

Analytic Number Theory

January 17, 2019

<i>CONTENTS</i>	2
-----------------	---

Contents

0	Introduction	3
1	Elementary techniques	4
1.1	Arithmetic functions	4

0 Introduction

—Lecture 1—

Lecturer: Thomas Bloom (tb634@cam.ac.uk, www.thomasbloom.org/ant.html)

Printed notes will be updated, but 1-2 weeks behind.

Example classes: weeks 3,5,7, tuesdays 330-5pm; prop-in sessions weeks 2,4,6,8. Rooms to be confirmed later.

What is analytic number theory? It's the study of numbers (regular integers, discrete) using analysis (real/complex, continuous) and some other quantitative questions.

For example, for the famous function $\pi(x)$, the number of primes no greater than x , we know $\pi(x) \sim \frac{x}{\log x}$.

Throughout this course, by *numbers* we'll mean natural numbers excluding 0.

We can also ask how many twin primes there are, i.e. how many p such that $p, p+2$ are both prime. This is not known yet (not even the finiteness); but from 2014, Zhang, Maynard, Polymath showed that there are infinitely many primes at most 246 apart, which is not that far from 2. The current guess is that the number is around $\frac{x}{(\log x)^2}$.

Another question we may ask: how many primes are there $\equiv a \pmod{q}$, $(a, q) = 1$. We know by Dirichlet's theorem that there are infinitely many.

A natural guess of the count is $\frac{1}{\phi(q)} \frac{x}{\log x}$, where $\phi(x)$ is the Euler Totient function. This is known to hold for small q .

In this course we'll talk about:

- (1) Elementary techniques (real analysis);
- (2) Sieve methods;
- (3) Riemann zeta function/prime number theory (complex analysis);
- (4) Primes in arithmetic progressions.

1 Elementary techniques

Review of asymptotic notation:

- $f(x) = O(g(x))$ if there is $c > 0$ s.t. $|f(x)| \leq c|g(x)|$ for all large enough x ;
- $f \ll g$ is the same thing as $f = O(g)$. This also defines what $f \gg g$ means in the natural way;
- $f \sim g$ if $\lim_{x \rightarrow \infty} \frac{f(x)}{g(x)} = 1$ (i.e. $f = (1 + o(1))g$);
- $f = o(g)$ if $\lim_{x \rightarrow \infty} \frac{f(x)}{g(x)} = 0$.

1.1 Arithmetic functions

Arithmetic functions are just functions $f : \mathbb{N} \rightarrow \mathbb{C}$; in other words, relabelling natural numbers with some complex numbers.

An important operation for multiplicative number theory ($fg = f(n)g(n)$) is multiplicative convolution,

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

Examples: $1(n) \equiv 1 \forall n$ (caution: 1 is not the identity function, and $1 * f \neq f$).
Möbius function:

$$\mu(n) = \begin{cases} (-1)^k & \text{if } n = p_1 \dots p_k \\ 0 & \text{if } n \text{ is divisible by a square} \end{cases}$$

Liouville function: $\lambda(n) = (-1)^k$ if $n = p_1 \dots p_k$ (primes not necessarily distinct),
Divisor function: $\tau(n) = \text{number of } d \text{ s.t. } d|n = \sum_{ab=n} 1 = 1 * 1$. This is sometimes also known as $d(n)$.

An arithmetic function is multiplicative if $f(nm) = f(n)f(m)$ when $(n, m) = 1$. In particular, a multiplicative function is determined by its values on prime powers.

Fact. If f, g are multiplicative, then so is $f * g$.

All the function we've seen so far $(\mu, \lambda, \tau, 1)$ are multiplicative.

Non-example: $\log n$ is definitely not multiplicative.

Fact. (Möbius inversion)

$1 * f = g \iff \mu * g = f$. That is,

$$\sum_{a|n} f(a) = g(n) \forall n \iff \sum_{d|n} g(d)\mu(n/d) = f(n) \forall n$$

e.g.

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & n = 1 \\ 0 & \text{else} \end{cases} = 1 * \mu$$

is multiplicative: it's enough to check identity for primes powers.

If $n = p^k$ then $\{d|n\} = \{1, p, \dots, p^k\}$. So $\text{LHS} = 1 - 1 + 0 + 0 + \dots = 0$, unless $k = 0$ when $\text{LHS} = \mu(1) = 1$.

Our goal is to study primes. The first guess might be to work with

$$1_p(n) = \begin{cases} 1 & n \text{ prime} \\ 0 & \text{else} \end{cases}$$

(e.g. $\pi(x) = \sum_{1 \leq n \leq x} 1_p(n)$). Instead, we work with von Mangoldt function

$$\wedge(n) = \begin{cases} \log p & n \text{ is a prime power} \\ 0 & \text{else} \end{cases}$$

(e.g. in a few lectures we'll look at $\psi(x) = \sum_{1 \leq n \leq x} \wedge(n)$).

Lemma. (1)

$1 * \wedge = \log$, and by Möbius inversion, $\mu * \log = \wedge$.

Note that it's easy to realize that \wedge is not multiplicative, else \log will be.

Proof. $1 * \wedge(n) = \sum_{d|n} \wedge(d)$. So if $n = p_1^{k_1} \dots p_r^{k_r}$, then above

$$\begin{aligned} &= \sum_{i=1}^r \sum_{j=1}^{k_i} \wedge(p_i^j) \\ &= \sum_{i=1}^r \sum_{j=1}^{k_i} \log(p_i) \\ &= \sum_{i=1}^r k_i \log(p_i) \\ &= \log n \end{aligned}$$

□

Note that the above tells us

$$\begin{aligned} \wedge(n) &= \sum_{d|n} \mu(d) \log(n/d) \\ &= \log n \sum_{d|n} \mu(d) - \sum_{d|n} \mu(d) \log d \\ &= - \sum_{d|n} \mu(d) \log d \end{aligned}$$

by the famous fact that $\sum_{d|n} \mu(d) = 0$ unless $n = 1$; but when $n = 1$, $\log n = 0$. Now we can try to evaluate

$$\begin{aligned} - \sum_{1 \leq n \leq x} \wedge(n) &= \sum_{1 \leq n \leq x} \sum_{d|n} \mu(d) \log d \\ &= - \sum_{d \leq x} \mu(d) \log d \left(\sum_{1 \leq n \leq x, d|n} 1 \right) \text{ (reverse order of summation)} \end{aligned}$$

But

$$\sum_{1 \leq n \leq x, d|n} 1 = \lfloor x/d \rfloor = x/d + O(1)$$

So we know the original sum is equal to

$$-x \sum_{d \leq x} \mu(d) \frac{\log d}{d} + O\left(\sum_{d \leq x} \mu(d) \log d\right)$$