A prímszámtétel bizonyításának története

Matematika BSc szakdolgozat

Szerző:
Szabó Lilla

Témavezető:
Dr. Waldhauser Tamás
Algebra és Számelmélet Tanszék

Szegedi Tudományegyetem Bolyai Intézet
2014

Köszönetnyilvánítás

Ezúton köszönöm Dr. Waldhauser Tamásnak, hogy témavezetőmként segítette szakdolgozatom elkészülését ötleteivel és tanácsaival.
Kovácsné Görgényi Ilonának és Kaló Juditnak, volt matematika tanáraimnak, hogy elindítottak a matematika útján.
Továbbá Marcus de Sautoy-nak, hogy A prímszámok zenéje című könyvével ihletet adott.
Végül, de nem utolsó sorban szeretném megköszönni szüleimnek, családomnak, páromnak és barátaimnak támogatásukat, türelmüket és megértésüket.

Tartalomjegyzék

Bevezetés

> „A prímszámok a számtan atomjai. A prímek az „oszthatatlan” számok: azok a számok, amelyek nem írhatók fel két kisebb szám szorzataként. A 13 és a 17 prímszám, a 15 azonban nem az, mert felírható mint 3-szor 5. A prímek csupán elszórt díszek a számok végtelen világában, ezen a matematikusok által évszázadok óta kutatott hatalmas területen. A kutatókat ma is csodálattal töltik el: 2, 3, 5, 7, 11, 13, 17, 19, 23... - időtlen számok ezek, a fizikai valóságtól függetlenül is léteznek; a természet ajándékai a matematikusoknak.” – *Marcus du Sautoy: A prímszámok zenéje*

Engem a fenti idézet indított el a prímszámok útján. Dolgozatom is ezekről a különleges építőkövekről fog szólni. Ezeknek a számoknak – melyeket felbonthatatlan számoknak is szokás nevezni – a történelme egészen az ókorig nyúlik vissza.

A dolgozat első részében áttekintjük az Euklidésztől a prímszámtételig vezető utat. Ezután részletesebben tanulmányozzuk Csebisev munkásságát és Riemann 1859-es cikkét, majd belemélyedünk a prímszámtétel bizonyításába. Mindezek után a teljesség igénye nélkül tekintünk néhány érdekesebb eredményt a prímszámok témakörében.

1. Történeti áttekintés

A legkorábbi lelet, mely a prímek ismeretére utalhat a Kr. e. 6500-ból származó ishangói csont elnevezésű lelet, melyet 1960-ban találtak Közép-Afrika egyik hegységében, az Egyenlítőnél. A csonton három oszlopba osztva rovátkacsoportok találhatók, melyekből az első oszlopban a 10 és 20 közötti prímeknek – $11, 13, 17$ és 19 – megfelelő számú rovátkák vannak. Nem tudni biztosan, hogy ez a csont, melyet a brüsszeli Belga Királyi Természettudományi Intézetben őriznek, lenne az első kísérlet a prímszámok megértésére, vagy a rovások csupán véletlenszerűek.

Bizonyíték van rá, hogy a kínaiaknak Kr. e. 1000-ben már világos képük volt a prímszámokról. Az ő szemükben ezek azok a férfias számok, amelyek ellenállnak a két kisebb szám szorzatára való felbontásnak.

A görögök ismerték fel először Kr. e. 4. században, hogy a prímek a számok építőkövei lehetnek. Felismerték, hogy az összetett számok felbonthatók prímszámok szorzatára. A Kr. e. 3. évszázadban élt Eratoszthenész, aki könyvtáros volt a hatalmas ókori alexandriai görög kutatóintézetben, volt az első ember, aki prímszámtáblázatot készített. Az ő módszerét Eratoszthenész szitájának hívjuk és a következőképpen fest:

1.1. Tétel (Eratoszthenész szitája)**.** Írjuk fel 2-től n-ig az egész számokat. Az első lépésben karikázzuk be 2-t, majd húzzuk át 2 összes nála nagyobb többszörösét. Ezután karikázzuk be a legkisebb még nem jelölt (nem bekarikázott vagy áthúzott) számot, jelenleg ez a 3, majd húzzuk át a nála nagyobb többszöröseit. Hasonlóan folytatva karikázzuk be a legkisebb még jelöletlen számot, legyen az p, és húzzuk át a többszöröseit p^2-től kezdve. Mivel a szitálás során korábban $2p, 3p, \ldots, (p-1)\,p$ már át lett húzva, ezért valóban elég lesz p^2-től kezdve áthúzni p többszöröseit. Az eljárás akkor fejeződik be, ha $p^2 > n$. Ekkor a bekarikázott és a jelöletlen számok adják meg az 1 és n közötti prímszámok listáját.

