Prosti brojevi

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, ...

• Distribucija niza prostih brojeva

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

T.1 Postoji beskonačno mnogo prostih brojeva tj.

$$\pi(x) \longrightarrow \infty, \quad x \to \infty.$$

Dokaz [Euler-ov 2. dokaz]

Euler-ova φ-fja je <u>multiplikativna</u>:

$(m,n) = NZD(m,n) = 1$, onda je

$$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n).$$

▽ Kineska teorema o ostacima:

$$\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \Rightarrow \left(\mathbb{Z}/mn\mathbb{Z}\right)^\times \cong \left(\mathbb{Z}/m\mathbb{Z}\right)^\times \times \left(\mathbb{Z}/n\mathbb{Z}\right)^\times$$

multiplikativna grupa prstena $\mathbb{Z}/mn\mathbb{Z}$

△

• Pretp. da ima samo konačno mnogo prostih brojeva $p_1, p_2, \ldots, p_k$.

$$P := p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_k$$

Onda je zbg multiplikativnosti φ-fje:

$$\varphi(P) = \prod_{i=1}^{k} \varphi(p_i) = \prod_{i=1}^{k} (p_i - 1) =$$

$$= \underbrace{(p_1-1)}_{2-1=1}\underbrace{(p_2-1)}_{3-1=2}\underbrace{(p_3-1)}_{5-1\ge 2}\cdots\underbrace{(p_k-1)}_{\ge 2} \ge 2^{k-1} \ge 2$$

Sledi da postoji bar jedan prirodan broj u intervalu $[2, P]$ koji je uzajamno prost sa P. Ali taj broj mora imati onda (bar jedan, i sve) prost faktor koji je $\neq p_i$, $\forall 1 \leq i \leq k$

2. dokaz [Goldbach]

Ideja - konstruisati niz $2 \leq n_1 < n_2 < n_3 < \dots$ u kome su svaka dva člana uzajamno prosta.

$n_1 = 3$

Za $i > 1$ induktivno definišemo

$$n_i = 2 + \prod_{1 \leq j < i} n_j$$

Svi članovi niza su neparni brojevi.

Za $i > j$ je $n_i \equiv 2 \pmod{n_j}$ $\rightarrow$

$NZD(n_i, n_j) \mid 2$, ali neparni su $\rightarrow$ $NZD(n_i, n_j) = 1$ za $i \neq j$

- Beskonačan niz prostih brojeva: $\{p_i\}$ izaberemo p_i da bude bilo koji prost faktor n_i
- Uzgred, indukcijom se lako pokazuje da je $n_i = 2^{2^{i-1}} + 1$

▼ $n_{i-1} = 2 + \prod_{1 \leq j < i-1} n_j = 2^{2^{i-2}} + 1$, po ind. pretpostavci

$\rightarrow \prod_{1 \leq j < i-1} n_j = 2^{2^{i-2}} - 1$

$$n_i = 2 + \left(\prod_{1 \le j < i-1} n_j \right) \cdot n_{i-1} = 2 + \left(2^{2^{i-2}} - 1\right)\left(2^{2^{i-2}} + 1\right)$$

Primedba 1: Iz Goldbach-ovog dokaza sledi da smo u intervalu $[1, x]$ našli $\log\log x$ različitih prostih brojeva tj. da je

$$\pi(x) \gg \log\log x, \qquad x \to \infty.$$

Notacija $f(x) \ll g(x)$, $x \to \infty$ (g pozitivna fja)

ako $\exists\, c > 0$. $|f(x)| \le c \cdot g(x)$, za sve $x \ge x_0$

$\ll$ isto što $\mathcal{O}$

↓ notacija Vinogradova — ↓ notacija Landau-a

Primedba 2: Ako $p \mid n_i = 2^{2^{i-1}} + 1$, sledi

$$2^{2^{i-1}} \equiv -1 \pmod{p},$$ pa:

