Analytic Number Theory

January 20, 2019

Contents

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 $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$ (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

Arithmetic functions are just functions $f : \mathbb{N} \to \mathbb{C}$; 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:

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

Liouville function: $\lambda(n) = (-1)^k$ if $n = p_1...p_k$ (primes not necessarily distinct),
Divisor function: $\tau(n) =$ number of d 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,

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

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 $\{d|n\} = \{1, p, ..., p^k\}$. So LHS=$1 - 1 + 0 + 0 + ... = 0$, unless $k = 0$ when 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. $\pi(x) = \sum_{1 \le n \le x} 1_p(n)$). Instead, we work with von Mangoldt funcion

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

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

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 $n = p_1^{k_1}...p_r^{k_r}$, 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

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

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

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

—Lecutre 2—

Lecturer's favourite book: *Multiplicative Number Theory.*

Room for example classes: MR14 (Tues 330-5pm, week 357).

1.2 Summation

Given an arithmetic function f, we can ask for estimates of $\sum_{1\leq n\leq x} f(n)$.
We say that f has *average order* g if $\sum_{1\leq n\leq x} f(n) \sim xg(x)$ (in some sense, the average size of f is g).

For example, if $f \equiv 1$, then $\sum_{1\ leqn\leq x} f(n) = \lfloor x \rfloor = x + O(1) \sim x$. So the average order of 1 is 1 (makes a lot of sense).
A slightly less trivial example is the identity function $f(n) = n$: we have $\sum_{1\leq n\leq x} n \sim \frac{x^2}{2}$, so the average order of n is $n/2$.

Lemma. (1, Partial summation)
If (a_n) is a sequence of complex numbers, and f is s.t. f' is continuous. Then $\sum_{1\leq n\leq x} f(n) = A(x)f(x) - \int_1^x A(t)f'(t)dt$, where $A(x) = \sum_{1\leq n\leq x} a_n$.
We can see that this is a discrete version of integration by parts.

Proof. Suppose $x = N$ is an integer. Note that $a_n = A(n) - A(n-1)$. So

$$\begin{aligned}\sum_{1\leq n\leq N} a_n f(n) &= \sum_{1\leq n\leq N} f(n)(A(n) - A(n-1)) \\ &= A(N)f(N) - \sum_{n=1}^{N-1} A(n)(f(n+1) - f(n)) \text{ using } A(0) = 0\end{aligned}$$

Now $f(n+1) - f(n) = \int_n^{n+1} f'(t)dt$. So

$$\begin{aligned}\sum_{1\leq n\leq N} a_n f(n) &= A(N)f(N) - \sum_{n=1}^{N-1} A(n)\int_n^{n+1} f'(t)dt \\ &= A(N)f(N) - \int_1^N A(t)f'(t)dt\end{aligned}$$

To be complete, we should also consider the case where x is not an integer. But if $N = \lfloor x \rfloor$,

$$\begin{aligned} A(x)f(x) &= A(N)f(x) \\ &= A(N)\left(f(N) + \int_N^x f'(t)dt\right) \end{aligned}$$

□

Lemma. (2)

$$\sum_{1 \le n \le x} \frac{1}{n} = \log x + \gamma + O\left(\frac{1}{x}\right)$$

where γ is some constant.

Proof. Apply partial summation with $f(x) = \frac{1}{x}$ and $a_n \equiv 1$, so $A(x) = \lfloor x \rfloor$. Then, writing $\lfloor t \rfloor = t - \{t\}$,

$$\begin{aligned} \sum_{1 \le n \le x} \frac{1}{n} &= \frac{\lfloor x \rfloor}{x} + \int_1^x \frac{\lfloor t \rfloor}{t^2} dt \\ &= 1 + O\left(\frac{1}{x}\right) + \int_1^x \frac{1}{t} dt - \int_1^x \frac{\{t\}}{t^2} dt \\ &= 1 + O\left(\frac{1}{x}\right) + \log x - \int_1^\infty \frac{\{t\}}{t^2} dt + \int_x^\infty \frac{\{t\}}{t^2} dt \\ &= \gamma + O\left(\frac{1}{x}\right) + \log x + O\left(\frac{1}{x}\right) \\ &= \log x + \gamma + O\left(\frac{1}{x}\right) \end{aligned}$$

where at the penultimate step we bound the error term by

$$\begin{aligned} \int_x^\infty \frac{\{t\}}{t^2} dt &\le \int_x^\infty \frac{1}{t^2} dt \\ &\le \frac{1}{x} \end{aligned}$$

and we actually know $\gamma = 1 - \int_1^\infty \frac{\{t\}}{t^2} dt$.
This γ is called Euler's constant (Euler-Mascheroni).
We know very little about this constant: we only know $\gamma = 0.577...$, and we don't even know if γ is irrational. □

