

MULTIPLIKATÍV SZÁMELMÉLET

Dr. TÓTH LÁSZLÓ

Pécsi Tudományegyetem, 2006

1. ELŐADÁS

• **Bevezetés.** Ennek az előadásnak a célja multiplikatív jellegű számelméleti problémák tárgyalása. Foglalkozunk a prímszámok eloszlásának kérdéseivel és speciális számelméleti függvények aszimptotikus tulajdonságaival. Egyik fő célunk a Dirichlet-tétel bizonyítása, amely szerint minden $a, a + b, a + 2b, \dots$ számtani sorozat, ahol a és b relatív prímek, végtelen sok prímszámot tartalmaz.

• **Előismeretek.** Ismertnek tekintjük az elemi számelmélet következő alapfogalmait és ezek fontosabb tulajdonságait: egész számok oszthatósága, egész számok legnagyobb közös osztója és legkisebb közös többszöröse, prímszámok, kongruenciák, teljes maradékrendszerek és redukált maradékrendszerek ($\text{mod } m$), Euler-függvény, multiplikatív számelméleti függvények. Alkalmazni fogjuk az Euler, Fermat és Wilson-féle kongruenciátételeket, valamint az $n!$ kanonikus alakjára vonatkozó Legendre-képletet.

• **Jelölések.** A következő jelöléseket használjuk.

Számhalmazok:

$\mathbb{N} = \{1, 2, 3, \dots\}$ a (nemnulla) természetes számok halmaza,

$\mathbb{N}_0 = \mathbb{N} \cup \{0\}$,

$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ az egész számok halmaza,

$\mathbb{Q} = \{\frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0\}$ a racionális számok halmaza,

$\mathbb{R}$ a valós számok halmaza,

$\mathbb{C}$ a komplex számok halmaza.

Relációk:

$a|b$ jelentése: a osztója b -nek, ahol $a, b \in \mathbb{Z}$,

$a \equiv b \pmod{m}$ jelentése: a kongruens b -vel (modulo m), ahol $a, b, m \in \mathbb{Z}$, $m \geq 2$,

(a, b) az $a, b \in \mathbb{Z}$ számok legnagyobb közös osztója (lko-já).

Függvények: $\log x$ a természetes logaritmus ($\log x \equiv \ln x$).

$\#A$ vagy $|A|$ az A véges halmaz számossága.

Ha mást nem mondunk, számon mindig egész számot értünk. A p betű mindig prímszámot jelöl.

• **A számelmélet alaptétele.** A prímszámok a természetes számok multiplikatív struktúrájának az építőkövei, mert minden természetes szám felírható prímszámok szorzataként. Pontosabban,

1. Tétel. (A számelmélet alaptétele) Minden $n > 1$ természetes szám esetén léteznek olyan $p_1, p_2, \dots, p_k$ prímszámok, hogy

$$n = p_1 p_2 \cdots p_k,$$

és ez a felírás a tényezők sorrendjétől eltekintve egyértelmű.

Egy $n > 1$ természetes szám prímtenyezős felbontásában ugyanaz a prímszám többször is szerepelhet, így n a következő alakban írható:

$$(1) \quad n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r},$$

ahol $p_1, p_2, \dots, p_r$ különböző prímszámok és $a_1, a_2, \dots, a_r \geq 1$ egészek, amelyet n kanonikus alakjának nevezünk. Használatos a következő jelölés is:

$$n = \prod_p p^{\nu_p(n)},$$

ahol a szorzat az összes p prímre vonatkozik és csak véges sok kitevő nemnulla.

• **A τ , σ és ϕ függvények.** Jelölje $\tau(n)$ és $\sigma(n)$ az $n \geq 1$ szám pozitív osztóinak számát, illetve n pozitív osztóinak összegét. Itt $\tau(n) = \#\{d \in \mathbb{N} : d|n\}$ vagy $\tau(n) = \sum_{d|n} 1$ és $\sigma(n) = \sum_{d|n} d$. Továbbá jelölje $\phi(n) = \#\{k \in \mathbb{N} : k \leq n, (k, n) = 1\}$ az Euler-függvényt. Emlékeztetünk arra, hogy ezek a függvények multiplikatívak (az f számelméleti függvény multiplikatív, ha $f(mn) = f(m)f(n)$ minden $m, n \in \mathbb{N}$, $(m, n) = 1$ esetén) és ha $n > 1$ kanonikus alakja (1), akkor

$$\tau(n) = \prod_{i=1}^r (a_i + 1), \quad \sigma(n) = \prod_{i=1}^r \frac{p_i^{a_i+1} - 1}{p_i - 1}, \quad \phi(n) = n \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right).$$

Feladat. Igazoljuk ezeket a képleteket.

Megoldás. Ha $d|n$, akkor $d = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}$, ahol $0 \leq b_i \leq a_i$ minden i -re. A b_i kitevőket egymástól függetlenül, $(a_i + 1)$ -féleképpen választhatjuk meg, így $\tau(n)$ e számok szorzata.

$$\sigma(n) = \prod_{i=1}^r (1 + p_i + p_i^2 + \cdots + p_i^{a_i}) = \prod_{i=1}^r \frac{p_i^{a_i+1} - 1}{p_i - 1}.$$

Az Euler-függvényre vonatkozó képletet például a logikai szita (a tartalmazás és kizárás elve) alapján vezethetjük le, amely indukcióval bizonyítható: Ha $A_1, A_2, \dots, A_r \subseteq E$ véges halmazok és $|X|$ az X halmaz elemeinek száma, akkor

$$\begin{aligned} \left| \bigcup_{i=1}^r A_i \right| &= \sum_{\emptyset \neq K \subseteq \{1, 2, \dots, r\}} (-1)^{|K|+1} \left| \bigcap_{i \in K} A_i \right| = \\ &= \sum_{i=1}^r |A_i| - \sum_{1 \leq i_1 < i_2 \leq r} |A_{i_1} \cap A_{i_2}| + \dots + (-1)^{k+1} \sum_{1 \leq i_1 < \dots < i_k \leq r} |A_{i_1} \cap \dots \cap A_{i_k}| + \dots + \\ &\quad + (-1)^{r+1} \left| \bigcap_{i=1}^r A_i \right|, \\ |E \setminus \bigcup_{i=1}^r A_i| &= \sum_{K \subseteq \{1, 2, \dots, r\}} (-1)^{|K|} \left| \bigcap_{i \in K} A_i \right| = \\ &= |E| - \sum_{i=1}^r |A_i| + \sum_{1 \leq i_1 < i_2 \leq r} |A_{i_1} \cap A_{i_2}| - \dots + (-1)^k \sum_{1 \leq i_1 < \dots < i_k \leq r} |A_{i_1} \cap \dots \cap A_{i_k}| + \dots + \\ &\quad + (-1)^r \left| \bigcap_{i=1}^r A_i \right|. \end{aligned}$$

Megjegyzés. Itt $K = \emptyset$ esetén $\cap_{i \in \emptyset} A_i = E$.

Legyen $E = \{1, 2, \dots, n\}$, $A_i = \{a \in \mathbb{N} : 1 \leq a \leq n, p_i | n\}$, $1 \leq i \leq r$, ekkor $\phi(n) = |E \setminus \cup_{i=1}^r A_i|$, ahol $|A_i| = \frac{n}{p_i}$, $|A_{i_1} \cap \dots \cap A_{i_k}| = |\{a : 1 \leq a \leq n, p_{i_1} \cdots p_{i_k} | a\}| = \frac{n}{p_{i_1} \cdots p_{i_k}}$ és kapjuk, hogy

$$\begin{aligned} \phi(n) &= n \left(1 - \sum_{i=1}^r \frac{1}{p_i} + \sum_{1 \leq i_1 < i_2 \leq r} \frac{1}{p_{i_1} p_{i_2}} - \dots + \right. \\ &\quad \left. + (-1)^k \sum_{1 \leq i_1 < \dots < i_k \leq r} \frac{1}{p_{i_1} \cdots p_{i_k}} + \dots + (-1)^r \frac{1}{p_1 \cdots p_r} \right) = \\ &= n \left(1 - \frac{1}{p_1} \right) \cdots \left(1 - \frac{1}{p_r} \right). \end{aligned}$$

Feladat. Igazoljuk, hogy minden $n \in \mathbb{N}$ -re

- 1) $\prod_{d|n} d = n^{\frac{\tau(n)}{2}}$,
- 2) ha n kanonikus alakja (1), akkor $2^r \leq \tau(n) \leq 2^{a_1 + \dots + a_r}$.

Megoldás. 1) Ha d befutja az n pozitív osztóit, akkor n/d is befutja ezeket az osztókat (fordított sorrendben) és így $\prod_{d|n} d = \prod_{d|n} \frac{n}{d} = n^{\tau(n)} / \prod_{d|n} d$, ahonnan $(\prod_{d|n} d)^2 = n^{\tau(n)}$.

- 2) $\tau(n) = \prod_{i=1}^r (a_i + 1) \geq \prod_{i=1}^r 2 = 2^r$ és $\tau(n) = \prod_{i=1}^r (a_i + 1) \leq \prod_{i=1}^r 2^{a_i} = 2^{a_1 + \dots + a_r}$.

• **Prímszámok.** Az 1. Tétel szerint a természetes számok tulajdonságainak vizsgálatához szükséges a prímszámok tulajdonságainak ismerete. A prímek sorozata a következő : 2, 3, 5, 7, 11, 13, 17, 19, ...

A prímszámok sorozatát vizsgálva megállapítható, hogy szabálytalanul helyezkednek el a természetes számok között. Néhány kérdés, amely megfogalmazható a prímekre vonatkozóan:

Melyek a prímszámok a természetes számok sorozatában ?

Hogyan dönthető el egy számról hogy prím-e vagy sem ?

Hány prímszám van egy adott számig ?

Hogyan adható meg az n -edik prímszám ?

Mit lehet mondani az n -edik prím nagyságáról ?

Van-e prímszám minden $a, a + b, a + 2b, \dots$ számtani sorozatban?

Vajon a prímek a természetes számok additív struktúrájának is az építőkövei ?

Feladat. Minden $n \geq 2$ szám felírható prímek összegeként.

Megoldás.

$$n = 2k = \underbrace{2 + 2 + \dots + 2}_k, \quad n = 2k + 1 = \underbrace{2 + 2 + \dots + 2}_{k-1} + 3.$$

Megjegyzés. A (mindmáig bizonyítatlan), 1742-ben kimondott Goldbach-sejtés szerint minden $n > 2$ páros szám felírható két prímszám összegeként.

Ebből azonnal következik, hogy minden $n > 5$ páratlan szám felírható három prímszám összegeként. Itt $n = 3 + (n - 3)$, ahol $n - 3 > 2$ páros szám.

Feladat. Igazoljuk, hogy minden $n \geq 12$ szám felírható 2 összetett szám összegeként.

Megoldás. Ha $n = 2k$ páros szám, ahol $k \geq 6$, akkor $n = 4 + 2(k - 2)$, ahol $k - 2 \geq 4$. Ha $n = 2k + 1$ páratlan, ahol $k \geq 6$, akkor $n = 9 + 2(k - 4)$, itt $k - 4 \geq 2$.

Megjegyzendő, hogy $n = 11$ nem írható fel így.

A továbbiakban ismertetjük a prímszámok néhány egyszerű tulajdonságát. Ezek egy része az elemi számelméletből ismert.

- **Végtelen sok prímszám van.**

2. Tétel. *Végtelen sok prímszám van.*

Első bizonyítás. (Euklidész) Tegyük fel, hogy állításunk nem igaz, tehát véges sok prímszám létezik, legyenek ezek: $p_1, p_2, \dots, p_k$. Tekintsük az $A = p_1 p_2 \cdots p_k + 1$ számot, amelynek van egy q prímosztója. A feltevés szerint $q = p_i$ valamely i -re, hiszen csak a $p_1, p_2, \dots, p_k$ prímek léteznek és következik, hogy $p_i | 1$, ami ellentmondás. $\square$

Második bizonyítás. Megmutatjuk, hogy minden $n \in \mathbb{N}$ számnál van nagyobb prímszám. Legyen $N = n! + 1 > 1$, így N -nek van legalább egy p prímosztója. Itt $p > n$, mert ha $p \leq n$ lenne, akkor $p | n!$, ahonnan $p | 1$, ami ellentmondás. $\square$

Harmadik bizonyítás. Tekintsük az $F_n = 2^{2^n} + 1, n \geq 0$ számsorozatot. Minden F_n számnak létezik egy q_n prímosztója. Az $F_n = 2^{2^n} + 1$ sorozat tagjai páronként relatív prímek, lásd Feladat. Így a q_n prímszámok páronként különbözők, tehát $q_1, q_2, \dots$ prímszámok végtelen sorozata. $\square$

Feladat. Az $F_n = 2^{2^n} + 1, n \geq 0$ sorozat tagjai páronként relatív prímek.

Megoldás. Valóban, legyen $n, m \in \mathbb{N}, n \neq m$, feltehető, hogy $m < n$ és $d \in \mathbb{N}, d | F_n, d | F_m$. Akkor

$$\begin{aligned} F_n - 2 &= 2^{2^n} - 1 = (2^{2^{n-1}} + 1)(2^{2^{n-1}} - 1) = (2^{2^{n-1}} + 1)(2^{2^{n-2}} + 1) \cdots (2^{2^m} + 1)(2^{2^m} - 1) \\ &= F_{n-1} F_{n-2} \cdots F_m (2^{2^m} - 1) = k F_m \end{aligned}$$

alapján $d | 2$, de $d = 2$ nem lehet, mert az F_n számok mind páratlanok, így $d = 1$.

Megjegyzés. Az $F_n = 2^{2^n} + 1, n \in \mathbb{N}_0$ számokat **Fermat-számoknak**, az ilyen alakú prímekeket pedig **Fermat-prímeknek** nevezzük. Fermat azt sejtette, hogy az F_n számok mind prímek. Nos, $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$ prímek, F_5 viszont nem prím, osztható 641-gyel (ezt először Euler igazolta). Nem tudjuk, hogy léteznek-e további Fermat-prímek.

Feladat. Felírható-e $F_n = 2^{2^n} + 1, n \geq 0$ két prímszám összegeként?

Megoldás. $F_0 = 3$ nem írható fel, $F_1 = 5 = 2 + 3$ felírható. Ha $n \geq 2$, akkor F_n nem írható két prímszám összegeként. Valóban, tegyük fel, hogy F_n két prím összege. Itt F_n páratlan, ezért az egyik prím a 2, tehát $F_n = 2 + p$, ahol p prím. De innen $p = 2^{2^n} - 1 = (2^{2^{n-1}} - 1)(2^{2^{n-1}} + 1)$ összetett, itt az első tényező ≥ 3 , a második ≥ 5 , ellentmondás.

A 2 az egyedüli páros prímszám, a többi prím $4k - 1$ alakú (3, 7, 11, 19, ...) vagy $4k + 1$ alakú (5, 13, 17, 29, ...).

3. Tétel. 1) *Végtelen sok $4k - 1$ alakú prím létezik.*

2) *Végtelen sok $4k + 1$ alakú prím létezik.*

Bizonyítás. 1) Az euklidészi bizonyításhoz hasonlóan tegyük fel, hogy véges sok $4k - 1$ alakú prím létezik: $p_1, p_2, \dots, p_r$. Legyen $B = 4p_1 p_2 \cdots p_r - 1$. Azonnali, hogy $2 \nmid B$ és

$p_1 \nmid B, p_2 \nmid B, \dots, p_r \nmid B$. Következik, hogy B -nek minden prímosztója $4k + 1$ alakú, de akkor B maga is $4k + 1$ alakú, s ez ellentmondás.

2) A második állítás hasonlóképpen igazolható. Tegyük fel, hogy véges sok $4k + 1$ alakú prímszám van: $p_1, p_2, \dots, p_s$. Ha a $C = 4p_1p_2\dots p_s + 1$ számot vizsgáljuk, akkor nem jutunk ellentmondásra, mert megtörténhet, hogy C -nek páros számú $4k - 1$ alakú prímosztója van. Legyen $D = (2p_1p_2\dots p_s)^2 + 1$, melyre $2 \nmid D, p_1 \nmid D, p_2 \nmid D, \dots, p_s \nmid D$. Kapjuk, hogy D -nek létezik egy $q = 4k - 1$ alakú prímosztója. Így $q \mid x^2 + 1$, ahol $x = 2p_1p_2\dots p_s$, azaz $x^2 \equiv -1 \pmod{q}$, innen $x^{q-1} \equiv (-1)^{\frac{q-1}{2}} \equiv (-1)^{2k-1} \equiv -1 \pmod{q}$. A Fermat-tétel szerint $x^{q-1} \equiv 1 \pmod{q}$, és kapjuk, hogy $-1 \equiv 1 \pmod{q}$. Innen $q = 2$, ellentmondás.

Másképp: Legyen $n \in \mathbb{N}, n > 1$. Olyan $4k + 1$ alakú prímét szerkesztünk, amely n -nél nagyobb. Tekintsük az $m = (n!)^2 + 1$ páratlan szám valamely p prímosztóját. Ekkor p páratlan, $p > n$ és $(n!)^2 \equiv -1 \pmod{p}$, $(n!)^{p-1} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$. A Fermat-tétel szerint $(n!)^{p-1} \equiv 1 \pmod{p}$, és kapjuk, hogy $(-1)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Innen $(-1)^{\frac{p-1}{2}} = 1$, azaz $p \equiv 1 \pmod{4}$. $\square$

A 2 és 3 príme kivételével minden prím $6k - 1$ alakú (5, 11, 17, ...) vagy $6k + 1$ alakú (7, 13, 19, ...). Itt a 3-nál nagyobb $6k, 6k + 2, 6k + 3$ és $6k + 4$ alakú számok biztosan összetettek. A $6k + 5$ alakú számok helyett tekinthetjük a $6k - 1$ alakúakat.

Hasonlóképpen igazolható, hogy végtelen sok $6k - 1$ alakú és végtelen sok $6k + 1$ alakú prímszám létezik, lásd Feladat. Mindezeknél általánosabb a Dirichlet-tétel, amelyet később bizonyítunk.

Feladat. Igazoljuk, hogy végtelen sok $6k - 1$ alakú prímszám van.

Megoldás. Tegyük fel, hogy véges sok $6k - 1$ alakú prím létezik: $p_1, p_2, \dots, p_r$. Legyen $N = 6p_1p_2\dots p_r - 1$. Azonnali, hogy $2 \nmid N$ és $p_1 \nmid N, p_2 \nmid N, \dots, p_r \nmid N$. Következik, hogy N -nek minden prímosztója $6k + 1$ alakú, de akkor N maga is $6k + 1$ alakú, s ez ellentmondás.

2. ELŐADÁS

Jelölje p_n az n -edik prímszámot: $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, \dots$

Feladat. A 2. Tétel euklideszi bizonyításának ötletét használva igazoljuk, hogy $p_n \leq 2^{2^{n-1}}$ minden $n \geq 1$ -re.

Megoldás. Az euklideszi bizonyítás alapján következik, hogy $p_{r+1} \leq p_1 p_2 \cdots p_r + 1$ igaz minden $r \geq 1$ -re.

n szerinti indukcióval: $n = 1$ -re $p_1 = 2 \leq 2^{2^0} = 2$ igaz. Tegyük fel, hogy a $k = 1, 2, \dots, n$ értékek mindegyikére $p_k \leq 2^{2^{k-1}}$. Akkor

$$p_{n+1} \leq p_1 p_2 \cdots p_n + 1 \leq 2^{2^0} \cdot 2^{2^1} \cdots 2^{2^{n-1}} + 1 = 2^{1+2+\cdots+2^{n-1}} + 1 \leq 2^{2^n-1} + 2^{2^n-1} = 2^{2^n}.$$

Jelölje $\pi(x)$ az x valós számnál nem nagyobb prímek számát: $\pi(x) = \sum_{p \leq x} 1$.

Feladat. Az előző feladatot használva igazoljuk, hogy $\pi(x) > \log \log x$ minden $x \geq 2$ esetén.

Megoldás. Az $x \geq 2$ rögzített értékre legyen $\pi(x) = n$, azaz $p_n \leq x < p_{n+1}$. Az előző Feladat szerint

$$\log \log p_{n+1} \leq \log \log 2^{2^n} = \log 2^n \log 2 < n \log 2 < n,$$

és innen

$$\pi(x) = n > \log \log p_{n+1} > \log \log x.$$

• **Ikerprímek.** A következő tétel arra mutat rá, hogy az egymásutáni prímszámok közötti különbség tetszőlegesen nagy lehet.

Állítás. Minden $n \in \mathbb{N}$ számhoz megadható n egymásutáni összetett szám.

Bizonyítás. Legyen $a_k = (n+1)! + k + 1$, ahol $k \in \{1, 2, \dots, n\}$. Ezek egymásutáni számok és mindegyik összetett, hiszen $k+1 | a_k$ és $a_k > k+1$ minden $k \in \{1, 2, \dots, n\}$ esetén. $\square$

Legyen $d_n = p_{n+1} - p_n$. Az előző tétel szerint a $(d_n)_{n \geq 1}$ sorozat nem korlátos.

Ez a tétel nem jelenti azt, hogy nagy számokat vizsgálva a prímek egyre ritkábban fordulnak elő. Léteznek olyan prímszámok, melyek különbsége 2. Ilyen prímek, úgynevezett **ikerprímek**, például a következők: $(3, 5), (5, 7), (11, 13), (17, 19), (10^9 + 7, 10^9 + 9), \dots, (242\,206\,083 \cdot 2^{38880} - 1, 242\,206\,083 \cdot 2^{38880} + 1), \dots$. Vannak olyan prímek, sőt végtelen sok, lásd később, amelyek nem tagjai ikerprímszámpároknak, pl. $23, 37, 47, \dots$. A prímszámelmélet egy nevezetes, mindmáig megoldatlan kérdése az, hogy létezik-e végtelen sok ikerprímszámpár.

Feladat. Lehet-e a $p, p+2, p+4$ számok mindegyike prímszám?

Megoldás. Ha $p = 3k+1$ alakú, $k \geq 1$, akkor $p+2 = 3k+3$ nagyobb mint 3 és osztható 3-mal, tehát nem prím.

Ha $p = 3k-1$ alakú, $k \geq 1$, akkor $p+4 = 3k+3$ nagyobb mint 3 és osztható 3-mal, tehát nem prím.

Marad a $p = 3$, melyre $3, 5, 7$ mind prímek, ezek az egyedüli "hármassikrek".

Feladat. Ha $p, q \geq 5$ ikerprímek, akkor $12 | p+q$.

Megoldás. 6-tal osztva minden $p > 3$ prímszám $6k+1$ vagy $6k+5$ alakú. Ha $p, q \geq 5$ ikerprímek, akkor így $p = 6k-1$ és $q = 6k+1$ alakú, ugyanazzal a k -val. Innen azonnali, hogy $p+q = 12k$ osztható 12-vel.

Feladat. Lehetnek-e $2^n - 1$ és $2^n + 1$ ikerprímek, ahol $n \in \mathbb{N}$?

Megoldás. Ha $2^n - 1$ prím, akkor n prím, ha pedig $2^n + 1$ prím, akkor $n = 2^k$ alakú, ezek ismert tulajdonságok. Tehát ikerprímeket csak $n = 2$ -re kapunk és ezek a 3, 5.