$$2^{2^i} \equiv \left(2^{2^{i-1}}\right)^2 \equiv (-1)^2 \equiv 1 \pmod{p}$$

Što znači da je red elementa 2 u grupi $(\mathbb{Z}/p\mathbb{Z})^\times$ tačno 2^i. Sledi

$$2^i \mid |(\mathbb{Z}/p\mathbb{Z})^\times| = p - 1 \quad \text{tj.}$$

$$p \equiv 1 \pmod{2^i}$$

Neka je sada k - fiksiran prirodan br.
Za svako $i \geq k$ izaberemo $p_i \mid n_i$, koje onda zadovoljava

$$p_i \equiv 1 \pmod{2^i}, \text{ a time pre: } p_i \equiv 1 \pmod{2^k}$$

Dakle, dobili smo: da aritmetička progresija

$$AP(1 \bmod 2^k) = \{1, 1+2^k, 1+2\cdot 2^k, 1+3\cdot 2^k, \ldots, 1+m\cdot 2^k, \ldots\}$$

sadrži ∞ mnogo prostih brojeva!

Riemann-ova zeta funkcija

$s \in \mathbb{C}$, $\mathrm{Re}(s) > 1$ Riemann, 1859.:

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}$$

Euler je proučavao ovu fju 100 godina ranije, ali kao fju realne promenljive s. Euler je pokazao da važi

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p} \frac{1}{1-\frac{1}{p^s}} \qquad (s>1) \qquad (1)$$

Opšta teorema o Euler-ovoj faktorizaciji:

f je multiplikativna fja ako $f(mn) = f(m)f(n)$, $\forall m,n \in \mathbb{N}$ $(m,n)=1$

T.2 [Euler-ova faktorizacija] Neka je f multiplikativna fja
Ako važi (bar jedan od uslova)

(i) $\sum_{n=1}^{\infty} |f(n)| < \infty$

ili

(ii) $\prod_{p} \left(1 + |f(p)| + |f(p^2)| + \dots\right) < \infty$

onda važi jednakost

$$\boxed{\sum_{n=1}^{\infty} f(n) = \prod_{p} \left(1 + f(p) + f(p^2) + \dots\right)} \qquad (2)$$

Ako je f i totalno multiplikativna $\left(f(p^j) = f(p)^j, \ \forall j \geq 1\right)$
onda je

$$\sum_{n=1}^{\infty} f(n) = \prod_{p} \frac{1}{1 - f(p)} .$$

Specijalno, za $s > 1$ i $f(n) = \frac{1}{n^s}$ važi uslov (i)
pa sledi Euler-ova faktorizacija (1).

Dokaz T.2 Pretp. (i). $\sum_{n=1}^{\infty} |f(n)| =: S_0 < +\infty$

Onda: za $\forall$ prost p red

$\sum_{k=0}^{\infty} f(p^k)$ konvergira apsolutno i $\sum_{k=0}^{\infty} |f(p^k)| \leq S_0$

Onda je za $x \in \mathbb{R}$

$$P(x) := \prod_{p \leq x} \left(1 + f(p) + f(p^2) + f(p^3) + \dots\right)$$

konačan proizvod apsolutno konvergentnih redova.

Odatle sledi da je (za fiksirano x)

$$P(x) = \sum_{\substack{n \geq 1 \\ p \mid n \Rightarrow p \leq x \\ \text{prost}}} f(n)$$

Označimo $S := \sum_{n=1}^{\infty} f(n)$ (konačno, jer po (i) red konvergira apsolutno)

$$S - P(x) = \sum_{\substack{n \geq 1 \\ p \mid n \text{ za neko } p > x}} f(n),$$ pa je

$$|S - P(x)| \leq \sum_{n > x} |f(n)| \longrightarrow 0, \quad x \to \infty \text{ (prema (2'))}$$

$$\Longleftrightarrow \quad P(x) \longrightarrow S, \quad x \to \infty,$$ što je upravo (2). ∎

- Pretp. da važi (ii). Dokazaćemo da onda mora da važi i (i).

