2015 10 05

5. Prime Number Theorem

We proved in the last session
(1) the analytic continuation of $\zeta(s)$ to $Re(s)>0$
(2) the non-vanishing of $\zeta(s)$ on $Re(s)=1$
These are the main ingredients to prove the prime number theorem.

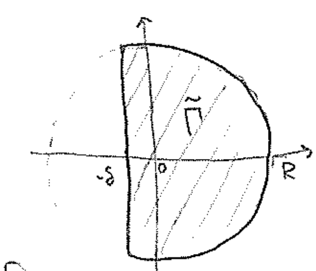
Theorem 20 (Donald J. Newman): Let $a_n \in \mathbb{C}$ with $|a_n| \leq 1$ for $n \in \mathbb{N}$. Consider the series

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s},$$

which converges to an analytic function, say $F(s)$, for $Re(s)>1$. If $F(s)$ can be analytically continued to $Re(s) \geq 1$, then the series converges to $F(s)$ for $Re(s) \geq 1$.

Proof: Let $w \in \mathbb{C}$ with $Re(w) \geq 1$. Thus $F(z+w)$ is analytic for $Re(z) \geq 0$. Choose $R \geq 1$ and let $\delta = \delta(R) > 0$ so that $F(z+w)$ is analytic on the region

$$\tilde{\Gamma} = \{ z \in \mathbb{C};\ Re(z) \geq -\delta \text{ and } |z| \leq R \}.$$



Let M denote the maximum of $|F(z+w)|$ on $\tilde{\Gamma}$ and let Γ denote the contour obtained by following the outside of $\tilde{\Gamma}$ in a counterclockwise path. Let A be the part of Γ with $Re(z)>0$ and B the remainder part of Γ. For $N \in \mathbb{N}$, consider the function

$$F(z+w) N^z \left(\frac{1}{z} + \frac{z}{R^2} \right),$$

which is analytic on $\tilde{\Gamma}$, except a (possible) simple pole at $z=0$. Then by Cauchy's residue theorem,

$$2\pi i F(w) = \int_{\Gamma} F(z+w) N^z \left(\frac{1}{z} + \frac{z}{R^2} \right) dz$$

$$= \int_{A} F(z+w) N^z \left(\frac{1}{z} + \frac{z}{R^2} \right) dz + \int_{B} F(z+w) N^z \left(\frac{1}{z} + \frac{z}{R^2} \right) dz \quad \text{—— (1)}$$

We see that on A, $F(z+w)$ is equal to its series. We split the series as

$$S_N(z+w) = \sum_{n=1}^{N} \frac{a_n}{n^{z+w}} \quad \text{and} \quad R_N(z+w) = F(z+w) - S_N(z+w)$$

Note that $S_N(z+w)$ is analytic for $z \in \mathbb{C}$. Let C be the contour given by the path $|z| = R$, taken in counterclockwise direction. Thus by Cauchy's residue theorem,

$$2\pi i S_N(w) = \int_C S_N(z+w) N^z \left(\frac{1}{z} + \frac{z}{R^2}\right) dz.$$

Note that $C = A \cup (-A) \cup \{iR, -iR\}$. Thus

$$2\pi i S_N(w) = \int_A S_N(z+w) N^z \left(\frac{1}{z} + \frac{z}{R^2}\right) dz + \int_{-A} S_N(z+w) N^z \left(\frac{1}{z} + \frac{z}{R^2}\right) dz.$$

By changing variable z to $-z$ in the above second integral,

$$\int_{-A} S_N(z+w) N^z \left(\frac{1}{z} + \frac{z}{R^2}\right) dz = \int_A S_N(-z+w) N^{-z} \left(\frac{1}{z} + \frac{z}{R^2}\right) dz.$$

Thus

$$2\pi i S_N(w) = \int_A \left(S_N(z+w) N^z + S_N(-z+w) N^{-z}\right) \left(\frac{1}{z} + \frac{z}{R^2}\right) dz.$$

