BIZ: (lsd TK)

Multiplikatív fgv-ek konvolúciós fgv-e is multiplikatív.

Következmény: Multiplikatív fgv-ek összegezési ill. megfordítása (Moebius tr.) fgv. ugyancsak multiplikatív, ezért ebben a témában is elegendő prímhatvány helyeken számolni a fgv értékeket.

10.1.

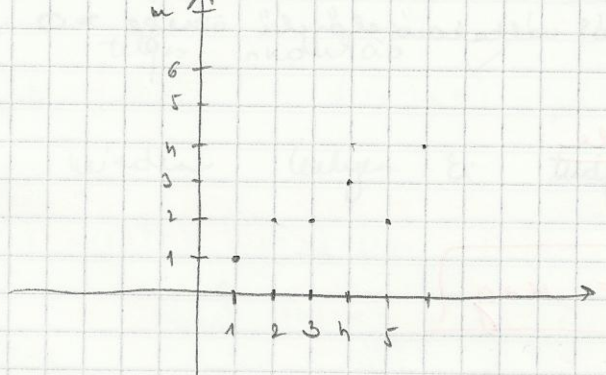
8. előadás

Számelméleti fgv-ek értékkészletének (42. tétel) vizsgálata (d fgv esetén)

$$d(n) = \sum_{d \mid n} 1$$

$d(n) = 1 \iff n = 1;$

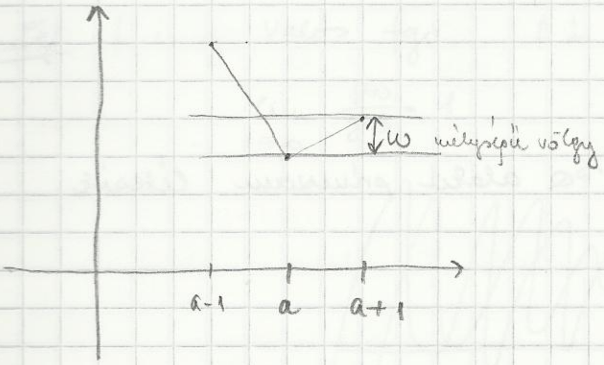
$d(n) = 2 \iff n = p$ prím



pl.: $n := p^{m-1}$ $\qquad$ p prím

$d(n) = m$

minden egész helyettesítési értéket sokszor veszi fel.



Völgy-tétel:

w legyen tetszőleges pozitív egész ($w \geq 2$)

Végtelen sok $a-1$, a, $a+1$ számhármas létezik, hogy $d(a-1) - d(a) > w$

$d(a+1) - d(a) > w$

BIZ (Dirichlet-tétel) → segédtétel

$a, b \in \mathbb{N}^+$, $(a,b) = 1$

$ak + b$ $(k = 0, 1 \dots)$ számtani sorozatban végtelen sok prímszám létezik.

(BIZ.: -)

Legyen $p_1, p_2, \dots p_w$

$q_1, q_2 \dots q_w$ különböző prímek

$P := \prod_{i=1}^{w} p_i$ $\qquad$ $Q := \prod_{i=1}^{w} q_i$

$$\left.\begin{array}{l} x \equiv 1 \pmod{P} \\ x \equiv -1 \pmod{Q} \end{array}\right\}$$

a megoldások: $x_0 + PQ \cdot k$ (modulo pq-ra egyértelmű)

$(k \in \mathbb{Z})$

feltehető, hogy $x_0 > 0$

$(x_0, PQ) = 1$ ✓

feltehető, hogy $\varepsilon > 0$

<u>Dirichlet-tétel</u> $\Rightarrow$ végtelen sok $x_0 + \varepsilon PQ$ alakú prímszám létezik

pl.: $a := p$ egy ilyen

$$d(a) = (d_1(p)) = 2$$

$$d(a-1) = \quad \Downarrow$$

$$p_i \mid P \mid a-1 \Rightarrow d(a-1) \geq 2^w$$

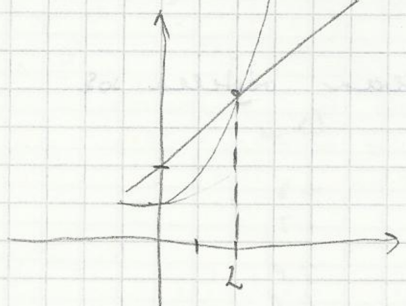
$$\underbrace{1}_{\binom{w}{0}}, \underbrace{p_1, \dots, p^w}_{\binom{w}{1}}, p_1 p_2 \cdots p_{w-1} p_w$$