Ugyanebben a században Euklidész bebizonyította a következő tételt.

1.2. Tétel. *Végtelen sok prímszám van.*

Bizonyítás. Legyen $p_1, p_2, \ldots, p_k$ prímek egy halmaza, $n = p_1 p_2 \cdots p_k + 1$ és p az n szám egy prímosztója. Ekkor p nem lehet eleme a $p_1, p_2, \ldots, p_k$ halmaznak, hiszen különben osztaná a $p_1 p_2 \cdots p_k$ szorzatot és az $n - p_1 p_2 \cdots p_k = 1$ különbséget, ami nem lehetséges. Tehát egy véges prímhalmaz nem tartalmazhatja az összes prímszámot. □

Az ókort követően a prímszámok körében számos kutatást végeztek, újabb tételeket mondtak ki és bizonyítottak be. Ezek közül néhányat a 6. fejezetben említek meg. Számunkra, a prímszámtétel bizonyításának szempontjából, azonban az 1700-as évektől kezdődő korszak a lényeges.

1737-ben Euler belátta [5], hogy a prímszámok reciprokösszege végtelen, azaz

$$\sum_p \frac{1}{p} = \infty,$$

másképp

$$\sum \frac{1}{p} \approx \log \sum \frac{1}{n} \approx \log(\log \infty).$$

Gauss 1792-ben táblázatokból megsejtette, hogy a prímek sűrűsége $\frac{1}{\log x}$, pontosabban $\pi(x) \approx \int_2^x \frac{dt}{\log t}$, melyet $\mathrm{Li}(x)$-szel jelölünk. Későbbi, pontosabb táblázatok kicsit más számokat tartalmaznak, de ezek csak még jobban erősítik a sejtést. Legendre körülbelül 1800-ban közreadott egy cikket, melyben a prímek sűrűségére az $\frac{1}{A \log x + B}$ kifejezést adta, empirikusan meghatározott A és B konstansokkal és $\pi(x)$-re pedig a következő becslést:

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

ahol $A = 1,08366$. Erről 1808-ban írt először *Théorie des Nombres* című munkájában. A világ viszont csak 1849-ben tudta meg [7], hogy valójában Gauss megelőzte Legendre-t. A következő évben Csebisev egyik megjelent cikkében ír a $\pi(x)$ függvénynek $\mathrm{Li}(x)$-szel való becsléséről.

Riemann 1859 novemberében a berlini Akadémia havonta megjelenő közleményében közreadott egy 9 oldalas cikket *Ueber die Anzahl der Primzahlen unter einer gegebenen Grösse* címmel [11], mely egyedüli cikke a prímszámok témakörében. A cikkben Riemann módszerei még az eredményeknél is fontosabbak. Ír az alábbi, 1.1. Definícióban szereplő függvény analitikus kiterjesztéséről, komplex zérushelyeiről, felhasználja a Fourier, illetve Möbius inverziót, explicit formulákat ad meg.

1.1. Definíció. Minden n természetes számra és s komplex számra

$$\zeta(s) = \sum_n \frac{1}{n^s}.$$

1896-ban Hadamard [8] és de la Vallée Poussin [13] egymástól függetlenül bebizonyították a prímszámtételt. 1899-ben de la Vallée Poussin publikált egy cikket, melyben leírja, hogy elég nagy x-re

$$\left| \frac{\pi(x) - \mathrm{Li}(x)}{\mathrm{Li}(x)} \right| < e^{-\sqrt{c \log x}}.$$

Koch 1901-ben belátta, hogy ha a fenti becslésben $e^{-\sqrt{c\log x}}$ helyett $x^{-\frac{1}{2}+\varepsilon}$-t írva a Riemann-sejtéssel ekvivalens állítást kapunk.

A következő fejezetekben részletesebben tekintjük Csebisev munkásságát, Riemann cikkét és a prímszámtétel bizonyítását.