Másképp: Ha $n = 1$, akkor 1, 3 nem ikerprímek, $n = 2$ -re 3, 5 ikerprímek. Ha $n \geq 3$, akkor $p = 2^n - 1, q = 2^n + 1 \geq 7$ és összegük $p + q = 2^{n+1}$ nem osztható 12-vel. Ezért az előző Feladat alapján nem lehetnek ikerprímek.

• **Eratosztenészi szita.**

Állítás. Ha $n \in \mathbb{N}$ összetett szám, akkor n -nek van olyan p prímosztója, amelyre $p \leq \sqrt{n}$.

Bizonyítás. Az n számnak léteznek (pozitív) prímosztói, és legyen p a legkisebb ezek közül. Így $n = pn_1$ és $p \leq n_1$. Kapjuk, hogy $p^2 \leq pn_1 = n$, ahonnan $p \leq \sqrt{n}$. $\square$

Így egy adott n számról úgy dönthető el, hogy prímszám vagy sem, hogy megnézzük osztható-e egy $p \leq \sqrt{n}$ prímszámmal. Ha igen, akkor n összetett, ha nem, akkor n biztosan prímszám. Például $n = 401$ esetén $\sqrt{n} < 21$, s mivel 401 nem osztható a 21-nél kisebb prímekekkel, következik, hogy 401 prímszám.

A következő eljárás, az úgynevezett eratosztenészi szita, arra szolgál, hogy meghatározzuk a prímekeket egy adott N számig. A 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, ..., N sorozat első tagja, a 2 prím, s húzzuk ki (szitáljuk ki) a 2 többszöröseit, melyek nem prímekek. Az első megmaradt szám, a 3 prím, s kiszitáljuk a 6, 9, ... számokat, amelyek nem prímekek (vannak olyan számok, például a 6, amelyek már az első szitálásnál kiestek). Az első megmaradt szám, az 5 ismét prím, s kiszitáljuk az 5 többszöröseit, stb. Az előző tétel szerint a szitálást elegendő a $p \leq \sqrt{N}$ prímekekkel végezni, és a megmaradt számok lesznek a keresett prímekek:

$$\boxed{2}, \boxed{3}, 4, \boxed{5}, 6, \boxed{7}, 8, 9, 10, \boxed{11}, 12, \boxed{13}, 14, 15, 16, \boxed{17}, \dots$$

• **A $\pi(x)$ függvény**

Láttuk, hogy végtelen sok prímszám van. Ha $x \in \mathbb{R}, x > 0$, jelölje $\pi(x) = \sum_{p \leq x} 1$ az x -nél nem nagyobb prímszámok számát. Így $\pi(1) = 0, \pi(2) = 1, \pi(3) = \pi(4) = 2,$

$\pi(10) = 4, \pi(100) = 25, \pi(1000) = 168, \pi(10^4) = 1129, \pi(10^5) = 9592, \pi(10^{10}) = 455\,052\,511, \pi(10^{18}) = 24\,739\,954\,287\,740\,860.$

Megjegyzés. Az x -nél nem nagyobb ikerprímszámpárok számát $\pi_2(x)$ -szel szokás jelölni:

$$\pi_2(x) = \sum_{\substack{p, p+2 \leq x \\ p, p+2 \text{ prím}}} 1.$$

Itt például $\pi_2(10) = 2, \pi_2(100) = 8, \pi_2(1000) = 35, \pi_2(10^{10}) = 27\,412\,679.$

A továbbiakban a $\pi(x)$ függvény viselkedését vizsgáljuk. Nyilvánvaló, hogy minden $x > 0$ -ra $\pi(x) \leq x$, sőt igaz a $\pi(x) \leq \frac{x+1}{2}$ egyenlőtlenség is, mert a 2-től különböző páros számok nem prímekek. Ugyanakkor $\lim_{x \rightarrow \infty} \pi(x) = \infty$, hiszen végtelen sok prímszám van. Kérdés, hogy milyen gyorsan tart $\pi(x)$ a végtelenbe.

4. Tétel. Ha $n \in \mathbb{N}$, akkor $\pi(n) \geq \frac{\log n}{2 \log 2}.$

Bizonyítás. (Erdős Pál) Minden $k \in \mathbb{N}, k \leq n$ szám felírható egyértelműen $k = a^2b$ alakban, ahol $a, b \in \mathbb{N}$ és b négyzetmentes (azaz nem osztható egyetlen prím négyzetével

sem). Itt $a^2b \leq n$ miatt $a \leq \sqrt{n}$, tehát a legfeljebb $\sqrt{n}$ (pontosabban $[\sqrt{n}]$) különböző értéket vehet fel. A b számok úgy állnak elő, mint n -nél nem nagyobb különböző prímek szorzatai, azaz $b = p_1^{u_1} p_2^{u_2} \dots p_{\pi(n)}^{u_{\pi(n)}}$, ahol mindegyik u_i értéke 0 vagy 1. Így b legfeljebb $2^{\pi(n)}$ különböző értéket vehet fel, s kapjuk, hogy az a^2b szorzatok száma legfeljebb $\sqrt{n}2^{\pi(n)}$, azaz $n \leq \sqrt{n}2^{\pi(n)}$, ahonnan a bizonyítandó egyenlőtlenséget kapjuk. $\square$

Megjegyzés. Az előbbi tétel szerint, ha $n \rightarrow \infty$, akkor $\pi(n) \rightarrow \infty$, s ez egy újabb, egyszerű bizonyítása annak a ténynek, hogy végtelen sok prím létezik.

Az alábbiakban pontosabb becsléseket vezetünk le a $\pi(x)$ függvényre.

Szükségünk van a következő, önmagában is érdekes eredményre.

5. Tétel. Ha $x \in \mathbb{R}, x \geq 2$, akkor

$$(1) \quad \prod_{p \leq x} p < 4^x.$$

Bizonyítás. (Erdős Pál, Kalmár László) Elegendő $x \in \mathbb{N}, x \geq 2$ értékekre bizonyítani, mert ha ezekre igaz a tétel, akkor minden $x \in \mathbb{R}, x \geq 2$ számra

$$\prod_{p \leq x} p = \prod_{p \leq [x]} p < 4^{[x]} \leq 4^x$$

is igaz. Legyen tehát $x = n \in \mathbb{N}, n \geq 2$. Indukcióval bizonyítunk. Ha $n = 2$, akkor (1) igaz. Tegyük fel, hogy (1) igaz minden $x \in \mathbb{N}, 2 \leq x \leq n-1$ számra és igazoljuk (1)-et $x = n$ -re, ahol $n \geq 3$.

Ha n páros, akkor n nem prím, így

$$\prod_{p \leq n} p = \prod_{p \leq n-1} p < 4^{n-1} < 4^n.$$

Ha n páratlan, akkor legyen $n = 2k + 1, k \geq 1$ és

$$\prod_{p \leq n} p = \prod_{p \leq 2k+1} p = \prod_{p \leq k+1} p \prod_{k+2 \leq p \leq 2k+1} p.$$

Itt az első szorzat kisebb mint 4^{k+1} , az indukciós feltétel szerint, a második szorzat pedig a következőképpen becsülhető. Tekintsük a $C_{2k+1}^k = \binom{2k+1}{k}$ binomiális együtthatót, s vegyük észre, hogy

$$\prod_{k+2 \leq p \leq 2k+1} p | C_{2k+1}^k = \frac{(k+2)(k+3) \cdots (2k+1)}{1 \cdot 2 \cdot 3 \cdots k},$$

mert a számlálóban szerepel minden $k+2$ és $2k+1$ közötti prím, a nevezőben viszont ezek a prímek nem szerepelnek, hiszen a nevező tényezői kisebbek ezeknél. Így

$$\begin{aligned} \prod_{k+2 \leq p \leq 2k+1} p &\leq C_{2k+1}^k = \frac{2 \cdot 3 \cdot 4 \cdots 2k(2k+1)}{1 \cdot 2 \cdot 3 \cdots k(k+1)!} = 2^k \frac{3 \cdot 5 \cdots (2k+1)}{2 \cdot 3 \cdots (k+1)} < \\ &< 2^k \frac{4 \cdot 6 \cdots (2k+2)}{2 \cdot 3 \cdots (k+1)} = 2^{2k} = 4^k. \end{aligned}$$

Kapjuk, hogy

$$\prod_{p \leq n} p < 4^{k+1} \cdot 4^k = 4^{2k+1} = 4^n$$

és a bizonyítást befejeztük. $\square$

Alkalmazni fogjuk a következő tételt.

6. Tétel. (Legendre) Ha $n \in \mathbb{N}$, akkor $n!$ kanonikus alakja

$$n! = \prod_{\substack{p \leq n \\ p \text{ prím}}} p^a, \quad \text{ahol } a = a(n, p) = \sum_{k=1}^{\infty} \left[\frac{n}{p^k} \right],$$

itt véges sok tag kivételével minden tag nulla.

Bizonyítás. Az $n!$ kanonikus alakjában csak olyan prímszámok szerepelnek, melyek n -nél nem nagyobbak. Legyen $p \leq n$ egy rögzített prímszám. Az $n! = 1 \cdot 2 \cdot 3 \cdots n$ tényezői közül p -vel oszthatók a következők: $p, 2p, \dots, \left[\frac{n}{p} \right] p$. Így

$$n! = p \cdot 2p \cdots \left[\frac{n}{p} \right] p n_1 = p^{\left[\frac{n}{p} \right]} \cdot 1 \cdot 2 \cdot 3 \cdots \left[\frac{n}{p} \right] n_1,$$

ahol $p \nmid n_1$. Ha $\left[\frac{n}{p} \right] \geq p$, akkor az $1 \cdot 2 \cdot 3 \cdots \left[\frac{n}{p} \right]$ szorzat tényezői között ismét vannak p -vel oszthatók, mégpedig $p, 2p, \dots, \left[\frac{\left[\frac{n}{p} \right]}{p} \right] p$, s ezek közül az utolsó értéke $\left[\frac{n}{p^2} \right] p$. Így

$$n! = p^{\left[\frac{n}{p} \right]} \cdot p \cdot 2p \cdots \left[\frac{n}{p^2} \right] p n_1 n_2 = p^{\left[\frac{n}{p} \right] + \left[\frac{n}{p^2} \right]} \cdot 1 \cdot 2 \cdot 3 \cdots \left[\frac{n}{p^2} \right] n_1 n_2,$$

ahol $p \nmid n_2$.

Ha $\left[\frac{n}{p^2} \right] \geq p$, akkor ezt az eljárást ismételjük, s kapjuk, hogy

$$n! = p^{\left[\frac{n}{p} \right] + \left[\frac{n}{p^2} \right] + \dots} n_1 n_2 \cdots$$

alakú, ahol az $n_1, n_2, \dots$ számok egyike sem osztható p -vel. $\square$

Más bizonyítás. Legyen

$$A_p(n, j) = \#\{k \in \mathbb{N} : k \leq n, \nu_p(k) = j\}$$

azoknak az $1 \leq k \leq n$ számoknak a száma, amelyek kanonikus alakjában p a j -edik hatványon szerepel. Akkor

$$A_p(n, j) = \left[\frac{n}{p^j} \right] - \left[\frac{n}{p^{j+1}} \right],$$

és innen

$$\begin{aligned} a(n, p) = \nu_p(n!) &= \sum_{k=1}^n \nu_p(k) = \sum_{j=1}^{\infty} j A_p(n, j) = \sum_{j=1}^{\infty} j \left[\frac{n}{p^j} \right] - \sum_{j=1}^{\infty} j \left[\frac{n}{p^{j+1}} \right] = \\ &= \sum_{j=1}^{\infty} j \left[\frac{n}{p^j} \right] - \sum_{j=1}^{\infty} (j-1) \left[\frac{n}{p^j} \right] = \sum_{j=1}^{\infty} \left[\frac{n}{p^j} \right]. \quad \square \end{aligned}$$

Megjegyzés. Az $a = a(n, p)$ kitevő így is megadható:

$$a = \sum_{k=1}^r \left[\frac{n}{p^k} \right]$$

az $r = r(n, p)$ számot a $p^r \leq n < p^{r+1}$ egyenlőtlenségek határozzák meg (azaz $r = \lceil \log n / \log p \rceil$).

Feladat. Hány nullában végződik a $100!$ szám?

Megoldás. $[100/5] + [100/25] + [100/125] + \dots = 20 + 4 = 24$.

Feladat. A Legendre-képletbeli minden $a(n, p)$ kitevőre

$$\frac{n}{p} - 1 < a(n, p) \leq \frac{n}{p-1}.$$

Bizonyítás. Az $x - 1 < [x] \leq x$ egyenlőtlenségek szerint:

$$a(n, p) \leq \frac{n}{p} + \sum_{k=2}^{\infty} \frac{n}{p^k} = \frac{n}{p} + \frac{n}{p^2} \cdot \frac{1}{1 - \frac{1}{p}} = \frac{n}{p-1},$$

ugyanakkor

$$a(n, p) = \left[\frac{n}{p} \right] + \sum_{k=2}^{\infty} \left[\frac{n}{p^k} \right] \geq \left[\frac{n}{p} \right] > \frac{n}{p} - 1. \quad \square$$

Feladat. Az előző Feladatot használva mutassuk meg, hogy végtelen sok prím létezik.

Útmutatás. $a(n, p) \leq n/(p-1)$, ahonnan $n! \leq \prod_{p \leq n} p^{n/(p-1)}$ és használjuk az $(n!)^2 \geq n^n$ egyenlőtlenséget.

7. Tétel. A $C_n^k = \binom{n}{k}$ binomiális együttható kanonikus alakja

$$C_n^k = \prod_{\substack{p \leq n \\ p \text{ prím}}} p^b, \quad \text{ahol } b = b(n, k, p) = \sum_{i=1}^{\infty} \left(\left[\frac{n}{p^i} \right] - \left[\frac{k}{p^i} \right] - \left[\frac{n-k}{p^i} \right] \right),$$

Továbbá itt minden p^b prímhatványra $p^b \leq n$.

Bizonyítás. Alkalmazzuk az ismert

$$C_n^k = \frac{n!}{k!(n-k)!}$$

képletet és az előbbi tételt. A $b = b(n, k, p)$ kitevő értéke

$$b = a(n, p) - a(k, p) - a(n-k, p) = \sum_{i=1}^{\infty} \left(\left[\frac{n}{p^i} \right] - \left[\frac{k}{p^i} \right] - \left[\frac{n-k}{p^i} \right] \right).$$

A $0 \leq [x+y] - [x] - [y] \leq 1$ egyenlőtlenségeket alkalmazva $x = k/p^i$ és $y = (n-k)/p^i$ -re kapjuk, hogy a fenti b összeg minden tagja 0 vagy 1. Így $0 \leq b \leq r$, ahol r a Legendre-képletben az összegzés felső határára vonatkozó r . Innen következik, hogy C_n^k egész szám (anélkül, hogy hivatkoznánk e szám algebrai vagy kombinatorikai jelentésére), s hogy $p^b \leq n$ minden p^b esetén. $\square$

3. ELŐADÁS

8. Tétel. *Létezik olyan C_1 valós szám, hogy $0 < C_1 < 1$ és*

$$(2) \quad \pi(x) > C_1 \frac{x}{\log x}$$

minden $x \geq 2$ valós szám esetén. Választható $C_1 = (\log 2)/4 = 0,173286\dots$.

Bizonyítás. A 7. Tétel szerint minden $n \in \mathbb{N}$ számra a $C_{2n}^n = \binom{2n}{n}$ binomiális együttható kanonikus alakja

$$C_{2n}^n = \prod_{p \leq 2n} p^b \leq \prod_{p \leq 2n} (2n) = (2n)^{\pi(2n)}$$

és

$$\begin{aligned} C_{2n}^n &= \frac{(2n)!}{(n!)^2} = \frac{2 \cdot 3 \cdots (2n-1)2n}{2 \cdot 3 \cdots (n-1)n \cdot n!} = 2^n \frac{3 \cdot 5 \cdots (2n-1)}{n!} > \\ &> 2^n \frac{2 \cdot 4 \cdot 6 \cdots (2n-2)}{1 \cdot 2 \cdots (n-1)n} = \frac{2^{2n-1}}{n} = \frac{2^{2n}}{2n}, \end{aligned}$$

ahonnan

$$\begin{aligned} \pi(2n) \log 2n &> 2n \log 2 - \log 2n \geq 2n \log 2 - \log 2^n = 2n \log 2 - n \log 2 = \\ &= n \log 2 \geq \frac{n+1}{2} \log 2, \end{aligned}$$

használva a $2n \leq 2^n$ és $n \geq \frac{n+1}{2}$ egyenlőtlenségeket. Kapjuk, hogy

$$\pi(2n) > \frac{(n+1) \log 2}{2 \log 2n},$$

amely páros természetes számok esetén ad alsó becslést a π függvényre. Legyen most $x \in \mathbb{R}, x \geq 2$, akkor az előbbieket szerint

$$\pi(x) \geq \pi(2 \left\lfloor \frac{x}{2} \right\rfloor) > \frac{\log 2}{2} \cdot \frac{\left\lfloor \frac{x}{2} \right\rfloor + 1}{\log 2 \left\lfloor \frac{x}{2} \right\rfloor} > \frac{\log 2}{2} \cdot \frac{\frac{x}{2}}{\log x} = \frac{\log 2}{4} \frac{x}{\log x},$$

ahol $\left\lfloor \frac{x}{2} \right\rfloor \geq 1$. Választható tehát $C_1 = \frac{\log 2}{4}$ és a (2) egyenlőtlenség fennáll minden $x \geq 2$ -re. $\square$

9. Tétel. *Létezik olyan C_2 valós szám, hogy $C_2 > 1$ és*

$$(3) \quad \pi(x) < C_2 \frac{x}{\log x}$$

minden $x \geq 2$ valós szám esetén. Választható $C_2 = 1 + 4 \log 2 = 3,772588\dots$.

Bizonyítás. Használjuk az 5. Tételt. Ha a $\prod_{p \leq x} p$ szorzatban minden tényezőt 2-vel helyettesítünk, akkor

$$2^{\pi(x)} \leq \prod_{p \leq x} p < 4^x,$$

ahonnan csak a $\pi(x) < 2x$ triviális egyenlőtlenség adódik.

Tekintsük ezért csak a $\sqrt{x}$ és x közötti p prímek szorzatát:

$$\prod_{p \leq x} p \geq \prod_{\sqrt{x} < p \leq x} p > (\sqrt{x})^{\pi(x) - \pi(\sqrt{x})}.$$

Az 5. Tételt alkalmazva így

$$(\sqrt{x})^{\pi(x) - \pi(\sqrt{x})} < 4^x,$$

ahonnan

$$(\pi(x) - \pi(\sqrt{x})) \log \sqrt{x} < x \log 4, \quad \pi(x) \log x < \pi(\sqrt{x}) \log x + 4x \log 2.$$

Használva, hogy $\pi(\sqrt{x}) \leq \sqrt{x}$ innen

$$\pi(x) \log x < \sqrt{x} \log x + 4x \log 2, \quad \frac{\pi(x) \log x}{x} < \frac{\log x}{\sqrt{x}} + 4 \log 2$$

következik, ahol $f(x) = \frac{\log x}{\sqrt{x}} < 1$ minden $x \geq 2$ -re (vizsgáljuk az f függvény változását). Választható így $C_2 = 1 + 4 \log 2$. $\square$

A 8. és 9. Tételek alapján léteznek a C_1 és C_2 állandók úgy, hogy $0 < C_1 < 1 < C_2$ és

$$\boxed{C_1 \frac{x}{\log x} < \pi(x) < C_2 \frac{x}{\log x}, \quad \forall x \geq 2.}$$

Ezt először P. L. Csebisevnek sikerült igazolnia a XIX. század közepén.

A $\pi(x)$ -re vonatkozó jóval pontosabb eredmény a következő, melyet J. Hadamard és Ch. de la Vallée Poussin bizonyítottak 1896-ban, egymástól függetlenül, komplex-függvénytan segítségével. Az első elemi bizonyítást Erdős Pál és A. Selberg adták 1949-ben, szintén egymástól függetlenül.

10. Tétel. (*Prímszámtétel*)

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{\frac{x}{\log x}} = 1,$$

azaz $\pi(x) \sim \frac{x}{\log x}$ ($a \sim b$ jelet olvasd: aszimptotikusan egyenlő).

Nem bizonyítjuk itt ezt a tételt, csak annyit jegyzünk meg, hogy e tétel szerint minden $\varepsilon > 0$ számhoz létezik olyan $x(\varepsilon) \in \mathbb{R}$ szám, hogy

$$(1 - \varepsilon) \frac{x}{\log x} < \pi(x) < (1 + \varepsilon) \frac{x}{\log x}$$

fennáll minden $x \geq x(\varepsilon)$ valós számra.

11. Tétel.

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{x} = 0.$$

Bizonyítás. Határértékre térünk ($x \rightarrow \infty$) a fenti (3) egyenlőtlenségben. $\square$

Ha $(a_n)_{n \geq 1}$ egy természetes számokból álló sorozat, akkor jelölje $u(x) = \sum_{a_n \leq x} 1$ a sorozat x -nél nem nagyobb tagjainak a számát. Az adott sorozat sűrűségén a $\lim_{x \rightarrow \infty} \frac{u(x)}{x}$ határértéket értjük, feltéve, hogy ez létezik. A páros számok sűrűsége

például $1/2$, a négyzetszámok sűrűsége nulla és a 11. Tétel szerint a prímszámok sűrűsége is nulla, azaz a prímek "ritkán" fordulnak elő a természetes számok között.

Feladat. Jelölje $\pi^*(x)$ a $p^m \leq x$ prímhatalványok számát. Igazoljuk, hogy minden $x \geq 2$ -re

$$\alpha \frac{x}{\log x} < \pi^*(x) < \beta \frac{x}{\log x},$$

alkalmas pozitív α és β állandókkal.

Megoldás. Azonnali, hogy $\pi^*(x) \geq \pi(x) > \alpha \frac{x}{\log x}$, lásd 8. Tétel. Továbbá,

$$\pi^*(x) = \sum_{p^m \leq x} 1 = \sum_{p \leq x} 1 + \sum_{\substack{p^m \leq x \\ m \geq 2}} 1 = \pi(x) + \sum_{\substack{p^m \leq x \\ m \geq 2}} 1,$$

ahol a 9. Tételt használva,

$$\begin{aligned} \sum_{\substack{p^m \leq x \\ m \geq 2}} 1 &= \sum_{2 \leq m \leq \log x / \log 2} \sum_{p \leq \sqrt[m]{x}} 1 = \sum_{2 \leq m \leq \log x / \log 2} \pi(\sqrt[m]{x}) \leq \\ &\leq \frac{\log x}{\log 2} \pi(\sqrt{x}) < \frac{\log x}{\log 2} \cdot \frac{C\sqrt{x}}{\log x} = C'\sqrt{x}. \end{aligned}$$

Kapjuk, hogy

$$\pi^*(x) \leq \pi(x) + C'\sqrt{x} < C'' \frac{x}{\log x} + C'\sqrt{x} < \beta \frac{x}{\log x}.$$

• Az n -edik prímszámra vonatkozó becslések

Jelölje p_n az n -edik prímszámot. Így $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, p_5 = 11, \dots$ és $p_n \rightarrow \infty$, ha $n \rightarrow \infty$. Most azt vizsgáljuk, hogy milyen nagyságrendű a p_n .

Először igazoljuk az alábbi, Bertrand-posztulátum illetve Csebisev- tétel néven ismert eredményt.

