

A prímszámok eloszlása, avagy az első 50 millió prímszám.

Klukovits Lajos

TTIK Bolyai Intézet

2014. április 8.

Prímszámok

Néhány definíció.

- 1 A „klasszikus számelméleti”. $p \in \mathbb{N}$ prím, ha $a|p \Rightarrow a = \pm 1, \pm p$.
- 2 Az „analitikus”. Az

$$1 - \frac{\sin \pi \Gamma(s)}{\sin \frac{\pi}{s}}$$

analitikus függvény egész zéróhelyei, ahol

$$\Gamma(s) = \int_0^{\infty} x^{s-1} e^{-x} dx, \quad x > 0.$$

- 3 Az „algebrai”. A véges testek karakterisztikái.

Két tulajdonságuk, amelyet mindenki elfogad.

Az első.

- Igen egyszerűen (is) definiálhatók, az egész számok „építőkövei”, de a leghaszabálytalanabban viselkedő matematikai objektumok egyike.
- Úgy fordulnak elő a természetes számok között, mint „pipacsok a búzamezőben”.
- Olyannak mutatkoznak, mint amelyekre egyetlen törvényszerűség sem vonatkozik. Nincs használható becslés arra, hogy egy prímszám után mikor jön a következő.

A második.

Mindezek ellenére van néhány olyan törvényszerűség, amelynek szinte katonás rendben tesznek eleget.

Két tulajdonságuk, amelyet mindenki elfogad.

Az első megállapítás melletti érvek.

- A prímek száma néhány 100 hosszúságú intervallumban:

intervallum	prímek száma
2 – 100	25
9.999.900 – 10.000.000	9
10.000.000 – 10.000.100	2

- Tudjuk, hogy az $[n, 2n]$ intervallumban van prím, de ez nagy n -re igen hosszú.
- Egy valamivel jobb becslés, miszerint az $[n, n + \sqrt{n}]$ intervallumban is van prím, csak sejtés.

Ikerprímek.

- **Definíció.** Ha valamely p rímre $p + 2$ is prím, akkor a $(p, p + 2)$ párt **ikerprímeknek** nevezzük.
- Például, $(3, 5)$, $(11, 13)$, $(41, 43), \dots$
- Természetes az a kérdés, hogy van-e végtelen sok ilyen pár.
- A válasz nem ismert, azt sejtik, hogy végtelen sokan vannak.
- A ma ismert 5 legnagyobb pár:

sorszám	a prímpár	jegyek	évszám
1.	$3.756.801.695.685 \cdot 2^{666.669} \pm 1$	200.700	2011
2.	$65.514.648.355 \cdot 2^{333.333} \pm 1$	100.355	2009
3.	$2.003.663.613 \cdot 2^{195.000} \pm 1$	58.711	2007
4.	$194.772.106.074.315 \cdot 2^{171.960} \pm 1$	51.780	2007
5.	$100.314.512.544.015 \cdot 2^{171.960} \pm 1$	51.780	2006

Sophie Germain prímek.

- **Definíció.** A p páratlan prím **Sophie Germain prím**, ha $2p - 1$ szintén prím.
- A Fermat sejtés vizsgálatakor merültek föl: A sejtés igaz $n > 2$ -re, ha n osztható valamely Sophie Germain prímmel.
- Számuk a mai napig ismeretlen.
- A ma ismert 5 legnagyobb Sophie Germain prím:

sorszám	Sophie Germain prím	jegyek	évszám
1.	$183.027 \cdot 2^{265.440} - 1$	79.911	2010
2.	$658.621.027.630.345 \cdot 2^{253.824} - 1$	76.424	2009
3.	$620.366.307.356.565 \cdot 2^{253.824} - 1$	76.424	2009
4.	$607.095 \cdot 2^{176.311} - 1$	53.081	2007
5.	$48.047.305.725 \cdot 2^{172.403} - 1$	51.910	2007

Rekord prímek.

