Part III – Analytic Number Theory (Unfinished course)

Based on lectures by Dr T. Bloom
Notes taken by Bhavik Mehta

Lent 2019

Contents

0 Introduction

Lecture 1 Analytic Number Theory is the study of numbers using analysis. It is a fascinating field because because a number - in particular in this course an integer - is discrete, whilst analysis involves the real/complex numbers which are continuous.

In this course, we will ask quantitative questions.

Example.

1. How many primes? We can define the function $\pi(x) = |\{n \mid n \leq x \text{ and } n \text{ is prime}\}|$. Then the prime number theorem, which we will prove in this course states
$$\pi(x) \sim \frac{x}{\log x}.$$
(We will always take 'numbers' to mean natural numbers, not including zero).

2. How many twin primes are there? That is, where p, $p+2$ are both prime. It is not known whether there are infinitely many but since 2014, there has been immense progress by Zhang, Maynard and a Polymath project which has determined there are infinitely many primes at most 246 apart. Guess: there are $\approx \frac{x}{(\log x)^2}$ many $\leq x$.

3. How many primes are there $\equiv a \bmod q$ where $(a, q) = 1$. We know, by Dirichlet's theorem proven in the 20th century, that there are infinitely many such. The guess for how many is
$$\frac{1}{\varphi(q)} \frac{x}{\log x}.$$
This is known for small q. Recall $\varphi(n) = |\{1 \leq m \leq n \mid (m, n) = 1\}|$

The course will be split up into 4 (roughly equal) parts

1. Elementary techniques (real analysis)
2. Sieve methods
3. Riemann Zeta function, Prime Number Theorem (complex analysis)
4. Primes in arithmetic progressions

1 Elementary Techniques

We begin with a review of asymptotic notations:

- $f(x) = \mathcal{O}(g(x))$ if there is $C > 0$ such that $|f(x)| \leq C|g(x)|$ for all large enough x. (Landau notation)
- $f \ll g$ is the same as $f = \mathcal{O}(g)$ (Vinogradov notation)
- $f \sim g$ if $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$ (i.e. $f = (1 + o(1))g$).
- $f = o(g)$ if $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 0$

1.1 Arithmetic Functions

Definition (Arithmetic function)**.** An **arithmetic function** is just a function $f : \mathbb{N} \to \mathbb{C}$.

Definition (Convolution)**.** An important operation for multiplicative number theory is the **multiplicative convolution**

$$f * g(n) \coloneqq \sum_{ab=n} f(a)g(b).$$

Example.

- $1(n) \coloneqq 1 \ \ \forall n$. Caution: $1 * f \neq f$.
- Möbius function:
$$\mu(n) = \begin{cases} (-1)^k & \text{if } n = p_1 \cdots p_k \\ 0 & \text{if } n \text{ not squarefree} \end{cases}$$
- Liouville function:
$$\lambda(n) = (-1)^k \text{ if } n = p_1 \cdots p_k, \text{ not necessarily distinct}$$
- Divisor function:
$$\begin{aligned} \tau(n) &= |\{d \mid d \text{ a factor of } n\}| \\ \tau &= 1 * 1 \end{aligned}$$

Definition (Multiplicative function)**.** An arithmetic function is a **multiplicative function** if $f(nm) = f(n)f(m)$ for $(n, m) = 1$. In particular, a multiplicative function is determined by its values on prime powers $f(p^k)$.

Fact. If f, g are multiplicative, then so is $f * g$. $\log n$ is not multiplicative. Note, almost all arithmetic functions are not multiplicative.

Lemma (Möbius inversion)**.**

$$1 * f = g \iff \mu * g = f.$$

Proof.
$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{otherwise} \end{cases}$$

Note the left hand side is $1 * \mu$. Since $1, \mu$ are multiplicative, $1 * \mu$ is multiplicative. Hence it is enough to check the identity for prime powers: If $n = p^k$, then $\{d \mid d \text{ divides } n\} = \{1, p, \ldots, p^k\}$ so the left hand side is $1 - 1 + 0 + \ldots + 0 = 0$, unless $k = 0$ when the left hand side is $\mu(1) = 1$.

The right hand side is the identity of convolution, and convolution is associative, giving the required result. □

Our ultimate goal is to study the primes. This would suggest that we should work with
$$1_p(n) = \begin{cases} 1 & \text{if } n \text{ prime} \\ 0 & \text{otherwise} \end{cases}$$

For example $\pi(x) = \sum_{1 \le n \le x} 1_p(n)$. This is an awkward function to work with. Instead, we work with the **von Mangoldt function**
$$\Lambda(n) = \begin{cases} \log p & \text{if } n \text{ is a prime power} \\ 0 & \text{otherwise.} \end{cases}$$

This function is easier to understand. Why?

Lemma 1.1.
$$1 * \Lambda = \log \quad \text{and} \quad \mu * \log = \Lambda$$

Proof. The second part follows immediately by Möbius inversion.
$$\begin{aligned} 1 * \Lambda(n) &= \sum_{d|n} \Lambda(d) \quad \text{so if } n = p_1^{k_1} \ldots p_k^{n_k} \\ &= \sum_{i=1}^{r} \sum_{j=1}^{k_i} \Lambda(p_i^j) \\ &= \sum_{i=1}^{r} \sum_{j=1}^{k_i} \log p_i \\ &= \sum_{i=1}^{r} k_i \log p_i = \sum_{i=1}^{r} \log p_i^{k_i} = \log n. \end{aligned}$$ □

We can write
$$\begin{aligned} \Lambda(n) &= \sum_{d|n} \mu(d) \log\left(\frac{n}{d}\right) \\ &= \log n \sum_{d|n} \mu(d) - \sum_{d|n} \mu(d) \log d \\ &= -\sum_{d|n} \mu(d) \log d. \end{aligned}$$

Example.

$$\begin{aligned}
\sum_{1\le n\le x}\Lambda(n) &= -\sum_{1\le n\le x}\sum_{d|n}\mu(d)\log d \\
&= -\sum_{d\le x}\mu(d)\log(d)\left(\sum_{\substack{1\le n\le x\\ d|n}}1\right) \\
&= -x\sum_{d\le x}\mu(d)\frac{\log d}{d} + O\left(\sum_{d\le x}\mu(d)\log d\right)
\end{aligned}$$

since

$$\sum_{\substack{1\le n\le x\\ d|n}}1 = \left\lfloor\frac{x}{d}\right\rfloor = \frac{x}{d} + O(1).$$

Index of Notation

Index