12. Tétel. Ha $n \in \mathbb{N}, n \geq 2$, akkor létezik olyan p prímszám, melyre $n < p < 2n$.

Bizonyítás. (Erdős Pál, 1932) Legyen

$$A = \prod_{n+1 \leq p \leq 2n} p.$$

Megmutatjuk, hogy ez a szorzat nem üres, van legalább egy tényezője, azaz $A > 1$. Tekintsük ismét a C_{2n}^n binomiális együtthatót. Az A szám osztója a

$$C_{2n}^n = \frac{(n+1)(n+2) \cdots 2n}{1 \cdot 2 \cdots n}$$

számnak, hiszen az A -beli p prímek mind szerepelnek a számlálóban és nem szerepelnek a nevezőben. A 8. Tétel szerint C_{2n}^n kanonikus alakja

$$C_{2n}^n = \prod_{p \leq 2n} p^{b(p)}, \quad \text{ahol} \quad b(p) = b(2n, n, p) = \sum_{i=1}^r \left(\left\lfloor \frac{2n}{p^i} \right\rfloor - 2 \left\lfloor \frac{n}{p^i} \right\rfloor \right),$$

s $r = r(n, p)$ -t a $p^r \leq 2n < p^{r+1}$ egyenlőtlenségek határozzák meg, $b(p) \leq r$ és

$$(1) \quad p^{b(p)} \leq 2n$$

minden $p \leq 2n$ prímre.

Ha $p > \sqrt{2n}$, akkor $p^2 > 2n$, így $r = 1$ és $b(p) \leq 1$. Bontsuk fel ezért a C_{2n}^n kanonikus alakját adó szorzatot három tényezőre úgy, hogy az elsőben szerepeljenek a $\sqrt{2n}$ -nél nem nagyobb prímelek, a másodikban a $\sqrt{2n}$ és n közötti prímelek, a harmadikban pedig éppen az A -beli prímelek:

$$C_{2n}^n = B \cdot C \cdot D,$$

ahol

$$B = \prod_{p \leq \sqrt{2n}} p^{b(p)}, \quad C = \prod_{\sqrt{2n} < p \leq n} p^{b(p)}, \quad D = \prod_{n+1 \leq p \leq 2n} p^{b(p)}.$$

A D szorzatban a fentiek alapján $b(p) \leq 1$, így $D \leq A$ és

$$(2) \quad A \geq D = \frac{C_{2n}^n}{B \cdot C}.$$

A C_{2n}^n -re már levezettünk egy alsó becslést:

$$C_{2n}^n > \frac{2^{2n}}{2n},$$

lásd korábban. A továbbiakban felső becslést keresünk a B és C szorzatokra. (2) alapján

$$B = \prod_{p \leq \sqrt{2n}} p^{b(p)} \leq \prod_{p \leq \sqrt{2n}} \sqrt{2n} \leq (2n)^{\pi(\sqrt{2n})}.$$

A C szorzatban $b(p) \leq 1$ minden p -re és ha $\frac{2n}{3} < p \leq n$, akkor $b(p) = 0$. Valóban, ekkor $1 \leq \frac{n}{p} < \frac{3}{2}$ és $2 \leq \frac{2n}{p} < 3$, így $b(p) = \left[\frac{2n}{p} \right] - 2 \left[\frac{n}{p} \right] = 2 - 2 = 0$. Következik, hogy

$$C \leq \prod_{\sqrt{2n} < p \leq (2n)/3} p < \prod_{p \leq (2n)/3} p < 4^{\frac{2n}{3}},$$

az 5. Tétel szerint, feltéve, hogy $n \geq 3$. Így (2)-ből

$$A > \frac{2^{2n}}{2n(2n)^{\pi(\sqrt{2n})} 4^{(2n)/3}} = \frac{2^{(2n)/3}}{(2n)^{\pi(\sqrt{2n})+1}}.$$

Ha $\sqrt{2n} > 15$, akkor $\sqrt{2n}$ -ig biztos nem prímelek a páros számok, a páratlanok közül pedig nem prím az 1, 9 és a 15. Így

$$\pi(\sqrt{2n}) + 1 \leq \left(\frac{\sqrt{2n} + 1}{2} - 2 \right) + 1 = \frac{\sqrt{2n} - 1}{2} < \frac{\sqrt{2n}}{2},$$

ahonnan

$$A > \frac{2^{(2n)/3}}{(2n)^{\sqrt{2n}/2}} = \left(\frac{2^{\sqrt{2n}}}{(\sqrt{2n})^3} \right)^{\sqrt{2n}/3}.$$

Igazoljuk, hogy $\frac{2^{\sqrt{2n}}}{(\sqrt{2n})^3} > 1$, ha n elég nagy. A $\sqrt{2n} = t$ jelöléssel azt kell igazolni, hogy $2^t > t^3$. Ez fennáll minden $t \geq 10$ esetén ($2^{10} = 1024 > 1000 = 10^3$). Így $A > 1$, ha $\sqrt{2n} > 15$, azaz ha $n \geq 113$. Ha $n < 113$, akkor közvetlen ellenőrzéssel győződünk meg a tétel helyességéről. Tekintsük a következő prímekeket: 2, 3, 5, 7, 13, 23, 43, 83, 127, ahol mindegyik kisebb az előző kétszeresénél és az utolsó nagyobb, mint 113. Ha $n = 1$, akkor választható $p = 2$ (ezért engedjük meg az egyenlőséget). Ha $2 \leq n < 113$ és $p \leq n < p'$, ahol p, p' a fenti sorozat két egymásutáni eleme, akkor $p' < 2p \leq 2n$, tehát p' -re teljesül a tulajdonság, s ezzel a bizonyítás teljes. $\square$

Feladat. Az előbbi tétel alkalmazásaként igazoljuk, hogy minden $n \in \mathbb{N}, n \geq 2$ esetén $p_n < 2^n$.

Megoldás. Indukcióval bizonyítunk. Ha $n = 2$, akkor $p_2 = 3 < 2^2$ igaz. Tegyük fel, hogy a tulajdonság igaz valamely $k \geq 2$ -re, azaz $p_k < 2^k$. Akkor a Tétel alapján 2^k és 2^{k+1} között létezik prímszám, mely nagyobb mint p_k , s így $p_{k+1} < 2^{k+1}$. $\square$

Feladat. Ha $n \in \mathbb{N}, n \geq 2$, akkor $n!$ kanonikus alakjában legalább egy prím kitevője 1.

Megoldás. Ha $n = 2$, akkor a tulajdonság igaz. Ha $n = 2k$, ahol $k \geq 2$, akkor a fenti Tétel szerint létezik p prímszám úgy, hogy $k < p < 2k$, így $p < n < 2p$. Ha pedig $n = 2k + 1$ alakú, $k \geq 1$, akkor létezik q prím, úgy, hogy $k < q < 2k < n$, ahonnan $q < n < 2q$. $\square$

Megjegyzés. Innen azonnal adódik, hogy ha $n \in \mathbb{N}, n \geq 2$, akkor $n!$ nem lehet teljes négyzet, teljes köb, általában teljes k -adik hatvány, ahol $k \geq 2$.

4. ELŐADÁS

A továbbiakban a 12. Tétel (Csebisev tétel) és a $\pi(x)$ -re vonatkozó egyenlőtlenségek alkalmazásaként az n -edik prímszámra vezetünk le becsléseket, melyek élesebbek mint a triviális $p_n > n$ és a múltkori feladatbeli $p_n < 2^n$.

13. Tétel. *Léteznek olyan C_3 és C_4 valós számok, hogy $0 < C_3 < 1 < C_4$ és minden $n \geq 2$ esetén*

$$(3) \quad \boxed{C_3 n \log n < p_n < C_4 n \log n.}$$

Választható $C_3 = 1/C_2 = 0,26507\dots$ és $C_4 = 18$.

Bizonyítás. Levezettük, hogy

$$C_1 \frac{x}{\log x} < \pi(x) < C_2 \frac{x}{\log x}, \quad x \geq 2$$

lásd 8. és 9. Tételek. Ha most $x = p_n$, akkor $\pi(p_n) = n$ és kapjuk, hogy

$$C_1 \frac{p_n}{\log p_n} < n < C_2 \frac{p_n}{\log p_n},$$

s innen

$$(4) \quad p_n > \frac{n}{C_2} \log p_n > \frac{n \log n}{C_2},$$

ami a bizonyítandó első egyenlőtlenség. Továbbá

$$(5) \quad p_n < \frac{1}{C_1} n \log p_n < 6n \log p_n$$

és logaritmálva

$$(6) \quad \log p_n < \log 6 + \log n + \log \log p_n.$$

Használva, hogy $p_n < 2^n$ (Feladat volt) a $\log p_n < n \log 2 < n$ egyenlőtlenséget kapjuk, s (6)-ba visszahelyettesítve:

$$\log p_n < \log 6 + \log n + \log n \leq 3 \log n,$$

ha $n \geq 6$. Ezt visszaírva (5)-be $p_n < 18n \log n$, amit igazolni akartunk. Az $n \in \mathbb{N}, 2 \leq n \leq 5$ értékekre közvetlenül ellenőrizhető a második egyenlőtlenség helyessége. $\square$

Feladat. Igazoljuk, hogy

$$(7) \quad \lim_{n \rightarrow \infty} \frac{\log p_n}{\log n} = 1.$$

Megoldás. Logaritmálva a (3) egyenlőtlenségekben:

$$\log n + \log \log n + \log C_3 < \log p_n < \log n + \log \log n + \log C_4,$$

majd $\log n$ -nel osztva és határértékre térve ($n \rightarrow \infty$) a bizonyítandó összefüggést kapjuk.

Felhasználva ezt következik a Prímszámtétel alábbi, másik alakja.

14. Tétel.

$$\lim_{n \rightarrow \infty} \frac{p_n}{n \log n} = 1,$$

azaz $p_n \sim n \log n$.

Bizonyítás. A 10. Tételben legyen $x = p_n$, akkor $\pi(x) = n$ és kapjuk, hogy

$$\lim_{n \rightarrow \infty} \frac{n \log p_n}{p_n} = 1,$$

amit összevetve (7)-tel következik az állítás. $\square$

Megjegyzések. Nagy n értékekre tehát p_n közelítőleg $n \log n$ -nel egyenlő. J. B. Rosser 1939-ben igazolta, hogy $p_n > n \log n$ fennáll minden $n \in \mathbb{N}$ számra. A 14. Tételből rögtön következik, hogy

$$\lim_{n \rightarrow \infty} \frac{p_{n+1}}{p_n} = 1.$$

Feladat. Igazoljuk, hogy $p_{n+1} < 2p_n$ minden $n \geq 1$ esetén.

Megoldás. Azonnali a Csebisev-tételből (12. Tétel), p_n és $2p_n$ között van prím, így $p_{n+1} < 2p_n$.

Feladat. Igazoljuk, hogy létezik végtelen sok olyan prímszám, melyeknek első számjegye 1-es (10-es számrendszerben felírva).

Megoldás. A Csebisev-tétel szerint (12. Tétel) minden $k \geq 1$ -re 10^k és $2 \cdot 10^k$ között van prímszám, s ez olyan szám, amelynek első jegye 1-es és $k + 1$ -jegyű. Így különböző k értékekre különböző ilyen prímekeket kapunk.

Feladat. Igazoljuk, hogy létezik végtelen sok olyan $n \geq 1$ szám, amelyre $d_{n+1} > d_n$, ahol $d_n = p_{n+1} - p_n$.

Megoldás. Tudjuk, hogy két szomszédos prím közötti különbség tetszőleges nagy lehet, lásd korábban, tehát a $(d_n)_{n \geq 1}$ sorozat nem korlátos.

Ha az adott tulajdonság nem lenne igaz, azaz ha csak véges sok n -re lenne $d_{n+1} > d_n$, akkor létezne $n_0 \in \mathbb{N}$ úgy, hogy $d_{n+1} \leq d_n$, $\forall n \geq n_0$. Így $d_{n_0+k} \leq d_{n_0+k-1} \leq \dots \leq d_{n_0+1} \leq d_{n_0}$, azaz $(d_{n_0+k})_{k \geq 1}$ korlátos, és így $(d_n)_{n \geq 1}$ is korlátos, ellentmondás.

Feladat. Jelölje c_n az n -edik összetett számot ($c_1 = 4, c_2 = 6, c_3 = 8, c_4 = 9, \dots$). Mutassuk meg, hogy

$$\lim_{n \rightarrow \infty} \frac{c_n}{n} = 1.$$

Megoldás. Nyilvánvaló, hogy $c_n > n$ minden $n \geq 1$ -re. Legyen $C(x) = \#\{n : n \leq x \text{ és } n \text{ összetett}\}$. Ekkor $C(c_n) = n$ és minden $x \geq 1$ -re $\pi(x) + C(x) + 1 = [x]$. Ha $x = c_n$, akkor $\pi(c_n) + n + 1 = c_n$. Innen $c_n > n + 1 > n$, amit már említettünk, másrészt minden $n \geq 1$ -re

$$c_n < A \frac{c_n}{\log c_n} + n + 1 < A \frac{c_n}{\log n} + n + 1,$$

ahol vehető pl. $A = 4$, lásd 9. Tétel. Kapjuk, hogy

$$c_n < \frac{n + 1}{1 - A/\log n},$$

elég nagy n -re (úgy, hogy a nevező pozitív). Tehát

$$1 + \frac{1}{n} < \frac{c_n}{n} < \frac{1 + 1/n}{1 - A/\log n},$$

s innen azonnali, hogy $c_n \sim n$.

• **A prímszámok reciprokainak összege**

15. Tétel. a) Létezik olyan C_5 állandó, hogy minden $x \geq 2$ esetén

$$\sum_{p \leq x} \frac{1}{p} > \log \log x + C_5,$$

ahol az összegzés a $p \leq x$ prímszámokra vonatkozik. Választható $C_5 = -1$.

b) A prímszámok reciprokaiból alkotott

$$\sum_p \frac{1}{p} = \sum_{n=1}^{\infty} \frac{1}{p_n}$$

végtelen sor divergens, összege ∞ .

Bizonyítás. a) (Euler) Legyen $[x] = n \geq 2$ és minden $p \leq n$ prímszám esetén értelmezzük az $a(p) \in \mathbb{N}$ számot a következőképpen: $p^{a(p)} \leq n < p^{a(p)+1}$, azaz $a(p) = \left\lfloor \frac{\log n}{\log p} \right\rfloor$. Tekintsük a

$$P_n = \prod_{p \leq n} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \dots + \frac{1}{p^{a(p)}}\right)$$

szorzatot. A szorzások elvégzésével egy összeget kapunk, melynek minden tagja

$$\frac{1}{p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}}$$

alakú, ahol $p_1, p_2, \dots, p_r$ jelöli az n -nél nem nagyobb prímeket és $0 \leq k_i \leq a(p_i)$ minden $i \in \{1, 2, \dots, r\}$ esetén. A számelmélet alaptétele szerint így az $1, 1/2, \dots, 1/n$ törtek mindegyikét megkapjuk és pontosan egyszer (s még másokat is), tehát

$$P_n \geq \sum_{k=1}^n \frac{1}{k}.$$

Ismert egyenlőtlenség szerint

$$\sum_{k=1}^n \frac{1}{k} > \log(n+1),$$

ahonnan

$$(1) \quad \log P_n > \log \log(n+1) > \log \log x$$

Másrészt, alkalmazva a mértani haladvány összegképletét:

$$(2) \quad P_n = \prod_{p \leq n} \left(1 - \left(\frac{1}{p}\right)^{a(p)+1}\right) \left(1 - \frac{1}{p}\right)^{-1} < \prod_{p \leq n} \left(1 - \frac{1}{p}\right)^{-1},$$

s így

$$\begin{aligned}\log P_n &< -\sum_{p \leq n} \log\left(1 - \frac{1}{p}\right) = \sum_{p \leq n} \log\left(1 - \frac{1}{p}\right)^{-1} = \sum_{p \leq n} \log \frac{p}{p-1} \\ &= \sum_{p \leq n} \log\left(1 + \frac{1}{p-1}\right) < \sum_{p \leq n} \frac{1}{p-1},\end{aligned}$$

használva a $\log(1 + \frac{1}{n}) < \frac{1}{n}$ egyenlőtlenséget $n = p-1$ -re. Így

$$\begin{aligned}\log P_n &< \sum_{p \leq n} \frac{1}{p} + \sum_{p \leq n} \left(\frac{1}{p-1} - \frac{1}{p}\right) = \sum_{p \leq n} \frac{1}{p} + \sum_{p \leq n} \frac{1}{p(p-1)} \\ &< \sum_{p \leq n} \frac{1}{p} + \sum_{n=2}^{\infty} \frac{1}{n(n-1)} = \sum_{p \leq n} \frac{1}{p} + \sum_{n=2}^{\infty} \left(\frac{1}{n-1} - \frac{1}{n}\right) = \sum_{p \leq n} \frac{1}{p} + 1,\end{aligned}$$

azaz

$$(3) \quad \log P_n < \sum_{p \leq x} \frac{1}{p} + 1.$$

(1) és (3) alapján a bizonyítandó egyenlőtlenséget kapjuk a $C_5 = -1$ választással.

b) Ha $n \rightarrow \infty$, akkor az előzőek szerint $\sum_{p \leq n} \frac{1}{p} \rightarrow \infty$. $\square$

Megjegyzés. A $C_5 = -1$ érték javítható. Az alábbiak szerint (ezeket a becsléseket később még használni fogjuk) vehető $C_5 = -1/2$. Valóban,

A

$$\sum_{k=1}^{\infty} \frac{x^k}{k} = \log \frac{1}{1-x}, \quad 0 \leq x < 1$$

képletet $x = 1/p$ -re alkalmazva, valamint a mértani sor összegképlete alapján kapjuk, hogy

$$-\log\left(1 - \frac{1}{p}\right) = \sum_{k=1}^{\infty} \frac{1}{kp^k} \leq \frac{1}{p} + \frac{1}{2} \sum_{k=2}^{\infty} \frac{1}{p^k} = \frac{1}{p} + \frac{1}{2p(p-1)},$$

ahonnan

$$\begin{aligned}-\sum_{p \leq n} \log\left(1 - \frac{1}{p}\right) &\leq \sum_{p \leq n} \frac{1}{p} + \frac{1}{2} \sum_{p \leq n} \frac{1}{p(p-1)} \leq \sum_{p \leq n} \frac{1}{p} + \frac{1}{2} \sum_{k=1}^{\infty} \frac{1}{k(k+1)} \\ &= \sum_{p \leq n} \frac{1}{p} + \frac{1}{2} \sum_{k=1}^{\infty} \left(\frac{1}{k} - \frac{1}{k+1}\right),\end{aligned}$$

azaz

$$(4) \quad -\sum_{p \leq n} \log\left(1 - \frac{1}{p}\right) \leq \sum_{p \leq n} \frac{1}{p} + \frac{1}{2}.$$

Összevetve az (1), (2) és (4) egyenlőtlenségeket készen vagyunk a $C_5 = -1/2$ értékkel.

Feladat. Mutassuk meg, hogy

$$\sum_p \frac{1}{p^2} < \frac{1}{2}.$$

Megoldás.

$$\begin{aligned} \sum_p \frac{1}{p^2} &< \sum_{n=2}^{\infty} \frac{1}{n^2} - \sum_{n=2}^{\infty} \frac{1}{(2n)^2} = \frac{3}{4} \sum_{n=2}^{\infty} \frac{1}{n^2} < \\ &< \frac{3}{4} \sum_{n=2}^{\infty} \frac{1}{n^2 - 1/4} = \frac{3}{4} \sum_{n=2}^{\infty} \left(\frac{1}{n - 1/2} - \frac{1}{n + 1/2} \right) = \frac{3}{4} \cdot \frac{2}{3} = \frac{1}{2}. \end{aligned}$$

Megjegyzések. 1. Pontosabb becslés:

$$\begin{aligned} \sum_p \frac{1}{p^2} &< \sum_{n=2}^{\infty} \frac{1}{n^2} - \sum_{n=2}^{\infty} \frac{1}{(2n)^2} - \sum_{n=2}^{\infty} \frac{1}{(3n)^2} + \sum_{n=1}^{\infty} \frac{1}{(6n)^2} = \\ &= \frac{1}{36} + \left(1 - \frac{1}{4} - \frac{1}{9} + \frac{1}{36}\right) \sum_{n=2}^{\infty} \frac{1}{n^2} < \frac{1}{36} + \frac{24}{36} \cdot \frac{2}{3} = \frac{17}{36} = 0,4722..., \end{aligned}$$

még pontosabban (használva, hogy $\zeta(2) = 1,644934\dots$):

$$\sum_p \frac{1}{p^2} < \frac{1}{36} + \frac{2}{3} \left(\frac{\pi^2}{6} - 1 \right) = 0,4577...,$$

másrészt

$$\sum_p \frac{1}{p^2} > \frac{1}{4} + \frac{1}{9} + \frac{1}{25} + \frac{1}{49} + \frac{1}{121} + \frac{1}{169} = 0,4357....$$

tehát a pontos érték első tizedesjegye 4.

2. Igazolható, hogy $\sum_p \frac{1}{p^2} = 0,4522474200410654985\dots$. $\square$

Kérdés, hogy $\sum_{p \leq x} \frac{1}{p}$ milyen gyorsan tart a végtelenbe. A továbbiakban megmutatjuk, hogy $\sum_{p \leq x} \frac{1}{p}$ aszimptotikusan egyenlő $\log \log x$ -szel, azaz

$$\lim_{x \rightarrow \infty} \frac{\sum_{p \leq x} \frac{1}{p}}{\log \log x} = 1.$$

Ezzel kapcsolatban érdekes tény, hogy $(\log \log 10^{18} = 3,7244\dots$ miatt)

$$\sum_{p \leq 10^{18}} \frac{1}{p} < 4.$$

A 10^{18} -nál kisebb prímek száma $\pi(10^{18})$, ami kb. $10^{18}/\log 10^{18} = 10^{16} \cdot 2,412747\dots$, tehát a prímek reciprokaiból álló divergens sor első 10^{16} tagjának összege még 4-nél kisebb. Ez nagyon meglepő!

5. ELŐADÁS

Megjegyzés. A 13. Tételbeli $p_n < 18n \log n$ becslés új bizonyítást szolgáltat a 15. Tétel b) pontjára:

$$\frac{1}{p_n} > \frac{1}{18n \log n}, \quad n \geq 2,$$

és használjuk, hogy a $\sum_{n=2}^{\infty} \frac{1}{n \log n}$ sor divergens.

