^1 K_N(-\tau)\, d\tau \to 1$$

as $N \to \infty$ by Lemma 1.1. Since

$$\sup_{t<\theta<1-t} |K_N(\theta)| = \sup_{t<\theta<1-t} \frac{1}{N+1} \frac{(\sin(\pi(N+1)\theta))^2}{(\sin(\pi\theta))^2} \to 0$$

as $N \to \infty$, we have

$$\int_t^{1-t} |F(\tau)||K_N(-\tau)|d\tau \le \sup_{t<\theta<1-t} |K_N(\theta)|\|F\|_{L^1} \to 0.$$

□

Fejér's theorem does not tell us that $S_N(F) \to F$ pointwise, which is not true in general. But $F * K_N$ is a trigonometric polynomial of degree at most N, whose n'th Fourier coefficient is $\widehat{F}(n)(1 - n/(N+1))$, which is very nearly $\widehat{F}(n)$ for N large.

1.3 Convergence in L^2

Our second investigation into convergence involves convergence in the metric $L^2([0,1])$. This is the space of functions $F : [0,1] \to \mathbb{C}$ with the metric

$$\|F\|_{L^2} = \left(\int_0^1 |F(\theta)|^2 d\theta \right)^{1/2}$$

which is an example of a *Hilbert space*. In this space, a sequence of functions F_N converges to F if

$$\|F - F_N\|_{L^2} \to 0.$$

First, the L^p analogue of Fejér's theorem. It requires the following lemma.

Lemma 1.5

If $1 \le p \le \infty$ and $F \in L^1([0,1])$ and $G \in L^p([0,1])$ then $F * G \in L^p([0,1])$ and

$$\|F * G\|_{L^p} \le \|F\|_{L^1}\|G\|_{L^p}.$$

Proof. The proof is just the (integral) triangle inequality for $p = \infty$. For finite p, let $H \in L^q([0,1])$ (with $1/q = 1 - 1/p$) be have $\|H\|_{L^q} \le 1$. We will use that L^p is dual to L^q. We have

$$\int_0^1 F * G(\theta)\overline{H}(\theta)d\theta = \int_0^1 F(\tau) \int_0^1 G(\theta - \tau)\overline{H}(\theta)d\theta d\tau$$

and by Hölder, the inner integral is at most $\|G\|_{L^p}$. Thus

$$\left| \int_0^1 F * G(\theta)\overline{H}(\theta)d\theta \right| \le \|G\|_{L^p}\|F\|_{L^1},$$

and this proves the lemma. □

Theorem 1.2: Fejér in L^p

We have $F * K_N \to F$ in $L^p([0,1])$. Trigonometric polynomials are dense in $L^p([0,1])$ for $p \geq 1$.

Proof. Suppose G is continuous and $\|F - G\|_{L^p} < \varepsilon$. Then

$$\|F * K_N - F\|_{L^p} \leq \|G * K_N - G\|_{L^p} + \|(F-G) * K_N\|_{L^p} + \|F - G\|_{L^p}.$$

The first quantity on the right can be made less than ε by Fejér's theorem and the Bounded Convergence Theorem, which can be applied since

$$\|G * K_N\|_{L^p} \leq \|G\|_{L^p} \|K_N\|_{L^1} = \|G\|_{L^p}.$$

Similarly, the middle and final terms are less than ε. Since continuous functions are dense in L^p, we have proved the theorem. □

Theorem 1.3

If $F \in L^2([0,1])$ then F is the limit of a convergent Fourier series with square-summable Fourier coefficients $\widehat{F}(n)$. Conversely, if $f : \mathbb{Z} \to \mathbb{C}$ is such that

$$\sum_{n \in \mathbb{Z}} |f(n)|^2$$

converges, then

$$F_N(\theta) = \sum_{|n| \leq N} f(n) e(n\theta)$$

converges to a function $F \in L^2([0,1])$.

Just like before, for an L^2 function F, we define

$$\widehat{F}(n) = \int_0^1 F(\theta) e(-n\theta) d\theta$$

which is well-defined since, by the triangle inequality and Cauchy-Schwarz,

$$\left| \int_0^1 F(\theta) e(-n\theta) d\theta \right| \leq \int_0^1 |F(\theta)| \, d\theta \leq \left(\int_0^1 1 d\theta \right)^{1/2} \left(\int_0^1 |F(\theta)|^2 d\theta \right)^{1/2} < \infty.$$

The second part of Theorem 1.3 is easy enough to establish using the fact that L^2 is a complete metric space.

Proof of second half of Theorem 1.3. We just need to show that the functions F_N form a Cauchy sequence. But for $N < M$

$$F_M(\theta) - F_N(\theta) = \sum_{N < |n| \leq M} f(n) e(n\theta)$$

and this is a trigonometric polynomial. By Parseval's identity,

$$\int_0^1 |F_M(\theta) - F_N(\theta)|^2 d\theta = \sum_{N<|n|\le M} |f(n)|^2 \le \sum_{N<|n|} |f(n)|^2$$

and the right hand side tends to zero by summability. □

To prove the other direction of Theorem 1.3 we need the following.

Lemma 1.6

Suppose $F \in L^2$ is such that $\widehat{F}(n) = 0$ for every $n \in \mathbb{Z}$. Then $F = 0$ almost everywhere.

Proof. From Lemma 1.2 we know that

$$\widehat{F * K_N}(n) = \left(1 - \frac{|n|}{N+1}\right)\widehat{F}(n).$$

Since $F * K_N$ is a trigonometric polynomial, we get from Plancherel that

$$\|F * K_N\|_{L^2}^2 = \sum_n \left(1 - \frac{|n|}{N+1}\right)^2 |\widehat{F}(n)|^2 = 0.$$

The proof concludes by using that $F * K_N \to F$ in L^2. □

Lemma 1.7: Bessel's inequality

For any function $F \in L^2([0,1])$, and any set of integers A we have

$$\sum_{a\in A} |\widehat{F}(a)|^2 \le \|F\|_{L^2}^2.$$

Proof. We have that

$$(F * K_N)(\theta) = \sum_{|n|\le N} \widehat{F}(n)\left(1 - \frac{|n|}{N+1}\right)e(n\theta),$$

so by Placherel's formula,

$$\|F * K_N\|_{L^2}^2 = \sum_{|n|\le N} |\widehat{F}(n)|^2\left(1 - \frac{|n|}{N+1}\right)^2 \ge \sum_{\substack{n\in A\\ |n|\le N}} |\widehat{F}(n)|^2\left(1 - \frac{|n|}{N+1}\right)^2.$$

But

$$\|F * K_N\|_{L^2} \le \|F\|_{L^2} + \|F - F * K_N\|_{L^2}$$

and taking $N \to \infty$ shows

$$\|F * K_N\|_{L^2} \le \|F\|_{L^2}.$$

□

Proof of first half of Theorem 1.3. By Bessel's inequality, we know that the sequence $|\widehat{F}(n)|$ is square-summable and so the polynomials $S_N(F)$ converge to a limit $\tilde{F}$ in L^2. But $F - \tilde{F}$ has everywhere vanishing Fourier coefficients, and so we must have $F = \tilde{F}$ almost everywhere by Lemma 1.3. □

2

SOME ADDITIVE COMBINATORICS

2.1 Fourier analysis in finite abelian groups

Let G be a finite abelian group written with addition, which we can always think of as $\mathbb{Z}/(m_1\mathbb{Z}) \oplus \cdots \oplus \mathbb{Z}/(m_r\mathbb{Z})$. There is a very simple form of Fourier analysis which works in this setting, which breaks any function $f : G \to \mathbb{C}$ into a linear of charcters.

Recall that a character γ is a function $\gamma : G \to S^1$ with

$$\gamma(a+b) = \gamma(a)\gamma(b).$$

For example, when $G = \mathbb{Z}/(N\mathbb{Z})$ then for any integer k with $0 \le k \le N-1$ we have the character

$$\gamma(n) = e(nk/N).$$

We can always multiply two characters γ and γ' pointwise to obtain a new character $\gamma \cdot \gamma'$:

$$(\gamma \cdot \gamma')(a) = \gamma(a)\gamma'(a).$$

If the set of characters of G is denoted G^*, then this multiplication turns G^* into a group with identity $\iota(a) \equiv 1$.

Lemma 2.1

The map $\boldsymbol{e}$ defined by $k \mapsto e(k/N\cdot)$ is an isomorphism from $\mathbb{Z}/(N\mathbb{Z})$ to $(\mathbb{Z}/(N\mathbb{Z}))^*$.

Proof. The map $\boldsymbol{e}$ is a group homomorphism as

$$(\boldsymbol{e}(k)\boldsymbol{e}(l))(n) = e(kn/N)e(ln/N) = e((k+l)n/N) = \boldsymbol{e}(k+l).$$

For k to be in the kernel of $\boldsymbol{e}$ we would need, in particular, that $e(k/N) = 1$ which means $k = 0$ and $\boldsymbol{e}$ is an injection. If γ is any character, then

$$1 = \gamma(0) = \gamma(N\cdot 1) = \gamma(1)^N$$

so that $\gamma(1)$ is an N'th root of unity, which means $\gamma(1) = e(k/N)$ for some k whence

$$\gamma(n) = \gamma(n\cdot 1) = \gamma(1)^n = e(kn/N).$$

□

Given two finite abelian groups, G_1 and G_2 with respective characters γ_1 and γ_2 we can define $\gamma_1 \oplus \gamma_2 : G_1 \oplus G_2 \to \mathbb{C}$ by

$$(\gamma_1 \oplus \gamma_2)(a_1, a_2) = \gamma_1(a_1)\gamma_2(a_2).$$

Lemma 2.2

The map $(\gamma_1, \gamma_2) \mapsto \gamma_1 \oplus \gamma_2$ defines an isomorphism from $G_1^* \oplus G_2^*$ to $(G_1 \oplus G_2)^*$.

Proof. Exercise. □

Theorem 2.1

If G is a finite abelian group, the set of all characters on G form a group called G^*, which is isomorphic to G. We also have the following formulae.

1. For any $\gamma \in \widehat{G}$,
$$\frac{1}{|G|}\sum_{a\in G}\gamma(a) = \begin{cases} 1 & \text{if } \gamma = \iota \\ 0 & \text{if } \gamma \neq \iota. \end{cases}$$
2. For any $a \in G^*$,
$$\frac{1}{|G|}\sum_{\gamma\in G^*}\gamma(a) = \begin{cases} 1 & \text{if } a = 0 \\ 0 & \text{if } a \neq 0. \end{cases}$$

Proof. The first part of the theorem comes from Lemma 2.1, the isomorphism

$$G \cong \mathbb{Z}/(m_1\mathbb{Z}) \oplus \cdots \oplus \mathbb{Z}/(m_r\mathbb{Z})$$

and Lemma 2.1. For the proof of (1), if $\gamma = \iota$ then the identity is immediate. If not, pick some s with $\gamma(s) \neq 0$. Then $a \mapsto a + s$ merely permutes the elements of G and so

$$\frac{1}{|G|}\sum_{a\in G}\gamma(a) = \frac{1}{|G|}\sum_{a\in G}\gamma(a+s) = \gamma(s)\left(\frac{1}{|G|}\sum_{a\in G}\gamma(a)\right)$$

and this can only happen if

$$\frac{1}{|G|}\sum_{a\in G}\gamma(a) = 0.$$

The proof of (2) follows from (1) and the isomorphism from G to G^*. The details are left to the reader. □

If f is a function on G and $\gamma \in G^*$, we define the Fourier coefficient of f at γ to be

$$\widehat{f}(\gamma) = \frac{1}{|G|}\sum_{a\in G} f(a)\overline{\gamma(a)}.$$

Fourier analysis on G is developed by the following theorem.