Combining this with (1), we have

$$2\pi i (F(w) - S_N(w)) = \int_A \left(R_N(z+w) N^z - S_N(-z+w) N^{-z}\right) \left(\frac{1}{z} + \frac{z}{R^2}\right) dz$$

① ——

$$+ \int_B F(z+w) N^z \left(\frac{1}{z} + \frac{z}{R^2}\right) dz.$$

We want $S_N(w) \to F(w)$ as $N \to \infty$. Write $z = x + iy$ with $x, y \in \mathbb{R}$. Then for $z \in A$, we have $|z| = R$ and thus

$$\frac{1}{z} + \frac{z}{R^2} = \frac{2x}{R^2}.$$

Since $|n^z| = n^x$, we have

$$|R_N(z+w)| \le \sum_{n=N+1}^{\infty} \frac{1}{n^{\mathrm{Re}(z+w)}} \le \sum_{n=N+1}^{\infty} \frac{1}{n^{x+1}} \le \int_N^{\infty} \frac{1}{u^{x+1}} du = \frac{1}{xN^x}.$$

Also, we have

$$|S_N(-z+w)| \le \sum_{n=1}^{N} \frac{1}{n^{-x+1}} \le N^{x-1} + \int_1^N u^{x-1} du \le N^{x-1} + \frac{N^x}{x}.$$

Thus

$$|S_N(-z+w)| \le N^x \left(\frac{1}{N} + \frac{1}{x}\right).$$

Combining the above estimates, we have

$$\left|\int_A \left(R_N(z+w)N^z - S_N(-z+w)N^{-z}\right)\left(\frac{1}{z}+\frac{z}{R^2}\right)dz\right|$$

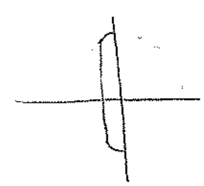
$$\le \int_A \left(\frac{1}{xN^x}N^x + N^x\left(\frac{1}{N}+\frac{1}{x}\right)N^{-x}\right)\frac{2x}{R^2}\,dz$$

$$= \int_A \left(\frac{2}{x}+\frac{1}{N}\right)\frac{2x}{R^2}\,dz$$

$$\le \int_A \left(\frac{4}{R^2}+\frac{2x}{NR^2}\right)dz$$

$$\le \left(\frac{4}{R^2}+\frac{2}{NR}\right)\pi R \qquad (\text{since } x \le R)$$

$$= \frac{4\pi}{R} + \frac{2\pi}{N}$$



We now estimate the integral over B. Divide B into two parts: $\mathrm{Re}(z) = -\delta$ and $-\delta < \mathrm{Re}(z) \le 0$. For $z \in B$ with $\mathrm{Re}(z) = -\delta$, since $|z| \le R$, we have

$$\left|\frac{1}{z}+\frac{z}{R^2}\right| = \left|\frac{1}{z}\right|\left|\frac{\bar z}{\bar z}+\frac{z\bar z}{R}\right| \le \frac{1}{\delta}\left(1+\frac{|z|^2}{R^2}\right) \le \frac{2}{\delta}.$$

Since $|F(z+w)| \le M$ for $z \in B$, we have 2015 10 07

$$\left|\int_B F(z+w)N^z\left(\frac{1}{z}+\frac{z}{R^2}\right)dz\right| \le \int_{-R}^{R} MN^{-\delta}\frac{2}{\delta}\,dz + 2\left|\int_{-\delta}^{0} MN^x\frac{2x}{R^2}\,dx\right|$$

$$\le \frac{4MR}{\delta N^\delta} + \frac{4M}{R^2}\underbrace{\left|\int_{-\delta}^{0} xN^x\,dx\right|}_{=\left(\frac{1}{\log N}-\frac{1}{N^\delta \log ?}\right)\ (\text{exercise})}$$

