Part III - Analytic Number Theory

Artur Avameri

Michaelmas 2022

Contents

-1 Introduction **2**

0 Prelude, Cramer's model **2**

1 Generating functions **3**

-1 Introduction

06 Oct 2022, Lecture 1

What is analytic number theory? Classical ANT is about counting primes, and conjectures about primes. For example:

- Landau's conjecture: Are there infinitely many primes of the form n^2+1?
- Goldbach's conjecture: Is every even number a sum of two primes?
- Are there infinitely many primes between n^2 and $(n+1)^2$?

In ANT, we try (amongst other things) to prove the existence of things, prove there are infinitely many of some things, prove asymptotics, prove mean values and distributions of arithmetic functions, etc. A lot of these problems are very difficult because primes have a multiplicative structure, but we are asking additive questions about them.

The prerequisites for this course are some real and complex analysis.

We will loosely follow the historical progression of the subject, starting with Euler and the introduction to analysis into number theory, proving e.g. $\sum_{p\le x}\frac{1}{p}\sim \log\log x$. We will then talk about of Dirichlet's theorem and complex analytic methods (e.g. the use of contour integration), Chebyshev's work on elementary estimates, the Riemann hypothesis and Hadamard's complex function theory. We will finish with the circle method (Hardy, Littlewood, Ramanujan), the sieve method (Brun, Selberg, Turan), and perhaps more recent work (e.g. the Green-Tao theorem).

Notation: $\log x$ always refers to the natural logarithm, $f(x)\sim g(x)$ if $\lim_{x\to\infty}\frac{f(x)}{g(x)}\to 1$, $f(x)=O(g(x))$ means $f(x)\le kg(x)$ for some k, and $f(x)=o(g(x))$ means $f(x)\le \epsilon g(x)$ for any $\epsilon>0$ as $x\to\infty$. $f\ll g$ means $f\le O(g)$.

0 Prelude, Cramer's model

As a child, Gauss conjectured that $\pi(x)\sim \mathrm{li}(x)=\int_2^x\frac{dy}{\log y}$. He reckoned that a number n has about a probability $\frac{1}{\log x}$ of being a prime, so the above integral is close to $\sum_{n\le x}\frac{1}{\log n}$.

Let $X_1,\dots,X_n$ be random variables such that each X_k is 1 with probability $\frac{1}{\log k}$ and 0 otherwise, and define a fake prime counting function $\pi(x)=\sum_{i\le n}X_i$, so $\mathbb{E}[\pi(x)]=1+\sum_{n\ge 3}\frac{1}{\log n}$ and $\mathrm{Var}(\pi(x))=\sum\mathrm{Var}(X_i)=\sum_{n\ge 3}\frac{1}{\log n}\sim\mathrm{li}(x)$, where the last asymptotic follows from estimating the sum using integrals.

Claim. $\mathrm{li}(x)\sim\frac{x}{\log x}$.

Proof.

$$\lim_{x\to\infty}\frac{\int_2^x\frac{1}{\log x}}{\frac{x}{\log x}}=\frac{\infty}{\infty}=\frac{\frac{1}{\log x}}{\frac{1}{\log x}-\frac{1}{(\log x)^2}}\to 1.$$

by L'Hopitals rule. □

We can do better by integrating by parts (with $u=y, v=\frac{1}{\log y}$):

$$\mathrm{li}(x)=\int_2^x\frac{dy}{\log y}=\left[\frac{y}{\log y}\right]_2^x-\int_2^x\frac{-1}{(\log y)^2}=\frac{x}{\log x}+\int_2^x\frac{dy}{(\log y)^2},$$

where the last integral is called $\mathrm{li}_2(x)$, and by L'Hopital we can show $\mathrm{li}_2(x)\sim\frac{x}{(\log x)^2}$ (and analogously define $\mathrm{li}_n(x)$, for which $\mathrm{li}_n(x)\sim\frac{x}{(\log x)^n}$).

If we integrate $\mathrm{li}_2(x)$ by parts again, it becomes $\frac{x}{(\log x)^2}+\int_2^x\frac{2dy}{(\log y)^3}$.

In general, we now get an asymptotic expansion

$$\mathrm{li}(x) = \frac{x}{\log x} + \frac{x}{(\log x)^2} + \frac{2x}{(\log x)^3} + \ldots + \frac{(N-1)!x}{(\log x)^N} + O\left(\frac{X}{(\log x)^N}\right).$$

Cramer's model says that to count the number of primes $\leq x$, we can evaluate $\prod_{p\leq\sqrt{x}}(1-\frac{1}{p}) \sim \frac{e^{-\gamma}}{\log\sqrt{x}} = \frac{2e^{-\gamma}}{\log x} \approx \frac{1.12}{\log x}$, which is off a little bit (PNT).