Theorem 2.2

Let $f, g : G \to \mathbb{C}$ be functions on a finite abelian group G. Then we have

Fourier inversion:

$$f(a) = \sum_{\gamma\in G^*}\widehat{f}(\gamma)\gamma(a),$$

Parseval's identity:

$$\frac{1}{|G|}\sum_{a\in G} f(a)\overline{g(a)} = \sum_{\gamma\in G^*}\widehat{f}(\gamma)\overline{\widehat{g}(\gamma)},$$

Plancherel's formula:

$$\frac{1}{|G|}\sum_{a\in G}|f(a)|^2 = \sum_{\gamma\in G^*}|\widehat{f}(\gamma)|^2.$$

Proof. The proof of each is a straightforward consequence of orthogonality. We prove (2), and leave the others as an exercise. The right hand side is

$$\sum_{\gamma\in G^*}\frac{1}{|G|^2}\sum_{a,b\in G} f(a)\overline{\gamma(a)g(b)}\gamma(b) = \frac{1}{|G|}\sum_{a,b\in G} f(a)\overline{g(b)}\cdot\frac{1}{|G|}\sum_{\gamma\in G^*}\gamma(b-a)$$

and the inner sum vanishes unless $b = a$, in which case it is 1. □

2.2 Patterns in $\mathbb{F}_p$

A big area of arithmetic combinatorics is *Ramsey theory*, which roughly states that one can find all sorts of patterns in large sets of data provided they are large enough. In arithmetic combinatorics, the sort of pattern we are looking for usually involves some arithmetic. In this case, we show that in any large set A of a finite field (where addition and multiplication make sense), we can find the sum and the product of two elements x and y. To be concrete, we'll work with a field of size p, but the proof works in general.

Theorem 2.3

Let p be a prime and let $\mathbb{F}_p$ be the field with p elements. Given any set $A \subseteq \mathbb{F}_p$ of size at least $100\sqrt{p}$, we can find $x, y \in \mathbb{F}_p$ such that $x+y$ and xy both belong to A.

We begin with a classical theorem about the Fourier coefficients of the squares (called Gauss sums).

Lemma 2.3

Let S be the set of squares in $\mathbb{F}_p$. Then

$$|\widehat{\mathbf{1}_S}(r)| = \begin{cases} \frac{p+1}{2p} & \text{if } r = 0 \\ \frac{1}{2\sqrt{p}} + O\left(\frac{1}{p}\right) & \text{if } r \neq 0. \end{cases}$$

Proof. First,

$$|\widehat{\mathbf{1}_S}(0)| = \frac{1}{p} \sum_{x \in \mathbb{F}_p} \mathbf{1}_S(x) = \frac{|S|}{p}.$$

One square is 0, and there are $(p-1)/2$ elements counting the remaining $|S|-1$ elements. Indeed, the map $x \mapsto x^2$ is a two-to-one map from the units to the non-zero squares.

For the remaining coefficients, we first observe that

$$\left| \sum_{x \in \mathbb{F}_p} e(rx^2/p) \right|^2 = \sum_{x,y \in \mathbb{F}_p} e(r(x^2-y^2)/p) = \sum_{x,y \in \mathbb{F}_p} e(r(x-y)(x+y)/p)$$

and we can make the invertible change of variables $u = x-y$, $v = x+y$ to get

$$\left| \sum_{x \in \mathbb{F}_p} e(rx^2/p) \right|^2 = \sum_{u \in \mathbb{F}_p} \sum_{v \in \mathbb{F}_p} e(ruv/p) = p$$

since the inner sum over v vanishes unless $u = 0$, in which case the inner sum is p. To conclude the proof

$$\widehat{\mathbf{1}_S}(r) = \frac{1}{p} + \frac{1}{2p} \sum_{x \neq 0} e(rx^2/p).$$

□

Proof of Theorem 2.2. We first observe that if $a, b \in A$ and $f(t) = t^2 - at + b$ is a quadratic polynomial with roots x and y, then by factoring f, we get

$$t^2 - (x+y)t + xy = (t-x)(t-y) = f(t) = t^2 - at + b$$

so that $x + y = a$ and $xy = b$. This means we need to show that there are $a, b \in A$ such that $t^2 - at + b$ factors. By the quadratic formula (which you can check works in $\mathbb{F}_p$) this is the same as showing that the discriminant $a^2 - 4b$ is a square in $\mathbb{F}_p$. This can be detected by

$$\sum_{a,b \in A} \mathbf{1}_S(a^2 - 4b) = \sum_{a,b \in A} \sum_r \widehat{\mathbf{1}_S}(r) e((a^2 - 4b)r/p)$$

where S is the set of squares in $\mathbb{F}_p$, and the equality follows by Fourier inversion.

Denote the contribution to the sum from $r = 0$ by M. Then

$$M = \widehat{\mathbf{1}_S}(0)|A|^2 = |A|^2 \cdot \frac{1}{p} \sum_{r \in \mathbb{F}_p} \mathbf{1}_S(r) e(0 \cdot r/p) = \frac{|A|^2|S|}{p}$$

and since there are $(p+1)/2$ squares in $\mathbb{F}_p$, we get

$$M = |A|^2 \cdot \frac{p+1}{2p} > \frac{|A|^2}{2}.$$

Next if

$$E = \sum_{r \neq 0} \widehat{\mathbf{1}_S}(r) \sum_{a,b \in A} e((a^2 - 4b)r/p)$$

then by the triangle inequality and the upper bound from Lemma 2.2, we have

$$|E| \leq \frac{1}{\sqrt{p}} \sum_{r \in \mathbb{F}_p} \left| \sum_{a \in A} e(ra^2/p) \right| \cdot \left| \sum_{b \in A} e(-4rb/p) \right|.$$

By Cauchy-Schwarz

$$|E|^2 \leq \frac{1}{p} \left(\sum_{r \in \mathbb{F}_p} \left| \sum_{a \in A} e(ra^2/p) \right|^2 \right) \left(\sum_{r \in \mathbb{F}_p} \left| \sum_{b \in A} e(-4rb/p) \right|^2 \right).$$

The second set of brackets is just

$$p^2 \sum_{r \in \mathbb{F}_p} |\widehat{\mathbf{1}_A}(4r)|^2 = p|A|$$

by Plancherel. The first set of brackets is

$$p^2 \sum_{r \in \mathbb{F}_p} |\widehat{f}(-r)|^2 = p \sum_{x \in \mathbb{F}_p} |f(x)|^2$$

where

$$f(x) = |\{a \in A : a^2 = x\}|$$

and we have again used Plancherel. But

$$\sum_x |f(x)|^2 \leq 4|A|$$

so we can conclude

$$|E| \leq 2|A|\sqrt{p}.$$

Since

$$\frac{|E|}{M} \leq \frac{4\sqrt{p}}{|A|} < 1$$

we have $M > |E|$ and so $M + E \geq M - |E| > 0$. □

2.3 Covering $\mathbb{F}_p$ by sums of products

Let A be a subset of $\mathbb{F}_p$ and denote

$$k \cdot AA = \{a_1 a_1' + \cdots + a_k a_k' : a_i, a_i' \in A\}.$$

Now $\mathbb{F}_p$ doesn't have any subfields, but if it did, and A were such a subfield, then we would have

$$k \cdot AA = A.$$

In this section, we'll show that $3 \cdot AA$ is all of $\mathbb{F}_p$ for all sets A with $|A| > p^{3/4}$. In particular, $3 \cdot AA$ is much larger than A.

Theorem 2.4

Let $A \subseteq \mathbb{F}_p$ be such that $|A| > p^{3/4}$. Then $3 \cdot AA = \mathbb{F}_p$.

Proof. We need to show that for $x \in \mathbb{F}_p$,

$$N_x = \sum_{a_1,\ldots,a_6 \in A} \mathbf{1}_{\{x\}}(a_1 a_2 + a_3 a_4 + a_5 a_6) > 0.$$

This can be detected with the Fourier transform:

$$N_x = \frac{1}{p} \sum_{r \in \mathbb{F}_p} \sum_{a_1,\ldots,a_6 \in A} e(r(x - a_1 a_2 - a_3 a_4 - a_5 a_6)/p).$$

The right hand side can be rewritten as

$$N_x = \frac{1}{p}\sum_{r\in\mathbb{F}_p} e(rx/p)\left(\sum_{a_1,a_2\in A} e(-ra_1a_2/p)\right)^3.$$

Like we did in the previous section, we extract the $r=0$ term to get $M=|A|^6/p$. For $r\neq 0$, we write

$$S_r = \sum_{a_1,a_2} e(-ra_1a_2/p) = p\sum_{a_1}\widehat{\mathbf{1}_A}(ra_1).$$

Then

$$|S_r|^2 \leq p^2\left(\sum_{a_1\in\mathbb{F}_p}\mathbf{1}_A(a_1)|\widehat{\mathbf{1}_A}(ra_1)|\right)^2 \leq p^2\left(\sum_{a_1\in\mathbb{F}_p}\mathbf{1}_A(a_1)^2\right)\left(\sum_{a_1\in\mathbb{F}_p}|\widehat{\mathbf{1}_A}(ra_1)|^2\right)$$

and by Plancherel, we get

$$|S_r|^2 \leq p|A|^2.$$

So, we have

$$N_x \geq \frac{|A|^6}{p} - \frac{1}{p}\sum_{r\in\mathbb{F}_p}|S_r|^3 \geq \frac{|A|^6}{p} - \sqrt{p}|A|\frac{1}{p}\sum_{r\in\mathbb{F}_p}|S_r|^2.$$

We can also write

$$S_r = p\widehat{f}(r)$$

where

$$f(y) = |\{(a_1,a_2)\in A^2 : a_1a_2 = y\}|.$$

By Plancherel again,

$$\sum_{r\in\mathbb{F}_p}|S_r|^2 = p\sum_{y\in\mathbb{F}_p}f(y)^2 = p|\{(a_1,a_2,a_3,a_4)\in A^4 : a_1a_2 = a_3a_4\}|$$

and this is at most $|A|^3/p$. So our error term E is at most $\sqrt{p}|A|^4$. We just need to check this is smaller than the main term and indeed

$$\frac{|E|}{M} \leq \frac{\sqrt{p}|A|^4}{|A|^6/p} = \frac{p^{3/2}}{|A|^2} < 1.$$

□

3

MOMENTS OF TRIGONOMETRIC POLYNOMIALS

3.1 Good partitions and Chang's Theorem

Let

$$S = \bigsqcup_{k=0}^{\infty} S_k$$

be a partition of a set $S \subseteq \mathbb{Z}$. We say the partition is a *good* partition if the following holds. If

$$a_1 + \cdots + a_l = a_{l+1} + \cdots + a_{2l}$$

for some integers $a_1, \ldots, a_{2l}$ then for some distinct i, j, the number a_i and a_j belong to the same part.

Example (Lacunary good partition)**.** *Let $S_k = \{n : 2^{k-1} \leq |n| < 2^k\}$ and $S_0 = \{0\}$, and set*

$$S = \bigcup_{k=0}^{\infty} S_{2k}.$$

Then if

$$a_1 + \cdots + a_l = a_{l+1} + \cdots + a_{2l}$$

we can rearrange the equation so that both sides have only positive integers, say

$$\sum_{i \in I} b_i = \sum_{j \in J} b_j$$

where $b_i = |a_i|$ and I and J are non-empty sets of indices. Suppose each a_j belongs to a distinct S_{k_j}. Then so do the b_j. Let b_{i_0} be the (unique) value of b_{i_0} for which k_{i_0} is maximal, and we assume $i_0 \in I$. Then the right hand side is certainly at most

$$\sum_{j \le k_{i_0}-2} 2^j < 2^{k_{i_0}-1} \le b_{i_0} \le \sum_{i \in I} b_i$$

which is a contradiction. We can perform a similar decomposition for those S_{2k+1}, and in doing so cover all of $\mathbb{Z}$ with a pair of good partitions.