② $\qquad$ $$\le \frac{4MR}{\delta N^\delta} + \frac{4M\delta}{R^2\log N}$$

Combining ① and ②, we get

$$\left|2\pi i\left(F(w)-S_N(w)\right)\right| \le \frac{4\pi}{R}+\frac{2\pi}{N}+\frac{4MR}{\delta N^\delta}+\frac{4M\delta}{R^2\log N}$$

i.e. $$\left|F(w)-S_N(w)\right| \le \frac{2}{R}+\frac{1}{N}+\frac{MR}{\delta N^\delta}+\frac{2M\delta}{R^2\log N}$$

Given $\varepsilon > 0$, choose $R = 3/\varepsilon$. Then for N sufficiently large,

$$|F(w)-S_N(w)| < \varepsilon.$$

It implies that $S_N(w) \to F(w)$ as $N \to \infty$. ■

Theorem 21: Let μ be the Möbius function. We have
$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n} = 0.$$

Proof: For $Re(s)>1$, we have
$$\frac{1}{\zeta(s)} = \prod_p \left(1-\frac{1}{p^s}\right) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}.$$
We have seen in Theorems 18 and 19 that the function $(s-1)\zeta(s)$ $=f(s)$ (say) is analytic and non-zero in $Re(s)\geq 1$. Thus
$$\frac{1}{\zeta(s)} = \frac{s-1}{f(s)},$$
which is analytic in $Re(s)\geq 1$. By theorem 20,
$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}$$
converges to
$$\frac{1}{\zeta(s)}$$
for $Re(s)\geq 1$. In particular, it converges at $s=1$. Since $\zeta(s)$ has a pole at $s=1$, $\frac{1}{\zeta(s)}$ has a zero at $s=1$. It follows that
$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n} = \frac{1}{\zeta(1)} = 0. \quad ■$$

Theorem 22: We have
$$\sum_{n\leq x} \mu(n) = o(x).$$

Proof: Take
$$a_n = \frac{\mu(n)}{n} \quad \text{and} \quad f(u) = u.$$
Then
$$A(x) = \sum_{n\leq x} \frac{\mu(n)}{n} = o(1)$$

by Theorem 21. By Abel's summation, we have

$$\sum_{n \le x} \mu(n) = A(x)x - \int_1^x A(u)\,du = o(x).$$

Theorem 23: Let $d(n)$ be the number of positive divisors of n. We have

use ... 42

$$\sum_{m=1}^{n} d(m) = \sum_{x=1}^{n} \left\lfloor \frac{n}{x} \right\rfloor = n\log n + (2\gamma - 1)n + O(n^{1/2}),$$

where γ is Euler's constant.

Proof: Let

$$D_n = \{(x,y) \in \mathbb{R}^2 ;\ x>0,\ y>0,\ xy \le n\}.$$

We say $(x,y) \in D_n$ is a <u>lattice point</u> of D_n if $x, y \in \mathbb{Z}$. Note that each lattice point in D_n satisfies $xy = m$ for some $m \in \mathbb{N}$ with $1 \le m \le n$. Thus $\sum_{m=1}^{n} d(m)$ is the number of lattice points in D_n. Note that for each fixed $x \in \{1, 2, \ldots, n\}$, there are $\lfloor \frac{n}{x} \rfloor$ many y with $xy \le n$. Thus

$$\sum_{m=1}^{n} d(m) = \sum_{x=1}^{n} \left\lfloor \frac{n}{x} \right\rfloor .$$

Divide the lattice points in D_n into three disjoint regions:

$$D_{n,1} = \{(x,y) \in \mathbb{N}^2 ;\ xy \le n,\ x<y\};$$
$$D_{n,2} = \{(x,y) \in \mathbb{N}^2 ;\ xy \le n,\ x>y\};$$
$$D_{n,3} = \{(x,y) \in \mathbb{N}^2 ;\ xy \le n,\ x=y\}.$$

