Hello!

- Petru Constantinescu, postdoc with Philippe Michel
- Exercise sessions are important!

Students present their solutions, active participation encouraged!

- Learning process is active, not passive!
- Exam: written, modelled after the exercises.

Topic of the course

Let $\mathbb{N} := \{1, 2, 3, \dots\}$.

Goal: Understand multiplicative structure of $\mathbb{N}$

$\mathbb{P} := \{p \in \mathbb{N} : p \text{ prime}\}$.

$\longrightarrow$ multiplicative building blocks of $\mathbb{N}$

Fundamental theorem of arithmetic

For all $n \in \mathbb{N}$, $\exists!\, v_n : \mathbb{P} \to \mathbb{N} \cup \{0\}$ such that $v_n(p) = 0$, for almost all $p \in \mathbb{P}$ and $n = \prod_{p \in \mathbb{P}} p^{v_n(p)}$, i.e. $n = p_1^{e_1} \cdots p_r^{e_r}$.

Goal: Understand the set $\mathbb{P}$.

Theorem (Euclid) $|\mathbb{P}| = \infty$.

Proof: Suppose for contradiction $\mathbb{P}$ is finite, so $\mathbb{P} = \{p_1, \dots, p_r\}$. Let $q := 1 + p_1 \dots p_r$. Then $p_i \nmid q$, $\forall i$. Therefore $q \in \mathbb{P}$, contradiction. $\square$

Let $\pi(x) = \#\{p \le x : p \text{ prime}\}$

Exercise: $\pi(x) \geq \log \log x$.

Refinements:

- Gauss conjectured that $\pi(x) \sim \frac{x}{\log x}$, i.e. $\lim_{x \to \infty} \frac{\pi(x)}{x/\log x} = 1$.

This is true, and is known as the **Prime Number Theorem** (we prove it in this course). It was proven in 1896 by Hadamard and de la Vallée Poussin (independently), more than 100 years after Gauss made the conjecture.

• Q: Are there infinitely many primes with last digit 3?

More generally, if $(a,b)=1$, is
$$|\{an+b : n\in\mathbb{N}\}\cap\mathbb{P}| = \infty \,?$$

Dirichlet: yes!

Proportion of primes $\equiv b \pmod a$ is $\frac{1}{\varphi(a)}$.
This is Prime Number Theorem in Arithmetic Progressions.

• Is $|\{n^2+1 : n\in\mathbb{N}\}\cap\mathbb{P}| = \infty$? Wide open.

Notation:

• Let $f,g : \Delta \to \mathbb{C}$ $(\Delta\subseteq\mathbb{C})$. We say $f = O(g)$ or $f \ll g$ if there is a constant $c>0$ s.t.
$$|f(z)| \le c|g(z)|, \quad \forall z\in\Delta.$$

• Let $z_0\in\Delta$ and $f,g : \Delta\setminus\{z_0\}\to\mathbb{C}$ s.t. g does not vanish near z_0. We say that $f=o(g)$ as $z\to z_0$ if $\lim\limits_{\substack{z\to z_0\\ z\in\Delta}} \frac{f(z)}{g(z)} = 0$.

We don't explicit limit point if $z_0 = \infty$.

Eg: Let $f(x) = x$ and $g(x) = x^2$.
For $x \geq 1$, $f = O(g)$ but g is NOT $O(f)$.
Also $f = o(g)$.

- We often use "big Oh" notation inside expressions. If $f, g, h : \Delta \to \mathbb{C}$, we write
$$f(z) = g(z) + O(h(z))$$
to mean $|f(z) - g(z)| \leq C|h(z)|$, $\forall z \in \Delta$, for some $C > 0$.

If $h = o(g)$, we call $g(z)$ main term and $h(z)$ error term.

Eg:
- $(x+1)^2 = x^2 + O(x)$ for $x \geq 1$
- $\lfloor x \rfloor = x + O(1)$.
- $\sqrt{x+1} = \sqrt{x} + \frac{1}{2\sqrt{x}} + O(x^{-3/2})$ for $x \geq 1$.
$- \frac{1}{8x^{3/2}} + O(x^{-5/2})$.

Further notation:
- For $f, g : \Delta \to \mathbb{C}$, we say $f \asymp g$ if $f = O(g)$ and $g = O(f)$.

• For two positive functions, we write $f(x) \sim g(x)$ as $x \to a$ if $\lim_{x\to a} \frac{f(x)}{g(x)} = 1$.