Example (Chang's good partition)**.** *Let p be a prime and for a non-zero integer n, let $v_p(n)$ denote the exponent of p in the factorization of n. Let $S_k = \{n : v_p(n) = k\}$ and $S_0 = \{0\}$, and take $S = \mathbb{Z}$. Then if*

$$a_1 + \cdots + a_l = a_{l+1} + \cdots + a_{2l}$$

and the a_i belong to distinct values of S_k, let i_0 be such that k_{i_0} is minimal. Then $p^{k_{i_0}} | a_i$ for each i, so

$$(a_1/p^{k_{i_0}}) + \cdots + (a_l/p^{k_{i_0}}) = (a_{l+1}/p^{k_{i_0}}) + \cdots + (a_{2l}/p^{k_{i_0}}).$$

Only $a_{i_0}/p^{k_{i_0}}$ is not divisible by p, so reducing everything modulo p gives a contradiction.

Theorem 3.1

Let $\{S_k\}$ be a good partition. For trigonometric polynomial F write

$$F_k(\theta) = \sum_{n \in S_k} \widehat{F}(n) e(n\theta),$$

and $\widehat{F} \ge 0$. Then for any even integer $q = 2l \ge 2$, there is a constant C_q such that

$$\|F\|_{L^q([0,1])} \ll \binom{q}{2}^{1/2} \left(\sum_k \|F_k\|^2_{L^q([0,1])} \right)^{1/2}.$$

Proof. We have

$$\|F\|^{2l}_{L^{2l}([0,1])} = \int_0^1 \left| \sum_k F_k(\theta) \right|^{2l} d\theta = \sum_{k_1,\ldots,k_{2l}} \int_0^1 F_{k_1}(\theta) \cdots F_{k_l}(\theta) \overline{F_{k_{l+1}}(\theta)} \cdots \overline{F_{k_{2l}}(\theta)} d\theta.$$

The product in the integrand on the right is

$$\sum_{n_1 \in S_{k_1}} \cdots \sum_{n_{2l} \in S_{k_{2l}}} \widehat{F}(n_1) \cdots \widehat{F}(n_{2l}) e((n_1 + \cdots + n_l - n_{l+1} - \cdots - n_{2l})\theta)$$

and these exponentials integrate to 0 unless

$$n_1 + \cdots + n_l = n_{l+1} + \cdots + n_{2l},$$

in which case they integrate to $\widehat{F}(n_1)\cdots\widehat{F}(n_{2l})$ which is positive. Since $n_i \in S_{k_i}$, the good partition property forces two of the k_i to be the same. Letting j_1, j_2 denote the respective indices of the first instance of $k_{j_1} = k_{j_2}$, we have

$$\sum_{k_1,\ldots,k_{2l}} \int_0^1 F_{k_1}(\theta)\cdots F_{k_l}(\theta) F_{k_{l+1}}(-\theta)\cdots F_{k_{2l}}(-\theta)\,d\theta \leq S_1 + S_2 + S_3$$

where

$$S_1 = \sum_{j_1,j_2\leq l} \sum_k \int_0^1 F_k(\theta)^2 F(\theta)^{l-2}\cdot F(-\theta)^l\,d\theta,$$

$$S_2 = \sum_{j_1\leq l<j_2} \sum_k \int_0^1 |F_k(\theta)|^2 |F(\theta)|^{2l-2}\,d\theta,$$

and

$$S_3 = \sum_{j_1,j_2\geq l} \sum_k \int_0^1 F_k(-\theta)^2 F(\theta)^{l}\cdot F(-\theta)^{l-2}\,d\theta.$$

By the integral triangle inequality, each of the integrals in S_1, S_2 and S_3 is at most

$$\int_0^1 |F_k(\theta)|^2 |F(\theta)|^{2l-2}\,d\theta \leq \|F_k\|_{L^{2l}}^2 \|F\|_{L^{2l}}^{2l-2},$$

the last inequality being Hölder. Combining all the different sums, we summarize

$$\|F\|_{L^{2l}([0,1])}^{2l} \leq \binom{2l}{2} \sum_k \|F_k\|_{L^{2l}}^2 \|F\|_{L^{2l}}^{2l-2}$$

or

$$\|F\|_{L^{2l}([0,1])} \leq \binom{2l}{2}^{1/2} \left(\sum_k \|F_k\|_{L^{2l}}^2\right)^{1/2}.$$

□

3.2 Chang's Theorem

The Erdős-Szemerédi Sum-Product conjecture states that for any finite set of positive integers, A, we have that for any $\varepsilon > 0$

$$\max\{|A+A|, |A\cdot A|\} \gg_\varepsilon |A|^{2-\varepsilon}.$$

Mei-Chu Chang proved a sum-product type theorem which works very well then A is a set of integers which defines very few products.

Theorem 3.2: Chang

Let A be a finite set of integers and let $l \geq 2$ be an integer. Suppose $|A\cdot A| \leq K|A|$ for some constant K. Then

$$\int_0^1 \left|\sum_{a\in A} e(a\theta)\right|^{2l} d\theta \leq C_{K,l}|A|^l.$$

This theorem relies on controlling the prime factorization of different integers in A. Because A defines so few products, it should be that there are very few "independent" primes appearing in the factorization of different a in A. For example, if A consisted only of distinct primes, then all pairwise products would be distinct as well. The tool for controlling the primes is Freiman's Lemma.

Lemma 3.1: Freiman's Lemma

Let B be a subset of $\mathbb{R}^d$ not contained in any affine subspace. Then $|B+B| \geq (d+1)|B| - d^2$.

Proof. The proof of this lemma proceeds by induction on d and $|B|$. We will work with midpoints, instead of sums, but cardinalities are the same. Let $\mathscr{C}$ be the convex hull of B, which is some convex body in $\mathbb{R}^d$. The boundary of this body contains a number of vertices (extreme points). Let v_0 be such a point. Let $\mathscr{C}'$ be the convex hull of $B \setminus \{v_0\}$, which is smaller than $\mathscr{C}$ because we removed an extreme point. There are d vertices v on the boundary of $\mathscr{C}'$ which are visible to v_0 in the sense that the line from v_0 to v does not pass through $\mathscr{C}'$. To see this, pick a maximal set $\{v_1, \ldots, v_k\}$ of extreme points which are visible to v_0. If $k < d$, then the set $\{v_0, \ldots, v_k\}$ lies in an affine hyperplane. But B is not contained in such a hyperplane, and so there must be an extreme point of $\mathscr{C}'$ not in this plane. There must therefore be a point which is visible to v_0, contradicting maximality. So $k \geq d$. Now there are two cases. Either $\mathscr{C}'$ is contained in an affine subspace V of dimension $d-1$, or not. In the former case, by induction, the set $B' = B \setminus \{v_0\}$ defines

$$|B'+B'| \geq d|B'| - (d-1)^2$$

midpoints, and these all lie in V. In addition, there are $|B|-1$ distinct midpoints between v_0 and B' which lie outside of V, as well as $(v_0+v_0)/2$, making for

$$|B| + d(|B|-1) - (d-1)^2 = (d+1)|B| - (d-1)^2 - d > (d+1)|B| - d^2.$$

If $\mathscr{C}'$ is not contained in an affine hyperplane, then $|B'+B'| \geq (d+1)(|B|-1) - d^2$ by induction, and defines as many midpoints which belong to $\mathscr{C}'$ by convexity. In addition, the points $(v_j+v_0)/2$ are distinct and lie outside $\mathscr{C}'$ since v_0 is an extreme point of $\mathscr{C}$. This makes for a total of

$$d + 1 + (d+1)(|B|-1) - d^2 = (d+1)|B| - d^2$$

midpoints, closing the induction. □

Lemma 3.2

Suppose $V \subseteq \mathbb{R}^d$ is an affine subspace of dimension at most K. Show there is a set $I \subseteq \{1,\dots,d\}$ with $|I| \leq K$ and such that projection

$$\sum_{k=1}^{d} c_k \boldsymbol{e}_k \mapsto \sum_{k\in I} c_k \boldsymbol{e}_k$$

is injective.

Proof. Exercise. □

Proof of Chang's Theorem. let $\mathscr{P}$ be the set of all primes (a finite set) which appear in the factorization of various elements of A. We can enumerate $\mathscr{P} = \{p_1,\dots,p_d\}$. Then the map

$$v(p_1^{r_1}\cdots p_d^{r_d}) = (r_1,\dots,r_d)$$

defines a map from A to $\mathbb{R}^d$ with the property that $v(A\cdot A) = v(A) + v(A)$. The assumption $|A\cdot A| \leq K|A|$ means that $|v(A)+v(A)| \leq K|A|$ and so A lies in an affine subspace V of dimension no more than K, by Freiman's Lemma. By Lemma 3.2, we can find a set I of at most K coordinates such that the projection of V onto these coordinates is injective. In particular, the projection of $v(A)$ onto coordinates from I is injective. This means that if we know the exponents of the primes p_i with $i \in I$ as they appear in the factorization of $a \in A$, then we can recover A. By relabeling, we can assume $I = \{1,\dots,r\}$ with $r \leq K$.

Inductively define the sets

$$A \supseteq A_{k_1} \supseteq A_{k_1,k_2} \supseteq \cdots \supseteq A_{k_1,\dots,k_r}$$

by letting

$$A_{k_1,\dots,k_j} = \{a \in A_{k_1,\dots,k_{j-1}} : v_{p_j}(a) = k_j\}$$

which are obtained from A by fixing the powers of the primes p_j appearing in $a \in A$, one at a time. Since we can recover $a \in A$ from knowing the exponents of $p_1,\dots,p_r$, we must that that each $A_{k_1,\dots,k_r}$ is empty or a singleton. Fixing the exponent of a prime in the prime factorization defines a good partition, so writing

$$F_A(\theta) = \sum_{a\in A} e(a\theta)$$

and similarly defining $F_{A_{k_1,\dots,k_j}}(\theta)$,

$$\begin{aligned}
\|F_A\|^2_{L^{2l}([0,1])} &\leq \binom{2l}{l} \sum_{k_1} \|F_{A_{k_1}}\|^2_{L^{2l}([0,1])} \\
&\leq \binom{2l}{l}^2 \sum_{k_1,k_2} \|F_{A_{k_1,k_2}}\|^2_{L^{2l}([0,1])} \\
&\vdots \\
&\leq \binom{2l}{l}^r \sum_{k_1,\dots,k_r} \|F_{A_{k_1,\dots,k_r}}\|^2_{L^{2l}([0,1])} \\
&\leq \binom{2l}{l}^r |A|.
\end{aligned}$$

The final inequality is because $F_{A_{k_1,\dots,A_{k_r}}}$ is a single exponential if there is some $a \in A$ (uniquely determined), belonging to $A_{k_1,\dots,A_{k_r}}$. □

To turn Chang's theorem into a sum-product type statement, notice that $\widehat{F_A}(n) = \mathbf{1}_A(n)$ and that $\widehat{(F_A^l)}(n) = \mathbf{1}_A *^{l\times} \cdots * \mathbf{1}_A(n)$ is the number of representations

$$n = a_1 + \cdots + a_l$$

of n as a sum of l elements of A, which is supported on the set $A +^{l\times} \cdots +^{} A$. So Plancherel applied to F_A^l gives

$$\int_0^1 |F_A(\theta)|^{2l} d\theta = \int_0^1 |F_A(\theta)^l|^2 d\theta = \sum_n \mathbf{1}_A * \cdots * \mathbf{1}_A(n)^2.$$

Since the map $(a_1,\dots,a_l) \mapsto a_1 + \cdots + a_l$ tells us

$$\sum_n \mathbf{1}_A * \cdots * \mathbf{1}_A(n) = |A|^l$$

we have by Cauchy-Schwarz that

$$\begin{aligned}
|A|^{2l} &= \left(\sum_{n \in A+\cdots+A} \mathbf{1}_A * \cdots * \mathbf{1}_A(n) \right)^2 \\
&\leq |A+\cdots+A| \sum_{n \in A+\cdots+A} \mathbf{1}_A * \cdots * \mathbf{1}_A(n)^2 \\
&= |A+\cdots+A| \int_0^1 |F_A(\theta)|^{2l} d\theta \\
&\leq |A+\cdots+A| C_{K,l} |A|^l
\end{aligned}$$

which proves the following corollary.