$$P_0 := \prod_p \left(1 + |f(p)| + |f(p^2)| + \dots\right) < +\infty$$

Definišimo

$$P_0(x) := \prod_{p \leq x} \left(1 + |f(p)| + |f(p^2)| + \dots\right)$$

$$= \sum_{\substack{n \geq 1 \\ p \mid n \Rightarrow p \leq x}} |f(n)| \geq \sum_{1 \leq n \leq x} |f(n)|$$

Dodatno, $P_0(x) \leq P_0, \quad \forall x > 0$

pa ~~su~~ parcijalne sume $\sum_{n \le x} |f(n)| \le P_0$

čitve ograničen, rastući (po x) niz, koji onda dakle konvergira, što je uslov (i). ◢

3. dokaz (T1) [Euler-ov 1. dokaz]

Definišimo aritmetičku funkciju $f(n) = \frac{1}{n}$, $\forall n \in \mathbb{N}$.

Ako bi postojalo samo konačno mnogo prostih $p_1, p_2, \dots, p_k$ onda je uslov (ii) (T2) trivijalno zadovoljen

$$\prod_{j=1}^{k} \left(1 + \frac{1}{p_j} + \frac{1}{p_j^2} + \frac{1}{p_j^3} + \dots\right) = \prod_{j=1}^{k} \frac{1}{1 - \frac{1}{p_j}} < +\infty$$

Onda bi po (T2) sledilo

$$\sum_{n=1}^{\infty} \frac{1}{n} = \prod_{p} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \dots\right) < \infty \quad \lightning$$

jer ovaj (harmonijski) red divergira ◢

- Dakle, prostih brojeva ima beskonačno mnogo i red $\sum_{p \text{ prost}} \frac{1}{p}$ ima beskonačno mnogo članova.

Konvergentan?

(T3) [Euler] $\sum_{p} \frac{1}{p}$ divergira (suma se po svim prostim brojevima p)

Pretp. da red $\sum \frac{1}{p}$ konvergira. $C := \sum \frac{1}{p} < \infty$

Primenimo ponovo (T2) za $f(n) = \frac{1}{n}$. Proverićemo da onda važi (ii).

$$\prod_{p \le x} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \dots\right) = \prod_{p \le x} \frac{1}{1 - \frac{1}{p}} = \prod_{p \le x} \left(1 + \frac{1}{p-1}\right) \le \prod_{p \le x} \left(1 + \frac{2}{p}\right)$$

Iz $e^t = 1 + t + \frac{t^2}{2!} + \frac{t^3}{3!} + \dots$ sledi $\boxed{e^t \ge 1 + t}$, za sve $t \ge 0$

odakle je

$$\prod_{p \le x} \left(1 + \frac{2}{p}\right) \le \prod_{p \le x} e^{\frac{2}{p}} = e^{\sum_{p \le x} \frac{2}{p}} \le e^{2C}$$

Dakle, parcijalni proizvodi $\prod_{p \le x} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \dots\right)$ čine ograničen, rastući (po x) niz, pa je odgovarajući beskonačni proizvod konvergentan, tj. važi uslov (ii) (T2). Ali onda bi sledilo

$$\sum_{n=1}^{\infty} \frac{1}{n} = \prod_{p} \frac{1}{1 - \frac{1}{p}} \le e^{2C}$$ ↯

Primedba Možemo da dobijemo i eksplicitnu donju ocenu za parcijalne sume $\sum_{p \le x} \frac{1}{p}$. Za $x \ge 2$

$$\prod_{p \le x} \frac{1}{1 - \frac{1}{p}} = \prod_{p \le x} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \dots\right) = \sum_{\substack{n \ge 1 \\ p \mid n \Rightarrow p \le x}} \frac{1}{n} \ge \sum_{n \le x} \frac{1}{n} \ge \lg x$$

[Analiza 1]