Lemma. (3)

$$\sum_{1 \le n \le x} \log n = x \log x - x + O(\log x)$$

Proof. Use partial summation again, with $f(x) = \log x$ and $a_n = 1$, so $A(x) = \lfloor x \rfloor$:

$$\begin{aligned}\sum_{1\le n\le x} \log n &= \lfloor x \rfloor \log x - \int_1^x \frac{\lfloor t \rfloor}{t} dt \\ &= x \log x + O(\log x) - \int_1^x 1 dt + O(\int_1^x \frac{1}{t} dt) \\ &= x \log x - x + O(\log x)\end{aligned}$$

□

1.3 Dinsar function

Recall that $\tau(n) = 1 * 1(n) = \sum_{d|n} 1$.

Theorem. (4)

$$\sum_{1\le n\le x} \tau(n) = x \log x + (2\gamma - 1)x + O(x^{1/2})$$

So average order of τ is $\log x$.

Proof. Note that we won't apply partial summation here: PS allows to get $\sum a_n f(n)$ from knowledge of $\sum a_n$; but $\tau(n)$ here is not differentiable, so PS is not going to apply.

$$\begin{aligned}\sum_{1\le n\le x} \tau(n) &= \sum_{1\le n\le x} \sum_{d|n} 1 \\ &= \sum_{1\le d\le x} \sum_{1\le n\le x, d|n} 1 \\ &= \sum_{1\le d\le x} \lfloor \frac{x}{d} \rfloor \\ &= \sum_{1\le d\le x} \frac{x}{d} + O(x) \\ &= x \sum_{1\le d\le x} \frac{1}{d} + O(x) \\ &= x \log x + \gamma x + O(x)\end{aligned}$$

where we applied lemma 2 at the last step. This is all correct, but the error term is larger than what we wanted. However, we have indeed prove that the average order of $\tau(x)$ is $\log x$.

To reduce error term, we use (Dirichlet's) hyperbola trick:

$$\begin{aligned}\sum_{1\le n\le x}\tau(n) &= \sum_{1\le n\le x}\sum_{ab=n}1\\ &= \sum_{ab\le x}1\\ &= \sum_{a\le x}\sum_{b\le \frac{x}{a}}1\end{aligned}$$

Note that now we're just counting number of integer points below the hyperbola $xy = n$ (relabelling variables).
When summing over $ab \le x$, we can sum over $a, b \le x^{1/2}$ separately, then subtract the repetition off. Then

$$\begin{aligned}\sum_{1\le n\le x}\tau(n) &= \sum_{a\le x^{1/2}}\sum_{b\le \frac{x}{a}}1+\sum_{b\le x^{1/2}}\sum_{a\le \frac{x}{b}}1-\sum_{a,b\le x^{1/2}}1\\ &= 2\sum_{a\le x^{1/2}}\lfloor\frac{x}{a}\rfloor-\lfloor x^{1/2}\rfloor^2\\ &= 2\sum_{a\le x^{1/2}}\frac{x}{a}+O(x^{1/2})-x+O(x^{1/2})\end{aligned}$$

by noting that $\lfloor x^{1/2}\rfloor^2 = (x^{1/2}+O(1))^2$. Now the above equals

$$\begin{aligned}&= 2x\log x^{1/2}+2\gamma x-x+O(x^{1/2})\\ &= x\log x+(2\gamma-1)x+O(x^{1/2})\end{aligned}$$

□

Improving this $O(x^{1/2})$ error term is a famous and hard problem. We should probably get $O(x^{1/4+\varepsilon})$, but this is open. The best known result is $O(x^{0.3149\ldots})$.

Note that this does *not* mean that $\tau(n) \ll \log n$. The average order is small doesn't say about the individual values being small.

We'll state the theorem we're proving and prove it in the next lecture:

Theorem. (5)

$$\tau(n) \le n^{O(\frac{1}{\log\log n})}$$

In particular, $\tau(n) \ll_\varepsilon n^\varepsilon\ \forall\varepsilon > 0$.