If we write $f(x) \sim g(x)$ it is assumed $a = \infty$.

We will prove PNT:

$$\pi(x) = \frac{x}{\log x} + O\left(\frac{x}{(\log x)^2}\right)$$

and the stronger version

$$\pi(x) = Li(x) + O\left(x e^{-c\sqrt{\log x}}\right),$$

for some $c > 0$.

where $Li(x) = \int_2^x \frac{1}{\log t} dt$

(Exercise: $Li(x) = x\left(\sum_{j=1}^{k} \frac{(j-1)!}{(\log x)^j}\right) + O\left(\frac{x \cdot k!}{(\log x)^{k+1}}\right)$)

We obtain this by studying analytic properties of Riemann zeta function $\zeta(s) = \sum_{n\geq 1} \frac{1}{n^s}$ $(Re(s) > 1)$.

Riemann hypothesis (RH) All "non-trivial" zeros of ζ lie on the vertical line $Re(s) = \frac{1}{2}$.

Note: $RH \iff \pi(x) = Li(x) + O_\varepsilon(x^{\frac{1}{2}+\varepsilon})$.

Arithmetic functions

Def: An arithmetic function is a function $f: \mathbb{N} \to \mathbb{C}$. Denote $\mathcal{R} = \{f: \mathbb{N} \to \mathbb{C}\}$ the set of all arithmetic functions.

Def (Dirichlet convolution). Let $f, g \in \mathcal{R}$. Dirichlet convolution $f * g \in \mathcal{R}$ is defined

$$(f*g)(n) = \sum_{d \mid n} f(d)\, g\left(\frac{n}{d}\right).$$

Lemma: $\forall f, g, h \in \mathcal{R}$

- $f * g = g * f$ ($*$ is commutative)
- $(f*g)*h = f*(g*h)$ ($*$ is associative)

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

$$((f*g)*h)(n) = \sum_{n=ab} h(b) \sum_{a=cd} f(c)\, g(d) =$$

$$= \sum_{n=bcd} h(b) f(c)\, g(d) = (f*(g*h))(n).$$

In particular, $(\mathcal{R}, +, *)$ is a commutative $\mathbb{C}$-algebra with multiplicative unit $e(n) = \begin{cases} 1, & n=1 \\ 0, & \text{else.} \end{cases}$

<u>Definition</u>: (Multiplicative functions)

- $f \in \mathcal{R}$ is multiplicative if $f \neq 0$ and $f(nm) = f(n) f(m)$, for all coprime integers n, m.

- $f \in \mathcal{R}$ is completely multiplicative if $f \neq 0$ and $f(nm) = f(n) f(m)$, $\forall\, n, m \in \mathbb{N}$.

<u>Remarks</u>
- f completely multiplicative $\Rightarrow$ f multiplicative
- f multiplicative $\Rightarrow$ $f(1) = 1$
- f multiplicative $\Rightarrow$ f is determined by its values on $\{p^l : p \in \mathbb{P}, l \in \mathbb{N}\}$.

<u>Examples</u>:
- $id_{\mathbb{N}}$ (comp mult)
- $\mathcal{E}(n) = 1$ (comp mult)
- $e(n) = \begin{cases} 1, & n = 1 \\ 0, & \text{else} \end{cases}$ (comp mult)
- $\tau(n) = |\{d \in \mathbb{N} : d \mid n\}|$. (mult)

<u>Pf</u>: $\tau(p^l) = l+1$, for $p \in \mathbb{P}$.
Let $n = p_1^{l_1} \cdots p_r^{l_r}$.

$\{d \in \mathbb{N} : d \mid n\} = \{p_1^{k_1} \cdots p_r^{k_r} : 0 \le k_i \le l_i\}$

$\Rightarrow \tau(p_1^{l_1} \cdots p_r^{l_r}) = (l_1+1)\cdots(l_r+1) = \tau(p_1^{l_1})\cdots\tau(p_r^{l_r})$.

$\Rightarrow \tau$ is mult. $\boxtimes$

- $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$. (mult)

<u>Pf</u>: CRT: $(n_1, n_2) = 1 \Rightarrow \mathbb{Z}/n_1n_2\mathbb{Z} \simeq (\mathbb{Z}/n_1\mathbb{Z}) \times (\mathbb{Z}/n_2\mathbb{Z})$ as rings.

$\varphi(p^l) = p^{l-1}(p-1)$.

<u>Theorem</u>: If $f, g \in \mathcal{A}$ multiplicative, then $f * g$ multiplicative.