Meier showed this is a bit off - the events "n is prime" and "$n+k$ is prime" are not independent (especially on short intervals). Depending on whether $p \mid k$ or not, we should consider one of $1-\frac{2}{p} < (1-\frac{1}{p})^2 < 1-\frac{1}{p}$.

11 Oct 2022, Lecture 2

Let $\mathbb{N}^+ = \mathbb{N}\cup\{0\}$. We have for $|z|<1$ that $1+z+z^2+\ldots = \frac{1}{1-z}$, and more generally $1+z^p+z^{2p}+\ldots = \frac{1}{1-z^p}$.

How do we sieve out $p_1, p_2 \ldots, p_k$? Using inculsion-exclusion.

$$\frac{1}{1-z} - \sum_i \frac{1}{1-z^{p_i}} + \sum_{i,j} \frac{1}{1-z^{p_ip_j}} + \ldots + (-1)^k \frac{1}{1-z^{p_1\ldots p_k}}.$$

Suppose we only had finitely many primes. Then the above expression is equal to z (corresponding to the number 1, the only number without prime factors). Let z tend toward $e^{2\pi i/p_1\ldots p_k}$ within $|z|<1$. Then the LHS goes to infinity, while z does not, contradiction.

1 Generating functions

The idea of generating functions is to take some discrete numbers, say $a_0, a_1, \ldots$ in $\mathbb{C}$, and turn it into something analytic, a function $\sum_{n\geq 0} a_n z^n$. Analogously, we can take (a_i) in a ring R, and have it be in correspondence with an element of $R[[X]]$, the set of all power series over R, which is a commutative ring.

Definition 1.1. For a power series $f(z) = \sum_{n\geq 0} a_n z^n$, the **order** of f, $\mathrm{ord}(f) = \min(n, a_n \neq 0)$.

This allows us to define a distance $d(a_n, b_n) = 2^{-\mathrm{ord}((a_n-b_n))_{n\geq 0}}$, which allows us to talk about convergence: $f_1+f_2+\ldots \to f$ if and only if $\mathrm{ord}(f_i)\to\infty$. Moreover, $\prod(1+f_i)\to f$ if and only if $\mathrm{ord}(f_i)\to\infty$.

Sidenote: Euler had an idea to prove the four squares theorem by showing every coefficient of $(\sum_{n\geq 0} z^{n^2})^4$ is nonzero. Jacobi extended this to$(\sum_{n\in\mathbb{Z}} z^{n^2})^4$ and managed to show the coefficient of z^n was $\sigma(n) - 4\sigma(n/4)$, which proves the four squares theorem (although Legendre did it before him).

We need to show power series have inverses. Let $f(z) = \sum a_n z^n$, $g(z) = \sum b_n z^n$. For g to be an inverse of f, we need $a_0b_0 = 1$ and $\sum a_k b_{n-k} = 0$, so $a_0 b_n = -\sum_{k\geq 1} a_k b_{n-k}$, which uniquely defines b_n. We can also formally define $L(1+f) = f - f^2/2 + f^3/3 + \ldots$, $E(f) = 1+f+f^2/2+\ldots$ (for $\mathrm{ord}(f)\neq 0$), $D(f) = \sum n a_{n-1} z^{n-1}$ etc.

How can we show the number of odd partitions of n is equal to the number of partitions of n into distinct parts? We can write

$$\prod_{k\geq 1}(1+z^k) = \prod_{k\geq 1}\left(\frac{1-z^{2k}}{1-z^k}\right) = \prod_{k\geq 1}\frac{1}{1-z^{2k-1}}$$

How does Euler approach the Basel problem? He writes $\sum \frac{z^n}{n^2} = \int_0^z \frac{-\log(1-t)}{t}dt$, relates that to the Li_2 function, guesses the answer from there, and then figures out a proof using different

methods.

Fibonacci numbers (argument by De Moivre): define $f(z) = \sum F_n z^n$. We have $F_{n+2} = F_{n+1} + F_n$, so $F_{n+2}z^{n+2} = F_{n+1}z^{n+2} + F_n z^{n+2}$. Sum this over all n to get $f(z) - (0 + z) = f(z)z + f(z)z^2$, whence $f(z) = \frac{z}{1-z-z^2}$. Do partial fraction decomposition on this to get $f(z) = \frac{z}{1-z-z^2} = \frac{A}{1-r^+z} + \frac{B}{1-r^-z}$, which when expanded gives Binet's formula (i.e. the first term gives $1 + r^+z + (r^+z)^2 + \ldots$).

We now talk about how Bernoulli found the formula for the sum of triangular numbers. We have $1+z+z^2+\ldots+z^{n-1} = \frac{1-z^n}{1-z}$, and by differentiation we get $1+2z+3z^2+\ldots+nz^{n-1} = \frac{A(z)}{(1-z)^2}$, similarly $1+3z+6z^2+\ldots = \frac{A(z)}{(1-z)^3}$ etc, so summing all of these gives the result if you plug in $z = 1$. Except you can't do that, since the denominator vanishes - so you apply L'Hopital. And then apply it again. And then eventually it works I think? We've reinvented a Taylor series expansion around $z = 1$.