Corollary 3.1

Let A be a finite set of integers and let $l \geq 2$ be an integer. Suppose $|A \cdot A| \leq K|A|$ for some constant K. Then

$$|A + \overset{l\times}{\cdots} + A| \gg_{K,l} |A|^l.$$

3.3 Rudin's Inequality

Rudin's inequality is one of the fundamental results used when applying Fourier analysis to arithmetic combinatorics. To state it, we need a definition.

Definition 3.1: Dissociated Set

A finite set Λ in an abelian group G is called dissociated if for any subset $\Lambda' \subseteq \Lambda$, the sum

$$S_{\Lambda'} = \sum_{\lambda \in \Lambda'} \lambda$$

is distinct. In other words, for any non-zero function $w : \Lambda \to \{-1, 0, 1\}$, we have

$$\sum_{\lambda \in \Lambda} w(\lambda) \cdot \lambda \neq 0.$$

Exercise. *Check that the "in other words" part of the above definition is justified.*

The dissiociated condition is a quantitative version of independence, and if $G = \mathbb{F}_2^d$ then it really is just saying that Λ forms an independent set. It is also an arithmetic version of probabilistic independence. To motivate this fact we recall Khintchine's inequality.

Theorem 3.3: Khintchine's inequality

Let $X_1, \ldots, X_n$ be independent with $X_j = \pm 1$ with equal probability. Then for any complex numbers $c_1, \ldots, c_n$ and any positive integer k,

$$\mathbb{E}\left|\sum_{j=1}^n c_j X_j\right|^{2k} \leq C_k \left(\sum_{j=1}^n |c_j|^2\right)^k.$$

First proof. We expand

$$\left|\sum_{j=1}^n c_j X_j\right|^{2k} = \sum_{1 \leq j_1, j_1', \ldots, j_k, j_k \leq n} c_{j_1} \cdots c_{j_k} \overline{c_{j_1'}} \cdots \overline{c_{j_k'}} X_{j_1} X_{j_1'} \cdots X_{j_k} X_{j_k'}.$$

Now write r_l for the number of times X_l appears in the product $X_{j_1} X_{j_1'} \cdots X_{j_k} X_{j_k'}$, so

that

$$X_{j_1} X_{j'_1} \cdots X_{j_k} X_{j'_k} = X_1^{r_1} \cdots X_n^{r_n}.$$

But $\mathbb{E}(X^{r_j}) = 0$ if r_j is odd, and is 1 if r_j is even. So the only terms which survive taking expectation are the ones where all r_j are even. This gives a bound of the form

$$\mathbb{E}\left|\sum_{j=1}^n c_j X_j\right|^{2k} \leq C_k \sum_{1 \leq j_1 \leq \cdots \leq j_k \leq n} |c_{j_1}|^2 \cdots |c_{j_k}|^2 = C_k \left(\sum_{1 \leq j \leq n} |c_j|^2\right)^k.$$

□

The number C_k has a combinatorial interpretation, and we could work it out explicitly, but instead we will try a different proof strategy.

Second proof. First we bound

$$\mathbb{E}\left|\exp\left(t\sum_{j=1}^n c_j X_j\right)\right| = \mathbb{E}\left(\exp\left(t\sum_{j=1}^n \Re(c_j) X_j\right)\right)$$

for t a real number. We may assume that the c_j are themselves real. Expanding

$$\mathbb{E}\left(\exp\left(t\sum_{j=1}^n c_j X_j\right)\right) = \frac{1}{2^k} \sum_{X_1=\pm 1} e(tc_1 X_1) \cdots \sum_{X_n=\pm 1} e(tc_n X_n) = \prod_{j=1}^n \left(\frac{e^{c_j t} + e^{-c_j t}}{2}\right)$$

and from the inequality $\cosh(x) \leq e^{x^2/2}$ (which can be seen from Taylor expansion) we have

$$\mathbb{E}\left(\exp\left(t\sum_{j=1}^n c_j X_j\right)\right) \leq \exp\left(\frac{t^2}{2}\sum_j c_j^2\right).$$

From this and Markov's inequality

$$\mathbb{P}\left(\left|\sum_{j=1}^n c_j X_j\right| \geq s\right) \leq \exp(-ts)\exp\left(\frac{t^2}{2}\sum_j c_j^2\right).$$

Setting

$$t = \frac{s}{\sum_j c_j^2},$$

we see that

$$\mathbb{P}\left(\left|\sum_{j=1}^n c_j X_j\right| \geq s\right) \leq \exp\left(-\frac{s^2}{2}\left(\sum_j c_j^2\right)^{-1}\right).$$

Now the p'th moment of Y is just

$$\mathbb{E}(Y^p) = p\int_0^\infty u^{p-1}\mathbb{P}(Y \geq u)\,du$$

so

$$\mathbb{E}\left|\sum_{j=1}^n c_j X_j\right|^p \leq p\int_0^\infty u^{p-1}\exp\left(-u^2/\left(2\sum_j c_j^2\right)\right)du$$

which, after an appropriate substitution, works out to

$$\mathbb{E}\left|\sum_{j=1}^{n} c_j X_j\right|^p \leq p2^{p/2}\Gamma(p/2)\left(\sum_j c_j^2\right)^{p/2}.$$

□

Rudin's inequality replaces the random variables in Khintchine's inequality with characters. The dissociative condition means that these characters are sufficiently independent. The proof uses aspects of both proofs presented above.

Theorem 3.4: Rudin's inequality

Let Λ be a dissociated subset of characters of a finite group G, and let c_λ be a complex number for each $\lambda \in \Lambda$. Then

$$\frac{1}{|G|}\sum_{x\in G}\exp\left(t\Re\left(\sum_{\lambda\in\Lambda} c_\lambda\lambda(x)\right)\right) \leq \exp\left(t^2/2\sum_\lambda |c_\lambda|^2\right).$$

It follows that

$$\frac{1}{|G|}\left|\left\{x\in G : \left|\sum_{\lambda\in\Lambda} c_\lambda\lambda(x)\right| \geq s\right\}\right| \leq 4\exp\left(-\frac{s^2}{4}\left(\sum_\lambda |c_\lambda|^2\right)^{-1}\right).$$

and

$$\frac{1}{|G|}\sum_{x\in G}\left|\sum_{\lambda\in\Lambda} c_\lambda\lambda(x)\right|^{2k} \ll k^k\left(\sum_{\lambda\in\Lambda}|c_\lambda|^2\right)^k.$$

Proof. Write $c_\lambda = r_\lambda\theta_\lambda$ where $r_\lambda \geq 0$ and θ_λ is a complex number of unit modulus (i.e. in polar coordinates). For $u \geq 0$ and $-1 \leq v \leq 1$ we have that $f(v) = \exp(uv)$ is convex, which means

$$\begin{aligned} e^{uv} &= f\left(\frac{1+v}{2}\cdot 1 + \frac{1-v}{2}\cdot(-1)\right) \\ &\leq \left(\frac{1+v}{2}\right)f(1) + \left(\frac{1-v}{2}\right)f(-1) \\ &= \frac{e^u + e^{-u}}{2} + v\frac{e^u - e^{-u}}{2} \\ &= \cosh(u) + v\sinh(u). \end{aligned}$$

and from this

$$\exp\left(t\Re\left(c_\lambda\lambda(x)\right)\right) \leq \cosh(tr_\lambda) + \Re\left(\theta_\lambda\lambda(x)\right)\sinh(tr_\lambda).$$

Taking products,

$$\exp\left(t\Re\left(\sum_\lambda c_\lambda\lambda(x)\right)\right) \leq \prod_{\lambda\in\Lambda}\left(\cosh(tr_\lambda) + \Re\left(\theta_\lambda\lambda(x)\right)\sinh(tr_\lambda)\right),$$

and then averaging over x gives

$$\frac{1}{|G|}\sum_{x\in G}\exp\left(t\Re\left(\sum_{\lambda}c_\lambda\lambda(x)\right)\right)\le\frac{1}{|G|}\sum_{x\in G}\prod_{\lambda\in\Lambda}(\cosh(tr_\lambda)+\Re(\theta_\lambda\lambda(x))\sinh(tr_\lambda))$$
$$=\frac{1}{|G|}\sum_{x\in G}\prod_{\lambda\in\Lambda}\left(\cosh(tr_\lambda)+\frac{1}{2}(\theta_\lambda\lambda(x))\sinh(tr_\lambda)+\frac{1}{2}\left(\overline{\theta_\lambda\lambda(x)}\right)\sinh(tr_\lambda)\right).$$

When we expand the product, we will get terms that involve some product of λ and $\overline{\lambda}$, and because of dissociativity, any such product will disappear when we average over x. Thus the only surviving term is the product of $\cosh(tr_\lambda)$, and this means

$$\frac{1}{|G|}\sum_{x\in G}\exp\left(t\Re\left(\sum_{\lambda}c_\lambda\lambda(x)\right)\right)\le\prod_{\lambda\in\Lambda}(\cosh(tr_\lambda))\le\exp\left(\frac{t^2}{2}\sum_{\lambda\in\Lambda}r_\lambda^2\right).$$

This is the first claimed statement of the theorem.

By Markov,

$$\frac{1}{|G|}\left|\left\{x\in G:\Re\sum_{\lambda\in\Lambda}c_\lambda\lambda(x)\ge s\right\}\right|\le\exp\left(-\frac{s^2}{2}\left(\sum_{\lambda}|c_\lambda|^2\right)^{-1}\right).$$

Replacing c_λ with $e(\theta)c_\lambda$, we have

$$\frac{1}{|G|}\left|\left\{x\in G:e(-\theta)\Re\sum_{\lambda\in\Lambda}c_\lambda\lambda(x)\ge s\right\}\right|\le\exp\left(-\frac{s^2}{2}\left(\sum_{\lambda}|c_\lambda|^2\right)^{-1}\right).$$

The event that

$$\left|\sum_{\lambda\in\Lambda}c_\lambda\lambda(x)\right|\ge s$$

is covered by the four events

$$e(\theta)\Re\sum_{\lambda\in\Lambda}c_\lambda\lambda(x)\ge s/2$$

with $\theta=0,\pi/3,\pi,3\pi/2$, so

$$\frac{1}{|G|}\left|\left\{x\in G:\left|\sum_{\lambda\in\Lambda}c_\lambda\lambda(x)\right|\ge s\right\}\right|\le 4\exp\left(-\frac{s^2}{4}\left(\sum_{\lambda}|c_\lambda|^2\right)^{-1}\right).$$

The rest is similar to how we proved Khintchine's inequality. □

Corollary 3.2: Chang's Structure Theorem

Let A be a subset of $\mathbb{F}_p$ with density $|A|/p=\alpha$. Let

$$\mathrm{Spec}_\varepsilon(A)=\{r\in\mathbb{F}_p:|\widehat{\mathbf{1}_A}(r)|\ge\varepsilon\cdot\alpha\}.$$

Then there is a dissociated set Λ such that

$$\mathrm{Spec}_\varepsilon(A)\subseteq\langle\Lambda\rangle=\left\{\sum_{\lambda\in\Lambda}w(\lambda)\cdot\lambda:w:\Lambda\to\{-1,0,1\}\right\}$$

and $|\Lambda|\ll\varepsilon^{-2}(1+\log(1/\alpha))$.