16. Tétel. a) Létezik olyan C_6 állandó, hogy minden $x \geq 2$ -re

$$\prod_{p \leq x} \left(1 - \frac{1}{p}\right) < \frac{C_6}{\log x},$$

vehető $C_6 = 1$.

b)

$$\lim_{x \rightarrow \infty} \prod_{p \leq x} \left(1 - \frac{1}{p}\right) = 0.$$

Bizonyítás. Az $F(x) = \log \prod_{p \leq x} \left(1 - \frac{1}{p}\right) = \sum_{p \leq x} \log\left(1 - \frac{1}{p}\right)$ jelöléssel, a 15. Tétel bizonyítása (2) és (1) képletei szerint $F(x) < -\log P_n < -\log \log x = \log \frac{1}{\log x}$.

b) Azonnali a) alapján. $\square$

Bizonyítás nélkül adjuk meg az ikerprímekre vonatkozó alábbi tulajdonságokat:

17. Tétel. (Viggo Brun, 1920) a) Az ikerprímek száma x -ig

$$\pi_2(x) < Kx \left(\frac{\log \log x}{\log x} \right)^2,$$

ahol K egy konstans.

b) $\pi_2(x)/\pi(x) \rightarrow 0$, $x \rightarrow \infty$, tehát az ikerprímek sűrűsége a prímek között 0.

c) Az ikerprímek reciprokaiból alkotott

$$\sum_{p, p+2 \text{ prím}} \frac{1}{p}$$

sor konvergens. $\square$

Megjegyzések. 1. A b) állítás azonnal következik az a)-ból: $\pi(x) > C_1 \frac{x}{\log x}$ alapján

$$\frac{\pi_2(x)}{\pi(x)} < K \frac{x}{\pi(x)} \left(\frac{\log \log x}{\log x} \right)^2 < KC_1^{-1} \frac{(\log \log x)^2}{\log x} \rightarrow 0.$$

2. A c) szerint vagy véges sok ikerprímpár van, vagy végtelen sok, de úgy, hogy a reciprokaik sora konvergens.

3. A sejtés az, hogy végtelen sok ikerprímpár van, pontosabban Hardy és Littlewood sejtése (1922) szerint

$$\pi_2(x) \sim 2 \prod_{p > 2} \left(1 - \frac{1}{(p-1)^2}\right) \frac{x}{\log^2 x},$$

ahol $\prod_{p>2} \left(1 - \frac{1}{(p-1)^2}\right) = 0,660161\dots$ az ún. ikerprím-konstans.

Ha f, g valós értékű függvények, akkor azt írjuk, hogy $f(x) = O(g(x))$ (olvasd "f(x) egyenlő nagy O g(x)"), ha létezik $a \in \mathbb{R}$ úgy, hogy $x \geq a$ esetén $g(x) > 0$ és $f(x)/g(x)$ korlátos, azaz $|f(x)| \leq M g(x), x \geq a$. Például $\sqrt{x} = O(x)$, $\sin x = O(1)$, azaz $\sin x$ korlátos, $\log x = O(\sqrt{x})$.

Továbbá, $f(x) = o(g(x))$ ("f(x) egyenlő kis o g(x)"), ha $\lim_{x \rightarrow \infty} f(x)/g(x) = 0$. Például $\sqrt{x} = o(x)$, $\log x = o(x^\varepsilon)$ minden $\varepsilon > 0$ esetén. Nyilván, ha $f(x) = o(g(x))$, akkor $f(x) = O(g(x))$ és fordítva általában nem.

• Mertens tételei

18. Tétel. (Mertens első tétele) *Létezik olyan C_7 valós szám, hogy minden $x \geq 2$ valós szám esetén*

$$\left| \sum_{p \leq x} \frac{\log p}{p} - \log x \right| < C_7,$$

(választható $C_7 = 1 + 2 \log 2 \approx 2,386294$), azaz

$$\sum_{p \leq x} \frac{\log p}{p} = \log x + O(1).$$

Bizonyítás. A bizonyítás ötlete a Legendre képlet (6. Tétel) ill. a 3. Előadás első Feladatában szereplő egyenlőtlenségek alkalmazása az $[x] = n$ szám faktoriálisára.

Logaritmált alakot írva:

$$\log n! = \sum_{p \leq n} a(n, p) \log p > \sum_{p \leq n} \left(\frac{n}{p} - 1 \right) \log p = n \sum_{p \leq n} \frac{\log p}{p} - \sum_{p \leq n} \log p,$$

és

$$\log n! = \sum_{p \leq n} a(n, p) \log p \leq \sum_{p \leq n} \left(\frac{n}{p} + \frac{n}{p(p-1)} \right) \log p = n \sum_{p \leq n} \frac{\log p}{p} + n \sum_{p \leq n} \frac{\log p}{p(p-1)}$$

és megjelent a vizsgálandó $\sum_{p \leq n} \frac{\log p}{p}$ kifejezés.

Itt

$$\sum_{p \leq n} \log p = \log \prod_{p \leq n} p < n \log 4$$

az 5. Tétel szerint, továbbá

$$\sum_{p \leq n} \frac{\log p}{p(p-1)} < \sum_{m=2}^{\infty} \frac{\log m}{m(m-1)} < 2 \sum_{m=2}^{\infty} \frac{\log m}{m^2} = 2C,$$

Az itt megjelenő sor konvergencia és összege $C < 3/2$ (ennek igazolása végett alkalmazzuk a Lagrange középértéktételt az $f(x) = -\frac{1+\log x}{x}$ függvényre, melynek deriváltja $f'(x) = \frac{\log x}{x^2}$).

Kapjuk, hogy

$$\frac{1}{n} \log n! - 2C < \sum_{p \leq n} \frac{\log p}{p} < \frac{1}{n} \log n! + \log 4.$$

Használjuk a $(\frac{n}{e})^n < n! < n^n, n \geq 2$ egyenlőtlenségeket (az első indukcióval könnyen igazolható, a második pedig azonnali). Kapjuk, hogy

$$(5) \quad n \log n - n < \log n! < n \log n,$$

ahonnan

$$\log n - 1 - 2C < \sum_{p \leq n} \frac{\log p}{p} < \log n + \log 4.$$

Következik, hogy $\sum_{p \leq n} \frac{\log p}{p} - \log n$ korlátos, azaz

$$\sum_{p \leq n} \frac{\log p}{p} = \log n + O(1),$$

s innen

$$\sum_{p \leq x} \frac{\log p}{p} = \sum_{p \leq n} \frac{\log p}{p} = \log x + \log \frac{n}{x} + O(1) = \log x + O(1),$$

ahol $\frac{x-1}{x} < \frac{n}{x} \leq 1$.

A C_7 állandóra vonatkozó becslés így kapható meg:

$$\begin{aligned} \sum_{p \leq n} \frac{\log p}{p(p-1)} &< \sum_{m=2}^{\infty} \frac{\log m}{m(m-1)} < \sum_{r=1}^{\infty} \sum_{m=2^{r-1}-1}^{2^r} \frac{\log 2^r}{m(m-1)} \\ &= \sum_{r=1}^{\infty} r \log 2 \sum_{m=2^{r-1}-1}^{2^r} \left(\frac{1}{m-1} - \frac{1}{m} \right) = \sum_{r=1}^{\infty} r \log 2 \left(\frac{1}{2^{r-1}} - \frac{1}{2^r} \right) \\ &= \sum_{r=1}^{\infty} \frac{r \log 2}{2^r} = 2 \log 2 = \log 4, \end{aligned}$$

alkalmazva, hogy $\sum_{k=1}^{\infty} kx^k = \frac{x}{(1-x)^2}$. Így használva az $\frac{n^n}{e^{n-1}} \leq n! \leq \frac{n^{n+1}}{e^{n-1}}, n \geq 2$ egyenlőtlenségekből (bizonyítás indukcióval) adódó

$$(6) \quad \log n! = n \log n - n + 1 + \theta_n \log n, \quad 0 \leq \theta_n \leq 1$$

(5)-nél erősebb, ún Stirling-képletet, kapjuk, hogy

$$\sum_{p \leq n} \frac{\log p}{p} > \log n + \frac{1}{n} - 1 - \log 4 > \log x - 1 - 2 \log 2,$$

mert $\log x - \log n = \log \frac{x}{n} < \log \frac{n+1}{n} < \frac{1}{n}$. És

$$-1 - 2 \log 2 < \sum_{p \leq x} \frac{\log p}{p} - \log x < 2 \log 2. \quad \square$$

Szükségünk van az Abel-összegzés következő alakjára, amelyet alkalmazunk $\sum_p \frac{1}{p}$ becslésére.

Állítás. (Abel-összegzés) Legyen f tetszőleges számelméleti függvény (azaz $f : \mathbb{N} \rightarrow \mathbb{R}$ függvény), $x > 1$ valós szám és legyen ψ folytonosan deriválható az $[1, x]$ intervallumon. Akkor az $F(x) = \sum_{n \leq x} f(n)$ jelöléssel minden $x > 1$ -re

$$(7) \quad \sum_{n \leq x} f(n)\psi(n) = F(x)\psi(x) - \int_1^x F(t)\psi'(t)dt.$$

Bizonyítás.

$$\begin{aligned} F(x)\psi(x) - \sum_{n \leq x} f(n)\psi(n) &= \sum_{n \leq x} f(n)(\psi(x) - \psi(n)) = \\ &= \sum_{1 \leq n \leq x} f(n) \int_n^x \psi'(t)dt = \int_1^x \psi'(t) \left(\sum_{1 \leq n \leq t} f(n) \right) dt = \int_1^x \psi'(t)F(t)dt. \quad \square \end{aligned}$$

Ehhez hasonló az összegek alábbi Abel-féle átrendezése:

Ha $n \in \mathbb{N}$ és $a_1, \dots, a_n, b_1, \dots, b_n, b_{n+1}$ valós (vagy komplex) számok, továbbá $A_k = a_1 + \dots + a_k, 1 \leq k \leq n$, akkor

$$\sum_{i=1}^n a_i b_i = a_1 b_1 + \sum_{i=2}^n (A_i - A_{i-1})b_i = \sum_{i=1}^{n-1} A_i(b_i - b_{i+1}) + A_n b_n = A_n b_{n+1} + \sum_{i=1}^n A_i(b_i - b_{i+1}).$$

19. Tétel. Létezik olyan C_8 állandó, hogy minden $x \geq 2$ valós számra

$$\sum_{p \leq x} \frac{1}{p} = \log \log x + C_8 + O\left(\frac{1}{\log x}\right),$$

ahol $C_8 \approx 0,261497$ az ún Mertens-állandó és az O -tag konstansa választható $2(1 + 2 \log 2) \approx 4,772588$ -nak.

Bizonyítás. Alkalmazzuk az Abel-összegzés fenti képletét az

$$f(n) = \begin{cases} \frac{\log p}{p}, & n = p \text{ prím}, \\ 0, & n \text{ nem prím}, \end{cases}$$

és $\psi(x) = \frac{1}{\log x}, \psi'(x) = -\frac{1}{x \log^2 x}$ választással.

Így

$$F(x) = \sum_{p \leq x} \frac{\log p}{p} = \log x + R(x),$$

ahol $F(x) = 0$, ha $x < 2$ és $R(x) = O(1)$ az előző Tétel szerint.

Kapjuk, hogy

$$\begin{aligned} \sum_{p \leq x} \frac{1}{p} &= \frac{\log x + R(x)}{\log x} + \int_2^x \frac{\log t + R(t)}{t \log^2 t} dt = \\ &= 1 + \frac{R(x)}{\log x} + \int_2^x \frac{dt}{t \log t} + \int_2^x \frac{R(t)dt}{t \log^2 t} = \\ &= 1 + \frac{R(x)}{\log x} + \log \log x - \log \log 2 + \int_2^\infty \frac{R(t)dt}{t \log^2 t} - \int_x^\infty \frac{R(t)dt}{t \log^2 t}, \end{aligned}$$

ahol $R(x) = O(1)$ miatt a fellépő improprius integrál konvergens:

$$\begin{aligned} \left| \int_2^\infty \frac{R(t)dt}{t \log^2 t} \right| &\leq \int_2^\infty \frac{|R(t)|dt}{t \log^2 t} = \int_2^\infty \frac{O(1)dt}{t \log^2 t} = \\ &= O\left(\int_2^\infty \frac{dt}{t \log^2 t}\right) = O\left(-\left[\frac{1}{\log t}\right]_2^\infty\right) = O\left(\frac{1}{\log 2}\right) = O(1). \end{aligned}$$

Legyen

$$C_8 = 1 - \log \log 2 + \int_2^\infty \frac{R(t)dt}{t \log^2 t},$$

ennek értékére vonatkozólag lásd később. Továbbá,

$$\begin{aligned} \left| \frac{R(x)}{\log x} - \int_x^\infty \frac{R(t)dt}{t \log^2 t} \right| &\leq \frac{|R(x)|}{\log x} + \int_x^\infty \frac{|R(t)|dt}{t \log^2 t} < \\ &< \frac{C_7}{\log x} + C_7 \int_x^\infty \frac{dt}{t \log^2 t} = \frac{2C_7}{\log x}, \quad C_7 = 1 + \log 4. \quad \square \end{aligned}$$

6. ELŐADÁS

20. Tétel. (Mertens második tétele) *Létezik olyan C_9 állandó, hogy minden $x \geq 2$ valós szám esetén*

$$\prod_{p \leq x} \left(1 - \frac{1}{p}\right) = \frac{C_9}{\log x} \left(1 + O\left(\frac{1}{\log x}\right)\right).$$

C_9 pontos értéke $C_9 = e^{-C}$, ahol C az Euler-állandó.

Bizonyítás. Írható, hogy

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

(az $\frac{1}{n+1} < \log(1 + \frac{1}{n}) < \frac{1}{n}$ egyenlőtlenségekben legyen $n = p - 1$), lásd 4. Előadás anyagát. Így

$$0 < \sum_{p \leq x} \left(\log\left(1 - \frac{1}{p}\right)^{-1} - \frac{1}{p}\right) < \sum_{p \leq x} \frac{1}{p(p-1)} < \sum_{n=2}^{[x]} \frac{1}{n(n-1)} = 1 - \frac{1}{[x]},$$

tehát a

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

sor konvergens, legyen A az összege, $A = 0,315718\dots$, és

$$\sum_{p > x} \left(\log\left(1 - \frac{1}{p}\right)^{-1} - \frac{1}{p}\right) = A - \sum_{p \leq x} \left(\log\left(1 - \frac{1}{p}\right)^{-1} - \frac{1}{p}\right) = O\left(\frac{1}{x}\right).$$

Kapjuk, hogy

$$-\sum_{p \leq x} \log\left(1 - \frac{1}{p}\right) = \sum_{p \leq x} \frac{1}{p} + A + O\left(\frac{1}{x}\right) = \log \log x + C_8 + A + O\left(\frac{1}{\log x}\right) + O\left(\frac{1}{x}\right),$$

ahonnan

$$\sum_{p \leq x} \log\left(1 - \frac{1}{p}\right) = -\log \log x - C_8 - A + O\left(\frac{1}{\log x}\right),$$

$$\prod_{p \leq x} \left(1 - \frac{1}{p}\right) = \exp(-\log \log x - C_8 - A + O\left(\frac{1}{\log x}\right)) = \frac{1}{\log x} \exp(-C_8 - A) \exp(O\left(\frac{1}{\log x}\right)).$$

Legyen $C_9 = \exp(-C_8 - A)$ és használva, hogy $0 < u < 1$ -re $e^u = 1 + O(u)$ kapjuk, hogy $\exp(O(\frac{1}{\log x})) = 1 + O(\frac{1}{\log x})$, s ezzel kész vagyunk. $\square$

Megjegyzés. Igazolható, hogy $A + C_8 = C$, azaz $C_9 = e^{-C}$, ahol C az Euler állandó, s innen adódik C_8 értékére az előző Tételbeli közelítő érték.

Feladat. Igazoljuk, hogy

$$\prod_{p \leq x} \left(1 - \frac{1}{p}\right)^{-1} = e^C \log x + O(1),$$

$$\prod_{p \leq x} \left(1 + \frac{1}{p}\right) = \frac{6}{\pi^2} e^C \log x (1 + o(1)) = O(\log x),$$

ahol C az Euler-állandó.

Megoldás. Mertens második tétele szerint

$$\begin{aligned} \prod_{p \leq x} \left(1 - \frac{1}{p}\right)^{-1} &= e^C \log x \left(1 + O\left(\frac{1}{\log x}\right)\right)^{-1} = \\ &= e^C \log x \left(1 + \frac{1}{1 + O(1/\log x)} - 1\right) = e^C \log x \left(1 + \frac{O(1/\log x)}{1 + O(1/\log x)}\right) = \\ &= e^C \log x \left(1 + O\left(\frac{1}{\log x}\right)\right) = e^C \log x + O(1). \end{aligned}$$

Ezt használva:

$$\begin{aligned} \prod_{p \leq x} \left(1 + \frac{1}{p}\right) &= \prod_{p \leq x} \left(1 - \frac{1}{p^2}\right) \prod_{p \leq x} \left(1 - \frac{1}{p}\right)^{-1} = \\ &= \frac{6}{\pi^2} (1 + o(1)) e^C \log x (1 + O(1/\log x)) = \frac{6}{\pi^2} e^C \log x (1 + o(1)) = O(\log x). \end{aligned}$$

Megjegyzés. $\prod_{p \leq x} \left(1 + \frac{1}{p}\right) = O(\log x)$ így látható be közvetlenül: $1 + t \leq \exp(t)$, $t > 0$ alapján

$$\begin{aligned} \prod_{p \leq x} \left(1 + \frac{1}{p}\right) &\leq \prod_{p \leq x} \exp\left(\frac{1}{p}\right) = \exp\left(\sum_{p \leq x} \frac{1}{p}\right) = \exp(\log \log x + O(1)) = \\ &= \log x \cdot O(1) = O(\log x) \end{aligned}$$

a 19. Tétel alapján. $\square$

• Van-e képlet a prímszámokra ?

Sokan próbálkoztak olyan képletek megadásával, melyek csak prímszámokat adnak, illetve megadják az n -edik prímszámot. Euler például vizsgálta az $f = X^2 + X + 41$ másodfokú polinomot, amelyre az $f(0), f(1), f(2), \dots, f(39)$ behelyettesítési értékek mind prímszámok, de $f(40) = 40^2 + 40 + 41 = 40 \cdot 41 + 41 = 41^2$ már nem prím.

Nem nehéz igazolni, hogy nem létezik olyan egész együttthatós, legalább elsőfokú polinom, melynek minden $x \in \mathbb{N}$ helyen vett helyettesítési értéke prímszám. Ez következik az alábbi erősebb állításból.

Állítás. Minden egész együttthatós, legalább elsőfokú f polinom esetén létezik végtelen sok $x \in \mathbb{N}$ szám úgy, hogy $f(x)$ összetett.

Bizonyítás. Az algebra alaptételéből következik, hogy minden $m \in \mathbb{Z}$ esetén az $f(x) = m$ egyenletnek véges sok $x \in \mathbb{N}$ megoldása van (esetleg nincs is ilyen megoldás). Így létezik $x_0 \in \mathbb{N}$ úgy, hogy $k = |f(x_0)| \geq 2$. Ha $x \equiv x_0 \pmod{k}$, akkor $f(x) \equiv f(x_0) \equiv 0 \pmod{k}$. Az $x_0 \pmod{k}$ maradékosztálynak van végtelen sok olyan $y \in \mathbb{N}$ eleme, hogy $|f(y)| \neq k$, s minden ilyen y -ra $f(y)$ összetett. $\square$

A polinomok helyett ezért fordult a matematikusok figyelme más képletek felé, pl. $2^n - 1$, lásd Mersenne-számok és $2^{2^n} + 1$, lásd Fermat-számok.

Jelölje p_n az n -edik prímszámot. A következő képlet megadja p_{n+1} -et $p_1, p_2, \dots, p_n$ ismeretében. $b = 2$ esetén ez J. M. Gandhi eredménye (1966), az alábbi egyszerű bizonyítást lásd Ch. Baxa, Über Gandhis Primzahlformel, Elem. Math. **47** (1992), 82-84.

21. Tétel. Ha $b \geq 2$ rögzített valós szám, akkor minden $n \geq 1$ -re

$$p_{n+1} = \left\lceil 1 - \frac{1}{\log b} \log \left(-\frac{1}{b} + \sum_{d|p_1 p_2 \dots p_n} \frac{\mu(d)}{b^d - 1} \right) \right\rceil,$$

ahol $\lceil \cdot \rceil$ az egészrészt jelöli.

Megjegyzés. A képletnek nincs gyakorlati jelentősége, de cáfolja azt a gyakran hangoztatott megállapítást, hogy "nincs képlet az n -edik prímszámmra".

Bizonyítás. A Möbius függvény tulajdonságát használva

$$\sum_{\substack{s=1 \\ (s, p_1 \dots p_n)=1}}^m \frac{1}{b^s} = \sum_{s=1}^m \frac{1}{b^s} \sum_{\substack{d|s \\ d|p_1 \dots p_n}} \mu(d) = \sum_{d|p_1 \dots p_n} \sum_{d|s} \mu(d) \sum_{s=1}^m \frac{1}{b^s},$$

ahol legyen $s = dk$, $k = s/d \leq m/d$ és kapjuk, hogy

$$\sum_{\substack{s=1 \\ (s, p_1 \dots p_n)=1}}^m \frac{1}{b^s} = \sum_{d|p_1 \dots p_n} \mu(d) \sum_{k=1}^{\lfloor m/d \rfloor} \frac{1}{b^{dk}} = \sum_{d|p_1 \dots p_n} \mu(d) \frac{1}{b^d - 1} \left(1 - \frac{1}{b^{d \lfloor m/d \rfloor}} \right).$$

Ha $m \rightarrow \infty$, akkor

$$\sum_{\substack{s=1 \\ (s, p_1 \dots p_n)=1}}^{\infty} \frac{1}{b^s} = \sum_{d|p_1 \dots p_n} \frac{\mu(d)}{b^d - 1}.$$

Minden $1 < s < p_{n+1}$ esetén $(s, p_1 \dots p_n) > 1$, ezért kapjuk, hogy

$$\frac{1}{b} + \frac{1}{b^{p_{n+1}}} + \sum_{\substack{s > p_{n+1} \\ (s, p_1 \dots p_n)=1}} \frac{1}{b^s} = \sum_{d|p_1 \dots p_n} \frac{\mu(d)}{b^d - 1},$$

$$b^{p_{n+1}} \left(-\frac{1}{b} + \sum_{d|p_1 \dots p_n} \frac{\mu(d)}{b^d - 1} \right) = 1 + \sum_{\substack{s > p_{n+1} \\ (s, p_1 \dots p_n)=1}} b^{p_{n+1}-s},$$

ahol a jobboldali összegre

$$0 < \sum_{\substack{s > p_{n+1} \\ (s, p_1 \dots p_n)=1}} b^{p_{n+1}-s} < \sum_{k=1}^{\infty} b^{-k} = \frac{1}{b-1} \leq 1,$$

tehát

$$1 < b^{p_{n+1}} \left(-\frac{1}{b} + \sum_{d|p_1 \dots p_n} \frac{\mu(d)}{b^d - 1} \right) < 2.$$

Logaritmálva:

$$0 < p_{n+1} \log b + \log \left(-\frac{1}{b} + \sum_{d|p_1 \dots p_n} \frac{\mu(d)}{b^d - 1} \right) < \log 2,$$

$$0 < p_{n+1} + \frac{1}{\log b} \log \left(-\frac{1}{b} + \sum_{d|p_1 \dots p_n} \frac{\mu(d)}{b^d - 1} \right) < \frac{\log 2}{\log b} \leq 1,$$

innen

$$p_{n+1} + \left[\frac{1}{\log b} \log \left(-\frac{1}{b} + \sum_{d|p_1 \dots p_n} \frac{\mu(d)}{b^d - 1} \right) \right] = 0,$$

és a bizonyítandó képletet kapjuk ($-[x] = [1-x]$ használatával, ahol x nem egész szám). $\square$

A következő tétel azt mutatja, hogy nem lehet azt mondani, hogy nincs olyan sorozat, amely csupa prímszámot állít elő.

