38. tétel

A prímszámelmélet elemei. $\sum \frac{1}{p}$ divergenciája. Dirichlet-tétele (bizonyítás spec. esetekben)

Tétel: A prímszámok száma végtelen.

BIZ.: 1, Euklidesz-féle ind.

2., Fermat-számok $\left(F_n = 2^{2^n}+1 \quad (n=0,1\ldots)\right)$

biz be, h. a F. számok páronként relatív prímek.

$k \geq 1 \wedge n \geq 0$ pozitív egészek $\wedge$! $d = (F_{n+k}, F_n)$

Mivel: $F_{n+k} = 2^{2^n 2^k} + 1 = (F_n - 1)^{2^k} + 1$

binomiális tétellel könnyen beláthato, h. F_{n+k} alakja:

$F_{n+k} = F_n t + 2 \qquad t>0 \ (\in \mathbb{Z})$

De: $d \mid F_n \wedge d \mid F_{n+k} \Rightarrow d \mid 2 \wedge$ így $d=1$, mivel a F-számok páratlanok.

Így a F-számok valóban páronként relatív prímek. Minden egyes F-szám tartalmaz legalább egy prímtényezőt, ami a relatív prímség miatt különbözik a többi F-szám prímtényezőitől. Így legalább annyi prím van, mint F-szám, azaz végtelen sok.

3., $\sum_{p \leq x} \frac{1}{p}$ div /p prím/

Tétel: $\exists\, c \in \mathbb{R}^+$, hogy $x>1$ $\quad c \cdot \log\log x < \sum_{p \leq x} \frac{1}{p}$

$$\sum_{m=1}^{n} \frac{1}{m} < \prod_{p \le n} \left(1 + \frac{1}{p} + \frac{1}{p^2} \dots\right)$$ Euler-féle azonosság

→ végtelen mértani sor összege

A jobb oldalon több szám található, mint a bal oldalon.

$$\log n < \prod_{p \le n} \frac{1}{1 - \frac{1}{p}} \quad / \log$$

$$\log n < \sum_{m=1}^{n} \frac{1}{m}$$

$$\overbrace{\log 1}^{0} - \log\left(1 - \frac{1}{p}\right)$$

$$\log\log n < - \sum_{p \le n} \log\left(1 - \frac{1}{p}\right)$$

Segédtétel:

$$0 < x \le \frac{1}{2} \quad - \log(1 - x) < 2x$$

$$\frac{1}{2} \log\log n < \sum_{p \le n} 2 \cdot \frac{1}{p}$$

BRUN: $\sum_{p,\, p+2 \text{ prím}} \frac{1}{p} = c \in \mathbb{R}$

ha p és $p+2$ prímek ⇒ ikerprímek

3: ha találunk egy minorálló fgv-t, amely a végtelenbe tart ⇒ végtelen sok ikerprím van.

Ma sem ismert, hány ikerprím van.

Járai Antal: ma ismert 2. legnagyobb ikerprím:

$$242206083 \cdot 2^{38880} \pm 1$$

Tétel: (Dirichlet)

Legyenek a, b zérustól különböző relatív prím természetes számok. Ekkor az $ak + b$ $(k = 0, 1, 2 \dots)$ végtelen számtani sorozat tagjai között végtelen sok prímszám van.

Speciális esetei: $(a=4;\ b=\pm 1)$

a; Tétel: Végtelen sok $4k-1$ alakú prímszám van. $(k=1,2\dots)$

BIZ.: ind. $p_1, p_2 \dots p_n$ (véges sok $4k-1$ alakú prím létezik)

$A := 4p_1 \cdot \dots \cdot p_n - 1$

1., ha A prím $\Rightarrow A = 4k-1$ alakú $\wedge$ különbözik $p_1; \dots ; p_n$-től

$\Rightarrow \lightning \quad p_{n+1} := A$

2., ha A nem prím $\Rightarrow \exists\, p$ prím, amelyre : $p \mid A$

$p \neq p_i \quad (i=1,\dots,n)$, mert ind $p \mid A \wedge p \mid 4p_1 \dots p_n \Rightarrow p \mid 1$

$\exists\, p$ amelynek az alakja $4k-1$: ind

$\underbrace{(4k_1+1)(4k_2+1)} = 4K+1$ nem állítható elő A.

mindig $4k+1$ alakú lesz, nem állítható elő $4k-1$ alakú $\lightning$

b; Tétel: Végtelen sok $4k+1$ alakú prímszám van. $(k=1,2\dots)$

BIZ.: konstrukciós bizonyítás:

$n > 1,\ n \in \mathbb{N}$

$m_1 := (n!)^2 + 1 \rightarrow 4k+1$ alakú szám

$\exists\, p$ prím, amelyre a $p \mid m_1 = (n!)^2 + 1$ $\wedge$ a $p = 4k+1$ alakú

páratlan

$p \nmid n!$

$(n!)^2 \equiv -1 \pmod p$, de $\underbrace{n! = 1\cdot 2\cdot 3 \cdot \dots \cdot n \text{, ha } p \mid n! \Rightarrow 2 \leq p \leq n}$

$\boxed{p > n}$

$p \nmid n! \Rightarrow (p, n)! = 1$

$n!^{p-1} \equiv 1 \pmod p$ (KIS-F. TÉTEL)

emeljük $\frac{p-1}{2}$-dik hatványra

$(n!)^{p-1} \equiv (-1)^{\frac{p-1}{2}} \pmod p$

$(-1)^{\frac{p-1}{2}} \equiv 1 \pmod p$

$(-1)^{\frac{4k-2}{2}} \equiv 1 \pmod p \Rightarrow p \mid 2 \ \lightning$

páros

ha $p = 4k+1$

$$(-1)^{\frac{4k}{2}} \equiv 1 \pmod p$$ ✓

Köv szám: $p_1 := p$

$$n_2 := (p_1!)^2 + 1 \;\dots \rightarrow p_2 = 4k+1$$

$$p_2 > p_1 > n$$

$$n_3 := (p_2!)^2 + 1 \;\dots \rightarrow p_3 = 4k+1$$

$$p_3 > p_2 > p_1 > n$$

Tétel: Minden $Q > 1$ egész szám esetén található egy p prím úgy, a $[p-Q, p+Q]$ intervallumban csak p a prím.

BIZ.: Legyen q prím, melyre $q > Q+2$,

$$s = 2 \cdot 3 \dots (q-1)(q+1)(q+2) \dots (2q-2).$$

Mivel $q \nmid s \Rightarrow (q, s) = 1$ így a Dirichlet-tétel miatt $\exists\, k > 0$ természetes szám, melyre $p = sk + q$ prím.

De: $p + i = 2 \dots (q-2)(q-1)(q+1)(q+2) \dots (q+(q-2))k + (q+i)$ osztható $(q+i)$-vel $\forall\, i = 1, 2 \dots, q-2$ esetén és a $p-i$ számok oszthatók $(q-i)$-vel $\Rightarrow$ $p+i$, $p-i$ összetett, ha $1 \le i \le q-2$.

$\Downarrow$

állítás: mivel $q-2 > Q$