Sa druge strane $\frac{1}{1 - \frac{1}{p}} = 1 + \frac{1}{p-1} \le e^{\frac{1}{p-1}}$, pa dobijamo

$$\lg x \le \prod_{p \le x} e^{\frac{1}{p-1}} \iff \lg \lg x \le \sum_{p \le x} \frac{1}{p-1}.$$

Konačno

$$\sum_{p\le x}\frac{1}{p}=\sum_{p\le x}\frac{1}{p-1}-\sum_{p\le x}\left(\frac{1}{p-1}-\frac{1}{p}\right)$$

$$\ge\sum_{p\le x}\frac{1}{p-1}-\sum_{n\ge 2}\left(\frac{1}{n-1}-\frac{1}{n}\right)=\left(\sum_{p\le x}\frac{1}{p-1}\right)-1\ge \lg\lg x-1$$

■

(T) [Kompleksna analiza, Analiza 2]

Za sve $z\in\mathbb{C}$ važi sledeća Weierstrass-ova faktorizacija:

$$\boxed{\sin z = z\prod_{k=1}^{\infty}\left(1-\frac{z^2}{\pi^2k^2}\right)}$$

$$\log\sin z=\log z+\sum_{k=1}^{\infty}\log\left(1-\frac{z^2}{\pi^2k^2}\right) \qquad / \text{izvod}$$

$$\frac{\cos z}{\sin z}=\frac{1}{z}+\sum_{k=1}^{\infty}\frac{-\frac{2z}{\pi^2k^2}}{1-\frac{z^2}{\pi^2k^2}}$$

$$z\operatorname{ctg} z=1-2\sum_{k=1}^{\infty}\left(\frac{z^2}{\pi^2k^2}+\left(\frac{z^2}{\pi^2k^2}\right)^2+\left(\frac{z^2}{\pi^2k^2}\right)^3+\dots\right)$$

$$=1-2\sum_{k=1}^{\infty}\sum_{m=1}^{\infty}\frac{z^{2m}}{\pi^{2m}k^{2m}}$$

$$=1-2\sum_{m=1}^{\infty}\frac{z^{2m}}{\pi^{2m}}\underbrace{\sum_{k=1}^{\infty}\frac{1}{k^{2m}}}_{\zeta(2m)}$$

$$\boxed{z\operatorname{ctg} z=1-2\sum_{m=1}^{\infty}\frac{\zeta(2m)}{\pi^{2m}}\cdot z^{2m}}$$

(3)

Izračunajmo Taylor-ove koeficijente u $z=0$

$$f(z) = z\,\frac{\cos z}{\sin z}$$

$$f'(z) = \frac{\cos z}{\sin z} + z\,\frac{-(\sin z)^2 - (\cos z)^2}{(\sin z)^2} = \frac{\cos z}{\sin z} - \frac{z}{(\sin z)^2}$$

$$f''(z) = \frac{-(\sin z)^2 - (\cos z)^2}{(\sin z)^2} - \frac{(\sin z)^2 - 2z\cdot(\sin z)(\cos z)}{(\sin z)^4}$$

$$= -\frac{2(\sin z)^2 - 2z(\sin z)(\cos z)}{(\sin z)^4} = -2\,\frac{\sin z - z\cdot\cos z}{(\sin z)^3}$$

Iz (3) vidimo da je (uspoređujući koeficijente uz z^2)

$$\frac{f''(0)}{2!} = -2\,\frac{\zeta(2)}{\pi^2}$$

$$f''(0) = -2\lim_{z\to 0}\frac{\left(z - \frac{z^3}{6} + \mathcal{O}(z^5)\right) - \left(z - \frac{z^3}{2} + \mathcal{O}(z^5)\right)}{\left(z - \frac{z^3}{6} + \mathcal{O}(z^5)\right)^3} = -2\cdot\frac{1}{3}$$

pa je

T4 $$\boxed{\zeta(2) = \frac{\pi^2}{6}}$$

Slično, ako računamo Taylorov koef. uz z^4 dobijemo:

$$\boxed{\zeta(4) = \frac{\pi^4}{90}}$$

4. dokaz (T1)