-
- | | a prím | jegyek | évszám | megj. |
|-----|-----------------------------------|------------|--------|--------------|
| 1. | $2^{57.885.161} - 1$ | 17.425.170 | 2013 | 48. Mersenne |
| 2. | $2^{43.112.609} - 1$ | 12.978.189 | 2008 | 47. Mersenne |
| 3. | $2^{42.643.801} - 1$ | 12.837.064 | 2009 | 46. Mersenne |
| 4. | $2^{37.156.667} - 1$ | 11.185.272 | 2008 | 45. Mersenne |
| 5. | $2^{32.582.657} - 1$ | 9.808.358 | 2006 | 44. Mersenne |
| 6. | $2^{30.402.457} - 1$ | 9.152.052 | 2005 | 43. Mersenne |
| 7. | $2^{25.964.591} - 1$ | 7.816.230 | 2005 | 42. Mersenne |
| 8. | $2^{24.036.583} - 1$ | 7.235.733 | 2004 | 41. Mersenne |
| 9. | $2^{20.996.011} - 1$ | 6.320.430 | 2003 | 40. Mersenne |
| 10. | $2^{13.466.917} - 1$ | 4.053.946 | 2001 | 39. Mersenne |
| 11. | $19.249 \cdot 2^{13.018.586} + 1$ | 3.918.990 | 2007 | |
- Érdekes, hogy a legnagyobb ismert nem-Mersenne prím csak a 10. a listán.

Még egy tulajdonság, ami nem a szabályos eloszlást mutatja.

Hézagok.

- Egyszerűen igazolható, hogy a prímek sorozatában akármekkora hézag is lehet.
- Ugyanis, tetszőleges $n \in \mathbb{N}$ esetén, a A jelöli az n -nél nem nagyobb prímszámok szorzatát, akkor az

$$A + 2, A + 3, A + 4, \dots, A + (n + 1)$$

egészek mindegyike összetett.

- De említettük, hogy léteznek ún. ikerprímek, amelyek száma nem ismert,
- és az ezektől különböző „hézagok” hossza sem nő monoton.

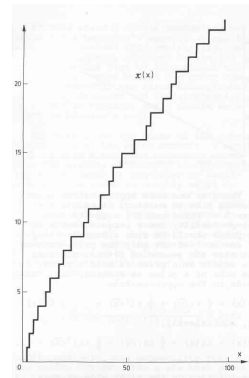
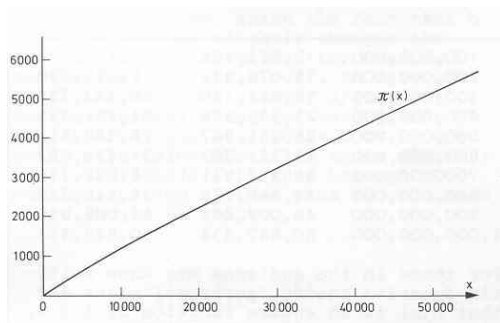
A „szabályszerű” viselkedés.

Egy alapvető fontosságú függvény.

Definíció. $\pi: \mathbb{R}^+ \rightarrow \mathbb{N}_0$, $\pi(x) = k$ pontosan akkor, ha az x -nél nem nagyobb prímek száma k .

Cél

Ezen $\pi(x)$ függvény viselkedését és közelítéseit fogjuk vizsgálni. Tekintsük először a grafikonját először a $[0, 100]$, majd a $[0, 50.000]$ intervallumon.

 $\pi(x)$  $\pi(x)$  $\pi(x)$

- Az utóbbi görbe alakja arra bátorít, hogy valamilyen formulát, legalább valamiféle empirikusat keressünk e függvény közelítésére.
- A XIX. század fordulója körül a 15 éves Gauss a $\pi(x)$ függvényt vizsgálva következő táblázatot alkotta meg.