22. Tétel. (Miller) *Létezik olyan x valós szám, hogy az $x_0 = x$, $x_{n+1} = 2^{x_n}$, $n \geq 0$ sorozatra $[x_n]$ prímszám minden $n \geq 1$ esetén.*

Bizonyítás. Defináljuk inductíve a következő sorozatot: $q_1 = 3$ és minden $n \geq 1$ -re legyen q_{n+1} egy olyan prím, hogy $2^{q_n} < q_{n+1} < q_{n+1} + 1 \leq 2^{q_n+1}$. Ilyen létezik a Bertrand-Csebisev tétel szerint.

Ha $q_{n+1} + 1 = 2^{q_n+1}$, akkor $q_{n+1} = 2^{q_n+1} - 1$ nem prím, mert osztható $2^{\frac{q_n+1}{2}} - 1$ -gyel, ellentmondás, tehát

$$(1) \quad 2^{q_n} < q_{n+1} < q_{n+1} + 1 < 2^{q_n+1}, \quad n \geq 0.$$

Legyen $\log_2^{(n)} t = \log \log_2^{(n-1)} t$, $n \geq 1$, $\log_2^{(0)} t = t$ a 2-es alapú iterált logaritmus és legyen

$$u_n = \log_2^{(n)} q_n, \quad v_n = \log_2^{(n)} (q_n + 1).$$

Akkor (1) alapján

$$q_n < \log_2 q_{n+1} < \log_2 (q_{n+1} + 1) < q_n + 1,$$

$$u_n < u_{n+1} < v_{n+1} < v_n, \quad n \geq 0,$$

tehát (u_n) és (v_n) monoton és korlátos sorozatok. Legyen

$$x = \lim_{n \rightarrow \infty} u_n.$$

Akkor $u_n < x < v_n$ minden $n \geq 1$ -re. Innen az $x_0 = x$, $x_{n+1} = 2^{x_n}$, $n \geq 0$ jelöléssel

$$\log_2^{(n)} q_n < x < \log_2^{(n)} (q_n + 1), \quad \log_2^{(n-1)} q_n < 2^x = x_1 < \log_2^{(n-1)} (q_n + 1),$$

$$\log_2^{(n-2)} q_n < 2^{x_1} = x_2 < \log_2^{(n-2)} (q_n + 1), \dots, \quad q_n < 2^{x_{n-1}} = x_n < q_n + 1$$

és $[x_n] = q_n$ prímszám minden n -re. $\square$

7. ELŐADÁS

• A Csebisev függvények

Ha $x \geq 1$ valós szám, legyenek

$$\theta(x) = \sum_{p \leq x} \log p = \log \prod_{p \leq x} p$$

$$\psi(x) = \sum_{p^m \leq x} \log p$$

a Csebisev-féle θ és ψ függvények. A ψ függvény esetén az összegzés a $p^m \leq x$ prímszámok szerint történik.

Már láttuk, hogy $\prod_{p \leq x} p < 4^x, x \geq 2$ (5. Tétel), s így $\theta(x) < (\log 4)x, x \geq 2$.

Ha $1 \leq x < 2$, akkor $\theta(x) = \psi(x) = 0$.

23. Tétel. Minden $x \geq 2$ esetén

$$a) \quad \psi(x) = \sum_{p \leq x} \left[\frac{\log x}{\log p} \right] \log p,$$

$$b) \quad \psi(x) = \log[1, 2, 3, \dots, [x]] \quad \text{az } 1, 2, 3, \dots, [x] \text{ számok lkt-jének logaritmusára,}$$

$$c) \quad \psi(x) = \sum_{m \leq \log x / \log 2} \theta(\sqrt[m]{x}).$$

Bizonyítás. a) Minden rögzített $p \leq x$ -re $p^m \leq x$ akkor és csak akkor, ha $m \leq \log x / \log p$, tehát $\log p$ éppen $\left[\frac{\log x}{\log p} \right]$ -szer jelenik meg.

b) Ez is azonnali az értelmezés szerint.

c) Most először m szerint összegezve:

$$\psi(x) = \sum_{m=1}^{\infty} \left(\sum_{p \leq \sqrt[m]{x}} \log p \right) = \sum_{m=1}^{\infty} \theta(\sqrt[m]{x}) = \sum_{m \leq \log x / \log 2} \theta(\sqrt[m]{x}).$$

A következő egyenlőtlenségek a fentiek alapján igazolhatók:

24. Tétel. Léteznek olyan C_{10}, C_{11} pozitív állandók, hogy minden $x \geq 2$ esetén

$$C_{10}x < \theta(x) < \psi(x) < C_{11}x.$$

Az alábbi tételek a $\theta(x)$ és $\psi(x)$ Csebisev függvények valamint a $\pi(x)$ függvény kapcsolatára mutatnak rá.

25. Tétel. Ha $x \geq 2$, akkor

$$a) \quad \theta(x) = \pi(x) \log x - \int_2^x \frac{\pi(t)}{t} dt,$$

$$b) \quad \pi(x) = \frac{\theta(x)}{\log x} + \int_2^x \frac{\theta(t)}{t \log^2 t} dt.$$

Bizonyítás. Abel-összegzéssel :

a) Legyen

$$f(n) = \begin{cases} 1, & n \text{ prím,} \\ 0, & n \text{ nem prím} \end{cases}$$

és $\psi(x) = \log x$. Ekkor $F(x) = \sum_{n \leq x} f(n) = \pi(x)$, s kapjuk, hogy

$$\theta(x) = \sum_{p \leq x} \log p = \pi(x) \log x - \int_2^x \frac{\pi(t)}{t} dt,$$

mert $\pi(t) = 0$, ha $t < 2$.

b) Most legyen

$$f(n) = \begin{cases} \log n, & n \text{ prím,} \\ 0, & n \text{ nem prím} \end{cases}$$

és $\psi(x) = \frac{1}{\log x}$. Ekkor $F(x) = \sum_{p \leq x} \log p = \theta(x)$, s $\theta(x) = 0$, ha $x < 1$ és kapjuk, hogy

$$\pi(x) = \sum_{p \leq x} 1 = \sum_{n \leq x} f(n) \frac{1}{\log n} = \frac{\theta(x)}{\log x} + \int_2^x \frac{\theta(t)}{t \log^2 t} dt.$$

mert $\pi(t) = 0$, ha $t < 2$. $\square$

26. Tétel.

$$i) \quad \theta(x) = \pi(x) \log x + O\left(\frac{x}{\log x}\right),$$

$$ii) \quad \psi(x) = \pi(x) \log x + O\left(\frac{x}{\log x}\right).$$

Bizonyítás.

i) Következik az előző Tétel a) pontja szerint, ahol

$$\int_2^x \frac{\pi(t)}{t} dt = \int_2^x O\left(\frac{1}{\log t}\right) dt = O\left(\int_2^x \frac{dt}{\log t}\right) = O\left(\frac{x}{\log x}\right),$$

mert

$$\begin{aligned} \int_2^x \frac{dt}{\log t} &= \int_2^{\sqrt{x}} \frac{dt}{\log t} + \int_{\sqrt{x}}^x \frac{dt}{\log t} < \frac{\sqrt{x}}{\log 2} + \frac{x - \sqrt{x}}{\log \sqrt{x}} \\ &< \frac{\sqrt{x}}{\log 2} + \frac{x}{\log \sqrt{x}} = \frac{\sqrt{x}}{\log 2} + \frac{2x}{\log x} = O\left(\frac{x}{\log x}\right). \end{aligned}$$

Ugyanez másképp: $\frac{1}{\log x}$ konvex függvény, ezért a grafikonja alatti terület $[2, x]$ -en kisebb, mint a végpontok által meghatározott trapéz területe, azaz

$$\int_2^x \frac{dt}{\log t} < \left(\frac{1}{\log 2} + \frac{1}{\log x}\right) \cdot \frac{x-2}{2} = O\left(\frac{x}{\log x}\right). \quad \square$$

27. Tétel. A következő állítások egyenértékűek:

$$\begin{aligned} a) \quad & \lim_{x \rightarrow \infty} \frac{\pi(x) \log x}{x} = 1, \\ b) \quad & \lim_{x \rightarrow \infty} \frac{\theta(x)}{x} = 1, \\ c) \quad & \lim_{x \rightarrow \infty} \frac{\psi(x)}{x} = 1. \end{aligned}$$

Bizonyítás. A 26. Tétel szerint

$$\begin{aligned} \frac{\theta(x)}{x} &= \frac{\pi(x) \log x}{x} + O\left(\frac{1}{\log x}\right), & \text{innen } a) \Leftrightarrow b), \\ \frac{\psi(x)}{x} &= \frac{\pi(x) \log x}{x} + O\left(\frac{1}{\log x}\right) & \text{innen } a) \Leftrightarrow c), \end{aligned}$$

Továbbá, $\psi(x) = \theta(x) + O(\sqrt{x})$ alapján $\frac{\psi(x)}{x} = \frac{\theta(x)}{x} + O(\frac{1}{\sqrt{x}})$, ahonnan $b) \Leftrightarrow c)$. $\square$

A 27. Tétel állításai igazak: a) éppen a prímszámtétel. Technikailag egyszerűbb b), illetve c) bizonyítása, és innen következik a prímszámtétel a) alakja.

• **A prímszámtétel élesebb alakjai**

Jelölje $\text{Li}(x)$ az ún **integrállogaritmust**:

$$\text{Li}(x) = \int_2^x \frac{dt}{\log t}.$$

Erre vonatkoznak az alábbiak:

Állítás. Ha $x \geq 2$, akkor

i)

$$\text{Li}(x) = \frac{x}{\log x} + \int_2^x \frac{dt}{\log^2 t} - \frac{2}{\log 2},$$

ii) általánosabban, minden $n \geq 1$ -re

$$\text{Li}(x) = \frac{x}{\log x} \left(1 + \sum_{k=1}^{n-1} \frac{k!}{\log^k x} \right) + n! \int_2^x \frac{dt}{\log^{n+1} t} + C_n,$$

ahol C_n nem függ az x -től,

iii) minden $n \geq 1$ -re

$$\int_2^x \frac{dt}{\log^n t} = O\left(\frac{x}{\log^n x}\right).$$

Bizonyítás. i) Parciálisan integrálva:

$$\text{Li}(x) = \int_2^x \frac{(t)' dt}{\log t} = \left[\frac{t}{\log t} \right]_2^x - \int_2^x t \left(\frac{1}{\log t} \right)' dt = \frac{x}{\log x} - \frac{2}{\log 2} + \int_2^x \frac{dt}{\log^2 t}.$$

ii) Hasonlóan, parciálisan integrálva többször, illetve indukcióval.

iii)

$$\begin{aligned} \int_2^x \frac{dt}{\log^n t} &= \int_2^{\sqrt{x}} \frac{dt}{\log^n t} + \int_{\sqrt{x}}^x \frac{dt}{\log^n t} < \frac{\sqrt{x}}{\log^n 2} + \frac{x - \sqrt{x}}{\log^n \sqrt{x}} < \\ &< \frac{\sqrt{x}}{\log^n 2} + \frac{x}{\log^n \sqrt{x}} = O\left(\frac{x}{\log^n x}\right), \end{aligned}$$

lásd a 26. Tétel bizonyítását. $\square$

Bizonyítás nélkül adjuk meg a következő eredményeket:

28. Tétel. Minden rögzített $n \geq 1$ -re

$$\pi(x) = \text{Li}(x) + O\left(\frac{x}{\log^n x}\right).$$

Például az $n = 1$, $n = 2$ és $n = 4$ értékekre:

$$(1) \quad \pi(x) = \frac{x}{\log x} + O\left(\frac{x}{\log^2 x}\right),$$

$$(2) \quad \pi(x) = \frac{x}{\log x} + \frac{x}{\log^2 x} + O\left(\frac{x}{\log^3 x}\right),$$

$$\pi(x) = \frac{x}{\log x} + \frac{x}{\log^2 x} + \frac{2x}{\log^3 x} + \frac{6x}{\log^4 x} + O\left(\frac{x}{\log^5 x}\right).$$

Ennél erősebb a Hadamard által bizonyított következő becslés:

29. Tétel. Létezik olyan $C > 0$ állandó, amelyre

$$\pi(x) = \text{Li}(x) + O\left(x \exp(-C\sqrt{\log x})\right).$$

Az (1) illetve a (2) becslésből kiindulva megmutatható, hogy az n -edik prímszámra

30. Tétel.

$$p_n = n \log n + n \log \log n + O(n),$$

$$p_n = n \log n + n \log \log n - n + n \frac{\log \log n}{\log n} + O\left(\frac{n}{\log n}\right).$$

Feladat. Adjunk becslést a $\sum_{p \leq x} p$ összegre.

Megoldás. Igazoljuk, hogy

$$\sum_{p \leq x} p = \frac{x^2}{2 \log x} + O\left(\frac{x^2}{\log^2 x}\right),$$

(ez E. Landau eredménye). Használjuk a prímszámtétel következő alakját:

$$(1) \quad \pi(x) = \frac{x}{\log x} + O\left(\frac{x}{\log^2 x}\right),$$

és az Abel-összegzést.

Legyen $f(n) = 1$, ha $n = p$ prím és $f(n) = 0$, ha n nem prím. Akkor $F(x) = \sum_{p \leq x} 1 = \pi(x)$, és legyen $\psi(x) = x$. Kapjuk, hogy

$$\begin{aligned} \sum_{n \leq x} f(n)\psi(n) &= \sum_{p \leq x} p = x\pi(x) - \int_2^x \pi(t)dt = \\ &= \frac{x^2}{\log x} + O\left(\frac{x^2}{\log^2 x}\right) - \int_2^x \left(\frac{t}{\log t} + O\left(\frac{t}{\log^2 t}\right)\right) dt, \end{aligned}$$

parciálisan integrálva

$$\begin{aligned} \sum_{p \leq x} p &= \frac{x^2}{\log x} + O\left(\frac{x^2}{\log^2 x}\right) - \left[\frac{t^2}{2 \log t}\right]_2^x - \frac{1}{2} \int_2^x \frac{t dt}{\log^2 t} + O\left(\int_2^x \frac{t}{\log^2 t} dt\right) = \\ &= \frac{x^2}{2 \log x} + O\left(\frac{x^2}{\log^2 x}\right) + O\left(x \int_2^x \frac{1}{\log^2 t} dt\right) = \frac{x^2}{2 \log x} + O\left(\frac{x^2}{\log^2 x}\right), \end{aligned}$$

használva a fenti Állítást. $\square$

8. ELŐADÁS

• Számelméleti függvények értékeire vonatkozó becslések

A τ , σ és ϕ nevezetes számelméleti függvények (lásd 1. Előadás) értékeit vizsgálva láthatjuk, hogy a felvett értékek nagyon "szabálytalanul" változnak. A τ függvény esetén például $\tau(p) = 2$ minden p prímszámra és τ minden $a \in \mathbb{N}$ értéket felvesz, mégpedig végtelen sokszor, mert $\tau(p^{a-1}) = a$ minden p prímszámra. Ugyanakkor nyilván $2 \leq \tau(n) \leq n$, ennél jobb a következő becslés:

Feladat. Igazoljuk, hogy $2 \leq \tau(n) \leq 2\sqrt{n}$ minden $n \geq 1$ -re.

Kérdés, hogy $\tau(n)$ függvény n -től függően milyen "nagy" értékeket vehet fel?

A σ és ϕ függvényekre $\sigma(n) \geq n+1$, $\phi(n) \leq n-1$ minden $n \geq 2$ -re és az egyenlőségek akkor és csak akkor igazak, ha n prím. Kérdés, hogy $\sigma(n)$ és $\phi(n)$ n -től függően milyen "nagy" illetve milyen "kicsi" értékeket vehet fel?

Állítás. Léteznek olyan C_1 és C_2 pozitív állandók, hogy minden $n \geq 2$ -re

$$a) \sigma(n) < C_1 n \log n,$$

$$b) \phi(n) > C_2 \frac{n}{\log n}.$$

Választható $C_1 = 1 + 1/\log 2 \approx 2,442695$, $C_2 = \log 2/2 \approx 0,346573$.

Bizonyítás. Minden $n \geq 2$ esetén

$$\sigma(n) = \sum_{d|n} d = \sum_{d|n} \frac{n}{d} = n \sum_{d|n} \frac{1}{d} \leq n \sum_{k=1}^n \frac{1}{k} < n(1 + \log n) \leq C_1 n \log n$$

ha $C_1 \geq 1 + 1/\log 2$ minden $n \geq 2$ -re, azaz ha $C_1 \geq 1 + 1/\log 2$ és

$$\frac{\phi(n)}{n} = \prod_{p|n} \left(1 - \frac{1}{p}\right) \geq \prod_{k=1}^r \left(1 - \frac{1}{k+1}\right) = \frac{1}{r+1} \geq \frac{1}{2r} \geq \frac{\log 2}{2 \log n},$$

ahol r az n különböző prímszámok száma, és használjuk, hogy $n \geq 2^r$, $\log n \geq r \log 2$.

Megjegyzés. Az előbbiek alapján:

$$\lim_{n \rightarrow \infty} \frac{\sigma(n)}{n^{1+\varepsilon}} = 0 \quad \text{és} \quad \lim_{n \rightarrow \infty} \frac{\phi(n)}{n^{1-\varepsilon}} = \infty$$

minden $\varepsilon > 0$ esetén. Így az is igaz, hogy $\lim_{n \rightarrow \infty} \phi(n) = \infty$.

Az előbbiek szerint $\sigma(n) = O(n \log n)$, $1/\phi(n) = O(\log n/n)$ és $\sigma(n) = o(n^{1+\varepsilon})$, $1/\phi(n) = o(n^{\varepsilon-1})$ minden $\varepsilon > 0$ esetén.

Nézzük most a τ függvényt. A $\lim_{n \rightarrow \infty} \tau(n)$ nem létezik, ugyanakkor

31. Tétel. Minden $\varepsilon > 0$ esetén

$$\lim_{n \rightarrow \infty} \frac{\tau(n)}{n^\varepsilon} = 0.$$

Bizonyítás. Legyen $\varepsilon > 0$ rögzített. Jelölés: $p^a || n$, ha $p^a | n$ és $p^{a+1} \nmid n$. Minden $n \geq 2$ -re

$$\frac{\tau(n)}{n^\varepsilon} = \prod_{p^a || n} \frac{a+1}{p^{a\varepsilon}} = \prod_{\substack{p^a || n \\ a+1 \leq p^{a\varepsilon}}} \frac{a+1}{p^{a\varepsilon}} \prod_{\substack{p^a || n \\ a+1 > p^{a\varepsilon}}} \frac{a+1}{p^{a\varepsilon}}$$

$$\leq \prod_{\substack{p^a \mid n \\ a+1 > p^{a\varepsilon}}} \frac{a+1}{p^{a\varepsilon}} \leq \prod_{\substack{p^a \mid n \\ p < e^{1/\varepsilon}}} \frac{a+1}{p^{a\varepsilon}},$$

ahol $a+1 > p^{a\varepsilon} \Leftrightarrow a\varepsilon \log p < \log(a+1) < a \Leftrightarrow \log p < 1/\varepsilon$, így az utolsó szorzatnak véges sok tényezője van, s kapjuk, hogy

$$\frac{\tau(n)}{n^\varepsilon} \leq \left(\max_{a \geq 1} \frac{a+1}{2^{a\varepsilon}} \right)^{e^{1/\varepsilon}} = C = \text{állandó}.$$

Ezzel igazoltuk, hogy $\tau(n) = O(n^\varepsilon)$. Ha most $\delta < \varepsilon$, akkor következik, hogy

$$\frac{\tau(n)}{n^\delta} < Cn^{\delta-\varepsilon} \rightarrow 0, \quad n \rightarrow \infty. \quad \square$$

Érvényes a következő általánosabb eredmény. Jelölje H a prímszámok halmazát.

32. Tétel. Ha $f : \mathbb{N} \rightarrow \mathbb{C}$ multiplikatív függvény és

$$\lim_{\substack{n \rightarrow \infty \\ n \in H}} f(n) = 0,$$

akkor

$$\lim_{n \rightarrow \infty} f(n) = 0.$$

Bizonyítás. Legyen $\varepsilon \in \mathbb{R}$ egy tetszőleges szám, melyre $0 < \varepsilon < 1$. Megmutatjuk, hogy létezik $n_0 = n_0(\varepsilon) \in \mathbb{N}$ úgy, hogy minden $n > n_0$ esetén $|f(n)| < \varepsilon$.

Tekintsük a következő halmazokat: $H_1 = \{p^a \in H : |f(p^a)| > 1\}$, mely a feltétel szerint véges, s legyen $A = \prod_{p^a \in H_1} |f(p^a)| \geq 1$; ha H_1 üres halmaz, akkor legyen $A = 1$, $H_2 = \{p^a \in H : \frac{\varepsilon}{A} < |f(p^a)| \leq 1\}$, ez szintén véges halmaz; $H_3 = \{p^a \in H : |f(p^a)| \leq \frac{\varepsilon}{A}\}$. A H_1, H_2, H_3 halmazok páronként diszjunktak és $H = H_1 \cup H_2 \cup H_3$. Legyen $n_0 = \prod_{p^a \in H_1 \cup H_2} p^a \in \mathbb{N}$, ha ez üres szorzat, akkor $n_0 = 1$. Ha $n \in \mathbb{N}, n > n_0$, akkor létezik $p^a \in H_3$ úgy, hogy $p^a \mid n$ és f multiplikativitása alapján

$$|f(n)| = \prod_{p^a \mid n} |f(p^a)| = \prod_{\substack{p^a \mid n \\ p^a \in H_1}} |f(p^a)| \prod_{\substack{p^a \mid n \\ p^a \in H_2}} |f(p^a)| \prod_{\substack{p^a \mid n \\ p^a \in H_3}} |f(p^a)| \leq A \cdot 1 \cdot \frac{\varepsilon}{A} = \varepsilon,$$

mivel a harmadik szorzat nem üres. $\square$

Megjegyzés. A 31. Tétel ennek következménye. Valóban, alkalmazzuk a 32. Tételt az $f(n) = \tau(n)/n^\varepsilon$ multiplikatív függvényre, ahol

$$f(p^a) = \frac{a+1}{p^{a\varepsilon}} \leq \frac{2a}{p^{a\varepsilon}} = 2 \frac{\log p^a}{p^{a\varepsilon} \log p} \leq \frac{2}{\log 2} \cdot \frac{\log p^a}{p^{a\varepsilon}} \rightarrow 0, \quad \text{mikor } p^a \rightarrow \infty,$$

használva, hogy $\lim_{x \rightarrow \infty} \frac{\log x}{x^\varepsilon} = 0$. $\square$

Így tehát $\tau(n) = o(n^\varepsilon)$. Most megmutatjuk, hogy $\tau(n) \neq O((\log n)^\varepsilon)$, pontosabban

33. Tétel. Minden $\varepsilon > 0$ esetén létezik olyan $(n_k)_{k \geq 1}$ sorozat, melyre

$$\lim_{k \rightarrow \infty} \frac{\tau(n_k)}{(\log n_k)^\varepsilon} = \infty.$$

Bizonyítás. Próbálkozzunk az $n_k = 2^k$ sorozattal. Ekkor

$$\frac{\tau(n_k)}{(\log n_k)^\varepsilon} = \frac{k+1}{k^\varepsilon (\log 2)^\varepsilon} \rightarrow \infty, \quad \text{mikor } k \rightarrow \infty$$

ha $\varepsilon < 1$.