$$d(a+1) \Downarrow$$

$$q_i \mid Q \mid a+1 \Rightarrow d(a+1) \geq 2$$

$$d(a-1) - d(a) \geq 2^w - 2 > w$$

$$d(a+1) - d(a) \geq 2^w - 2 > w \quad (\text{ha } w > 2)$$



$$2^w > w + 2 \Rightarrow 2^w - 2 > w$$

Hegy tétel (H)

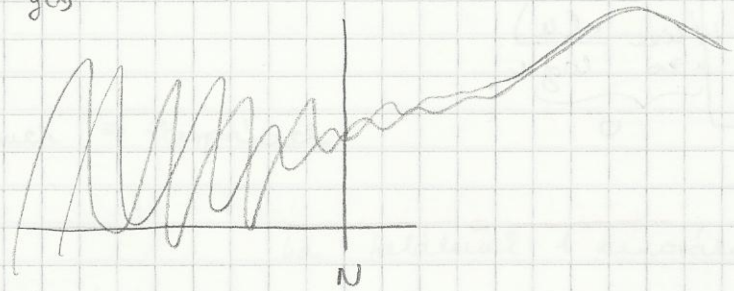
Tétel: $\forall\ \overset{\varepsilon\text{-tól függő}}{} \varepsilon \in \mathbb{R}^+$-hoz $\exists\ c = c(\varepsilon) > 0$, hogy $d(n) < c \cdot n^{\varepsilon}$ $(n \geq 1)$

(BIZ.: lsd. +k)
↳ segédtételt nem kell.

d átlagérték fgv-e $\underline{\underline{\overline{D}(n)}} = \frac{D(n)}{n}$, ahol $D_n = d(1)+\dots+d(n)$

Def: f és g valós fgv. f és g aszimptotikusan egyenlő, ha

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$$



Nem kis x-ekre mondja meg a def.

Jelölés $f \sim g$ → aszimptotikusan egyenlő g-vel.

Tétel: $\overline{D} \sim \log$ → (e alapú)

BIZ.: $\log n < \sum_{m=1}^{n} \frac{1}{m} < \log n + 1$ → segédtétel

ST: $D(n) = d(1)+d(2)+\dots+d(n) = \sum_{m=1}^{n}\left[\frac{n}{m}\right]$ ✓
hány osztó hányszor fordul elő

$$D(n) = \sum_{m=1}^{n}\left[\frac{n}{m}\right] \ge \sum_{m=1}^{n}\left(\frac{n}{m}-1\right) = \sum_{m=1}^{n}\left[\frac{n}{m}-n\right] = n\sum_{m=1}^{n}\frac{1}{m} - n >$$

$$> n\cdot\log n - n$$

$\underline{D_n > n\cdot\log n}$

$$D_n = \sum_{m=1}^{1}\left[\frac{n}{m}\right] \le \sum_{m=1}^{n}\frac{1}{m} < \underline{n\cdot\log n + n}$$

→ n-el végig osztottunk

$$n\cdot\log n - n < D_n < n\cdot\log n + n \quad /:n$$

$$\log n - 1 < \overline{D}(n) < \log n + 1$$

$$\boxed{-1 < \overline{D}(n) - \log n < 1}$$

$$-1 < r(n) := \overline{D}(n) - \log n < 1 \Rightarrow \qquad |r(n)| < 1$$

$$\frac{\overline{D}(n)}{\log n} - 1 = \frac{r(n)}{\log n} \Rightarrow \qquad n \geq 1$$

$$\Rightarrow \boxed{\lim_{n\to\infty} \frac{\overline{D}(n)}{\log n} = 1} + \underbrace{\lim_{n\to\infty} \frac{r(n)}{\log n}}_{0}$$

A prímszámelmélet elemei ... (38)

....