2. Dirichlet-sorok

Ebben a fejezetben néhány függvény Dirichlet-sorát fogjuk vizsgálni. Ehhez szükségünk lesz az alábbi két definícióra, illetve két tételre.

2.1. Definíció. Az $f(n)$ számelméleti függvényhez tartozó Dirichlet-sor a következő:

$$F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}.$$

2.1. *Megjegyzés.* A fenti definícióban levő sor nem minden $f(n)$ függvényre konvergál. A konvergencia igazolása fontos kérdés, de erre mi most nem térünk ki. A később belátott lemmákban ezeket a sorokat formálisan fogjuk tekinteni.

Az 2.1. Tételben szereplő speciális Dirichlet-sorról – melyben $f(n)$ azonosan 1 – később részletesebben is beszélünk.

2.2. Definíció. Mangoldt-függvénynek nevezzük a következő képlettel definiált Λ számelméleti függvényt:

$$\Lambda(n) = \begin{cases} \log p, & \text{ha } n = p^{\alpha}; \\ 0, & \text{különben.} \end{cases}$$

Euler 1737-ben mondta ki az alábbi tételt.

2.1. Tétel. *Minden $2 \le s \in \mathbb{N}$ számra*

$$\zeta(s) = \sum_{n} \frac{1}{n^s} = \prod_{p} \frac{1}{\left(1 - \frac{1}{p^s}\right)},$$

ahol p a prímszámokon, n pedig a természetes számokon fut végig.

Ez ma Euler-szorzatként ismert. A fenti tételt később Dirichlet $s > 1$ valós számokra alkalmazta.

A következő tétel két sor szorzatáról szól:

2.2. Tétel. *Legyen $A(s) = \sum_{k=1}^{\infty} \frac{a_k}{k^s}$ és $B(s) = \sum_{l=1}^{\infty} \frac{b_l}{l^s}$. Ekkor szorzatuk a következő:*

$$A(s)B(s) = \sum_{n=1}^{\infty} \frac{c_n}{n^s},$$

ahol a szorzat együtthatóinak sorozata a két sor együtthatóinak konvolúciója, tehát $c_n = \sum_{kl=n} a_k b_l$.

Bizonyítás. Tekintsük a két sor szorzatát és alakítsuk a következő módon:

$$A(s)B(s) = \sum_{k=1}^{\infty} \frac{a_k}{k^s} \cdot \sum_{l=1}^{\infty} \frac{b_l}{l^s} = \sum_{k} \sum_{l} \frac{a_k}{k^s} \frac{b_l}{l^s} = \sum_{k} \sum_{l} \frac{a_k b_l}{(kl)^s}.$$

A fenti Dirichlet-sorban $\frac{1}{n^s}$ együtthatója

$$\sum_{kl=n} a_k b_l = c_n.$$

Tehát

$$A(s)B(s) = \sum_{n=1}^{\infty} \frac{c_n}{n^s}.$$

□

2.1. Lemma. *A $\delta(n)$ számelméleti függvényhez tartozó Dirichlet-sor a konstans 1 függvény.*

Bizonyítás. Tekintsük a $\delta(n)$ függvényhez tartozó Dirichlet-sort:

$$\delta(s) = \frac{1}{1^s} + \frac{0}{2^s} + \frac{0}{3^s} + \ldots = \frac{1}{1^s} = 1.$$

□

2.2. Lemma. *A konstans* 1 *függvényhez tartozó Dirichlet-sor* $\zeta(s)$.

Bizonyítás. Tekintsük a konstans 1 függvényhez tartozó Dirichlet-sort:

$$\frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \ldots = \sum_{n=1}^{\infty} \frac{1}{n^s} = \zeta(s).$$

□

2.3. Lemma. *A* $\log(n)$ *függvényhez tartozó Dirichlet-sor* $-\zeta'(s)$.

Bizonyítás. Deriváljuk a $\zeta(s)$ függvény Dirichlet-sorát tagonként:

$$\zeta(s) = \sum \frac{-\log n}{n^s}.$$

Ebből következik, hogy

$$\sum_{n=1}^{\infty} \frac{\log(n)}{n^s} = -\sum_{n=1}^{\infty} \left(-\frac{\log(n)}{n^s}\right) = -\zeta'(s).$$