We have $|D_{n,1}| = |D_{n,2}|$. Let $(x,y) \in D_{n,1}$. Then

$$x^2 < xy \le n \implies x \le \sqrt{n}.$$

Also, for a fixed x, the number of y satisfying $xy \le n$ and $y > x$ is $\lfloor \frac{n}{x} \rfloor - \lfloor x \rfloor$. Also, $|D_{n,3}| = \lfloor \sqrt{n} \rfloor$. Thus

$$\sum_{x=1}^{n} \left\lfloor \frac{n}{x} \right\rfloor = 2 \sum_{x=1}^{\lfloor \sqrt{n} \rfloor} \left(\left\lfloor \frac{n}{x} \right\rfloor - \lfloor x \rfloor \right) + \lfloor \sqrt{n} \rfloor$$

$$= 2 \sum_{x=1}^{\lfloor \sqrt{n} \rfloor} \left(\frac{n}{x} - x + O(1) \right) + \lfloor \sqrt{n} \rfloor$$

$$= \underbrace{2n \left(\log \lfloor \sqrt{n} \rfloor + \gamma + O\left(\frac{1}{\sqrt{n}} \right) \right)}_{\text{(by Theorem 14)}} - 2 \left(\frac{\lfloor \sqrt{n} \rfloor (\lfloor \sqrt{n} \rfloor + 1)}{2} \right) + O(\sqrt{n}).$$

Since $\lfloor\sqrt{n}\rfloor = \sqrt{n} - \{\sqrt{n}\}$ and $\log(1-r) = O(r)$ for $0<r<1$ we have

$$\log\lfloor\sqrt{n}\rfloor = \log\left(\sqrt{n}-\{\sqrt{n}\}\right) = \log\sqrt{n} + \log\left(1 - \frac{\{\sqrt{n}\}}{\sqrt{n}}\right) = \log\sqrt{n} + O\left(\frac{1}{\sqrt{n}}\right)$$

Combining all the above estimates

$$\sum_{m=1}^{n} d(m) = \sum_{x=1}^{n} \left\lfloor \frac{n}{x} \right\rfloor$$

$$= 2n\left(\log\sqrt{n} + \gamma + O\left(\frac{1}{\sqrt{n}}\right)\right) - n + O(\sqrt{n})$$

$$= n\log n + (2\gamma - 1)n + O(\sqrt{n}).$$

■

2015 10 09

Proposition 24: Given a function $f:\mathbb{R}^+ \to \mathbb{C}$, let

$$F(x) = \sum_{n\le x} f\left(\frac{x}{n}\right).$$

Then we have

$$f(x) = \sum_{n\le x} \mu(n) F\left(\frac{x}{n}\right).$$

Proof: By proposition 10,

$$f(x) = \sum_{n\le x}\left(\sum_{k\mid n}\mu(k)\right) f\left(\frac{x}{n}\right)$$

$$= \sum_{k\ell\le x} \mu(k) f\left(\frac{x}{k\ell}\right)$$

$$= \sum_{k\le x} \mu(k)\left(\sum_{\ell\le x/k} f\left(\frac{x}{k\ell}\right)\right)$$