Ha $\varepsilon \geq 1$ legyen $m = [\varepsilon]$ és $n_k = (2 \cdot 3 \cdots p_{m+1})^k$, ahol p_{m+1} az $m+1$ -edik prímszám. Így

$$\tau(n_k) = (k+1)^{m+1} > k^{m+1} = \left(\frac{\log(2 \cdot 3 \cdots p_{m+1})^k}{\log(2 \cdot 3 \cdots p_{m+1})} \right)^{m+1} = C(\log n_k)^{m+1},$$

ahol C nem függ a k -tól. Kapjuk, hogy

$$\frac{\tau(n_k)}{(\log n_k)^\varepsilon} > C(\log n_k)^{m+1-\varepsilon} \rightarrow \infty,$$

mert $m+1-\varepsilon > 0$. $\square$

Később pontosabb becsléseket vezetünk le a vizsgált függvényekre nézve.

Feladat. Legyen f egy számelméleti függvény. Mutassuk meg, hogy a következő állítások ekvivalensek:

i) $f(n) = O(n^\varepsilon)$ minden $\varepsilon > 0$ -ra.

ii) $f(n) = o(n^\varepsilon)$ minden $\varepsilon > 0$ -ra.

Feladat. Igazoljuk, hogy minden $n \geq 1$ -re

a) $\sigma(n) + \phi(n) \geq 2n$;

a) $Cn^2 < \sigma(n)\phi(n) \leq n^2$,

alkalmas $C > 0$ állandóval.

Feladat. Igazoljuk, hogy:

a) $\lim_{n \rightarrow \infty} \frac{\sigma(n!)}{n!} = \infty$,

b) $\lim_{n \rightarrow \infty} \frac{\phi(n!)}{n!} = 0$.

Sok esetben a vizsgált $f(n)$ számelméleti függvényre vonatkozó

$$\frac{1}{n} \sum_{k=1}^n f(k)$$

számtani középarányos jól közelíthető elemi függvényekkel. A $\tau(n)$ függvényre például igaz a következő:

34. Tétel. i) Létezik olyan $C > 0$ valós szám, hogy

$$\left| \frac{1}{n} \sum_{k=1}^n \tau(k) - \log n \right| < C$$

minden $n \geq 2$ esetén (választható $C = 1$),
 ii)

$$\lim_{n \rightarrow \infty} \frac{1}{n \log n} \sum_{k=1}^n \tau(k) = 1.$$

Bizonyítás. i)

$$S(n) = \sum_{k=1}^n \tau(k) = \sum_{k=1}^n \sum_{d|k} 1 = \sum_{d=1}^n \sum_{1 \leq j \leq n/d} 1 = \sum_{d=1}^n \left[\frac{n}{d} \right],$$

mert rögzített d esetén $k = jd$, ahol $1 \leq j \leq n/d$.

Elhagyva az egészcsoportot,

$$\frac{1}{n} S(n) \leq \sum_{d=1}^n \frac{1}{d} < 1 + \log n \quad \text{és} \quad \frac{1}{n} S(n) > \frac{1}{n} \sum_{d=1}^n \left(\frac{n}{d} - 1 \right) = \sum_{d=1}^n \frac{1}{d} - 1 > \log n - 1,$$

ahonnan

$$-1 < \frac{1}{n} \sum_{k=1}^n \tau(k) - \log n < 1.$$

ii) Azonnali i) alapján. $\square$

Azt írjuk, hogy $f(x) = g(x) + O(h(x))$, ha $f(x) - g(x) = O(h(x))$.

A 34. Tétel szerint

$$\frac{1}{n} \sum_{k=1}^n \tau(k) = \log n + O(1), \quad \text{azaz} \quad \sum_{k=1}^n \tau(k) = n \log n + O(n).$$

és innen következik, hogy

$$\frac{1}{n} \sum_{k=1}^n \tau(k) \sim \log n.$$

Azt mondjuk, hogy az f függvény **átlagértéke** vagy **középértéke** a g függvény, ha

$$\frac{1}{n} \sum_{k=1}^n f(k) \sim \frac{1}{n} \sum_{k=1}^n g(k),$$

azaz

$$\lim_{n \rightarrow \infty} \frac{\sum_{k=1}^n f(k)}{\sum_{k=1}^n g(k)} = 1.$$

A $\tau(n)$ függvény átlagértéke tehát $\log n$.

Igazolható a következő élesebb becslés:

35. Tétel. (Dirichlet, 1849)

$$\sum_{n \leq x} \tau(n) = x(\log x + 2C - 1) + O(\sqrt{x}),$$

ahol C az Euler-állandó.

Az (u, v) koordináta-rendszer első negyedében tekintsük az $uv = n$ egyenlőoldali hiperbolát. Ezen annyi rácspont van, ahányféleképpen $n = ab$ kétféleképpen szorzatként írható, azaz $\tau(n)$. Így $\sum_{n \leq x} \tau(n)$ egyenlő az $uv = n \leq x$ hiperbolákon lévő rácspontok számával, azaz a tengelyek és az $uv = x$ hiperbola közötti rácspontok számával.

Legyen $R(x) = \sum_{n \leq x} \tau(n) - x \log x - (2C - 1)x$. A fenti $R(x) = O(\sqrt{x})$ eredmény tovább javítható, G. Voronoj 1903-ban igazolta, hogy $R(x) = O(x^{1/3} \log x)$, ugyanakkor G. H. Hardy és E. Landau 1915-ben egymástól függetlenül megmutatták, hogy $R(x) \neq O(x^{1/4})$.

Legyen α az $R(x) = O(x^\alpha)$ feltételnek eleget tevő α kitevők infimuma. Nem ismert α pontos értéke, azaz $R(x)$ pontos nagyságrendje. Ez a Dirichlet-féle osztóprobléma. Általánosan elfogadott az a sejtés, hogy $\alpha = 1/4$. A legjobb felső korlát M. N. Huxley eredménye (1993): $\alpha \leq 23/73 \approx 0.315068$.

36. Tétel.

$$\sum_{n \leq x} \sigma(n) = \frac{\pi^2}{12} x^2 + O(x \log x).$$

Megjegyzés. Ebben a képletben a maradéktag javítható, az eddigi legjobb eredmény $O(x(\log x)^{2/3})$ (A. Walfisz, 1963).

37. Tétel.

$$\sum_{n \leq x} \phi(n) = \frac{3}{\pi^2} x^2 + O(x \log x).$$

Megjegyzés. Az előző képletben a maradéktag javítható, az eddigi legjobb eredmény $O(x(\log x)^{2/3}(\log \log x)^{4/3})$ (A. Walfisz, 1963).

• Függvények extrémális nagyságrendje

Legyen f egy számelméleti függvény, g pedig egy növekvő függvény, melyre $g(n) > 0$, ha $n \geq n_0$. Azt mondjuk, hogy f **maximális** (ill. **minimális**) nagyságrendje g , ha

$$\limsup_{n \rightarrow \infty} \frac{f(n)}{g(n)} = 1 \left(\text{ill. } \liminf_{n \rightarrow \infty} \frac{f(n)}{g(n)} = 1 \right).$$

Itt az első összefüggés például azt jelenti, hogy

i) minden $\varepsilon > 0$ esetén létezik $N(\varepsilon)$ úgy, hogy minden $n \geq N(\varepsilon)$ -ra $f(n) < (1 + \varepsilon)g(n)$ és

ii) minden $\varepsilon > 0$ esetén $f(n) > (1 - \varepsilon)g(n)$ végtelen sok n -re.

Ehhez elegendő belátni, hogy

a) $f(n) \leq g(n)(1 + o(1))$, ha $n \rightarrow \infty$, és

b) $f(n_k) \geq g(n_k)(1 + o(1))$, ha $k \rightarrow \infty$, valamely $(n_k)_{k \geq 1}$ sorozatra.

Világos, hogy a τ függvény minimális nagyságrendje $g(n) = 2$, mert $\tau(n) \geq 2$ minden $n \geq 2$ -re és $\tau(p) = 2$ minden p prímmre. A következő eredmény a τ függvény maximális nagyságrendjére vonatkozik.

38. Tétel. A $\log \tau(n)$ függvény maximális nagyságrendje $\frac{\log 2 \log n}{\log \log n}$, azaz

$$\limsup_{n \rightarrow \infty} \frac{\log \tau(n) \log \log n}{\log n} = \log 2.$$

Bizonyítás. Először igazoljuk a fenti a) egyenlőtlenséget, ahol $f(n) = \log \tau(n)$, $g(n) = \frac{\log 2 \log n}{\log \log n}$.

Az $n = \prod_{i=1}^r p_i^{a_i} \geq 2$ jelöléssel

$$\log \tau(n) = \log \prod_{i=1}^r (a_i + 1) = \sum_{i=1}^r \log(a_i + 1).$$

Vágjuk szét ezt az összeget így:

$$\log \tau(n) = \sum_{p_i < f(n)} \log(a_i + 1) + \sum_{p_i \geq f(n)} \log(a_i + 1) \equiv S_1(n) + S_2(n),$$

ahol az $f(n)$ függvényt később határozzuk meg.

$S_2(n)$ -et így becsüljük:

$$(1) \quad S_2(n) \leq \sum_{p_i \geq f(n)} \log 2^{a_i} = \log 2 \sum_{p_i \geq f(n)} a_i \leq \log 2 \frac{\log n}{\log f(n)},$$

mert

$$\log n = \log \prod_{i=1}^r p_i^{a_i} = \sum_{i=1}^r a_i \log p_i \geq \sum_{p_i \geq f(n)} a_i \log p_i \geq \log f(n) \sum_{p_i \geq f(n)} a_i.$$

$S_1(n)$ becslése: $2^{a_i} \leq p_i^{a_i} \leq n$ miatt $a_i + 1 \leq \frac{\log n}{\log 2} + 1 < 4 \log n$ ($n \geq 2$), s így

$$(2) \quad S_1(n) \leq \sum_{p_i < f(n)} \log(4 \log n) = (\log 4 + \log \log n) \pi(f(n)) \leq (\log 4 + \log \log n) \frac{C_2 f(n)}{\log f(n)}$$

a 9. Tétel szerint. (1) és (2) szerint

$$\begin{aligned} \log \tau(n) &< \frac{1}{\log f(n)} (C_2 f(n) (\log 4 + \log \log n) + (\log 2) \log n) \\ &= \frac{\log 2 \log n}{\log \log n} \left(1 + \frac{C_2 f(n)}{\log 2 \log n} (\log 4 + \log \log n) \right) \left(\frac{\log f(n)}{\log \log n} \right)^{-1}. \end{aligned}$$

Keressünk most olyan $f(n)$ -et, melyre

$$\frac{\log f(n)}{\log \log n} \rightarrow 1, \quad \frac{f(n) \log \log n}{\log n} \rightarrow 0.$$

Ekkor azt kapjuk, hogy

$$(3) \quad \log \tau(n) < \frac{\log 2 \log n}{\log \log n} \cdot \frac{1 + o(1)}{1 + o(1)} = \frac{\log 2 \log n}{\log \log n} (1 + o(1)),$$

amit igazolni akartunk. Vehető

$$f(n) = \frac{\log n}{(\log \log n)^2}.$$

Most igazoljuk a b) egyenlőtlenséget az $n_k = p_1 p_2 \dots p_k$ választással.

$$\log n_k = \theta(p_k) = \sum_{p \leq p_k} \log p \leq \pi(p_k) \log p_k = k \log p_k$$

(elegendő ezt használni). Így

$$(4) \quad \log \tau(n_k) = k \log 2 \geq \frac{\log 2 \log n_k}{\log p_k}.$$

Ugyanakkor a θ függvényre vonatkozó egyenlőtlenség szerint (6. Előadás)

$$\log n_k = \theta(p_k) > A p_k,$$

valamely $A > 0$ állandóval, innen

$$\log \log n_k > \log A + \log p_k,$$

s (4)-be helyettesítve

$$(5) \quad \begin{aligned} \log \tau(n_k) &> \frac{\log 2 \log n_k}{\log \log n_k - \log A} = \frac{\log 2 \log n_k}{\log \log n_k} \cdot \frac{\log \log n_k}{\log \log n_k - \log A} = \\ &= \frac{\log 2 \log n_k}{\log \log n_k} (1 + o(1)), \end{aligned}$$

(a maradéktagra az erősebb $O(1/\log \log n_k)$ is igaz), s kész vagyunk.

(Ugyanez rövidebben: $A p_k < \log n_k < B p_k$ alapján $\log A + \log p_k < \log \log n_k < \log B + \log p_k$, ahonnan $\log \log n_k = \log p_k (1 + o(1))$, $k \rightarrow \infty$) $\square$

Megjegyzés. A bizonyított tétel azt jelenti, hogy ha $n \geq N(\varepsilon)$, akkor

$$\tau(n) < \exp((1 + \varepsilon) \log 2 \log n / \log \log n) = 2^{(1+\varepsilon) \log n / \log \log n} = n^{(1+\varepsilon) \log 2 / \log \log n}$$

és végtelen sok n -re

$$\tau(n) > \exp((1 - \varepsilon) \log 2 \log n / \log \log n) = 2^{(1-\varepsilon) \log n / \log \log n} = n^{(1-\varepsilon) \log 2 / \log \log n}.$$

Tehát "átlagosan"

$$\tau(n) \approx n^{\log 2 / \log \log n}.$$

Nézzük most a $\phi(n)$ és az $\sigma(n)$ függvényeket.

39. Tétel. A $\phi(n)$ függvény maximális nagyságrendje n és minimális nagyságrendje $\frac{e^{-C} n}{\log \log n}$, ahol C az Euler-állandó.

Bizonyítás. A maximális nagyságrend azonnali, mert $\phi(n) \leq n$, $n \geq 1$ és minden p prímre

$$\frac{\phi(p)}{p} = 1 - \frac{1}{p} \rightarrow 1 \quad (p \rightarrow \infty).$$

Igazoljuk, hogy

- a) $\phi(n) \geq \frac{e^{-C}n}{\log \log n}(1 + o(1))$ és
 b) $\phi(n_k) \leq \frac{e^{-C}n_k}{\log \log n_k}(1 + o(1))$ valamely $(n_k)_{k \geq 1}$ sorozatra.
 a) bizonyítása: minden $n \geq 2$ -re

$$\frac{\phi(n)}{n} = \prod_{p|n} \left(1 - \frac{1}{p}\right) = \prod_{\substack{p|n \\ p \leq g(n)}} \left(1 - \frac{1}{p}\right) \prod_{\substack{p|n \\ p > g(n)}} \left(1 - \frac{1}{p}\right) \equiv P_1(n)P_2(n),$$

ahol $g(n)$ -et majd később választjuk meg. Itt

$$P_2(n) = \prod_{\substack{p|n \\ p > g(n)}} \left(1 - \frac{1}{p}\right) > \prod_{\substack{p|n \\ p > g(n)}} \left(1 - \frac{1}{g(n)}\right) = \left(1 - \frac{1}{g(n)}\right)^{\alpha(n)},$$

ahol $\alpha(n) = \#\{p : p|n, p > g(n)\}$ és

$$n \geq \prod_{p|n} p \geq \prod_{\substack{p|n \\ p > g(n)}} p > g(n)^{\alpha(n)},$$

innen $\log n > \alpha(n) \log g(n)$, $\alpha(n) < \frac{\log n}{\log g(n)}$.

Kapjuk, hogy

$$P_2(n) > \left(1 - \frac{1}{g(n)}\right)^{\frac{\log n}{\log g(n)}} = \left(1 - \frac{1}{g(n)}\right)^{-g(n)\left(-\frac{\log n}{g(n) \log g(n)}\right)} \rightarrow e^0 = 1,$$

azaz $P_2(n) > 1 + o(1)$, ha $\frac{\log n}{g(n) \log g(n)} \rightarrow 0$ ($n \rightarrow \infty$). Választható $g(n) = \log n$.

$P_1(n)$ -et Mertens második tétele alkalmazásával becsüljük:

$$P_1(n) = \prod_{\substack{p|n \\ p \leq \log n}} \left(1 - \frac{1}{p}\right) \geq \prod_{p \leq \log n} \left(1 - \frac{1}{p}\right) = \frac{e^{-C}}{\log \log n}(1 + o(1)).$$

Innen

$$\frac{\phi(n)}{n} > \frac{e^{-C}}{\log \log n}(1 + o(1))(1 + o(1)) = \frac{e^{-C}}{\log \log n}(1 + o(1)).$$

b) bizonyítása: olyan $(n_k)_{k \geq 1}$ sorozatot keresünk, melyre

$$\frac{\phi(n_k)}{n_k} = \prod_{p|n_k} \left(1 - \frac{1}{p}\right)$$

kicsi. Legyen $n_k = p_1 p_2 \dots p_k$, ekkor

$$\frac{\phi(n_k)}{n_k} = \prod_{p \leq p_k} \left(1 - \frac{1}{p}\right) = \frac{e^{-C}}{\log p_k}(1 + o(1)),$$

ahol $\log n_k = \theta(p_k) < B p_k$ valamely B állandóval, innen $\log \log n_k < \log B + \log p_k$, $\log p_k > \log \log n_k - \log B$,

$$\frac{1}{\log p_k} < \frac{1}{\log \log n_k - \log B} = \frac{1}{\log \log n_k} \cdot \frac{\log \log n_k}{\log \log n_k - \log B} = \frac{1}{\log \log n_k}(1 + o(1)).$$

Innen

$$\phi(n_k) \leq \frac{e^{-C}n_k}{\log \log n_k}(1 + o(1)). \quad \square$$

40. Tétel. A $\sigma(n)$ függvény minimális nagyságrendje n és maximális nagyságrendje $e^C n \log \log n$, ahol C az Euler-állandó.

Bizonyítás. A minimális nagyságrend azonnali, mert $\sigma(n) \geq n, n \geq 1$ és minden p prímre

$$\frac{\sigma(p)}{p} = 1 + \frac{1}{p} \rightarrow 1 \quad (p \rightarrow \infty).$$

Másrészt a $\sigma(n)\phi(n) \leq n^2, n \geq 1$ egyenlőtlenség (lásd Feladat) és az előző Tétel alapján,

$$\sigma(n) \leq \frac{n^2}{\phi(n)} \leq \frac{n^2}{\frac{e^{-C}n}{\log \log n}(1+o(1))} = e^C n \log \log n(1+o(1)).$$

Azt kell még igazolni, hogy alkalmas $(n_k)_{k \geq 1}$ sorozatra $\sigma(n_k) \geq e^C n_k \log \log n_k(1+o(1)), k \rightarrow \infty$. Legyen

$$n_k = \prod_{p \leq e^k} p^k, \quad k \geq 1.$$

$$\frac{\sigma(n_k)}{n_k} = \prod_{p \leq e^k} \left(1 - \frac{1}{p^{k+1}}\right) \left(1 - \frac{1}{p}\right)^{-1},$$

ahol Mertens második tétele alapján:

$$\prod_{p \leq e^k} \left(1 - \frac{1}{p}\right)^{-1} = e^C \log e^k(1+o(1)) = e^C \cdot k(1+o(1)),$$

$$\begin{aligned} \prod_{p \leq e^k} \left(1 - \frac{1}{p^{k+1}}\right) &= \prod_p \left(1 - \frac{1}{p^{k+1}}\right) \prod_{p > e^k} \left(1 - \frac{1}{p^{k+1}}\right)^{-1} = \\ &= \zeta^{-1}(k+1) \prod_{p > e^k} \left(1 - \frac{1}{p^{k+1}}\right)^{-1}. \end{aligned}$$

Itt ζ a Riemann-féle dzétafüggvény, amelyre $\zeta^{-1}(k+1) = 1+o(1)$, ha $k \rightarrow \infty$ (**Feladat**), és

$$1 < \prod_{p > e^k} \left(1 - \frac{1}{p^{k+1}}\right)^{-1} < \prod_{p > e^k} \left(1 - \frac{1}{p^2}\right)^{-1} = 1+o(1).$$

Továbbá, a Csebisev függvényekre vonatkozó egyenlőtlenségek szerint

$$\log n_k = \sum_{p \leq e^k} k \log p \geq \sum_{p \leq e^k} \log p = \theta(e^k) > Ae^k,$$

$$\log n_k = k \sum_{p \leq e^k} \log p = k\theta(e^k) < Bke^k,$$

(elég csak az egyik irányú egyenlőtlenség) innen

$$\log A + k < \log \log n_k < \log B + \log k + k, \quad \log \log n_k = k(1+o(1)), \quad k \rightarrow \infty.$$

Kapjuk, hogy

$$\frac{\sigma(n_k)}{n_k} = e^C \log \log n_k (1 + o(1)),$$

amit igazolnunk kellett. $\square$

Feladat. Mutassuk meg, hogy minden $n \geq 1$ -re

$$\phi(n) > A \frac{n}{\log \log n}$$

és

$$\sigma(n) < Bn \log \log n,$$

alkalmas A és B állandókkal.