~~Végtelen~~ sok prímszám létezik:

1., Euklidész-féle ind. (lásd első félév) ✓

2., $F_n = 2^{2^n} + 1$, $(n = 0, 1 \dots)$ (Fermat-f. számok)

$k \geq 1$ $(F_n, F_{m+k}) = 1$ $\Rightarrow$ végtelen sok prím létezik

(lásd TK) ✓

3., $\sum_{p \leq x} \frac{1}{p}$ div (p prímszám)

Tétel: $\exists\, c \in \mathbb{R}^+$, hogy $x > 1$

$$c \cdot \log\log x < \sum_{p \leq x} \frac{1}{p}$$

végtelen mértani sor összege

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

a jobb oldalon minden szám megtalálható, mint a baloldalon, sőt, még több is.

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

$$\left(\log n < \sum_{n=1}^{n} \frac{1}{n}\right)$$

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

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

behelyettesítve

ST

$$0 < x \le \frac{1}{2}$$

$$-\log(1-x) < 2x$$

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

$p, p+2$ prímek $\Rightarrow$ ikerprímek

BRUN:

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

ha találunk 1 minoráló fgv-t, amely a végtelenbe tart $\Rightarrow$ végtelen sok ikerprím van.

vagy véges sok összeadandója volt
vagy konvergens a sor (végtelen elem.)
} ma sem ismert, h. hány db ikerprím van.

Ma ismert 2. legnagyobb ikerprím:

(K.H.J)-Járai Antal : $242206083 \cdot 2^{38880} \pm 1$

Mersenne-f. számok:

$M_p = 2^p - 1$ $\quad p$, és M_p is prím.

A ma ismert legnagyobb prímszám: (34.)

$2^{1257787} - 1$ (12,5 km)

IV. 8. 9. előadás

Dirichlet-tétel speciális esetei

($4k-1$, $4k+1$ alakú prímek)

VIZSGA: V. 20
V. 27
VI. 22.

D. tétel: (430)

pl.: $a=4$, $b=-1$ $4k-1$ alakú számok

$k = 1, 2 \dots$ stb.

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

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

1, Ha A prím $\Rightarrow A = 4K-1$ alakú és különbözik $p_1, \dots, p_n$-től $\Rightarrow$ ↯ $p_{n+1} := A$

2, Ha A nem prím $\Rightarrow \exists\, p$ prím, amelyre: $p \mid A$ (ind)

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

$\Rightarrow p \mid 1$ ↯

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

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

elő A. $\rightarrow$ mindig $4k+1$ lesz $\Rightarrow$ nem lesz $4k-1$ alakú osztója ↯

Ennél a lépésnél bukik el a $4k+1$ alakú prímek biz.-a.

$(4k_1-1)(4k_2-1) = 4k+1$.

Konstrukciós BZ:

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

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

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

páratlan

$\Downarrow$

$p \nmid n!$

$(n!)^2 \equiv -1 \pmod p$, de:

$n! = 1 \cdot 2 \cdot 3 \dots n$ ha $\underbrace{p' \mid n! \Rightarrow 2 \le p' \le n}$

$\boxed{p > n}$

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

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

emeljük $\frac{p-1}{2}$-dik hatványra

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

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

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

ptlan

ha $p = 4k+1$

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

köv szám : $p_1 := p$

$m_2 := (p_1!)^2 + 1 \dots \Rightarrow p_2 = 4k+1$

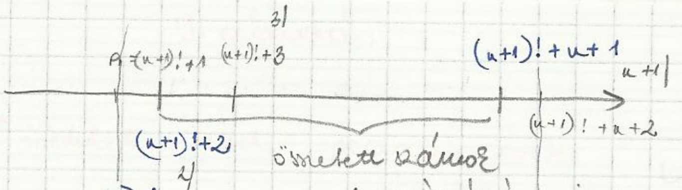
$p_2 > p_1 > n$

$m_3 : (p_2!)^2 + 1 \dots \Rightarrow p_3 = 4k+1$

$p_3 > p_2 > p_1 > n$

$\vdots$

1)



$n \geq 1$ n hosszúságú intervallumban nem $\exists$ prím

$(n+1)!+2,\ (n+1)!+3, \ldots\ (n+1)!+n+1$ összetett számok

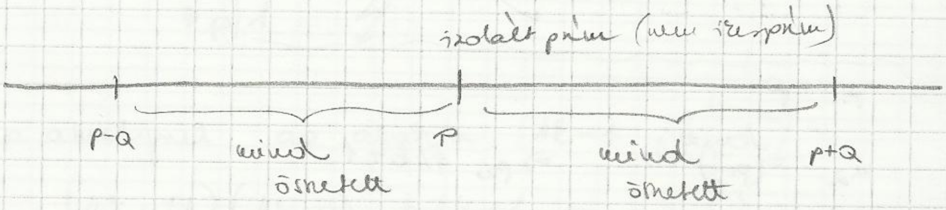
2) BERTRAND-FÉLE POSZTULÁTUM (Csebisev-tétel)

$n>1$ $(n, 2n)$ mindig $\exists$ legalább 1 prímszám.