Proof. Let Λ be any subset of $\mathrm{Spec}_\varepsilon(A)$ which is maximal (with respect to cardinality) and dissociated. If $r \in \mathrm{Spec}_\varepsilon(A)$ does not belong to Λ, then by maximality, $\{r\} \cup \Lambda$ is not dissociated which means there is a function $w : \{r\} \cup \Lambda \to \{-1, 0, 1\}$, not identically 0, with

$$w(r) \cdot r + \sum_{\lambda \in \Lambda} w(\lambda) \cdot \lambda = 0.$$

Because Λ is dissociated, it cannot be that $w(r) = 0$, so we may assume $w(r) = -1$ whence

$$r = \sum_{\lambda \in \Lambda} w(\lambda) \cdot \lambda \in \langle \Lambda \rangle.$$

Since each $\lambda \in \Lambda$ belongs to $\mathrm{Spec}_\varepsilon(A)$, we have

$$\theta(\lambda) \frac{1}{p} \sum_{a \in A} e(-a\lambda/p) \geq \varepsilon\alpha$$

for some complex number $\theta(\lambda)$ of unit modulus. Extend θ to a function on $\mathbb{F}_p$ by setting $\theta = 0$ outside of Λ. Then

$$\sum_{a \in A} \widehat{\theta}(a) = \frac{1}{p} \sum_{a \in A} \sum_{\lambda \in \Lambda} \theta(\lambda) e(-a\lambda/p) \geq \varepsilon\alpha|\Lambda|.$$

Thus

$$\varepsilon\alpha|\Lambda| \leq \frac{1}{p} \sum_{a \in A} |p \cdot \widehat{\theta}(a)| = \frac{1}{p} \int_0^\infty \left| \{a \in A : |p \cdot \widehat{\theta}(a)| \geq s\} \right| ds$$

The integrand is bounded by $|A|$, trivially, and by $4p\exp(-s^2/4|\Lambda|)$, using Rudin's inequality. Splitting the integral

$$\frac{1}{p} \int_0^T |A| ds + \int_T^\infty 4\exp(-s^2/4|\Lambda|) ds \ll T\alpha + |\Lambda|^{1/2} \exp(-T^2/4|\Lambda|).$$

Take $T = 2|\Lambda|^{1/2}(\log(1/\alpha))^{1/2}$, and we get

$$\varepsilon\alpha|\Lambda| \ll \alpha|\Lambda|^{1/2} \left((\log(1/\alpha))^{1/2} + 1 \right).$$

□

3.4 Littlewood's Problem

Suppose $A = \{a_1 < \ldots < a_N\} \subseteq \mathbb{Z}^+$ and $f : \mathbb{N} \to \mathbb{C}$ is a function supported on A. We are going to study the trigonometric polynomial

$$F_A(\theta) = \sum_{a \in A} f(a) e(a\theta).$$

Specifically we will establish the bound

$$\|F_A\|_1 = \int_0^1 |F_A(\theta)| d\theta \gg \log N$$

provided $|f(a)| \geq 1$ for each $a \in A$. This was conjectured by Littlewood and proved independently by McGehee-Pigno-Smith and Konyagin. For a function $g : \mathbb{T} \to \mathbb{C}$ we define its Fourier transform

$$\widehat{g} : \mathbb{Z} \to \mathbb{C}$$

given by

$$\widehat{g}(n) = \int_0^1 g(\theta) e(-n\theta) d\theta.$$

Then

$$\widehat{F_A}(n) = \int_0^1 \sum_{a \in A} f(a) e((a-n)\theta) d\theta = f(n).$$

We will show that

$$\sum_{k=1}^{N} \frac{|f(a_k)|}{k} = \sum_{k=1}^{N} \frac{\widehat{F_A}(a_k)}{k} \ll \|F_A\|_1.$$

Since the left hand side is asymptotic to $\log N$, the Littlewood conjecture will follow.

The method of attack is one which is standard in this problem. We want to bound $\|\widehat{F}_A\|_1$ from below. By Parseval, for any Fourier series $g(\theta)$,

$$\sum_n f(n)\overline{\widehat{g}(n)} = \int_0^1 F_A(\theta)\overline{g(\theta)} d\theta \leq \|g\|_\infty \|F_A\|_1.$$

So we want to construct a test function g which is bounded, but whose Fourier transform correlates with f.

Begin by splitting A into parts

$$A_0 = \{a_1\},\ A_1 = \{a_2, a_3, a_4, a_5\}, A_2 = \{a_6, \ldots, a_{21}\}, \ldots$$

of size 4^j. Consider trigonometric polynomials

$$G_j(\theta) = \sum_{a \in A_j} \frac{\overline{\theta_a}}{4^j} e(a\theta)$$

where $f(a) = \theta_a |f(a)|$. In this way, when $a \in A_j$

$$\widehat{G_j}(a)\widehat{F_A}(a) = \frac{|f(a)|}{4^j}$$

and $\widehat{G_j}(a)\widehat{F_A}(a) = 0$ when $a \notin A_j$. We also have

$$\|G_j\|_2^2 = \sum_{a \in A_j} 4^{-2j} = 4^{-j}$$

from which we deduce $\|G_j\|_2 = 2^{-j}$.

Next, the function $|G_j(\theta)|$ has a Fourier expansion

$$|G_j(\theta)| = \sum_{n=-\infty}^{\infty} c_j(n) e(n\theta).$$

We will make use of the functions

$$H_j(\theta) = \frac{c_0}{4} + \frac{1}{2}\sum_{n=1}^{\infty} c_j(-n)e(-n\theta).$$

Because $|G_j|$ is real, $c_j(n) = \overline{c_j(-n)}$ and we have that

$$\|H_j\|_2^2 = \frac{1}{16}\left(|c_0|^2 + 4\sum_{n=1}^{\infty}|c_j(-n)|^2\right) \leq \frac{2}{16}\sum_{n=-\infty}^{\infty}|c_j(n)|^2$$

so that

$$\|H_j\|_2 \leq \frac{\sqrt{2}}{4}\|G_j\|_2 < 3\cdot 2^{-j-3}$$

These functions aren't yet suitable test functions, but before adjusting them, we record a few useful facts.

Lemma 3.3

Let $h : \mathbb{T} \to \mathbb{C}$ be such that $\Re(h) \geq 0$ and suppose $\widehat{h}$ is supported on negative integers. Then the following hold.

1. We have the inequality $|\exp(-h)| \leq 1$.
2. The function $\exp(-h)$ has Fourier transform supported on the negative integers.
3. We have the inequality $\|\exp(-h) - 1\|_2 \leq \|h\|_2$.

Proof. 1. This is fairly simple. Writing $h = h_1 + ih_2$ for functions $h_1, h_2 : \mathbb{T} \to \mathbb{R}$, we have by assumption that $h_1 \geq 0$ so

$$|\exp(-h)| = \exp(-h_1) \leq 1.$$

2. Expanding in a Taylor series,

$$\exp(-h(\theta)) = \sum_{k\geq 0}\frac{(-1)^k}{k!}(h(\theta))^k,$$

so it suffices to show that h^k has a Fourier transform supported on the negative integers for each k. But, in general, if f and g are Fourier series, then

$$\widehat{fg}(n) = \sum_{i+j=n}\widehat{f}(i)\widehat{g}(j)$$

and so if f and g have Fourier transforms supported on the negative integers, so too does fg.

3. The claimed statement follows from the inequality $|e^{-z}-1| \le |z|$ for any z with positive real part.

□

Now, back to our proof strategy, we want a bounded function g which has a Fourier series which correlates strongly with f, so that we can bound from below

$$\sum_n f(n)\overline{\widehat{g}(n)}.$$

This quantity is basically maximized when $\widehat{g} = f$, however then we cannot hope to put a good bound on g. Since f is supported on A, we can modify g by altering its Fourier coefficients away from A in hopes of making it smaller. This comes from introducing some smoothing-type factors, of the form

$$S_j(\theta) = \exp(-H_j(\theta)).$$

Now

$$|S_j(\theta)| = \exp(-\Re(H_j(\theta)))$$

and since $\overline{c_j(n)} = c_j(-n)$

$$\Re H_j(\theta) = \frac{1}{4}\left(c_0 + \sum_{n=-\infty}^{\infty} c_j(n)e(n\theta)\right) = \frac{|G_j(\theta)|}{4}.$$

This means that S_j is bounded. Another useful fact is that S_j has a Fourier transform vanishing on positive integers. Since

$$\operatorname{supp}(\widehat{g_1 g_2}) \subseteq \operatorname{supp}(\widehat{g_1}) + \operatorname{supp}(\widehat{g_2}),$$

it follows that any product of S_j's has vanishing positive Fourier coefficients.

We define the test functions T_j iteratively. First $T_0 = \frac{1}{5}G_0$. Next define

$$T_{j+1} = T_j S_{j+1} + \frac{1}{5}G_{j+1},$$

so that we get

$$T_1 = \frac{1}{5}G_0 S_1 + \frac{1}{5}G_1,\ T_2 = \frac{1}{5}G_0 S_1 S_2 + \frac{1}{5}G_1 S_2 + \frac{1}{5}G_2,$$

and in general

$$T_j = \sum_{m=0}^{j} \frac{G_m}{5} S_{m+1}\cdots S_j = \sum_{m=0}^{j} \frac{G_m}{5} \exp\left(-(H_{m+1}+\cdots+H_j)\right).$$

Now we note some of the useful properties of these test functions. First, since by construction $\|G_j\|_\infty \le 1$, we have $\|T_0\|_\infty \le 1$, and inductively

$$|T_j(\theta)| \le |S_j(\theta)| + \frac{1}{5}|G_j(\theta)| = \exp(-|G_j(\theta)|/4) + \frac{1}{5}|G_j(\theta)| \le 1$$

from the inequality

$$\exp(-x/4) + \frac{x}{5} \leq 1, \text{for } x \in [0,1].$$

So we know that our test functions are bounded. Next we want to show that they will correlate on the Fourier side. Here, we make use of the fact that the smoothing factors have vanishing positive Fourier coefficients. In particular, suppose $n \in A_j$, and $k \geq j$, then we claim that

$$\left|\widehat{T_k}(n) - 1/5\widehat{G_j}(n)\right| \leq \frac{|\widehat{G}_j(n)|}{10}.$$

To see why, let's investigate the Fourier support of the test functions, as it is a key aspect of the proof. From

$$T_k = \sum_{m=0}^{k} \frac{G_m}{5} \exp\left(-\sum_{m<l\leq k} H_l\right)$$

we see that T_k can only have a non-zero Fourier coefficient at $n \in A_j$ if

$$n \in \operatorname{supp}(\widehat{G_m}) + \operatorname{supp}\left(\exp\left(-\sum_{m<l\leq k} H_l\right)^\wedge\right) = A_m + \operatorname{supp}\left(\exp\left(-\sum_{m<l\leq k} H_l\right)^\wedge\right)$$

for some $m \leq k$. Since the second summand in the above sumset has non-positive elements, the elements of A_m need to be larger than n, which is to say $m \geq j$; so in fact for $n \in A_j$ we have

$$T_k = \sum_{m=j}^{k} \frac{G_m}{5} \exp\left(-\sum_{m<l\leq k} H_l\right).$$

Thus, by linearity, and the fact that $\widehat{G_m}(n) = 0$ for $m > j$ (since $n \in A_j$) we get

$$\begin{aligned}
\widehat{T_k}(n) - 1/5\widehat{G_j}(n) &= \frac{1}{5}\sum_{m=j}^{k}\left(G_m \exp\left(-\sum_{m<l\leq k} H_l\right)\right)^\wedge(n) - \widehat{G_j}(n) \\
&= \frac{1}{5}\sum_{m=j}^{k}\left(G_m \exp\left(-\sum_{m<l\leq k} H_l\right) - G_m\right)^\wedge(n) \\
&= \frac{1}{5}\sum_{m=j}^{k}\left(G_m\left(\exp\left(-\sum_{m<l\leq k} H_l\right) - 1\right)\right)^\wedge(n).
\end{aligned}$$