9. ELŐADÁS

• Numerikus adatok a MAPLE segítségével

– lásd a mellékelt MAPLE munkafájlt –

Az első 100 prímszám:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97,
101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191,
193, 197, 199,
211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293,
307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389, 397,
401, 409, 419, 421, 431, 433, 439, 443, 449, 457, 461, 463, 467, 479, 487, 491, 499,
503, 509, 521, 523, 541

A prímek sorozata: $[n, p_n]$, ahol $n = 1, \dots, 100$:

[1, 2], [2, 3], [3, 5], [4, 7], [5, 11], [6, 13], [7, 17], [8, 19], [9, 23], [10, 29], [11, 31], [12, 37],
[13, 41], [14, 43], [15, 47], [16, 53], [17, 59], [18, 61], [19, 67], [20, 71], [21, 73],
[22, 79], [23, 83], [24, 89], [25, 97], [26, 101], [27, 103], [28, 107], [29, 109], [30, 113],
[31, 127], [32, 131], [33, 137], [34, 139], [35, 149], [36, 151], [37, 157], [38, 163],
[39, 167], [40, 173], [41, 179], [42, 181], [43, 191], [44, 193], [45, 197], [46, 199],
[47, 211], [48, 223], [49, 227], [50, 229], [51, 233], [52, 239],
[53, 241], [54, 251], [55, 257], [56, 263], [57, 269], [58, 271], [59, 277],
[60, 281], [61, 283], [62, 293], [63, 307], [64, 311], [65, 313], [66, 317],
[67, 331], [68, 337], [69, 347], [70, 349], [71, 353], [72, 359], [73, 367],
[74, 373], [75, 379], [76, 383], [77, 389], [78, 397], [79, 401], [80, 409],
[81, 419], [82, 421], [83, 431], [84, 433], [85, 439], [86, 443],
[87, 449], [88, 457], [89, 461], [90, 463], [91, 467], [92, 479],
[93, 487], [94, 491], [95, 499], [96, 503], [97, 509], [98, 521], [99, 523], [100, 541]

Az osztók halmaza: $[n, n \text{ osztóinak halmaza}]$, $n = 1, \dots, 20$:

[1, {1}], [2, {1, 2}], [3, {1, 3}], [4, {1, 2, 4}], [5, {1, 5}], [6, {1, 2, 3, 6}], [7, {1, 7}],
[8, {1, 2, 4, 8}], [9, {1, 3, 9}], [10, {1, 2, 5, 10}], [11, {1, 11}], [12, {1, 2, 3, 4, 6, 12}],
[13, {1, 13}], [14, {1, 2, 7, 14}], [15, {1, 3, 5, 15}], [16, {1, 2, 4, 8, 16}], [17, {1, 17}],
[18, {1, 2, 3, 6, 9, 18}], [19, {1, 19}], [20, {1, 2, 4, 5, 10, 20}]

Az $[n, \tau(n)]$ sorozat, $n = 1, \dots, 20$:

[1, 1], [2, 2], [3, 2], [4, 3], [5, 2], [6, 4], [7, 2], [8, 4], [9, 3], [10, 4],
[11, 2], [12, 6], [13, 2], [14, 4], [15, 4], [16, 5], [17, 2], [18, 6], [19, 2], [20, 6]

A $\tau(n)$ értékek sorozata, $n = 1, \dots, 20$:

1, 2, 2, 3, 2, 4, 2, 4, 3, 4, 2, 6, 2, 4, 4, 5, 2, 6, 2, 6

Az $[n, \sigma(n)]$ sorozat, $n = 1, \dots, 20$:

[1, 1], [2, 3], [3, 4], [4, 7], [5, 6], [6, 12], [7, 8], [8, 15], [9, 13], [10, 18],
[11, 12], [12, 28], [13, 14], [14, 24], [15, 24], [16, 31], [17, 18], [18, 39], [19, 20], [20, 42]

A $\sigma(n)$ értékek sorozata, $n = 1, \dots, 20$:

1, 3, 4, 7, 6, 12, 8, 15, 13, 18, 12, 28, 14, 24, 24, 31, 18, 39, 20, 42

Az $[n, \phi(n)]$ sorozat, $n = 1, \dots, 20$:

[1, 1], [2, 1], [3, 2], [4, 2], [5, 4], [6, 2], [7, 6], [8, 4], [9, 6], [10, 4],
[11, 10], [12, 4], [13, 12], [14, 6], [15, 8], [16, 8], [17, 16], [18, 6], [19, 18], [20, 8]

A $\phi(n)$ értékek sorozata, $n = 1, \dots, 20$:

1, 1, 2, 2, 4, 2, 6, 4, 6, 4, 10, 4, 12, 6, 8, 8, 16, 6, 18, 8

Az $[n, \mu(n)]$ sorozat, $n = 1, \dots, 20$:

$[1, 1], [2, -1], [3, -1], [4, 0], [5, -1], [6, 1], [7, -1], [8, 0], [9, 0], [10, 1],$
 $[11, -1], [12, 0], [13, -1], [14, 1], [15, 1], [16, 0], [17, -1], [18, 0], [19, -1], [20, 0]$

A $\mu(n)$ értékek sorozata, $n = 1, \dots, 20$:

$1, -1, -1, 0, -1, 1, -1, 0, 0, 1, -1, 0, -1, 1, 1, 0, -1, 0, -1, 0$

• **A Dirichlet karakterek alaptulajdonságai**

Legyen $m \in \mathbb{N}, m \geq 2$. A $\chi : \mathbb{N} \rightarrow \mathbb{C}$ számelméleti függvény neve **Dirichlet karakter** (mod m), röviden **karakter** (mod m), ha

- i) χ nem azonosan nulla,
- ii) $\chi(ab) = \chi(a)\chi(b)$ minden $a, b \in \mathbb{N}$ esetén, azaz χ teljesen multiplikatív,
- iii) $\chi(a) = \chi(b)$ minden $a \equiv b \pmod{m}$ esetén, azaz χ periodikus (mod m),
- iv) $\chi(a) = 0$ minden $a \in \mathbb{N}, (a, m) > 1$ -re.

Példák. Minden m -re karakter

$$\chi_0(a) = \begin{cases} 1, & (a, m) = 1, \\ 0, & (a, m) > 1, \end{cases}$$

melynek neve **főkarakter** (mod m).

Ha $m = p > 2$ prímszám, akkor

$$\chi(a) = \begin{cases} \left(\frac{a}{p}\right), & (a, p) = 1, \\ 0, & (a, p) > 1, \end{cases}$$

valós karakter, ún. kvadratikus karakter, ahol $\left(\frac{a}{p}\right)$ a Legendre-szimbólumot jelöli.

Ha $m = 5$, akkor például

$$\chi(a) = \begin{cases} 1, & a \equiv 1, \\ i, & a \equiv 2, \\ -i, & a \equiv 3, \pmod{5} \\ -1, & a \equiv 4, \\ 0, & a \equiv 0 \end{cases}$$

is karakter. Itt i), iii), iv) azonnali, ii) pedig ellenőrizhető: például $a \equiv 2, b \equiv 4 \pmod{5}$ esetén $\chi(ab) = \chi(8) = \chi(3) = -i = i(-1) = \chi(a)\chi(b)$.

41. Tétel. a) Minden χ karakterre $\chi(1) = 1$.

b) Minden χ (mod m) karakterre és minden $(a, m) = 1$ -re $\chi(a)^{\phi(m)} = 1$, azaz $\chi(a)$ egy $\phi(m)$ -edik egységgyök.

c) Minden m -re a (mod m) karakterek száma véges.

Bizonyítás. a) χ nem azonosan nulla és teljesen multiplikatív, így $\chi(1) = 1$, lásd elemi számelméleti tétel.

b) Az Euler tétel szerint $(a, m) = 1$ -re $a^{\phi(m)} \equiv 1 \pmod{m}$ és az ii), iii) feltételek alapján $\chi(a)^{\phi(m)} = \chi(a^{\phi(m)}) = \chi(1) = 1$.

c) Egy χ karaktert az $(a, m) = 1$ -re felvett $\chi(a)$ értékek határoznak meg. $\phi(m)$ számú ilyen a van és a b) pont alapján $\chi(a)$ is $\phi(m)$ számú értéket vehet fel. Így a (mod m) karakterek száma $\leq \phi(m)^{\phi(m)}$, tehát véges. $\square$

Megjegyzés. Ez a becslés várhatóan pontatlan a multiplikativitás miatt. Igazolni fogjuk, hogy a (mod m) karakterek száma $\phi(m)$.

42. Tétel. *A $(\text{mod } m)$ karakterek csoportot alkotnak a függvényszorzásra nézve.*

Bizonyítás. Karakterek szorzata is karakter, ez azonnali a definíció szerint. A χ_0 főkarakter az egységelem, továbbá χ inverze a $\chi^{\phi(m)-1}$, amely szintén karakter, ahol

$$\chi(a)\chi^{\phi(m)-1}(a) = \chi(a)^{\phi(m)} = 1 = \chi_0(a),$$

minden $(a, m) = 1$ -re, lásd előző Tétel/b). $\square$

Megjegyzés. Itt $\chi^{\phi(m)-1}(a) = \chi(a)^{-1} = \overline{\chi(a)}$ (komplex konjugált).

43. Tétel. *Ha χ egy $(\text{mod } m)$ karakter, akkor*

$$\sum_{a(\text{mod } m)} \chi(a) \equiv \sum_{a=1}^m \chi(a) = \begin{cases} \phi(m), & \chi = \chi_0 \quad (\text{főkarakter}), \\ 0, & \chi \neq \chi_0. \end{cases}$$

Bizonyítás. Ha $\chi = \chi_0$ a főkarakter, akkor

$$\sum_{a=1}^m \chi_0(a) = \underbrace{1 + 1 + \dots + 1}_{\phi(m) \text{ - szer}} = \phi(m).$$

Ha $\chi \neq \chi_0$, akkor létezik b úgy, hogy $(b, m) = 1$ és $\chi(b) \neq 1$. Használva, hogy ekkor $b, 2b, \dots, mb$ is teljes maradékrendszer, következik, hogy

$$\sum_{a=1}^m \chi(a) = \sum_{a=1}^m \chi(ab) = \chi(b) \sum_{a=1}^m \chi(a),$$

ahonnan $\sum_{a=1}^m \chi(a) = 0$. $\square$

Szükségünk van a következő eredményre, amelyet bizonyítás nélkül adunk meg:

44. Tétel. *a) Ha $m \geq 2$, $(a, m) = 1$ és $a \not\equiv 1 \pmod{m}$, akkor létezik olyan χ karakter $(\text{mod } m)$, melyre $\chi(a) \neq 1$.*

b) Minden $m \geq 3$ esetén a χ_0 főkarakteren kívül van más karakter is.

Ennek segítségével igazolható:

45. Tétel. *Ha $m \geq 2$, akkor a $(\text{mod } m)$ karakterek száma $\phi(m)$ és minden $a \in \mathbb{N}$ -re*

$$\sum_{\chi} \chi(a) = \begin{cases} \phi(m), & a \equiv 1 \pmod{m}, \\ 0, & a \not\equiv 1 \pmod{m}, \end{cases}$$

ahol az összegzés a $(\text{mod } m)$ karakterekre vonatkozik.

Bizonyítás. Legyen K_m a $(\text{mod } m)$ karakterek száma, χ_0 a főkarakter, a többi pedig $\chi_1, \dots, \chi_{K_m-1}$.

Ha $a \equiv 1 \pmod{m}$, akkor

$$\sum_{\chi} \chi(a) = \sum_{j=0}^{K_m-1} \chi_j(a) = \sum_{j=0}^{K_m-1} 1 = K_m.$$

Ha $a \not\equiv 1 \pmod{m}$ és $(a, m) \neq 1$, akkor $\sum_{\chi} \chi(a) = 0$.

Ha pedig $a \not\equiv 1 \pmod{m}$ és $(a, m) = 1$, akkor $m \geq 3$, így a 44. Tétel alapján létezik olyan χ karakter, melyre $\chi(a) \neq 1$. Ekkor $\chi\chi_0, \chi\chi_1, \dots, \chi\chi_{K_m-1}$ is karakterek és páronként különbözőek, tehát megadják a $(\text{mod } m)$ karaktereket, lásd 42. Tétel, így

$$\sum_{j=0}^{K_m-1} \chi_j(a) = \sum_{j=0}^{K_m-1} \chi(a)\chi_j(a) = \chi(a) \sum_{j=0}^{K_m-1} \chi_j(a),$$

ahonnan $\sum_{j=0}^{K_m-1} \chi_j(a) = 0$. Ezzel igazoltuk, hogy

$$\sum_{\chi} \chi(a) = \begin{cases} K_m, & a \equiv 1 \pmod{m}, \\ 0, & a \not\equiv 1 \pmod{m}. \end{cases}$$

Továbbá így

$$K_m = \sum_{a=1}^m \sum_{j=0}^{K_m-1} \chi_j(a) = \sum_{j=0}^{K_m-1} \sum_{a=1}^m \chi_j(a) = \sum_{a=1}^m \chi_0(a) = \phi(m),$$

használva a 43. Tételt. $\square$

46. Tétel. Ha $m \geq 2$ és $(a, m) = (b, m) = 1$, akkor

$$\sum_{\chi} \chi(a)\bar{\chi}(b) = \begin{cases} \phi(m), & a \equiv b \pmod{m}, \\ 0, & a \not\equiv b \pmod{m}, \end{cases}$$

ahol az összegzés a $(\text{mod } m)$ karakterekre vonatkozik.

Bizonyítás. A $(b, m) = 1$ feltétel miatt létezik b' úgy, hogy $bb' \equiv 1 \pmod{m}$. Így, $\bar{\chi}(b) = 1/\chi(b) = \chi(b')$ és használva a 45. Tételt,

$$\sum_{\chi} \chi(a)\bar{\chi}(b) = \sum_{\chi} \chi(a)\chi(b') = \sum_{\chi} \chi(ab') = \begin{cases} \phi(m), & ab' \equiv 1 \pmod{m}, \\ 0, & ab' \not\equiv 1 \pmod{m}, \end{cases}$$

ahol $ab' \equiv 1 \pmod{m} \Leftrightarrow abb' \equiv b \pmod{m} \Leftrightarrow a \equiv b \pmod{m}$. $\square$

Feladat. Adjuk meg a $(\text{mod } m)$ karaktereket, ahol $2 \leq m \leq 8$.

Megoldás. Ha $m = 2$, akkor $\phi(2) = 1$, csak a χ_0 főkarakter van.

Ha $m = 3$, akkor $\phi(3) = 2$ karakter van, ezek értékei a másodrendű egységgyökök: ± 1 .

a	1	2	3
$\chi_0(a)$	1	1	0
$\chi_1(a)$	1	-1	0

Ha $m = 4$, akkor $\phi(4) = 2$ karakter van, az értékek: ± 1 .

a	1	2	3	4
$\chi_0(a)$	1	0	1	0
$\chi_1(a)$	1	0	-1	0

Ha $m = 5$, akkor $\phi(5) = 4$ karakter van, az értékek: $\pm 1, \pm i$. Továbbá: $\chi(2)\chi(3) = \chi(1) = 1 \Rightarrow \chi(3) = 1/\chi(2)$ és $\chi(4) = \chi^2(2)$ és a táblázat kitölthető.

Minden sorban és oszlopban, az elsőket kivéve, a számok összege nulla, lásd tulajdonságok (!)

a	1	2	3	4	5
$\chi_0(a)$	1	1	1	1	0
$\chi_1(a)$	1	-1	-1	1	0
$\chi_2(a)$	1	i	$-i$	-1	0
$\chi_3(a)$	1	$-i$	i	-1	0

Ha $m = 6$, akkor $\phi(6) = 2$ karakter van:

a	1	2	3	4	5	6
$\chi_0(a)$	1	0	0	0	1	0
$\chi_1(a)$	1	0	0	0	-1	0

Ha $m = 7$, akkor a karakterek száma $\phi(7) = 6$, itt az $\omega = \cos \frac{\pi}{3} + i \sin \frac{\pi}{3}$ jelöléssel a 6-odrendű egységgyökök: $1, -1, \omega, -\omega, \omega^2, -\omega^2$.

Továbbá: $\chi^2(6) = \chi(1) = 1, \chi(6) = \pm 1$, és feltételek: $\chi(2)\chi(3) = \chi(6), \chi(2)\chi(4) = \chi(8) = \chi(1) = 1, \chi(2)\chi(6) = \chi(5)$.

Ha $\chi(6) = 1$, akkor $\chi(2) = x, \chi(3) = 1/x, \chi(4) = 1/x, \chi(5) = x$.

Ha $\chi(6) = -1$, akkor $\chi(2) = x, \chi(3) = -1/x, \chi(4) = 1/x, \chi(5) = -x$.

Ugyanakkor: $x^3 = \chi^3(2) = \chi(8) = \chi(1) = 1$, tehát x harmadrendű egységgyök: $x = 1, \omega^2, -\omega$, ahol $1 - \omega + \omega^2 = 0$.

a	1	2	3	4	5	6	7
$\chi_0(a)$	1	1	1	1	1	1	0
$\chi_1(a)$	1	1	-1	1	-1	-1	0
$\chi_2(a)$	1	ω^2	$-\omega$	$-\omega$	ω^2	1	0
$\chi_3(a)$	1	$-\omega$	ω^2	ω^2	$-\omega$	1	0
$\chi_4(a)$	1	ω^2	ω	$-\omega$	$-\omega^2$	-1	0
$\chi_5(a)$	1	$-\omega$	$-\omega^2$	ω^2	ω	-1	0

Ha $m = 8$, akkor $\phi(8) = 4$ karakter van, ezek mind valósak. Valóban, $\chi^2(3) = \chi(9) = \chi(1) = 1 \Rightarrow \chi(3) = \pm 1, \chi^2(5) = \chi(25) = \chi(1) = 1 \Rightarrow \chi(5) = \pm 1, \chi(7) = \pm 1$.

További feltétel: $\chi(3)\chi(5) = \chi(7)$.

Ha $\chi(3) = 1$, akkor $\chi(5) = \chi(7) = 1$ a főkarakter vagy $\chi(5) = \chi(7) = -1$.

Ha $\chi(3) = -1$, akkor $\chi(5) = -\chi(7) = 1$ vagy $\chi(5) = -\chi(7) = -1$.

a	1	2	3	4	5	6	7	8
$\chi_0(a)$	1	0	1	0	1	0	1	0
$\chi_1(a)$	1	0	1	0	-1	0	-1	0
$\chi_2(a)$	1	0	-1	0	1	0	-1	0
$\chi_3(a)$	1	0	-1	0	-1	0	1	0

□

Feladat. Igazoljuk a következő ortogonalitási tulajdonságot: Ha χ és ψ két $(\text{mod } m)$ karakter, akkor

$$\sum_{a=1}^m \chi(a) \overline{\psi}(a) = \begin{cases} \phi(m), & \chi = \psi, \\ 0, & \chi \neq \psi. \end{cases}$$

Megoldás. A 43. Tétel szerint:

$$\sum_{a=1}^m \chi(a) \overline{\psi}(a) = \sum_{a=1}^m (\chi \overline{\psi})(a) = \begin{cases} \phi(m), & \chi \overline{\psi} = \chi_0, \\ 0, & \chi \overline{\psi} \neq \chi_0, \end{cases}$$

ahol $\chi \overline{\psi} = \chi_0 \Leftrightarrow \chi(a) \overline{\psi}(a) = 1, \forall a \in \mathbb{Z} \Leftrightarrow \chi(a) = \psi(a) \Leftrightarrow \chi = \psi$. $\square$

Feladat. Igazoljuk, hogy minden $\chi \pmod{m \geq 2}$ karakterre $\chi(m-1) = \pm 1$.

Megoldás. $\forall m \geq 2$: $(m-1)^2 = m^2 - 2m + 1 \equiv 1 \pmod{m}$, és innen $\chi^2(m-1) = \chi((m-1)^2) = \chi(1) = 1$, tehát $\chi(m-1) = \pm 1$. $\square$

10. ELŐADÁS

Feladat. Lehet-e egy pozitív egészekből álló végtelen számtani sorozat minden tagja prímszám?

Megoldás. Legyen $a, a+r, a+2r, \dots, a+nr, \dots$ egy számtani sorozat, ahol $a > 1$ ($a = 1$ nem prím, kizárt) és $r \geq 0$. Ha $r = 0$, akkor lehet minden tag prím, pl. $2, 2, 2, \dots$. Ha $r \geq 1$, akkor $a+ar = a(1+r)$ összetett ($a \geq 2, 1+r \geq 2$), nem lehet minden tag prím. $\square$

Megjegyzés. Példák véges sok tagú számtani sorozatokra, amelyek tagjai mind prímek. Háromtagú: $3, 7, 11$, $3, 11, 19$, négytagú: $41, 47, 53, 59$, öttagú: $5, 11, 17, 23, 29$, hattagú: $7, 37, 67, 97, 127, 157$, tíztagú: $199 + 210k, 0 \leq k \leq 9$.

Feladat. Mutassuk meg, hogy végtelen sok olyan prímszám van, amely nem tagja egyetlen ikerprímszámpárnak sem.

Megoldás. A Dirichlet-tétel szerint (bizonyítását lásd későbbiekben) végtelen sok $15k+7$ alakú prím létezik, ahol $(15, 7) = 1$. Itt $(15k+7) - 2 = 15k+5$ osztható 5-tel, $(15k+7) + 2 = 15k+9$ osztható 3-mal, tehát nem prím. $\square$

Feladat. Mutassuk meg, hogy minden $k \geq 1$ esetén létezik végtelen sok olyan p prímszám, hogy a $p-k, \dots, p-2, p-1, p+1, p+2, \dots, p+k$ számok mindegyike összetett szám (azaz létezik végtelen sok ún. "izolált" prím).

Megoldás. Legyen q prím, úgy, hogy $q \geq k+2$ és legyen

$$a = 2 \cdot 3 \cdot \dots \cdot (q-2)(q-1)(q+1)(q+2) \dots (2q-2),$$

ahol $(a, q) = 1$. A Dirichlet-tétel alapján létezik végtelen sok $p = a\ell + q$ alakú prím. Itt minden $1 \leq i \leq k$ -ra

$$\begin{aligned} p-i &= (a\ell + q) - i = 2 \cdot 3 \cdot \dots \cdot (q-2)(q-1)(q+1)(q+2) \dots (2q-2)\ell + q - i = \\ &= (q-i)(2 \cdot 3 \cdot \dots \cdot (q-i-1)(q-i+1) \dots (q-2)(q-1)(q+1)(q+2) \dots (2q-2)\ell + 1). \end{aligned}$$

Következik, hogy $(q-i) \mid (p-i)$ és $q-i \geq q-k \geq 2$ és $q-i < (a\ell + q) - i = p-i$, tehát $p-i$ összetett. Hasonlóan, $q+j$ összetett minden $1 \leq j \leq k$ -ra. $\square$

Feladat. Mutassuk meg, hogy ha minden $a, b \geq 1$, $(a, b) = 1$ esetén az $ak+b, k \geq 1$ számtani sorozatban létezik legalább egy prím, akkor végtelen sok létezik.

Megoldás. Az ötlet: tekintsük az $ak+b, a^2k+b, \dots, a^nk+b, \dots$ sorozatokat, ahol $(a^n, b) = 1$, tehát a feltétel szerint mindegyikben van legalább egy prím. Ezek mind $ak+b$ alakúak, de nem biztos, hogy különbözőek.

Páronként különböző prímekeket így lehet megadni: Ha $a = 1$, akkor $1+b, 2+b, 3+b, \dots$ végtelen sok prímet tartalmaz. Legyen $a \geq 2$ és $p_1 = ak_1 + b$ prím. Legyen n_1 olyan nagy, hogy $ak_1 < a^{n_1}$. Akkor bármely $p_2 = a^{n_1}k_2 + b$ prímre $p_1 < p_2$, mert $p_1 = ak_1 + b < a^{n_1} + b \leq a^{n_1}k_2 + b = p_2$. Legyen most n_2 olyan, hogy $ak_2 < a^{n_2}$. Akkor bármely $p_3 = a^{n_2}k_2 + b$ prímre $p_1 < p_2 < p_3$, és ezt folytatjuk. $\square$

A Dirichlet-tétel bizonyítása érdekében szükségünk van arra, hogy minden $\chi \neq \chi_0 \pmod{m}$ karakterre $L(1, \chi) \neq 0$, ahol

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

a χ karakter Dirichlet-sora. Először ezt valós karakterekre bizonyítjuk.

47. Tétel. Ha χ egy $(\text{mod } m)$ valós karakter és $S(n) = \sum_{d|n} \chi(d)$, akkor $S(n) \geq 0$ minden $n \in \mathbb{N}$ -re és $S(n) \geq 1$ minden n négyzetszámra.