$$= \sum_{k\le x} \mu(k) F\left(\frac{x}{k}\right).$$

■

Theorem 25 (Prime Number Theorem): We have

$$\pi(x) \sim \frac{x}{\log x}.$$

Proof: By theorem 12, it suffices to prove that

$$\psi(x) = \sum_{p^k\le x} \log p \sim x.$$

Let
$$F(x) = \sum_{n\le x}\left(\psi\left(\frac{x}{n}\right) - \left\lfloor\frac{x}{n}\right\rfloor + 2\gamma\right).$$
By proposition 24, we have
$$\psi(x) - \lfloor x\rfloor + 2\gamma = \sum_{n\le x}\mu(n)F\left(\frac{x}{n}\right)$$
i.e. $$\psi(x) = x + O(1) + \sum_{n\le x}\mu(n)F\left(\frac{x}{n}\right).$$
Our goal is to show
$$\sum_{n\le x}\mu(n)F\left(\frac{x}{n}\right) = o(x).$$
We have
$$F(x) = \sum_{n\le x}\psi\left(\frac{x}{n}\right) - \sum_{n\le x}\left\lfloor\frac{x}{n}\right\rfloor + 2\gamma\lfloor x\rfloor. \qquad \text{—— (1)}$$
Note that
$$\begin{aligned}\sum_{n\le x}\psi\left(\frac{x}{n}\right) &= \sum_{n\le x}\sum_{m\le x/n}\Lambda(m)\\ &= \sum_{n\le x}\Lambda(m)\left(\sum_{n\le x/m}1\right)\\ &= \sum_{n\le x}\Lambda(m)\left\lfloor\frac{x}{m}\right\rfloor\\ &= \sum_{p\le x}\log p\left(\left\lfloor\frac{x}{p}\right\rfloor + \left\lfloor\frac{x}{p^2}\right\rfloor + \cdots\right)\\ &= \log(\lfloor x\rfloor!)\\ &= \sum_{n\le x}\log n.\end{aligned}$$
actually a finite sum ending at $\lfloor x/p^k\rfloor$ where $p^k \| x$

We have seen in the proof of theorem 15 that
$$\sum_{n\le x}\log n = x\log x - x + O(\log x).$$
Thus
$$\sum_{n\le x}\psi\left(\frac{x}{n}\right) = x\log x - x + O(\log x). \qquad \text{—— (2)}$$
By theorem 23,

$$\sum_{n=1}^{\lfloor x \rfloor} \left\lfloor \frac{\lfloor x \rfloor}{n} \right\rfloor = \lfloor x \rfloor \log \lfloor x \rfloor + (2\gamma - 1)\lfloor x \rfloor + O(x^{\frac{1}{2}}).$$

Note that

$$\sum_{n=1}^{\lfloor x \rfloor} \left\lfloor \frac{\lfloor x \rfloor}{n} \right\rfloor \le \sum_{n=1}^{\lfloor x \rfloor} \left\lfloor \frac{x}{n} \right\rfloor \le \sum_{n=1}^{\lfloor x \rfloor} \left\lfloor \frac{\lfloor x \rfloor + 1}{n} \right\rfloor.$$

Thus

$$\sum_{n=1}^{\lfloor x \rfloor} \left\lfloor \frac{x}{n} \right\rfloor = x \log x + (2\gamma - 1)x + O(x^{\frac{1}{2}}). \qquad \text{——} \quad (3)$$

Combining (1), (2), and (3), we have

$$F(x) = \left(x\log x - x + O(\log x)\right) - \left(x \log x + (2\gamma - 1)x + O(x^{\frac{1}{2}})\right) + (2\gamma x + O(1))$$

$$= O(x^{\frac{1}{2}}).$$

Thus there exists a constant $c > 0$ such that for $x \ge 1$,

$$|F(x)| < c x^{\frac{1}{2}}.$$

Let $t \in \mathbb{N}$ with $t \ge 2$. Then

$$\left| \sum_{n \le x/t} \mu(n) F\left(\frac{x}{n}\right) \right| \le \sum_{n \le \frac{x}{t}} \left| F\left(\frac{x}{n}\right) \right|$$

$$\le \sum_{n \le x/t} c \left(\frac{x}{n}\right)^{1/2}$$

$$\le c x^{\frac{1}{2}} \left(1 + \int_1^{x/t} \frac{du}{u^{1/2}}\right)$$

$$\le c x^{\frac{1}{2}} \left(1 + 2\left(\frac{x}{t}\right)^{1/2} - 2\right)$$

$$\le 2 \frac{cx}{t^{1/2}}. \qquad \text{——} \quad (4)$$

Observe that F is a step function. In particular, if $a \in \mathbb{Z}$ with $a \le x < a+1$ then $F(x) = F(a)$.