□

2.4. Lemma. *A $\mu(n)$ számelméleti függvényhez tartozó Dirichlet-sor $\frac{1}{\zeta(s)}$.*

Bizonyítás. Mivel $1 = \delta * 1$, a Möbius-féle inverziós formula alapján

$$\delta = 1 * \mu.$$

A 2.2. Tételből következik, hogy

$$1(s) = \zeta(s)M(s),$$

ahol 2.1. és 2.2. Lemmák alapján $1(s)$ a $\delta(n)$, $\zeta(s)$ az $1(n)$, $M(s)$ pedig a $\mu(n)$ függvény Dirichlet-sorát jelöli. Ebből következik, hogy

$$\frac{1}{\zeta(s)} = M(s).$$

□

2.5. Lemma. *A $\Lambda(n)$ számelméleti függvényhez tartozó Dirichlet-sor $-\frac{\zeta'(s)}{\zeta(s)}$.*

Bizonyítás. Jelölje $f(s)$ a Λ számelméleti függvényhez tartozó Dirichlet-sort:

$$f(s) = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}.$$

Először belátjuk, hogy

$$(1 * \Lambda)(n) = \log n,$$

azaz

$$\log n = \sum_{d|n} \Lambda(d).$$

Legyen $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$ az n szám prímfelbontása. Tekintsük n egy d osztóját. Ha d nem prímhatvány, akkor $\Lambda(d) = 0$. Ha $d = p_i^{\beta_i}$ alakú, ahol $i \in \{1, 2, \dots, m\}$ és $0 \leq \beta_i \leq \alpha_i$, akkor $\Lambda(d) = \log p_i$. Ilyen tagból a fenti összegben α_i darab van. Ez alapján kapjuk, hogy

$$\sum_{d|n} \Lambda(d) = \alpha_1 \log p_1 + \alpha_2 \log p_2 + \ldots + \alpha_m \log p_m = \log n.$$

A 2.1. Tételből és a 2.3. Lemmából következik, hogy

$$\zeta(s)f(s) = -\zeta'(s),$$

tehát $f(s) = \frac{-\zeta'(s)}{\zeta(s)}$. □

3. Csebisev eredményei

Csebisev 1850-ben látta be az alábbi tételt:

3.1. Tétel (Csebisev Tétel)**.** *Bármely $n \geq 1$ egész esetén létezik olyan p prím, melyre $n < p \leq 2n$.*

3.1. *Megjegyzés.* Az alábbi tételek bizonyításánál Erdős gondolatmenetét [4] fogjuk követni.

Csebisev következő tétele több tétel bizonyításának szempontjából is fontos.

3.2. Tétel. *Bármely $n \in \mathbb{N}$-re $\prod_{p \leq n} p < 4^n$.*

Bizonyítás. Teljes indukcióval bizonyítunk. Tekintsük a bizonyítandó egyenlőtlenséget $n = 1$-re:

$$\prod_{p \leq 1} p = 1 < 4^1 = 4,$$

ezután $n = 2$-re:

$$\prod_{p \leq 2} p = 2 < 4^2 = 16.$$

Legyen $n > 2$, és tegyük fel, hogy $1, 2, \ldots, n-1$-re teljesül az állítás.

(i) Ha n páros, akkor n nem lehet prím, így az indukciós hipotézisből következik, hogy

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

(ii) Ha n páratlan, akkor felírható $2k+1$ alakban, ahol k pozitív egész. Bontsuk szét a szorzatot:

$$\prod_{p \leq 2k+1} p = \prod_{p \leq k+1} p \cdot \prod_{k+2 \leq p \leq 2k+1} p = \Pi_1 \Pi_2.$$

Az indukciós hipotézis alapján

$$\Pi_1 < 4^{k+1}.$$

Mivel a Π_2-ben levő prímek nagyobbak, mint $k+2$, ezért

$$\mathrm{lnko}(\Pi_2, k!) = 1.$$

Mivelhogy

$$\Pi_2 \,|(k+2) \cdots (2k+1)\ ,$$

ahol

$$(k+2)\cdots(2k+1) = \frac{(2k+1)!}{(k+1)!} = \frac{(2k+1)!k!}{(k+1)!k!} = \binom{2k+1}{k}k!,$$