<u>Ex</u>: $\tau = \varepsilon * \varepsilon$ mult, but NOT completely mult.

$\tau(4) = 3 \neq 4 = \tau(2)^2$.

<u>Pf</u>: Suppose $(n_1, n_2) = 1$.

$$(f*g)(n_1n_2) = \sum_{d \mid n_1n_2} f(d)\, g\left(\frac{n_1n_2}{d}\right) =$$

$$= \sum_{\substack{d_1 \mid n_1 \\ d_2 \mid n_2}} f(d_1d_2)\, g\left(\frac{n_1}{d_1} \cdot \frac{n_2}{d_2}\right)$$

$\{d \mid n_1n_2\} \to \{d_1 \mid n_1\} \times \{d_2 \mid n_2\}$

$d_1d_2 \leftarrow (d_1, d_2)$

$$= \sum_{d_2 | m_2} f(d_2) g\left(\frac{n_2}{d_2}\right) \sum_{d_2 | n_2} f(d_2) g\left(\frac{n_2}{d_2}\right)$$

$$= (f * g)(n_2) \cdot (f * g)(n_2).$$ ☒

Units in $\mathcal{A}$

Theorem $f \in \mathcal{A}$ unit $\iff f(1) \neq 0$.

Pf: "$\Rightarrow$" Suppose $\exists g \in \mathcal{A}$ s.t. $f * g = e$.
Then $1 = e(1) = f(1) g(1) \to f(1) \neq 0$.

"$\Leftarrow$" We inductively define $g \in \mathcal{A}$ s.t. $f * g = e$.
Set $g(1) = \frac{1}{f(1)}$.

Suppose $g(1), \dots, g(n-1)$ already defined. Set

$$g(n) := -\frac{1}{f(1)} \sum_{d | n} f(d) g\left(\frac{n}{d}\right).$$

Then $f * g(n) = e(n)$, $\forall n \in \mathbb{N}$. (easy exercise). ☒

Rmk: We denote the inverse of f by f^{-1}.

Proposition: If $f \in \mathcal{A}^\times$ multiplicative, then so is f^{-1}.

Proof: Let $g \in \mathcal{A}$ multiplicative defined by
$$g(p^\ell) = f^{-1}(p^\ell),\ p \in \mathbb{P},\ \ell \in \mathbb{N}.$$

Then $f*g$ multiplicative and
$$(f*g)(p^\ell) = \sum_{k=0}^{\ell} f(p^k)\, g(p^{\ell-k}) = \sum_{k=0}^{\ell} f(p^k) f^{-1}(p^{\ell-k})$$
$$= (f*f^{-1})(p^\ell) = e(p^\ell).$$
$\Rightarrow f*g = e$, as both $f*g$ and e are determined uniquely by their values on prime powers.
By uniqueness of inverse, $g = f^{-1}$. $\blacksquare$

Example: Let $\mu := \varepsilon^{-1}$ Möbius function.

Lemma: $$\mu(n) = \begin{cases} 1, & n = 1 \\ (-1)^r, & n = p_1 \cdots p_r \\ 0, & \text{else}. \end{cases}$$ product of distinct primes.

Note: $|\mu| =$ indicator set of square-free numbers.

Pf: $\mu(1) = 1$ ✓

$$\mu(p^\ell) = -\frac{1}{\varepsilon(1)} \sum_{k=1}^{\ell} \varepsilon(p^k)\mu(p^{\ell-k}) = -\sum_{k=0}^{\ell-1} \mu(p^k)$$

$\mu(p) = -1$ and inductively for $\ell \geq 2$, $\mu(p^\ell) = 0$.

Now $\mu = \varepsilon^{-1} \Rightarrow \mu$ is mult, so claim follows. $\blacksquare$

__Theorem__ (Möbius Inversion Formula). Let $f, g \in \mathcal{A}$.

$$g(n) = \sum_{d|n} f(d), \quad \forall n \in \mathbb{N}$$

$$\Longleftrightarrow \quad f(n) = \sum_{d|n} \mu(d)\, g\!\left(\frac{n}{d}\right).$$

__Proof__: $g = f * \varepsilon \Longleftrightarrow g * \mu = (f * \varepsilon) * \mu = f * (\varepsilon * \mu) = f$. $\blacksquare$

__Exercise__: $\dfrac{\varphi(n)}{n} = \displaystyle\sum_{d|n} \frac{\mu(d)}{d}$.