Thus

$$\sum_{x/t < n \le x} \mu(n) F\left(\frac{x}{n}\right) = F(1) \sum_{x/2 < n \le x/1} \mu(n) + \cdots + F(t-1) \sum_{x/t < n \le x/(t-1)} \mu(n).$$

Thus

$$\left| \sum_{x/t < n \le x} \mu(n) F\left(\frac{x}{n}\right) \right| \le |F(1)| \left| \sum_{x/2 < n \le x/1} \mu(n) \right| + \cdots + |F(t-1)| \left| \sum_{x/t < n \le x/(t-1)} \mu(n) \right|$$

$$\le \left(|F(1)|+\cdots+|F(t-1)|\right) \max_{2\le i\le t}\left|\sum_{x/i<n\le x/(i-1)} \mu(n)\right|$$

$$\le \sum_{i=1}^{t} Ci^{\frac{1}{2}} \cdot \max_{2\le i\le t}\left|\sum_{x/i<n\le x/(i-1)} \mu(n)\right|$$

$$= O\left(t^{\frac{3}{2}}x\right).$$

Thus for any given $\varepsilon>0$, choose $t=t(\varepsilon)$ so that

$$\frac{2c}{t^{1/2}} < \frac{\varepsilon}{2}.$$

Then by (4)

$$\left|\sum_{n\le x/t} \mu(n)F\left(\frac{x}{n}\right)\right| < \frac{\varepsilon}{2}x.$$

Now, for (fixed) ε and t, we can choose x sufficiently large so that

$$\left|\sum_{x/t<n\le x} \mu(n)F\left(\frac{x}{n}\right)\right| < \frac{\varepsilon}{2}x.$$

Combining these two inequalities, we have

$$\left|\sum_{n\le x} \mu(n)F\left(\frac{x}{n}\right)\right| < \varepsilon x$$

i.e. $\displaystyle\sum_{n\le x} \mu(n)F\left(\frac{x}{n}\right) = o(x).$ ∎

2015 10 14

Remark 1: In 1896, Hadaman and de la Vallée Possoin proved

$$\pi(x) \sim \frac{x}{\log x}.$$

Let

$$Li(x) = \int_2^x \frac{1}{\log t}\,dt \sim \frac{x}{\log x}\sum_{k=0}^{\infty}\frac{k!}{(\log x)^k} = \frac{x}{\log x} + \frac{x}{(\log x)^2} + \frac{2x}{(\log x)^3} + \cdots.$$

In 1899, de la vallée Poussin proved that as $x\to\infty$, there exists some $a>0$ such that

$$\pi(x) = Li(x) + O\left(xe^{-a\sqrt{\log x}}\right).$$

Remark 2: The main ingredient in the proof of theorem 25 is that

$$\sum_{n\le x} \mu(n) = o(x),$$

which is a consequence of the analytic continuation and non-vanishing of $\zeta(s)$ at $\mathrm{Re}(s)=1$. The Riemann Hypothesis (RH) states that the 'non-trivial zeros' of $\zeta(s)$ all have real part $\frac{1}{2}$. In 1901, Helge von Koch proved that RH is true if and only if

$$\pi(x) = \mathrm{Li}(x) + O(\sqrt{x}\log x).$$

Remark 3: We proved in A1 that

$$N_n = \#\{v \in \mathbb{F}_q[x];\ \deg v = n,\ v \text{ is monic and irreducible}\}$$
$$= \frac{1}{n}\sum_{d\mid n} \mu(d)\, q^{\frac{n}{d}}.$$

Thus we have

$$N_n = \frac{q^n}{n} + O\left(\frac{q^{n/2}}{n}\right).$$

In other words, the "RH in $\mathbb{F}_q[t]$" is true.