Gauss.

x	$\pi(x)$	$x/\pi(x)$
10	4	2.5
100	25	4.0
1000	168	6.0
10,000	1,229	8.1
100,000	9,592	10.4
1,000,000	78,498	12.7
10,000,000	664,579	15.0
100,000,000	5,761,455	17.4
1,000,000,000	50,847,534	19.7
10,000,000,000	455,052,512	22.0

Prímszámok

x	$\pi(x)$	$x/\pi(x)$
10	4	2.5
100	25	4.0
1000	168	6.0
10,000	1,229	8.1
100,000	9,592	10.4
1,000,000	78,498	12.7
10,000,000	664,579	15.0
100,000,000	5,761,455	17.4
1,000,000,000	50,847,534	19.7
10,000,000,000	455,052,512	22.0

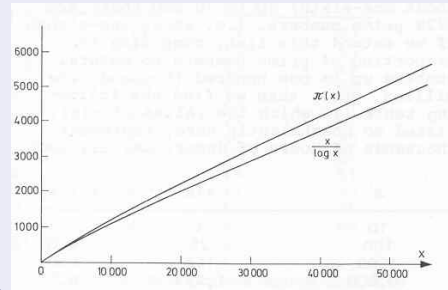
Gauss észrevétele:

a jobb oldali oszlopban a számok különbsége közelítőleg $2,3 \approx \log 10$, 10 hatványainként az $x/\pi(x)$ hányados ennyivel nő, így sejtése szerint $\pi(x)$ aszimptotikusan egyenlő $x/\log x$ -szel, azaz

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

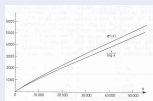
A $\pi(x)$ első közelítése.

- Bizonyítás hiányában csak empirikus érveket adott, meghatározta az összes prímszámot $3 \cdot 10^6$ -ig, és összehasonlította a két függvényt.



- Első látásra meglepő lehet a két görbe „távolodása”.

Gauss sejtése.



Utóbbi észrevételünk azt szuggerálhatná, hogy talán nem is igaz a sejtés, hiszen a két függvény eltérése szemmel láthatóan nő. Ez azonban csak látszólag van így: attól, hogy a két függvény eltérése minden határon túl nő, hányadosuk még tarthat 1-hez.

- Gauss sejtését csak 1896-ban igazolta egymástól függetlenül Hadamard és de la Vallée Poussin. Azóta a „Nagy Prímszámteétel” néven szokás említeni.
- Az előbbi észrevétel azért fölveti, hogy nincs-e jobb empirikus formula $\pi(x)$ -re, mint $x/\log x$.

További becslések.

x	$\pi(x)$	$x/\pi(x)$
10	4	2.5
100	25	4.0
1000	168	6.0
10,000	1,229	8.1
100,000	9,592	10.4
1,000,000	78,498	12.7
10,000,000	664,579	15.0
100,000,000	5,761,455	17.4
1,000,000,000	50,847,534	19.7
10,000,000,000	455,052,512	22.0

Finomítás.

A táblázatot tovább elemezve észrevehetjük, hogy

$$\frac{x}{\pi(x)} \approx \log x - 1$$

amiből

$$\pi(x) \approx \frac{x}{\log x - 1}$$

így vélelmezhető, hogy sűrűbb beosztást véve még jobb közelítés kapható.

További becslések.

Újabb finomítás: Legendre

1808-ban Legendre egy jobb empirikus formulát tett közzé

$$\pi(x) \approx \frac{x}{\log x - 1,08366}.$$

Gauss.

- Tovább elemezve az empirikus adatokat Gauss úgy találta, hogy egy elég nagy $y \in \mathbb{R}$ szám közelében a prímek előfordulásának relatív gyakorisága jó közelítéssel $1/\log y$,
- amiből következően egy nagy $x \in \mathbb{R}$ számnál nem nagyobb prímek számát jól közelíti az alábbi ún. **logaritmikus összeg**:

$$Ls(x) = \frac{1}{\log 2} + \frac{1}{\log 3} + \dots + \frac{1}{\log[x]}.$$

Gauss.