Iz (T4) imamo da je

$$\frac{\zeta(2)^2}{\zeta(4)} = \frac{\frac{\pi^4}{36}}{\frac{\pi^4}{90}} = \frac{5}{2}$$

a iz Eyler-ove faktorizacije sa druge strane je

$$\frac{\zeta(2)^2}{\zeta(4)} = \prod_p \frac{1-\frac{1}{p^4}}{\left(1-\frac{1}{p^2}\right)^2} = \prod_p \frac{p^4-1}{p^4} \cdot \frac{p^4}{(p^2-1)^2} = \prod_p \frac{p^2+1}{p^2-1}$$

pa je

$$\frac{5}{2} = \frac{5}{3} \cdot \frac{10}{8} \cdot \frac{26}{24} \cdot \frac{50}{48} \cdot \dots$$

Ako bi postojalo samo konačno mnogo prostih brojeva, onda bi proizvod na d.s. bio konačan, pa bi bio razlomak $\frac{M}{N}$, gde je $M = 5 \cdot 10 \cdot 26 \cdot 50 \cdot \dots$

$N = \underline{3} \cdot 8 \cdot 24 \cdot 48 \cdot \dots$

Ali $\frac{M}{N} = \frac{5}{2}$ tj. $2M = 5N$.

Kako $3 \mid N \longrightarrow 3 \mid M$.

Ali: M je proizvod brojeva oblika p^2+1 ($0^2+1 \equiv 1 \pmod 3$, $1^2+1 \equiv 2 \pmod 3$, $2^2+1 \equiv 2 \pmod 3$)

od kojih nijedan nije deljiv sa 3. ↯

Beskvadratni brojevi

$n \in \mathbb{N}$ je <u>beskvadratan</u> ako nije deljiv sa d^2, ni za jedno $d \in \mathbb{N}$, $d > 1$.

- Osnovna teorema aritmetike (jedinstvenost faktorizacije u $\mathbb{Z}$):

$$\left\{\begin{array}{l}\text{konačni podskupovi}\\ \text{skupa prostih brojeva}\end{array}\right\} \xleftrightarrow{\text{bijekcija}} \left\{\begin{array}{l}\text{beskvadratni}\\ \text{prirodni brojevi}\end{array}\right\}$$

$$S \longmapsto \prod_{p \in S} p$$

- Sada, ako bi postojalo samo konačno mnogo prostih brojeva ($=k$) onda bi : beskvadratnih prirodnih brojeva bilo samo konačno mnogo ($=2^k$).

5. dokaz (T1) [J. Perott, 1881.]

- Posmatrajmo prvih N prirodnih br: $1, 2, 3, \ldots, N-1, N$

Hoćemo da "prosejemo" beskvadratne brojeve:

- da eliminišemo prvo brojeve deljive sa 2^2
- zatim deljive sa 3^2
- pa sa $4^2, 5^2$ itd.

Ukupno (i najviše) smo eliminisali (eliminisali smo i manje - jer imamo preklapanja - brojeve deljive sa $2^2 \cdot 3^2$ itd.)

$$\sum_{k=2}^{\infty} \left\lfloor \frac{N}{k^2} \right\rfloor \leq N \sum_{k=2}^{\infty} \frac{1}{k^2} = N \cdot \left(\zeta(2) - 1\right)$$

Ako sa $A(N)$ označimo ukupan broj beskvadratnih brojeva u $[1, N]$, dobijamo dalje da je

$$A(N) \geq N - N \cdot (\zeta(2) - 1) = N \cdot (2 - \zeta(2)) \quad \text{[T4]}$$

$$= N \cdot \left(2 - \frac{\pi^2}{6}\right) \geq 0.355\, N$$

Specijalno, $A(N) \longrightarrow \infty$, $N \to \infty$, pa beskvadratnih, a time i prostih, brojeva ima ∞ mnogo ◢