és $\mathrm{lnko}(\Pi_2, k!) = 1$, ezért

$$\Pi_2 \,\Big|\, \binom{2k+1}{k}.$$

A 7.3. segédtétel alapján

$$\binom{2k+1}{k} < \frac{2^{2k+1}}{2} = 4^k.$$

Tehát

$$\Pi_1\Pi_2 < 4^{k+1}4^k = 4^{2k+1} = 4^n.$$

□

Csebisev egyik 1850-ben megjelent cikkében [1] arról ír, hogy a $\pi(x)$ függvénynek $\mathrm{Li}(x)$-szel való becslésében a relatív hiba kisebb, mint 11%, ha x elég nagy, tehát

$$0,89 \cdot \mathrm{Li}(x) < \pi(x) < 1,11 \cdot \mathrm{Li}(x),$$

ha x elég nagy. Leírta, hogy Legendre formulája semmilyen A-ra illetve B-re nem lehet jobb, mint $\mathrm{Li}(x)$. Szintén Csebisev belátta, hogy ha a $\frac{\pi(x)}{\mathrm{Li}(x)}$ hányados konvergál, akkor csak 1-hez konvergálhat. Azt viszont nem tudta belátni, hogy konvergál. A következőkben belátjuk a fentebb említett becslést $\pi(x)$-re, pontos értékek megadása nélkül.

3.3. Tétel. *Létezik olyan $B > 0$ konstans, amelyre $\pi(x) < B\frac{x}{\log x}$.*

Bizonyítás. A tételt először természetes számokra látjuk be, majd pozitív valós számokra.

Bontsuk szét a 3.1. Tételben szereplő szorzatot a következőképpen:

$$4^n > \prod_{p\le n} p = \prod_{p\le\sqrt{n}} p \cdot \prod_{\sqrt{n}<p\le n} p.$$

Becsüljük a szorzatot úgy hogy az első tényezőben minden p helyett 1-et, a másodikban pedig $\sqrt{n}$-et írunk. Ekkor a következőt kapjuk:

$$\prod_{p\le\sqrt{n}} p \cdot \prod_{\sqrt{n}<p\le n} p > 1 \cdot \prod_{\sqrt{n}<p\le n} \sqrt{n} = \sqrt{n}^{\pi(n)-\pi(\sqrt{n})}.$$

Tehát

$$4^n > \sqrt{n}^{\pi(n)-\pi(\sqrt{n})},$$

amiből mindkét oldal logaritmusát véve következik, hogy

$$\frac{1}{2}(\pi(n) - \pi(\sqrt{n})) \log n < n \log 4.$$

Átrendezve az egyenlőtlenséget kapjuk, hogy

$$\frac{\pi(n)}{\frac{n}{\log n}} < 2\log 4 + \frac{\pi(\sqrt{n})}{\frac{n}{\log n}} < 2\log 4 + \frac{\sqrt{n}}{\frac{n}{\log n}} = 2\log 4 + \frac{\log n}{\sqrt{n}},$$

ahol a 7.1. Lemma (2)-es pontja alapján

$$\frac{\log n}{\sqrt{n}} = \frac{\log \sqrt{n}^2}{\sqrt{n}} = 2\frac{\log \sqrt{n}}{\sqrt{n}} \to 0,$$

tehát létezik egy olyan B konstans, amellyel $2\log 4 + \frac{\log n}{\sqrt{n}}$ felülről becsülhető.

Ha $x \notin \mathbb{N}$ és $x > e$, akkor $[x]$-t kell tekintenünk. Mivel $\frac{x}{\log x}$ a 7.1. Lemma (1)-es pontja szerint szigorúan monoton növő, ezért az állítás igaz lesz minden $e < x$ valós számra, hiszen

$$\pi(x) = \pi([x]) < B\frac{[x]}{\log[x]} < B\frac{x}{\log x}.$$

□

3.4. Következmény. *Létezik olyan $b > 0$ konstans, amelyre $p_n > b \cdot n \log n$.*

Bizonyítás. Tudjuk, hogy $n = \pi(p_n)$, ahol p_n az n-edik prímszámot jelöli. Az előző tételből következik, hogy

$$n = \pi(p_n) < B\frac{p_n}{\log p_n}.$$

Az egyenlőtlenséget átrendezve kapjuk, hogy

$$p_n > \frac{1}{B} n \log p_n > \frac{1}{B} n \log n.$$

Végül legyen $\frac{1}{B} = b$, így megkapjuk az állításban szereplő egyenlőtlenséget. □