- Vélhetően még jobb közelítést ad, legalábbis analitikusan jobban használható, az ún. „logaritmikus integrál”:

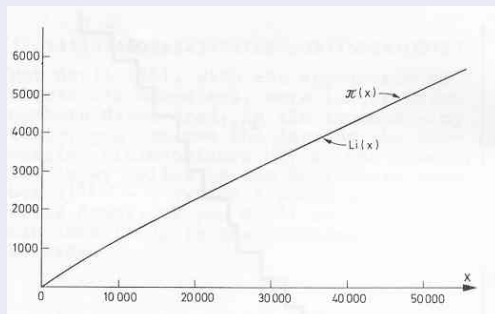
$$Li(x) = \int_2^x \frac{dt}{\log t}.$$

- Alapos számolással ez jogosítható, a két függvény eltérése korlátos.

$$Ls(n) - 1,5 < Li(n) < Ls(n),$$

Gauss.

A két görbe.



- A két függvény grafikonja láthatóan (a rajz pontosságán belül) gyakorlatilag megegyezik a $[0, 50.000]$ intervallumon.

XIX. század.

- A század közepén Riemann — részben elméleti megfontolásokkal — tovább javította a becsléseket.
- Azt sejtette: annak a valószínűsége, hogy egy nagy $n \in \mathbb{N}$ szám prím legyen még közelebb lehet $1/\log n$ -hez, ha nemcsak a prímeket vesszük figyelembe, hanem a prímtványokat is.
- Pontosabban, a prímnégzeteket fél prímnek, valamely prímszám köbét egyharmad prímnek, és így tovább, tekinthetjük. Ez a logaritmikus integrál alábbi közelítéséhez vezet

$$\pi(n) + \frac{1}{2}\pi(\sqrt{n}) + \frac{1}{3}\sqrt[3]{n} + \dots \approx Li(n),$$

- amiből $\pi(n)$, vagy $\pi(x)$ megkapható.

Riemann függvénye.

$$\pi(x) \approx \underbrace{\text{Li}(x) + a_2 \text{Li}(\sqrt{x}) + a_3 \text{Li}(\sqrt[3]{x}) + \dots + a_k \pi(\sqrt[k]{x}) + \dots}_{R(x)}$$

• ahol

$$a_k = \begin{cases} \frac{1}{k}, & \text{ha } k \text{ páros sok különböző prím szorzata,} \\ -\frac{1}{k}, & \text{ha } k \text{ páratlan sok különböző prím szorzata,} \\ 0, & \text{különben.} \end{cases}$$

Ezen $R(x)$, az ún. **Riemann-féle közelítő függvény**, az eddigieknél jobb közelítést ad, például

Riemann függvénye.

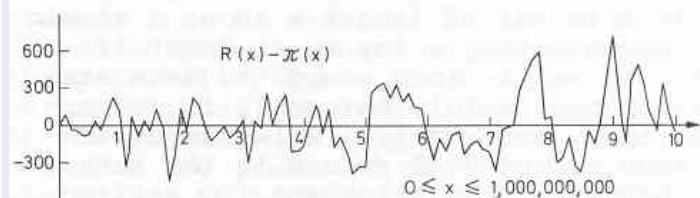
Összehasonlítás.

x	$\pi(x)$	$R(x)$	$\pi(x) - R(x)$
100.000.000	5.761.455	5.761.552	-97
200.000.000	11.078.937	11.079.090	-153
400.000.000	21.336.326	21.336.185	141
600.000.000	31.324.703	31.324.622	81
800.000.000	41.146.179	41.146.248	-69
1.000.000.000	50.864.534	50.847.455	79

Az előjel gyakran változik, amit a következő ábra is mutat.

Riemann függvénye.

Összehasonlítás.



Riemann függvénye.

Az $R(x)$ függvény „jószágát” a következő táblázat is mutatja.

x	$\pi(x)$	$R(x)$
100,000,000	5,761,455	5,761,552
200,000,000	11,078,937	11,079,090
300,000,000	16,252,325	16,252,355
400,000,000	21,336,326	21,336,185
500,000,000	26,355,867	26,355,517
600,000,000	31,324,703	31,324,622
700,000,000	36,252,931	36,252,719
800,000,000	41,146,179	41,146,248
900,000,000	46,009,215	46,009,949
1,000,000,000	50,847,534	50,847,455

Riemann függvénye.