(BIZ —)
Nézzük meg!

3) Végtelen sok izolált prím van:

Legyen Q tetszőlegesen nagy pozitív egész

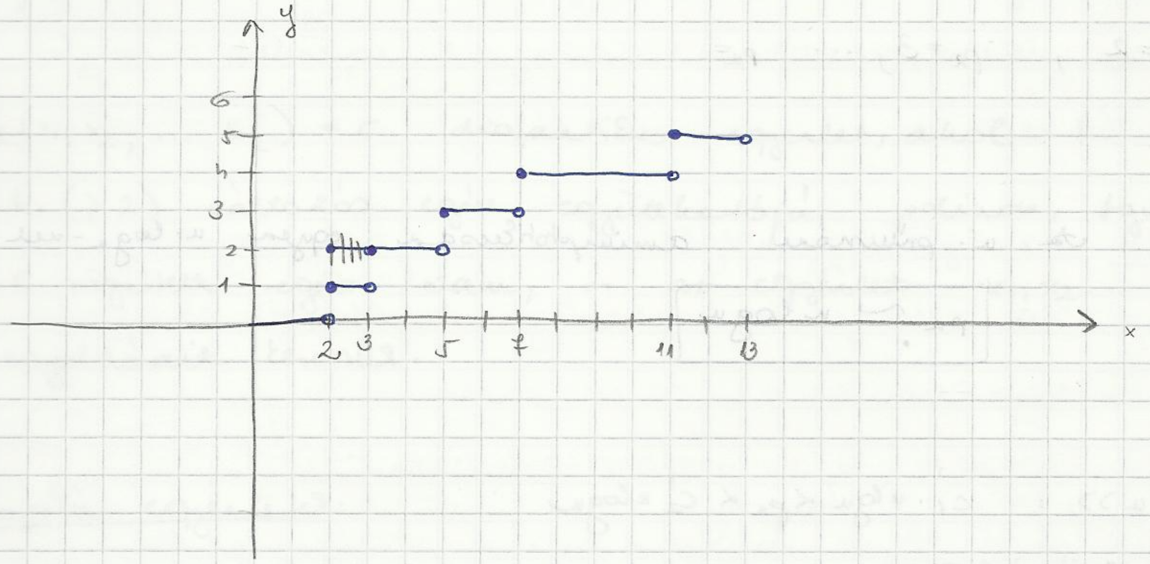


Végtelen sok ilyen p prím $\exists$.

BIZ: Lásd tk → akit érdekel, amúgy nem kell!

$(x \in \mathbb{R}^+)$ $\pi(x) := \sum_{p \le x} 1$ (megszámolja x-ig hány prím van)

$\pi(12) = 5$



Nagy prímszám tétel: (Hadamard, de la Vallée Poussin tétel)

$$\boxed{\lim_{x \to \infty} \frac{\pi(x)}{\frac{x}{\log x}} = 1}$$

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

$\sim$: aszimptotikusan megegyezik

(eredeti biz: komplex fgv-tannal
1949 Erdős, Selberg → elemi bizonyítás)

Erdős: (Fields-medál (matematikai Nobel-díj) matematikusok adják egymás között)

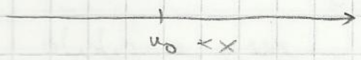
Csebisev-tétel:

$\exists\ c_1, c_2 \in \mathbb{R}^+$

$$x \gg : \quad c_1 \frac{x}{\log x} < \pi(x) < c_2 \frac{x}{\log x}$$

$x \gg$: x elég nagy; c_1: $\left(\frac{8}{9}\right)$; c_2: $\left(\frac{10}{9}\right)$

$\exists\ n_0$, amelytől ha nagyobb, már igaz az állítás



(Nagy prímszámtételben a $c = 1$)