By Cauchy-Schwarz, for any two g_1 and g_2, we have

$$|\widehat{g_1 g_2}(n)| \leq \int_0^1 |g_1(\theta) g_2(\theta) e(-n\theta)| d\theta \leq \|g_1\|_2 \|g_2\|_2$$

so that

$$\begin{aligned}\widehat{T_k}(n) - 1/5\widehat{G_j}(n) &= \frac{1}{5}\sum_{m=j}^{k}\left(G_m\left(\exp\left(-\sum_{m<l\le k}H_l\right)-1\right)\right)^{\wedge}(n)\\ &\le \frac{1}{5}\sum_{m=j}^{k}\|G_m\|_2\left\|\exp\left(-\sum_{m<l\le k}H_l\right)-1\right\|_2\\ &\le \frac{1}{5}\sum_{m=j}^{k}\|G_m\|_2\left\|\sum_{m<l\le k}H_l\right\|_2,\end{aligned}$$

the last inequality coming from Lemma 3.4, part (3). From the bounds already established on $\|G_i\|_2$ and $\|H_i\|_2$ we get

$$\left|\widehat{T_k}(n) - 1/5\widehat{G_j}(n)\right| \le \frac{1}{5}\sum_{m=j}^{k}\frac{1}{2^m}\cdot\sum_{l=m+1}^{k}\frac{3}{2^{l+3}} \le \frac{1}{10\cdot 4^j} = \frac{|\widehat{G}_j(n)|}{10}.$$

We're nearly done. By our choice of A_j, if $a_l \in A_j$ then certainly $3l > 4^j$, so

$$|\widehat{G_j}(a_l)| = 4^{-j} > \frac{1}{3l}$$

and the way we have constructed things gives that

$$\widehat{G_j}(a_l)\widehat{F_A}(a_l) = \frac{|f(a_l)|}{4^j}$$

and so

$$\begin{aligned}\Re\left(\widehat{T_j}(a_l)\widehat{F_A}(a_l)\right) &\ge \Re\left(\frac{1}{5}\widehat{G_j}(a_l)\widehat{F_A}(a_l)\right) - \frac{|f(a_l)||\widehat{G_j}(a_l)|}{10}\\ &\ge \frac{|f(a_l)||\widehat{G_j}(a_l)|}{10}\\ &> \frac{|f(a_l)|}{30l}.\end{aligned}$$

So far we have that $\|T_j\|_\infty \le 1$ and so we get

$$|T_j * F_A(0)| \le \|F_A\|_1.$$

But on the other hand, we see that for j large enough

$$|T_j * F_A(0)| = \left|\sum_{l=1}^{N}\widehat{T}_j(a_l)f(a_l)\right| > \sum_{l=1}^{N}\frac{|f(a_l)|}{30l}.$$

4

EQUIDISTRIBUTION

4.1 Weyl's Criterion

For $u \in \mathbb{R}$ we write

$$\|u\| = \min_{n \in \mathbb{Z}} |u - n|$$

for the distance from u to the nearest integer, and $u \pmod 1 = u - \lfloor u \rfloor$. Then given a sequence $\{u_n\}$, we are often interested in the distribution of the sequence $\{u_n \pmod 1\}$ in $[0,1]$. One of the fundamental tools in the area is Dirichlet's principle.

Lemma 4.1: Dirichlet

Suppose $\alpha \in \mathbb{R}$. Then for any integer Q, there is a positive integer $q \le Q$ with

$$\|q\alpha\| \le \frac{1}{Q}.$$

Proof. Consider the $Q+1$ numbers $r\alpha \pmod 1$ with $r = 0, \ldots, Q$. Upon dividing $[0,1]$ into Q intervals of length $1/Q$, on interval contains two such numbers by the pigeon hole principle, say $r_1 < r_2$ and $r_1\alpha, r_2\alpha \in [j/Q, (j+1)/Q]$. Then $q\alpha = (r_2 - r_1)\alpha \in [-1/Q, 1/Q]$ (modulo 1) and hence $\|q\alpha\| \le 1/Q$. □

Exercise. *Show that if $\alpha_1, \ldots, \alpha_d$ are real numbers then for any Q, there is an integer*

$q \le Q$ *with*

$$\|q\alpha_j\| \le \frac{1}{Q^{1/d}}$$

for each j.

A first connection to the number theoretic nature of α comes in the following corollary.

Corollary 4.1: Dirichlet

If α is irrational, then there are arbitrarily large q for which $\|q\alpha\| \le 1/q$.

Proof. For each n, taking $Q = n$ in Dirichlet's principle gives an integer $q_n \le n$ such that

$$\|q_n\alpha\| \le \frac{1}{n} \le \frac{1}{q_n}.$$

In particular, since $1/n \to 0$, we must have $\|q_n\alpha\| \to 0$, and since $\|q_n\alpha\| > 0$ (because α is irrational), this forces the existence of infinitely many distinct values of q_n. □

Theorem 4.1

For $\gamma \in \mathbb{R}$, sequence $\{n\gamma \pmod 1\}$ is dense if and only if γ is irrational.

Proof. Indeed, if $\gamma = a/q$ then $n\gamma \pmod 1 \in \{0, 1/q, \ldots, 1-1/q\}$, a discrete set. On the other hand, suppose (α, β) in an interval in $[0,1]$ and let ε be such that $0 < \varepsilon < \beta - \alpha$. We can find q such that $q\gamma \pmod 1$ belongs to $(-\varepsilon/2, \varepsilon/2)$, by the above corollary. The sequence $\{kq\gamma \pmod 1\}$, whose consecutive points differ by at most ε, must contain a point from (α, β). □

Definition 4.1: Equidistribution

We say the sequence $\{u_n\}$ is equidistributed modulo 1 if for $0 \le \alpha < \beta \le 1$ we have

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n \le N} \mathbf{1}_{(\alpha,\beta)}(u_n \pmod 1) = \beta - \alpha.$$

In other words, asymptotically, the interval (α, β) contains the expected number of elements of the sequence $\{u_n \pmod 1\}$.

Lemma 4.2

The sequence $\{u_n\}$ with $0 \le u_n \le 1$ is equidistributed modulo 1 if and only if

$$\frac{1}{N}\sum_{n\le N} f(u_n) \to \int_0^1 f(\theta)d\theta$$

for any Riemann integrable f.

Proof. Suppose f is Riemann integrable and let I be its integral. Then for $\varepsilon > 0$ and Q sufficiently large, we can approximate the integral by upper and lower Riemann sums according to a partition $0 = t_0 < \ldots < t_Q = 1$ as

$$S_- = \sum_{k=1}^{Q}(t_k - t_{k-1})m_k,\ S_+ = \sum_{k=1}^{Q}(t_k - t_{k-1})M_k$$

where

$$m_k = \inf_{t\in(t_{k-1},t_k)} f(t),\ M_k = \sup_{t\in(t_{k-1},t_k)} f(t)$$

and $|S_\pm - I| < \varepsilon$. Now if equidistribution holds and N is sufficiently large, then for $\varepsilon' > 0$

$$(t_k - t_{k-1}) - \varepsilon' \le \frac{1}{N}\sum_{u_n\in(t_{k-1},t_k)} 1 \le (t_k - t_{k-1}) + \varepsilon'$$

so that

$$m_k(t_k - t_{k-1} - \varepsilon') \le \frac{1}{N}\sum_{u_n\in(t_{k-1},t_k)} f(u_n) \le M_k(t_k - t_{k-1} + \varepsilon').$$

Summing over k

$$S_- - \sum_k m_k\varepsilon' \le \frac{1}{N}\sum_n f(u_n) \le S_+ + \sum_k M_k\varepsilon'$$

and we can take ε' small enough to get

$$S_- - \varepsilon \le \frac{1}{N}\sum_n f(u_n) \le S_+ + \varepsilon$$

provided N is sufficiently large. This proves that for N sufficiently large in terms of ε,

$$\left| I - \frac{1}{N}\sum_n f(u_n)\right| < 2\varepsilon.$$

Conversely, take $f = \mathbf{1}_{(\alpha,\beta)}$ which is Riemann integrable. Then

$$\beta - \alpha = \int_0^1 f(\theta)d\theta \approx \frac{1}{N}\sum_{u_n\in(\alpha,\beta)} 1.$$

□

A good way to measure equidistribution is via the discrepancy

$$D_N(\alpha,\beta) = \frac{1}{N}\sum_{n\le N} \mathbf{1}_{(\alpha,\beta)}(u_n(\mathrm{mod}\ 1)) - (\beta-\alpha).$$

We will relate discrepancy to exponentials and this will give way to a second criterion for equidistribution: Weyl's criterion.

Theorem 4.2: Erdős-Turán

Let $\{u_n\}$ be an arbitrary sequence of real numbers and define

$$\widehat{U}_N(h) = \frac{1}{N}\sum_{n\le N} e(hu_n).$$

Then for $H \ge 1$

$$\sup_{\alpha,\beta} |D_N(\alpha,\beta)| \ll \frac{1}{H} + \sum_{h=1}^{H} \frac{1}{h}|\widehat{U}_N(h)|.$$

Corollary 4.2

The sequence $\{u_n\}$ is equidistributed modulo 1 if and only if

$$\lim_{N\to\infty} \widehat{U}_N(h) = 0$$

for every $h \ge 1$.

Proof. Since $\int_0^1 e(h\theta)d\theta = 0$, the only if part follows from Lemma 4.1. The if part follows from the Erdős-Turán inequality, since equidistribution is (by definition) equivalent to $|D_N(\alpha,\beta)| \to 0$. □

Lemma 4.3

Let K_N be the Fejér kernel of order N. Then

$$K_{N-1}(\theta) \le \frac{1}{4N\|\theta\|^2}$$

and provided $N\|\theta\| \le 1/2$, we have

$$K_{N-1}(\theta) \ge \frac{4N}{\pi^2}.$$

Proof. First let $n \in \mathbb{Z}$ be such that $-1/2 \le \theta - n \le 1/2$. Then from calculus,

$$|\sin(\pi\theta)| = |\sin(\pi(\theta-n))| \ge 2|\theta-n| = 2\|\theta\|$$

and so

$$K_{N-1}(\theta) = \frac{1}{N}\frac{(\sin(\pi N)\theta))^2}{(\sin(\pi\theta))^2} \leq \frac{1}{4N\|\theta\|^2}.$$

Next,

$$|\sin(\pi N\theta)| = |\sin(\pi N\|\theta\|)| \geq 2N\|\theta\|$$

and

$$|\sin(\pi\theta)| \leq \pi\|\theta\|$$

so

$$K_{N-1}(\theta) = \frac{1}{N}\frac{(\sin(\pi N)\theta))^2}{(\sin(\pi\theta))^2} \geq \frac{4N^2\|\theta\|^2}{N\pi^2\|\theta\|^2}.$$

□

Lemma 4.4

Let H and N be positive integers and let $\alpha \in \mathbb{R}$. Then for any sequence $\{u_n\}$

$$\frac{1}{N}|\{n \leq N : \alpha \leq u_n \leq \alpha + 1/H (\text{mod } 1)\}| \leq \frac{\pi^2}{4H} + \frac{\pi^2}{2H}\sum_{h=1}^{H}|\widehat{U}_N(h)|.$$

Proof. Let S be the the set on the left hand side. For $u_n \in S$, we have

$$-1/2H \leq u_n - \alpha - 1/2H \leq 1/2H (\text{mod } 1),$$

so

$$K_H(u_n - \alpha - 1/2H) \geq \frac{4H}{\pi^2}.$$

By positivity of K_H, we have that

$$\sum_{n\leq N} K_H(u_n - \alpha - 1/2H) \geq \frac{4H}{\pi^2}|S|.$$

But

$$\sum_{n\leq N} K_H(u_n - \alpha - 1/2H) = \frac{1}{H+1}\sum_{|h|\leq H}\left(1 - \frac{|h|}{H+1}\right)e(-h(\alpha + 1/2H))\widehat{U_N}(h).$$

The proof follows easily via the triangle inequality. □

Proof of Erdős-Turán. Throughout, we write $D_N(\alpha+\theta, \beta+\theta)$ which means the N-discrepancy of the interval (α, β) shifted by θ modulo 1, remarking that in doing so, but preserving the same orientation. We may assume K is sufficiently large, otherwise the theorem is trivial because of the implicit constant. Since we are working modulo 1, we can extend the definition of $D_N(\alpha, \beta)$ to any α and β with $\alpha < \beta < \alpha + 1$.