- Az $R(x)$ függvény a logaritmusfüggvény egész függvénye:

$$R(x) = 1 + \sum_{n=1}^{\infty} \frac{1}{n\zeta(n+1)} \frac{(\log x)^n}{n!},$$

ahol $\zeta(n) = \sum_{k=1}^{\infty} \frac{1}{k^n}$, az ún. Riemann-féle *zeta-függvény*.

- A múlt század 20-as éveiben az indus Ramanujan megadta a Riemann-féle közelítő függvény integrálélellátását:

$$R(x) = \int_0^{\infty} \frac{(\log x)^t}{t\Gamma(t+1)\zeta(t+1)} dt,$$

ahol $\Gamma(t) = \int_0^{\infty} x^{t-1} e^{-x} dx$, az ún. *gamma-függvény*.

 $\pi(x)$

Egy kis összegzés 1.

- Emlékeztetünk: Gauss és Legendre empirikus megfontolásokkal, míg Riemann elméleti megfontolások révén jutott közelítő formulájához, függvényéhez. A prímszámtétel bizonyítása egyiküknek sem sikerült.
- Gauss empirikus megfontolása — miszerint egy az n -nel egyező nagyságrendű egész prím voltának valószínűsége közelítőleg $1/\log n$ — alapján következtethetünk arra, hogy
- egy n körüli a hosszúságú intervallumban közelítőleg $a/\log n$ számú prím van,
- legalábbis akkor, ha n az a -hoz képest elegendően nagy, de az intervallum is „elegendően hosszú” ahhoz, hogy a statisztikai következtetések plauzibilisek legyenek.

 $\pi(x)$

Egy kis összegzés 2.

- Hasonlóan kapható az a következtetés is, hogy nagy n közelében véletlenszerűen kiválasztott két szám mindegyike prím legyen közelítőleg $1/\log^2 n$.
- Ennek alapján arra is gondolhatunk, hogy egy n körüli a hosszúságú intervallumban közelítőleg $a/\log^2 n$ számú ikerprím van.
- Sőt, egy további heurisztikus gondolatmenettel az is megkapható, hogy ezek száma közelítőleg

$$c \frac{a}{\log^2 n},$$

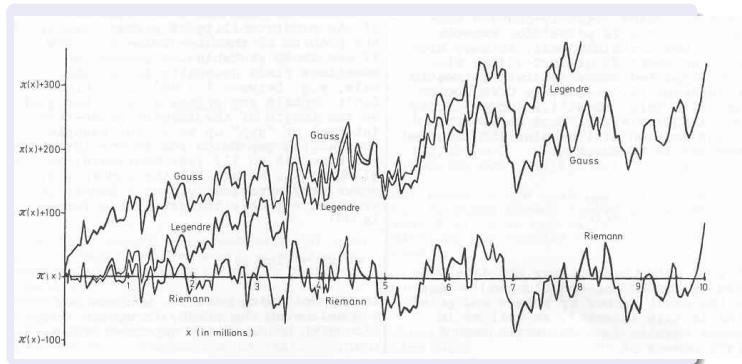
ahol $c \approx 1,3203236 \dots$ konstans.

Az előbbieknél a valósággal való szembesítést a következő táblázat mutatja.

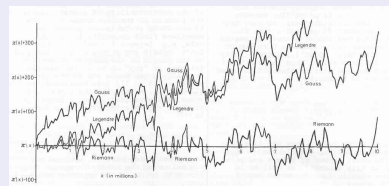
Prímszámok, ikerprímek.

Interval	Prime numbers		Prime twins	
	expected	found	expected	found
100,000,000–100,150,000	8142	8154	584	601
1,000,000,000–1,000,150,000	7238	7242	461	466
10,000,000,000–10,000,150,000	6514	6511	374	389
100,000,000,000–100,000,150,000	5922	5974	309	276
1,000,000,000,000–1,000,000,150,000	5429	5433	259	276
10,000,000,000,000–10,000,000,150,000	5011	5065	221	208
100,000,000,000,000–100,000,000,150,000	4653	4643	191	186
1,000,000,000,000,000–1,000,000,000,150,000	4343	4251	166	161

A becslések összehasonlítása.