Bizonyítás. χ (teljesen) multiplikatív, így az S összegzési függvény is multiplikatív és minden p^a prímszakra

$$S(p^a) = \sum_{k=0}^a \chi(p^k) = 1 + \sum_{k=1}^a \chi(p)^k,$$

ahol $\chi(p) \in \{-1, 0, 1\}$. Így

$$S(p^a) = \begin{cases} 1 + a, & \text{ha } \chi(p) = 1, \\ 1, & \text{ha } \chi(p) = 0, \\ 0, & \text{ha } \chi(p) = -1 \text{ és } a \text{ páratlan,} \\ 1, & \text{ha } \chi(p) = -1 \text{ és } a \text{ páros.} \end{cases}$$

Tehát $S(p^a) \geq 0$, s innen $S(n) \geq 0$ minden $n \in \mathbb{N}$ -re. Továbbá, ha a páros, akkor $S(p^a) \geq 1$ és innen $S(t^2) \geq 1$ minden $t \in \mathbb{N}$ -re. $\square$

Már használtuk a korábbiakban a parciális vagy Abel-összegzést, itt megadjuk ennek a következő alakját:

48. Tétel. (parciális összegzés) Legyen $(a_n)_{n \geq 1}$ és $(b_n)_{n \geq 1}$ két komplex számsorozat és legyenek $0 < y < x$ valós számok.

a) Ha $S(y, x) = \sum_{y \leq n \leq x} a_n$, akkor

$$\sum_{y \leq n \leq x} a_n b_n = S(y, x) b_{[x]} + \sum_{y \leq n \leq x-1} S(y, n) (b_n - b_{n+1});$$

b) Ha még az is teljesül, hogy $(b_n)_{n \geq [y]}$ nemnegatív és csökkenő, akkor

$$\left| \sum_{y \leq n \leq x} a_n b_n \right| \leq b_{[y]} \max_{y \leq n \leq x} |S(y, n)|;$$

c) Ha még $S(y, x)$ korlátos és $\lim_{n \rightarrow \infty} b_n = 0$, akkor a $\sum_{n=1}^{\infty} a_n b_n$ sor konvergens és

$$\sum_{n \leq y} a_n b_n = \sum_{n=1}^{\infty} a_n b_n + O(b_{[y]}), \quad \text{mikor } y \rightarrow \infty.$$

Bizonyítás. a)

$$\sum_{y \leq n \leq x} a_n b_n = \sum_{y \leq n \leq x} (S(y, n) - S(y, n-1)) b_n = \sum_{y \leq n \leq x} S(y, n) b_n - \sum_{y \leq n \leq x} S(y, n-1) b_n,$$

ahol az üres összeg nulla. A második összegben legyen $n := n + 1$, így

$$\sum_{y \leq n \leq x} a_n b_n = \sum_{y \leq n \leq x} S(y, n) b_n - \sum_{y \leq n \leq x-1} S(y, n) b_{n+1} =$$

$$= \sum_{y \leq n \leq x-1} S(y, n)(b_n - b_{n+1}) + S(y, x)b_{[x]}.$$

b) Az a) pont szerint

$$\begin{aligned} \left| \sum_{y \leq n \leq x} a_n b_n \right| &\leq |S(y, x)| b_{[x]} + \sum_{y \leq n \leq x-1} |S(y, n)| (b_n - b_{n+1}) \leq \\ &\leq \max_{y \leq n \leq x} |S(y, n)| \left(b_{[x]} + \sum_{y \leq n \leq x-1} (b_n - b_{n+1}) \right) = \max_{y \leq n \leq x} |S(y, n)| (b_{[x]} + b_y^* - b_{[x]}), \end{aligned}$$

ahol $b_y^* = b_y = b_{[y]}$, ha y egész és $b_y^* = b_{[y]+1} \leq b_{[y]}$, ha y nem egész.

c) A Cauchy-féle konvergenciakritérium szerint következik, hogy a $\sum_{n=1}^{\infty} a_n b_n$ sor konvergens és

$$\sum_{n=1}^{\infty} a_n b_n = \sum_{n \leq y} a_n b_n + \sum_{n > y} a_n b_n = \sum_{n \leq y} a_n b_n + \lim_{x \rightarrow \infty} \sum_{y < n \leq x} a_n b_n,$$

ahol

$$\sum_{y < n \leq x} a_n b_n = \begin{cases} \sum_{y \leq n \leq x} a_n b_n = O(b_{[y]}), & \text{ha } y \text{ nem egész,} \\ \sum_{y \leq n \leq x} a_n b_n - a_y b_y = O(b_y) = O(b_{[y]}), & \text{ha } y \text{ egész,} \end{cases}$$

a b) alapján, ahol a_y korlátos, mert $S(y, x)$ korlátos. $\square$

49. Tétel. Ha $\chi \neq \chi_0$ egy (mod m) karakter és $f(n)$ egy függvény, amely $n \geq a$ esetén nemnegatív és csökkenő, akkor minden $a \leq x < y$ esetén

$$\sum_{x \leq n \leq y} \chi(n) f(n) = O(f(x)).$$

Ha még $\lim_{n \rightarrow \infty} f(n) = 0$, akkor a $\sum_{n=1}^{\infty} \chi(n) f(n)$ sor konvergens és minden $x \geq a$ -ra

$$\sum_{n \leq x} \chi(n) f(n) = \sum_{n=1}^{\infty} \chi(n) f(n) + O(f(x)).$$

Bizonyítás. A 48. Tételben legyen $a_n = \chi(n)$, $b_n = f(n)$. Azt kell belátnunk, hogy $S(x, y) \equiv \sum_{x \leq n \leq y} \chi(n)$ korlátos (x és y szerepe fel van cserélve).

Tekintsük először az $S(1, y) = \sum_{n \leq y} \chi(n)$ összeget, amelyre

$$S(1, m) = \sum_{n=1}^m \chi(n) = 0, \quad S(1, 2m) = 2 \sum_{n=1}^m \chi(n) = 0,$$

lásd 43. Tétel, általában $S(1, km) = 0$ minden $k \in \mathbb{N}$ -re.

Továbbá, tetszőleges y -ra, ha $[y] = qm + r$, $0 \leq r < m$, akkor

$$S(1, y) = \sum_{n=1}^{qm} \chi(n) + \sum_{n=qm+1}^{qm+r} \chi(n) = S(1, qm) + \sum_{n=1}^r \chi(n)$$

és

$$|S(1, y)| \leq \sum_{n=1}^r |\chi(n)| = \sum_{\substack{n=1 \\ (n, m)=1}}^r 1 = \phi(m).$$

Végül,

$$S(x, y) = \sum_{n \leq y} \chi(n) - \sum_{n \leq x} \chi(n) + \chi(x) = S(1, y) - S(1, x) + \chi(x)$$

ahol $\chi(x) = 0$, ha x nem egész. Kapjuk, hogy

$$|S(x, y)| \leq |S(1, y)| + |S(1, x)| + 1 = 2\phi(m) + 1. \quad \square$$

50. Tétel. Ha $\chi \neq \chi_0$ egy $(\text{mod } m)$ karakter, akkor minden $s > 0$ valós számra

$$\sum_{n \leq x} \frac{\chi(n)}{n^s} = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} + O\left(\frac{1}{x^s}\right), \quad x \geq 1,$$

$$\sum_{n \leq x} \frac{\chi(n) \log n}{n^s} = \sum_{n=1}^{\infty} \frac{\chi(n) \log n}{n^s} + O\left(\frac{\log x}{x^s}\right), \quad x \geq e^{1/s}.$$

Bizonyítás. Használjuk a 49. Tételt az $f(n) = \frac{1}{n^s}$ majd az $f(n) = \frac{\log n}{n^s}$ függvényre, ez utóbbi csökkenő, ha $n \geq e^{1/s}$.

51. Tétel. Ha $\chi \neq \chi_0$ egy $(\text{mod } m)$ valós karakter, akkor $L(1, \chi) \neq 0$.

Bizonyítás. Elegendő belátni a következőket. Az

$$S(n) = \sum_{d|n} \chi(d) \quad \text{és} \quad B(x) = \sum_{n \leq x} \frac{S(n)}{\sqrt{n}}$$

jelölésekkel:

$$(a) \quad \lim_{x \rightarrow \infty} B(x) = \infty$$

$$(b) \quad B(x) = 2\sqrt{x} \cdot L(1, \chi) + O(1), \quad x \rightarrow \infty.$$

Valóban, ha $L(1, \chi) = 0$ lenne, akkor b) alapján $B(x) = O(1)$, ami ellentmond a)-nak.

(a) bizonyítása:

$$B(x) \geq \sum_{\substack{n \leq x \\ n=t^2}} \frac{1}{\sqrt{n}} = \sum_{t \leq \sqrt{x}} \frac{1}{t} \rightarrow \infty, \quad \text{ha } x \rightarrow \infty,$$

a harmonikus sor tulajdonsága szerint, használva a 47. Tételt.

(b) bizonyítása: összegzési képleteket használva az

$$f(n) = \frac{\chi(n)}{\sqrt{n}}, \quad g(n) = \frac{1}{\sqrt{n}}, \quad F(x) = \sum_{n \leq x} f(n), \quad G(x) = \sum_{n \leq x} g(n),$$

jelölésekkel kapjuk, hogy

$$B(x) = \sum_{de \leq \sqrt{x}} \frac{\chi(d)}{\sqrt{de}} = \sum_{n \leq \sqrt{x}} \frac{\chi(n)}{\sqrt{n}} G\left(\frac{x}{n}\right) + \sum_{n \leq \sqrt{x}} \frac{1}{\sqrt{n}} F\left(\frac{x}{n}\right) - F(\sqrt{x})G(\sqrt{x}),$$

ahol az 50. Tétel i) pontja szerint

$$F(x) = \sum_{n \leq x} \frac{\chi(n)}{\sqrt{n}} = L\left(\frac{1}{2}, \chi\right) + O\left(\frac{1}{\sqrt{x}}\right),$$

innen

$$G(x) = \sum_{n \leq x} \frac{1}{\sqrt{n}} = 2\sqrt{x} + \zeta\left(\frac{1}{2}\right) + O\left(\frac{1}{\sqrt{x}}\right).$$

Így

$$\begin{aligned} B(x) &= \sum_{n \leq \sqrt{x}} \frac{\chi(n)}{\sqrt{n}} \left(2\sqrt{\frac{x}{n}} + \zeta\left(\frac{1}{2}\right) + O\left(\sqrt{\frac{n}{x}}\right) \right) + \\ &+ \sum_{n \leq \sqrt{x}} \frac{1}{\sqrt{n}} \left(L\left(\frac{1}{2}, \chi\right) + O\left(\sqrt{\frac{n}{x}}\right) \right) - 2L\left(\frac{1}{2}, \chi\right) \sqrt[4]{x} + O(1) = \\ &= 2\sqrt{x} \sum_{n \leq \sqrt{x}} \frac{\chi(n)}{n} + \zeta\left(\frac{1}{2}\right) \sum_{n \leq \sqrt{x}} \frac{\chi(n)}{\sqrt{n}} + O\left(\frac{1}{\sqrt{x}} \sum_{n \leq \sqrt{x}} |\chi(n)|\right) + \\ &+ L\left(\frac{1}{2}, \chi\right) \sum_{n \leq \sqrt{x}} \frac{1}{\sqrt{n}} + O\left(\frac{1}{\sqrt{x}} \sum_{n \leq \sqrt{x}} 1\right) - 2L\left(\frac{1}{2}, \chi\right) \sqrt[4]{x} + O(1) = \\ &= 2\sqrt{x} \left(L(1, \chi) + O\left(\frac{1}{\sqrt{x}}\right) \right) + \zeta\left(\frac{1}{2}\right) \left(L\left(\frac{1}{2}, \chi\right) + O\left(\frac{1}{\sqrt{x}}\right) \right) + O(1) + \\ &+ L\left(\frac{1}{2}, \chi\right) (2\sqrt[4]{x} + O(1)) + O(1) - 2L\left(\frac{1}{2}, \chi\right) \sqrt[4]{x} + O(1) = \\ &= 2\sqrt{x} \cdot L(1, \chi) + O(1). \quad \square \end{aligned}$$

52. Tétel. Ha $\chi \neq \chi_0$ egy tetszőleges (mod m) karakter, akkor

$$L'(1, \chi) \sum_{n \leq x} \frac{\mu(n)\chi(n)}{n} = \begin{cases} O(1), & \text{ha } L(1, \chi) \neq 0, \\ \log x + O(1), & \text{ha } L(1, \chi) = 0, \end{cases}$$

ahol

$$L'(s, \chi) = - \sum_{n=1}^{\infty} \frac{\chi(n) \log n}{n^s}.$$

Bizonyítás. Ha f teljesen multiplikatív és

$$(1) \quad \alpha(x) = \sum_{n \leq x} f(n) \beta\left(\frac{x}{n}\right), \quad \text{akkor} \quad \beta(x) = \sum_{n \leq x} \mu(n) f(n) \alpha\left(\frac{x}{n}\right),$$

ahol μ a Möbius-függvény.

Legyen most $f(n) = \chi(n)$ és $\beta(x) = x$, akkor

$$\alpha(x) = x \sum_{n \leq x} \frac{\chi(n)}{n} = x \left(L(1, \chi) + O\left(\frac{1}{x}\right) \right) = xL(1, \chi) + O(1),$$

használva az 50. Tételt, ahonnan

$$\begin{aligned} x = \beta(x) &= \sum_{n \leq x} \mu(n) \chi(n) \alpha\left(\frac{x}{n}\right) = \sum_{n \leq x} \mu(n) \chi(n) \left(\frac{x}{n} L(1, \chi) + O(1) \right) = \\ &= xL(1, \chi) \sum_{n \leq x} \frac{\mu(n) \chi(n)}{n} + O(x), \end{aligned}$$

és x -szel osztva

$$L(1, \chi) \sum_{n \leq x} \frac{\mu(n) \chi(n)}{n} = O(1).$$

Ha most $L(1, \chi) \neq 0$, akkor készen vagyunk, hiszen $L'(1, \chi)$ konvergens.

Ha $L(1, \chi) = 0$, akkor használjuk ismét a fenti (1) összefüggést az $f(n) = \chi(n)$ és $\beta(x) = x \log x$ választással. Most

$$\begin{aligned} \alpha(x) &= \sum_{n \leq x} \chi(n) \frac{x}{n} \log \frac{x}{n} = x \log x \sum_{n \leq x} \frac{\chi(n)}{n} - x \sum_{n \leq x} \frac{\chi(n) \log n}{n} = \\ &= x \log x \left(L(1, \chi) + O\left(\frac{1}{x}\right) \right) - x \left(-L'(1, \chi) + O\left(\frac{\log x}{x}\right) \right) \\ &= L'(1, \chi)x + O(\log x), \end{aligned}$$

használva, hogy $L(1, \chi) = 0$. Így

$$\begin{aligned} x \log x = \beta(x) &= \sum_{n \leq x} \mu(n) \chi(n) \left(L'(1, \chi) \frac{x}{n} + O\left(\log \frac{x}{n}\right) \right) = \\ &= L'(1, \chi)x \sum_{n \leq x} \frac{\mu(n) \chi(n)}{n} + O\left(\sum_{n \leq x} \log \frac{x}{n} \right), \end{aligned}$$

ahol az O tag $O(x)$. $\square$

A prímszámelméletben fontos szerepe van annak a függvénynek, melynek összegzési függvénye a log függvény. Ez a **von Mangoldt függvény**, amely így adott: $\Lambda(1) = 0$ és

$$\Lambda(n) = \begin{cases} \log p, & \text{ha } n = p^a \text{ prímszaktvány,} \\ 0, & \text{ha } n \text{ nem prímszaktvány.} \end{cases}$$

Állítás. Minden $n \geq 1$ -re

a)

$$\sum_{d|n} \Lambda(d) = \log n,$$

b)

$$\Lambda(n) = \sum_{d|n} \mu(d) \log n/d = - \sum_{d|n} \mu(d) \log d.$$

Bizonyítás. a) Ha $n = p_1^{a_1} \dots p_r^{a_r}$ alakú, akkor figyelembevéve, hogy Λ csak a prím hatványokon vesz fel nullától különböző értékeket:

$$\begin{aligned} \sum_{d|n} \Lambda(d) &= \sum_{b_1=1}^{a_1} \Lambda(p_1^{b_1}) + \dots + \sum_{b_r=1}^{a_r} \Lambda(p_r^{b_r}) \\ &= a_1 \log p_1 + \dots + a_r \log p_r = \log(p_1^{a_1} \dots p_r^{a_r}) = \log n. \end{aligned}$$

b) A Möbius-féle megfordítási képlet szerint,

$$\begin{aligned} \Lambda(n) &= \sum_{d|n} \mu(d) \log \frac{n}{d} = \log n \sum_{d|n} \mu(d) - \sum_{d|n} \mu(d) \log d \\ &= (\log n) \delta(n) - \sum_{d|n} \mu(d) \log d = - \sum_{d|n} \mu(d) \log d \end{aligned}$$

minden $n \geq 1$ -re. $\square$

53. Tétel. Ha $\chi \neq \chi_0$ egy tetszőleges (mod m) karakter, akkor

$$\sum_{p \leq x} \frac{\chi(p) \log p}{p} = \begin{cases} O(1), & \text{ha } L(1, \chi) \neq 0, \\ -\log x + O(1), & \text{ha } L(1, \chi) = 0. \end{cases}$$

Bizonyítás. Fejezzük ki kétféleképpen a $\sum_{n \leq x} \frac{\chi(n) \Lambda(n)}{n}$ összeget, ahol $\Lambda(n)$ a von Mangoldt függvény. Egyrészt

$$\sum_{n \leq x} \frac{\chi(n) \Lambda(n)}{n} = \sum_{p^a \leq x} \frac{\chi(p^a) \log p}{p^a} = \sum_{p \leq x} \frac{\chi(p) \log p}{p} + \sum_{\substack{p^a \leq x \\ a \geq 2}} \frac{\chi(p^a) \log p}{p^a},$$

ahol a második összeg így majorálható:

$$\begin{aligned} \left| \sum_{\substack{p^a \leq x \\ a \geq 2}} \frac{\chi(p^a) \log p}{p^a} \right| &\leq \sum_{\substack{p^a \leq x \\ a \geq 2}} \frac{\log p}{p^a} < \sum_{p \leq \sqrt{x}} \log p \sum_{a=2}^{\infty} \frac{1}{p^a} = \\ &= \sum_{p \leq \sqrt{x}} \frac{\log p}{p(p-1)} < \sum_{n=2}^{\infty} \frac{\log n}{n(n-1)} = O(1), \end{aligned}$$

s így

$$(2) \quad \sum_{p \leq x} \frac{\chi(p) \log p}{p} = \sum_{n \leq x} \frac{\chi(n) \Lambda(n)}{n} + O(1).$$

Másrészt,

$$\begin{aligned} \sum_{n \leq x} \frac{\chi(n) \Lambda(n)}{n} &= \sum_{n \leq x} \frac{\chi(n)}{n} \sum_{d|n} \mu(d) \log \frac{n}{d} = \sum_{d \leq x} \frac{\mu(d) \chi(d)}{d} \sum_{e \leq x/d} \frac{\chi(e) \log e}{e} = \\ &= \sum_{d \leq x} \frac{\mu(d) \chi(d)}{d} \left(-L'(1, \chi) + O\left(\frac{d}{x} \log \frac{x}{d}\right) \right) = \\ &= -L'(1, \chi) \sum_{n \leq x} \frac{\mu(n) \chi(n)}{n} + O\left(\frac{1}{x} \sum_{d \leq x} \log \frac{x}{d}\right) = \\ &= -L'(1, \chi) \sum_{n \leq x} \frac{\mu(n) \chi(n)}{n} + O(1), \end{aligned}$$

lásd 50. Tétel. Ezt (2)-be helyettesítve és használva az 52. Tételt a bizonyítás kész. $\square$

54. Tétel. Ha f egy tetszőleges számelméleti függvény, $m \geq 2$ és $(a, m) = 1$, akkor

$$(3) \quad \sum_{\substack{n \leq x \\ n \equiv a \pmod{m}}} f(n) = \frac{1}{\phi(m)} \left(\sum_{n \leq x} f(n) + \sum_{\chi \neq \chi_0} \bar{\chi}(a) \sum_{n \leq x} \chi(n) f(n) \right),$$

$$(4) \quad \sum_{\substack{p \leq x \\ p \equiv a \pmod{m}}} \frac{\log p}{p} = \frac{1}{\phi(m)} \left(\log x + \sum_{\chi \neq \chi_0} \bar{\chi}(a) \sum_{p \leq x} \frac{\chi(p) \log p}{p} \right) + O(1).$$

Bizonyítás. Használjuk a 46. Tétel ortogonalitási összefüggését:

$$\sum_{\substack{n \leq x \\ n \equiv a \pmod{m}}} f(n) = \sum_{n \leq x} f(n) \frac{1}{\phi(m)} \sum_{\chi} \chi(n) \bar{\chi}(a) = \frac{1}{\phi(m)} \sum_{\chi} \bar{\chi}(a) \sum_{n \leq x} \chi(n) f(n),$$

ahol az összegzés a $(\text{mod } m)$ karakterekre vonatkozik. Különválasztva a χ_0 főkaraktert, következik (3).

(3)-ban legyen

$$f(n) = \begin{cases} \frac{\log p}{p}, & \text{ha } n = p \text{ prím,} \\ 0, & \text{másképp,} \end{cases}$$

és használjuk, hogy

$$\sum_{p \leq x} \frac{\log p}{p} = \log x + O(1),$$

lásd 18. Tétel. $\square$

55. Tétel. Ha $\chi \neq \chi_0$ egy tetszőleges $(\text{mod } m)$ karakter, akkor $L(1, \chi) \neq 0$.

Bizonyítás. Legyen $N(m) = \#\{\chi : \chi \neq \chi_0 \text{ és } L(1, \chi) = 0\}$. Alkalmazzuk az előző Tétel (4) képletét $a = 1$ esetén, melyre $\chi(1) = 1$ minden χ karakterre. Kapjuk, hogy

$$\sum_{\substack{p \leq x \\ p \equiv 1 \pmod{m}}} \frac{\log p}{p} = \frac{1}{\phi(m)} \left(\log x + \sum_{\chi \neq \chi_0} \sum_{p \leq x} \frac{\chi(p) \log p}{p} \right) + O(1) =$$

$$(5) \quad = \frac{1}{\phi(m)} (\log x - N(m) \log x) + O(1) = \frac{1 - N(m)}{\phi(m)} \log x + O(1),$$

használva az 53. Tételt. Itt a kiindulási összeg nemnegatív, ezért $1 - N(m) \geq 0$, $N(m) \leq 1$ kell legyen.

Ugyanakkor, ha $L(1, \chi) = 0$, akkor χ nem valós karakter, lásd 51. Tétel, így $\chi \neq \bar{\chi}$ és $L(1, \bar{\chi}) = 0$, tehát $N(m)$ páros szám.

A fentiek szerint $N(m) = 0$, amit bizonyítani akartunk. $\square$

56. Tétel. (Dirichlet) Ha $(a, m) = 1$, akkor

i) Végtelen sok $p \equiv a \pmod{m}$ prímszám létezik. (Másképp: az $a + km, k \in \mathbb{N}_0$ számtani sorozat tagjai között végtelen sok prímszám van.)

ii)

$$\sum_{\substack{p \leq x \\ p \equiv a \pmod{m}}} \frac{\log p}{p} = \frac{1}{\phi(m)} \log x + O(1).$$

iii)

$$\sum_{\substack{p \leq x \\ p \equiv a \pmod{m}}} \frac{1}{p} = \frac{1}{\phi(m)} \log \log x + C_{a,m} + O\left(\frac{1}{\log x}\right),$$

ahol $C_{a,m}$ állandó, mely függ a -tól és m -től.

Bizonyítás. ii) azonnal következik az (5) összefüggésből, ahol $N(m) = 0$.

i) következik ii)-ből.

iii) Legyen

$$F(x) = \sum_{\substack{p \leq x \\ p \equiv a \pmod{m}}} \frac{\log p}{p} = \frac{\log x}{\phi(m)} + R(x),$$

ahol $R(x) = O(1)$ és használjuk az Abel-összegzés módszerét, lásd a 19. Tétel bizonyítását. $\square$

Ha pl. $m = 4$, akkor $a = 1$ vagy $a = 3$ lehet, $\phi(4) = 2$ és kapjuk, hogy

$$\sum_{\substack{p \leq x \\ p \equiv 1 \pmod{4}}} \frac{1}{p} = \frac{1}{2} \log \log x + C_{1,4} + O\left(\frac{1}{\log x}\right),$$

$$\sum_{\substack{p \leq x \\ p \equiv 3 \pmod{4}}} \frac{1}{p} = \frac{1}{2} \log \log x + C_{3,4} + O\left(\frac{1}{\log x}\right),$$

ahol $C_{1,4}, C_{3,4}$ állandók.