Now consider the integral

$$J = \int_0^1 D_N(\alpha+\theta, \beta+\theta) K_H(\theta) d\theta.$$

By definition of D_N we get

$$J = \int_0^1 \frac{1}{N} \sum_{n \le N} \mathbf{1}_{(\alpha+\theta,\beta+\theta)}(u_n) K_H(\theta) d\theta - (\beta-\alpha)$$

owing to the fact that K_H integrates to 1. Plugging in the definition of K_H,

$$\begin{aligned} J &= \frac{1}{N} \int_0^1 \sum_{n \le N} \mathbf{1}_{(\alpha+\theta,\beta+\theta)}(u_n) \sum_{|h| \le H} \left(1 - \frac{|h|}{H+1}\right) e(h\theta) d\theta - (\beta-\alpha) \\ &= \frac{1}{N} \sum_{n \le N} \sum_{|h| \le H} \left(1 - \frac{|h|}{H+1}\right) \int_{u_n-\beta}^{u_n-\alpha} e(h\theta) d\theta - (\beta-\alpha) \\ &= \frac{1}{N} \sum_{n \le N} \sum_{1 \le |h| \le H} \left(1 - \frac{|h|}{H+1}\right) \frac{e(h(u_n-\alpha)) - e(h(u_n-\beta))}{2\pi i h}, \end{aligned}$$

where we note that $(\beta-\alpha)$ cancels with the integral of the term where $h = 0$. The final line is

$$\begin{aligned} &\frac{1}{N} \sum_{n \le N} \sum_{1 \le |h| \le H} \left(1 - \frac{|h|}{H+1}\right) \frac{e(h(u_n-\alpha)) - e(h(u_n-\beta))}{2\pi i h} \\ &= \sum_{1 \le |h| \le H} \left(1 - \frac{|h|}{H+1}\right) \frac{1}{2\pi i h} \widehat{U}_N(h) \left(e(-h\alpha) - e(-h\beta)\right) \\ &= \sum_{1 \le |h| \le H} \left(1 - \frac{|h|}{H+1}\right) \frac{1}{2\pi i h} \widehat{U}_N(h) e(-h(\alpha+\beta)/2) \left(e(h(\beta-\alpha)/2) - e(-h(\beta-\alpha)/2)\right) \end{aligned}$$

and so

$$|J| \le \sum_{1 \le |h| \le H} \frac{|\widehat{U}_N(h)|}{\pi h} \cdot 2|\sin(\pi h(\beta-\alpha))|. \tag{1}$$

Now since K_H has mass 1,

$$\int_0^1 D_N(\alpha, \beta) K_H(\theta) d\theta = D_N(\alpha, \beta),$$

so

$$\int_0^1 \left(D_N(\alpha,\beta) - D_N(\alpha+\theta, \beta+\theta)\right) K_H(\theta) d\theta = J - D_N(\alpha,\beta)$$

and we can therefore estimate $D_N(\alpha,\beta)$ as

$$|D_N(\alpha,\beta)| \le |J| + \left| \int_0^1 \left(D_N(\alpha,\beta) - D_N(\alpha+\theta,\beta+\theta)\right) K_H(\theta) d\theta \right|. \tag{2}$$

This means we need only estimate the integral on the right hand side, say E. Set

$$\overline{D_N}(\beta-\alpha) = \sup_\theta |D_N(\alpha+\theta, \beta+\theta)|.$$

Then by Lemma 4.1, the contribution to E when $1/H \le \|\theta\| \le 1/2$ is at most

$$4\overline{D_N}(\beta-\alpha)\int_{1/H}^{1/2}\frac{1}{4H\theta^2}\,d\theta \le \frac{1}{2}\overline{D_N}(\beta-\alpha), \tag{3}$$

at least provided H is large enough. Now we estimate the contribution from $\|\theta\| \le 1/H$ (which we may replace by $|\theta| \le 1/H$ by periodicity). For such θ

$$\begin{aligned} D_N(\alpha,\beta) - D_N(\alpha+\theta,\beta+\theta) &= \sum_{\substack{n\le N\\ \alpha<u_n\le\beta}} 1 - \sum_{\substack{n\le N\\ \alpha+\theta<u_n\le\beta+\theta}} 1 \\ &= \sum_{\substack{n\le N\\ 0\le u_n\le\beta}} 1 - \sum_{\substack{n\le N\\ 0\le u_n\le\alpha}} 1 - \sum_{\substack{n\le N\\ 0<u_n\le\beta+\theta}} 1 + \sum_{\substack{n\le N\\ 0<u_n\le\alpha+\theta}} 1 \\ &= D_N(\alpha,\alpha+\theta) - D_N(\beta,\beta+\theta) \end{aligned}$$

unless $\beta+\theta$ or $\alpha+\theta > 1$. However, in the latter cases, we can still interpret $D_N(\alpha,\beta) - D_N(\alpha+\theta,\beta+\theta)$ as a difference of two discrepancies in intervals of length θ. In any case, because $|\theta| \le 1/H$, this difference is at most

$$\frac{2}{H} + \max_{\gamma=\alpha,\beta}\frac{1}{N}\sum_{\substack{n\le N\\ \gamma\le u_n\le\gamma+1/H}} 1 \ll \frac{1}{H} + \sum_{h=1}^{H}|\widehat{U_N}(h)|,$$

by Lemma 4.1. Again, since K_H integrates to 1, this shows that

$$\left|\int_{-1/H}^{1/H}\big(D_N(\alpha,\beta) - D_N(\alpha+\theta,\beta+\theta)\big)K_H(\theta)\,d\theta\right| \ll \frac{1}{H} + \sum_{h=1}^{H}|\widehat{U_N}(h)|.$$

Plugging the remaining estimate (3) and the bound from (1), we have

$$|D_N(\alpha,\beta)| \le \frac{1}{2}\overline{D_N}(\beta-\alpha) + \sum_{1\le|h|\le H}\frac{|\widehat{U}_N(h)|}{\pi h}\cdot 2|\sin(\pi h(\beta-\alpha))| + O\left(\frac{1}{H} + \frac{1}{H}\sum_{h=1}^{H}|\widehat{U_N}(h)|\right).$$

The left hand side depends on α and β while the right depends only on $\beta-\alpha$. Choose α,β with $\beta-\alpha$ so that the left hand side is nearly maximized, i.e. so that $|D_N(\alpha,\beta)| \ge \frac{3}{4}\overline{D_N}(\beta-\alpha)$. The theorem follows from crude estimates. □

4.2 The Large Sieve

A sieve problem in number theory is a sort of "quantitative" version of the Chinese Remainder Theorem. The CRT says, among other things, that if $p_1,\dots,p_l$ are distinct primes, then there are integers n satisfying the simultaneous congruence

$$n \equiv r_i \pmod{p_i}.$$

However, such n may be much larger than the given primes p_i, in fact as large as $p_1\cdots p_l$. A sieve-like interpretation of this statement is that there are not too many integers $n \le N$ which satisfy all of these congruences.

A general sieve problem arises when we replace the constraint $n \equiv r_i \pmod{p_i}$ with a list of possible constraints

$$n \equiv r \pmod{p_i} \text{ for some } r \in A_p$$

where for each prime p we have a set of residue classes A_p modulo p.

Example. *Suppose for each prime p in the range $1 \le p \le 2\sqrt{N}$ we set $A_p = \{1, \dots, p-1\}$, the set of non-zero residue classes. Then the set of all n in the range $N \le n \le 2N$ with $n \equiv r \pmod{p}$ for some $r \in A_p$ is the same as those n which are not divisible by any prime $p \le N$. But if n is composite, it has a prime factor which is at most $\sqrt{n} \le 2\sqrt{N}$. In other words, the n which pass this congruence constraint are precisely the primes between N and $2N$.*

The above example is an instance of a “small" sieve, so-called because there are only a small number of residue classes modulo p which are forbidden – in this case, just the 0 class. A “large" sieve is one where A_p is much smaller, i.e. we forbid a large number of classes.

To discuss this problem further, we need to set up some notation. We will take A to be subset of integers less than N, and for a prime p we let $A_p = \{a \pmod{p} : a \in A\}$. For a residue class $r \pmod{p}$, we write

$$A(p;r) = \{a \in A : a \equiv r \pmod{p}\}$$

so that

$$A = \bigcup_{r \in A_p} A(p;r).$$

We also have that for $a \in A$

$$\mathbf{1}_{A(p,r)}(a) = \frac{1}{p} \sum_{x \pmod{p}} e((r-a)x/p)$$

and so

$$|A(p,r)| = \frac{1}{p} \sum_{x \pmod{p}} \sum_{a \in A} e((r-a)x/p) = \frac{1}{p} \sum_{x \pmod{p}} e(rx/p) F_A(-x/p).$$

Here we are writing, as is often the case,

$$F_A(\theta) = \sum_{a \in A} e(a\theta).$$

Meanwhile, we expect

$$|A(p,r)| \approx |A|/p = \frac{F_A(0)}{p},$$

which would hold if the elements of A were uniformly distributed mod p. So, in the interest of comparing the two, we look at

$$D_A(p,r) = |A(p,r)| - \frac{|A|}{p} = \frac{1}{p}\sum_{x=1}^{p-1} e(rx/p)F_A(-x/p).$$

This shows that understanding the distribution of A modulo p is understood by evaluating F_A at the various p'th roots of unity.

The Large Sieve inequality lets us compare the function F_A at various points of $\mathbb{T}$ to an integral (essentially a Riemann sum estimate) provided the points are sufficiently equidistributed in the sense of well-separation.

Lemma 4.5: Gallagher

Let $f \in C^1[0,1]$. Then

$$|f(x)| \le \int_0^1 |f(t)| + |f'(t)|dt$$

and

$$|f(1/2)| \le \int_0^1 |f(t)| + \frac{1}{2}|f'(t)|dt.$$

Proof. Apply simple estimates to the identity

$$f(x) = \int_0^1 f(t)dt + \int_0^x tf'(t)dt - \int_x^1 (1-t)f'(t)dt.$$

□

Corollary 4.3

Let $f \in C^1[0,1]$. Then for $0 < \delta < 1/2$,

$$|f(x)| \le \int_{x-\delta/2}^{x+\delta/2} \frac{1}{\delta}|f(t)| + \frac{1}{2}|f'(t)|dt.$$

Proof. Apply a change of variables in Gallagher's lemma. □

Theorem 4.3: The analytic large sieve inequality

Let $a_1, \dots, a_N$ be complex numbers and let

$$S(\theta) = \sum_{n=1}^{N} a_n e(n\theta).$$

Suppose we have numbers $\theta_1, \dots, \theta_R$ which are δ-separated modulo 1, i.e. that $\|\theta_i - \theta_j\| \geq \delta$. Then

$$\frac{1}{R}\sum_{r=1}^{R} |S(\theta_r)|^2 \leq \left(\frac{\pi N}{R} + \frac{\delta^{-1}}{R}\right)\sum_{n=1}^{N} |a_n|^2.$$

Notice that by Plancherel, the sum of $|a_n|^2$ is precisely what we would get if we integrated $|S(\theta)|^2$. So this inequality is basically comparing the Riemann sum with the integral. The condition that the points are well separated is important, otherwise we could just take them all to be the same or very close together, which makes this statement false.