Do chess probability (equivalently rephrased as how many times do you have to flip a p-biased coin to get 3 heads) to get $p^3(\sum \binom{n+2}{2}(1-p)^n) = 1$, replace $1 - p = z$ to get $\sum \binom{n+2}{2} z^n = \frac{1}{(1-z)^3}$. So probability leads naturally to generating functions.

13 Oct 2022, Lecture 3

Let $p(n)$ be the number of ways of partitioning n. Then Ramanujan showed

$$\sum_{n\geq 0} p(5n+4)z^n = 5\prod_{n\geq 1}\frac{(1-z^{5n})^5}{(1-z^n)^6}.$$

This is true formally in $\mathbb{C}[[z]]$ and analytically when $|z| < 1$. From this it follows that $5 \mid p(5n+4)$.

Theorem 1.1 (Binomial theorem)**.** $\sum_{n=0} \binom{m}{n} = (1+x)^m$ for $m \in \mathbb{N}$.

This also holds formally for $m \in \mathbb{Q}$, and $m \in \mathbb{C}$ if $|x| < 1$.

Theorem 1.2. Given $f(z) = \sum_{n\geq 0} a_n z^n$, define $A_N = \sum_{n=0}^N a_n z^n$. Then

$$g(z) = \sum_{N\geq 0} A_N z^N = \frac{f(z)}{1-z}.$$

Proof. The idea is that $\frac{1}{1-z} = 1 + z + z^2 + \ldots$, so the coefficient of each z^N is $a_N + a_{N-1} + \ldots = A_N$. □

Theorem 1.3. (i):

$$\sum_{n=0}^{N}\binom{n+m-1}{m-1} = \binom{N+m}{m}.$$

(ii):

$$\sum_{n\geq 0}\binom{n+m-1}{m-1}z^n = \frac{1}{(1-z)^m}.$$

Proof. I think (i) is just hockey stick identity in Pascal's triangle? And the second is the chess game again. □

For a power series, $R = \lim_{n\to\infty} \sup|a_n|^{1/n}$. So $\sum a_n z^n$ always converges for $|z| < R$ and always diverges for $|z| > R$.

Theorem 1.4 (Abel limit theorem)**.** If $f(z) = \sum_{n\geq 0} a_n z^n$ converges in $|z| < 1$ and we let $A_n = \sum_{n=0}^N a_n$, then $\lim_{z\to 1} f(z) = \lim_{N\to\infty} A_N = A$ if this limit exists.

Proof. Let $g(z) = \sum_{N\geq 0} A_N z^N = \frac{f(z)}{1-z}$ for $|z| < 1$. Then

$$f(z) - A = (1-z)\sum_{N\geq 0}(A_N z^N - Az^N) = (1-z)\left(\sum_{N<M}(A_N - A)z^N\right) + \epsilon\sum_{N\geq M} z^N$$

where we choose M such that $|A_N - A| < \epsilon$ for $N \geq M$. So $\lim_{z\to 1} f(z) - A < \epsilon + \epsilon$, done. □

Theorem 1.5 (Tauber's first theorem)**.** If $a_n = o(\frac{1}{n})$ as $n \to \infty$, then convergence of $\sum_{n\geq 0} a_n z^n$ implies convergence of $\sum a_n$.

Proof.

$$\left|\sum_{n=0}^{N} a_n - f(z)\right| = \sum_{n=0}^{N} a_n(1-z^n) - \sum_{n=N+1}^{\infty} a_n z^n.$$

But $|1 - z^n| < n|1 - z|$, so the LHS above is at most

$$\sum_{n=0}^{N} n|1-z||a_n| + \frac{1}{N}\sum_{n>N} n|a_n||z|^n.$$

The first term above is at most $\frac{\epsilon}{2} + \frac{\epsilon}{2}$ and the second term is at most $\frac{1}{N(1-|z|)}\sup_{n>N}(n|a_n|)$, so we're done. □

Theorem 1.6 (Tauber's second theorem)**.** If $A_N - (\sum_{i=0}^{N-1} A_i)/N$ converges to 0, then we have the above convergence implication again.

These are useful since there is a Tauberian way to prove PNT.

Infinite products: Let $z_1, \ldots, z_n \in \mathbb{C}$. Suppose we're interested in $\lim_{n\to\infty}\prod_{n=1}^{N}(1+z_n)$. One condition is that this converges if $\sum |z_i|$ converges, since the infinite product is at most $e^{\sum_{i=1}^{N}|z_i|} - 1 \leq \sum |z_i| + \sum |z_i||z_j| + \ldots \leq \sum |z_i| + \frac{1}{2}\sum |z_i|^2 + \frac{1}{3!}(\sum |z_i|)^3 + \ldots$.