A becslések összehasonlítása.



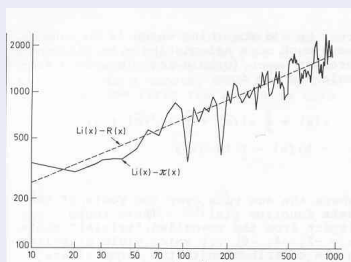
Elemzés.

1. Kis x -ekre, ha $x \leq 10^6$, a Legendre-féle empirikus formula jobb a Gauss-féle $\text{Li}(x)$ logaritmikus integrálnál.
2. Az utóbbi azonban $x \geq 5 \cdot 10^6$ -tól egyértelműen jobb.
3. A Riemann-féle közelítés mindkettőnél jobb, de az $R(x) - \pi(x)$ értékek oscilációja egyre nő, de csak lassan. $x \leq 10^9$ -ig nem nő néhány 100 fölé.

A becslések összehasonlítása.

- Vizsgáljuk meg az $\text{Li}(x) - \pi(x)$ különbség-függvényt.
- 10^7 -ig pozitív, és az ábra sugallata szerint egyre nő, azaz Li felső becslést ad mindig. Ezt támaszthatná alá az is, hogy $R(x) < \text{Li}(x)$.

Az újabb vizsgálatok ellentmondanak e vélekedésnek.



A becslések összehasonlítása.

1. Elég nagy x -re — amikor már nagyra nő az $R(x) - \pi(x)$ különbség — az $\text{Li}(x)$ már nem fölülről közelíti $\pi(x)$ -et, azaz

$$\exists x_0 \in \mathbb{R}, \quad \pi(x_0) > \text{Li}(x_0).$$

2. Ilyen x_0 létezését Littlewood igazolta.
3. Skewes megmutatta, hogy ha igaz a Riemann hipotézis, akkor a legkisebb ilyen x_0 -ra

$$x_0 < 10^{10^{34}}$$

4. Skewes: a Riemann hipotézis nélkül a felső korlát

$$x_0 < 10^{10^{964}},$$

5. A jelenleg ismert legjobb becslés

$$1,65 \cdot 10^{1165}$$

Prímszámok

Néhány tisztán deduktíven nyert eredmény.

- 1 **Euklidész IX. 21. Tétel.** *Prímszámok bármely sokaságánál van több.*
- 2 **Euler (XVIII. sz.):** A prímszámok reciprokaiból álló sor divergens, míg pl.

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}.$$

- 3 **Mertens (XIX. sz. vége)**

$$\sum_{p < x} \frac{1}{p} = \log \log x + c + \varepsilon(x),$$

ahol $\lim_{x \rightarrow \infty} \varepsilon(x) = 0$ (konvergenca „gyors”), $c \approx 0,261498$.

Prímszámok

A legutóbbi alapján.

- $\pi(10^{18}) \approx 50 \cdot 10^{18}$,
- és becsljük meg mennyi lehet ennyi prímszám reciprokának összege:

$$\begin{aligned} \sum_{p < 10^{18}} \frac{1}{p} &\approx \\ \log \log(10^{18}) + c + \varepsilon(10^{18}) &\approx \log(41,446.531.673.892) + 0,261198 \\ &\approx 3,985.902.203.314 < 4 \end{aligned}$$

- Ugyanis $\varepsilon(10^{18}) \approx 0$
- Mivel $\pi(10^9) \approx 50 \cdot 10^6$, hasonló számolással az első 50 millió prímszám reciprokának összege közelítőleg csak 3,3.

További becslések.

Csebisev (1850)

- Létezik olyan $a, b \in \mathbb{R}$ konstans, hogy elég nagy $x \in \mathbb{R}$ -re

$$a \cdot \frac{x}{\log x} < \pi(x) < b \cdot \frac{x}{\log x}$$

- Például, $a = 0,89$ és $b = 1,11$ ilyen.
- Ez az első komoly lépés a prímszámtétel felé.