The quantity δ^{-1}/R on the right can be thought of as typically about 1 since we will likely take $\delta \approx 1/R$, which is the average separation of R points modulo 1. The quantity N/R is needed as well. If we took $a_n = \mathbf{1}_{q|n}$ and $\theta_r = r/q$, so that $R = q$ and $\delta = 1/q$, then

$$S(\theta_r) = \sum_{\substack{n \leq N \\ q|n}} e(nr/q) = \lfloor N/q \rfloor = \sum_{n \leq N} |a_n|^2.$$

Proof of the analytic large sieve inequality. Apply the preceding corollary to $S(\theta_r)^2$, and use that the intervals $(\theta_r - \delta/2, \theta_r + \delta/2)$ are disjoint modulo 1 to get

$$\sum_{r=1}^{R} |S(\theta_r)|^2 \leq \int_0^1 \frac{1}{\delta}|S(\theta)|^2 + \frac{1}{2}|S(\theta)S'(\theta)|d\theta.$$

To the first integrand we apply Plancherel to get

$$\frac{1}{\delta}\int_0^1 |S(\theta)|^2 d\theta = \frac{1}{\delta}\sum_{n \leq N} |a_n|^2.$$

To the second, apply Cauchy-Schwarz and then Plancherel:

$$\begin{aligned}\left(\int_0^1 |S(\theta)S'(\theta)|d\theta\right)^2 &\leq \int_0^1 |S(\theta)|^2 d\theta \int_0^1 |S'(\theta)|^2 d\theta \\ &= \left(\sum_{n \leq N} |a_n|^2\right)\left(\sum_{n \leq N} |2\pi n a_n|^2\right) \\ &\leq 2\pi N\left(\sum_{n \leq N} |a_n|^2\right)^2.\end{aligned}$$

□

Let's return to (4.2). It says that if we regard $d(r) = D_A(p,r)$ as a function of r on $\mathbb{F}_p$, then

$$\widehat{d}(x) = \frac{1}{p} F_A(-x/p)$$

except when $x = 0$, since $\widehat{d}(0) = 0$. So by Plancherel,

$$p \sum_{x \pmod p} |d(x)|^2 = \sum_{x=1}^{p-1} |F_A(x/p)|^2,$$

and we have just absorbed the minus sign in front of x/p on the right into the sum. A sieve wants to take information *from different primes* into account, so we sum this over all primes $p \le Q$ to get the following formula.

Theorem 4.4: The arithmetic large sieve inequality

Let N and Q be positive integers and let A be a subset of $\{1,\dots,N\}$. Then

$$\sum_{p \le Q} p \sum_{r=0}^{p-1} (|A(p,r)| - |A|/p)^2 = \sum_{p \le Q} \sum_{x=1}^{p-1} |F_A(x/p)|.$$

From the analytic large sieve inequality, it follows that

$$\sum_{p \le Q} p \sum_{r=0}^{p-1} (|A(p,r)| - |A|/p)^2 \le (\pi N + Q^2)|A|.$$

Proof. We only need to establish the second claim. We are applying the analytic large sieve inequality to the function F_A at the points $\theta = x/p$ with $1 \le x \le p-1$. These points are reduced fractions, so they are distinct, and in fact

$$\left| \frac{x}{p} - \frac{x'}{p'} \right| = \frac{|x' - x|}{pp'} \ge \frac{1}{Q^2}$$

so we may take $\delta = 1/Q^2$. □

Corollary 4.4

Let N and Q be positive integers and let A be a subset of $\{1,\dots,N\}$ such that for each prime $p \le Q$, A avoids $w(p)$ residue classes modulo p for some number $w(p) \in \{0,\dots,p-1\}$. Then

$$|A| \le \frac{\pi N + Q^2}{\sum_{p \le Q} \frac{w(p)}{p}}.$$

Proof. There are $w(p)$ values of r with $|A(p,r)| = 0$. □

We finally arrive at the original motivation for the large sieve inequality, due to Linnik.

Corollary 4.5

Let $\varepsilon > 0$ and let B denote the set of primes $p \le x$ such that each $n \le x^\varepsilon$ reduces to a quadratic residue modulo p. Then

$$|B| \le C$$

for some constant C depending only on ε.

Proof. Let

$$S_\varepsilon(x) = \{n \le x : \forall q \text{ prime}, q|n \implies q \le x^\varepsilon\}$$

denote the set of x^ε-smooth numbers up to x. Then a fact from sieve theory tells us

$$|S_\varepsilon(x)| \sim C_\varepsilon x$$

as $x \to \infty$. However, if p is a prime in B, then each $n \in S_\varepsilon(x)$ is a quadratic residue modulo p, since all of its prime factors are and quadratic residues are closed under multiplication. In other words, the number $w(p)$ of residue classes modulo p which are avoided by $S_\varepsilon(x)$ is at least $(p-1)/2$ – namely, the quadratic non-residues. Thus, applying the preceding corollary with $N = x$ and $Q = \sqrt{x}$

$$C_\varepsilon x \sim |S_\varepsilon(x)| \le \frac{C_\varepsilon(\pi+1)x}{\sum_{p\in B}\frac{p-1}{2p}}.$$

□

4.3 Roth's Theorem on Irregularity of Distribution

Let A be a subset of integers from $[1, N]$. Denote

$$A(x; q, h) = \{a \in A : a \le x, a \equiv h \pmod q\}.$$

We write α for the density of A, so $|A| = \alpha N$. We write

$$E(x; q, h) = \sum_{\substack{n\le x \\ n\equiv h (\mathrm{mod}\ q)}} 1.$$

We expect that

$$|A(x; q, h)| \approx \frac{|A|}{N} \sum_{\substack{n\le x \\ n\equiv h (\mathrm{mod}\ q)}} 1 = \alpha E(x; q, h).$$

Finally, we denote by $V(x;q)$ the variance

$$V(x;q) = \sum_{h(\mathrm{mod}\ q)} \big(|A(x;q,h)| - \alpha E(x;q,h)\big)^2.$$

Theorem 4.5: Roth

We have

$$\sum_{q\le Q}\sum_{n=1}^{N}\frac{1}{q}V(n;q) + Q\sum_{q\le Q}V(N;q) \gg \alpha(1-\alpha)Q^2N.$$

In particular, by choosing $Q = N^{1/2}$, there is an x_0 and q_0 such that

$$\frac{V(x_0;q_0)}{q_0} \gg \alpha(1-\alpha)N^{1/2}.$$

Proof. We can assume that Q is at least 2, and set $Q_0 = [Q/2]$. Consider the balanced function of A on $[1,N]$,

$$f_A = \mathbf{1}_A - \alpha\mathbf{1}_{[1,N]}.$$

Then

$$V(x;q) = \sum_{h(\mathrm{mod}\ q)}\left(\sum_{\substack{n\le x\\ n\equiv h(\mathrm{mod}\ q)}} f_A(n)\right)^2.$$

We set

$$F(\theta) = \sum_{n\le N} f_A(n)e(n\theta)$$

and

$$I(\theta) = \sum_{l=0}^{Q_0-1} e(l\theta),$$

and we consider the integral

$$\mathscr{I} = \int_0^1 \sum_{q=1}^{Q} |I(q\theta)F(\theta)|^2 d\theta.$$

We will prove the theorem by estimating $\mathscr{I}$ from above and below.

To begin, observe that

$$|I(\theta)| = \left|\sum_{l=0}^{Q_0-1} e(l\theta)\right| = \frac{|e(Q_0\theta/2) - e(-Q_0\theta/2)|}{|e(\theta/2) - e(-\theta/2)|} = Q_0\frac{|\sin(Q_0\pi\theta)|}{|Q_0\pi\theta|}\frac{|\pi\theta|}{|\sin(\pi\theta)|}$$

and this is at least $\frac{2}{\pi}Q_0$ if $\|\theta\| \le Q_0^{-1}$ using that

$$1 \ge \sin(x)/x \ge 2/\pi.$$

Since for some $q \le Q$ we have $\|q\theta\| \le Q^{-1} \le Q_0^{-1}$ (by Dirichlet's Theorem), it follows that

$$\sum_{q=1}^{Q}|I(q\theta)|^2 \ge \left(\frac{2}{\pi}Q_0\right)^2.$$

We conclude that

$$\mathscr{I} = \int_0^1 |F(\theta)|^2 \sum_{q=1}^{Q} |I(q\theta)|^2 d\theta \gg Q^2 \int_0^1 |F(\theta)|^2 d\theta = Q^2 \sum_n f_A(n)^2$$

the last step being Parseval's identity. Since

$$\sum_n f_A(n)^2 = \alpha(1-\alpha)N$$

we have shown the lower bound $\mathscr{I} \gg \alpha(1-\alpha)Q^2N$.

Next we give an upper bound for $\mathscr{I}$. We first observe that

$$F(\theta)I(q\theta) = \sum_{n\le N} f_A(n) \sum_{l=0}^{Q_0-1} e((n+ql)\theta) = \sum_{m\le N+(Q_0-1)q} r_q(m)e(m\theta)$$

where

$$r_q(m) = \sum_{\substack{n+ql=m \\ l\le Q_0-1}} f_A(n).$$

If we set

$$D(u,v;q,h) = \sum_{\substack{u\le n\le v \\ n\equiv h (\mathrm{mod}\ q)}} f_A(n)$$

then we have

$$r_q(m) = D(m-q(Q_0-1),m;q,m) = D(1,m;q,m) - D(1,m-qQ_0;q,m),$$

so that

$$r_q(m)^2 \le D(1,m;q,m)^2 + D(1,m-qQ_0;q,m)^2$$

and notice that $D(1,m-qQ_0;q,m) = D(1,m-qQ_0;q,m-qQ_0)$. Now

$$\mathscr{I} = \sum_{q=1}^{Q} \int_0^1 |F(\theta)I(q\theta)|^2 d\theta = \sum_{q=1}^{Q} \sum_m r_q(m)^2.$$

Considering the support of f_A, we have that

$$\sum_{m=N+1}^{N+q(Q_0-1)} D(1,m;q,m)^2 = \sum_{m=N+1}^{N+q(Q_0-1)} D(1,N;q,m)^2 \le QV(N;q),$$

and so, we arrive at

$$\begin{aligned}
&\sum_{m=1}^{N+q(Q_0-1)} r_q(m)^2 \\
&\le \sum_{m=1}^{N+q(Q_0-1)} D(1,m;q,m)^2 + D(1,m-qQ_0;q,m-qQ_0)^2 \\
&\le 2 \sum_{m=1}^{N+q(Q_0-1)} D(1,m;q,m)^2 \\
&\ll \sum_{m=1}^{N} D(1,m;q,m)^2 + QV(N;q).
\end{aligned}$$

Finally, since $D(1,m;q,m) = D(1,m+j;q,m)$ for $0 \le j < q$ (since none of the numbers $m+k$ with $k \le j$ are congruent to $m \bmod q$) we have

$$D(1,m;q,m)^2 = \frac{1}{q}\sum_{j=0}^{q-1} D(1,m+j;q,m)^2$$

and so

$$\mathscr{I} \ll \sum_{q=1}^{Q}\frac{1}{q}\sum_{m=1}^{N}\sum_{j=0}^{q-1} D(1,m+j;q,m)^2 + \sum_{q=1}^{Q} QV(N;q).$$

The theorem follows since

$$V(m;q) = \sum_{h(\bmod q)} D(1,m;q,h)^2.$$

□