A ζ függvény használatával.

További formulák kaphatók $\pi(x)$ -re a Riemann-féle zeta- függvény zéróhelyeinek fölhasználásával.

További becslések.

$$\begin{aligned} \pi(x) + \frac{1}{2}\pi(\sqrt{x}) + \frac{1}{3}\pi(\sqrt[3]{x}) + \dots \\ = \text{Li}(x) - \sum_{\varrho} \text{Li}(x^{\varrho}), \end{aligned}$$

ahol a ϱ végigfutja a ζ függvény zéróhelyeit.

$$\pi(x) = R(x) - \sum_{\varrho} R(x^{\varrho}),$$

ahol a ϱ végigfutja a ζ függvény zéróhelyeit.

Prímszámok

A Riemann-hipotézisre támaszkodva zárásul megadunk két becslést a Gauss-féle közelítő függvényre. Az elsőről tudjuk, hogy ekvivalens a hipotézissel, míg a második csak sejtés.

- $$|\text{Li}(x) - \pi(x)| < \sqrt{x} \log x,$$

- Tetszőleges $0 < c < 1$ konstansra

$$|\text{Li}(x) - \pi(x)| < x^c$$

Riemann-hipotézis 1.

A „klasszikus” zeta-függvény.

- Euler 1740:

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

- Ha $s \in \mathbb{R}$, akkor a definiáló sor konvergens minden $s > 1$ -re, és divergens minden más esetben.
- Euler tétele. Ha P jelöli az összes prímszámok halmazát, akkor

$$\zeta(s) = \prod_{p \in P} \frac{1}{1 - p^{-s}}.$$

- A XIX. században Riemann és mások igazolták, hogy az előbbi sor, ill. végtelen szorzat akkor is konvergens, ha s olyan komplex szám amelynek valós része nagyobb 1-nél.
- Ettől kezdve említik e függvényt Riemann-féle zeta-függvénynek.

Riemann-hipotézis 2.

A függvény kiterjesztése.

- Igazolták, hogy ha $s > 1$, ill. $\Re(s) > 1$, akkor az (1)-ben definiált ζ függvényre teljesül az

$$\left(1 - \frac{2}{2^s}\right) \zeta(s) = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n^s} \quad (2)$$

függvényegyenlet.

- (2) jobb oldala azonban nemcsak $\Re(s) > 1$ -re hanem minden olyan $s \in \mathbb{C}$ -re konvergens, amelyre $\Re(s) > 0$.
- Ez lehetővé teszi a ζ függvény kiterjesztését a $\{s \in \mathbb{C} : \Re(s) > 0\}$ halmazra, kivéve az

$$s = 1 + \frac{2\pi in}{\log 2}$$

értékeket, ahol $n > 0$ egész.

Riemann-hipotézis 3.

A függvény további kiterjesztése.

- A kiterjesztett ζ függvény a $0 < \Re(z) < 1$ sávban azonban a

$$\zeta(s) = 2^s \pi^{s-1} \sin\left(\frac{\pi s}{2}\right) \Gamma(1-s) \zeta(1-s) \quad (3)$$

egyenletet is kielégíti, s ez

- lehetővé teszi analitikus kiterjesztését a teljes komplex síkra, kivéve — az eddigieken kívül — az $s = 0$ esetet.
- (3)-ból azonnal adódik, hogy $\zeta(2k) = 0$ minden $k < 0$ -ra.
- Ezen egészek a ζ függvény triviális zéróhelyei.

Riemann-hipotézis 4.

A hipotézis.

- Riemann sejtése szerint a nem-valós zéróhelyek mindegyikének valós része $\frac{1}{2}$.
- Ezen sejtést szokás **Riemann-hipotézisként** említeni.
- Jelenleg több, mint 6 millió komplex zéróhely ismert, és mindegyikük valós része $\frac{1}{2}$.