3.5. Segédtétel. *Minden $n \in \mathbb{N}$-re $\binom{2n}{n} = \prod_{p \le 2n} p^{\alpha_p}$, ahol $p^{k_p} \le 2n \le p^{k_p+1}$, illetve $\alpha_p \le k_p$.*

Bizonyítás. Legyen

$$\binom{2n}{n} = \frac{(2n)!}{n! \cdot n!} = \prod_{p \le 2n} p^{\alpha_p}.$$

Tekintsünk egy rögzített p prímet. A p kitevője $(2n)!$-ban és $n!$-ban a 7.1. Segédtétel alapján $\nu_p((2n)!) = \sum_{i=1}^{\infty} \lfloor \frac{2n}{p^i} \rfloor$, illetve $\nu_p(n!) = \sum_{i=1}^{\infty} \lfloor \frac{n}{p^i} \rfloor$. Mivel azonos alapú hatványok osztásánál a kitevők kivonódnak, így kapjuk, hogy

$$\alpha_p = \sum_{i=1}^{\infty} \left\lfloor \frac{2n}{p^i} \right\rfloor - 2 \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor.$$

Vegyük észre, hogy minden $k_p < i$-re az összegben az alsó egészrészek értéke nulla lesz, tehát

$$\alpha_p = \sum_{i=1}^{k_p} \left\lfloor \frac{2n}{p^i} \right\rfloor - 2 \sum_{i=1}^{k_p} \left\lfloor \frac{n}{p^i} \right\rfloor.$$

A 7.2. Segédtétel alapján tudjuk, hogy

$$\left\lfloor \frac{2n}{p^i} \right\rfloor - 2 \left\lfloor \frac{n}{p^i} \right\rfloor = \begin{cases} 1, & \text{ha } \{x\} \ge \frac{1}{2}; \\ 0, & \text{ha } \{x\} < \frac{1}{2}. \end{cases}$$

Mivel az összeg minden tagja legfeljebb 1 és összesen k_p tagja van, így az összeg legfeljebb k_p. □

3.6. Tétel. *Létezik olyan $A > 0$ konstans, amelyre $\pi(x) > A \frac{x}{\log x}$.*

Bizonyítás. Először páros számokra látjuk be a tételt. Az előbbi segédtételt felhasználva kapjuk, hogy

$$\binom{2n}{n} = \prod_{p \le 2n} p^{\alpha_p} \le \prod_{p \le 2n} p^{k_p}.$$

Minden p-re becsüljük a p^{k_p} hatványt $2n$-nel:

$$\prod_{p \le 2n} p^{k_p} \le \prod_{p \le 2n} 2n = (2n)^{\pi(2n)}.$$

Ebből és a 7.4. Segédtételből következik, hogy

$$2^{2n} \le 2n \binom{2n}{n} \le (2n) \cdot (2n)^{\pi(2n)} = (2n)^{\pi(2n)+1}.$$

Vegyük mindkét oldal logaritmusát és rendezzük át az egyenlőtlenséget. Így a következőt kapjuk:

$$\frac{2n \log 2}{\log(2n)} - 1 \le \pi(2n).$$

Melyből az alábbi következik:

$$\frac{\pi(2n)}{\frac{2n}{\log(2n)}} \geq \log 2 - \frac{1}{\frac{2n}{\log(2n)}} = \log 2 - \frac{\log(2n)}{2n},$$

ahol a 7.1. Lemma (2)-es pontja alapján $\frac{\log 2n}{2n} \to 0$, tehát létezik egy olyan $A > 0$ konstans, amellyel $\log 2 - \frac{\log(2n)}{2n}$ alulról becsülhető.

Tetszőleges $x \in \mathbb{R}$-re legyen $2n$ a legnagyobb páros szám, ami x-nél kisebb vagy egyenlő. Ekkor $2n \leq x < 2n + 2$. Tudjuk, hogy

$$\pi(x) \geq \pi(2n) > A\frac{2n}{\log 2n},$$

és $2n > x - 2$ miatt a 7.1. Lemma alapján $\frac{2n}{\log 2n} > \frac{x-2}{\log(x-2)}$. Tehát

$$A\frac{2n}{\log 2n} \geq A\frac{x-2}{\log(x-2)}.$$

A 7.1. Lemmából következik, hogy

$$\frac{\frac{x}{\log x}}{\frac{x-2}{\log(x-2)}} \to 1,$$

ezért létezik egy olyan pozitív A', melyre $A\frac{x-2}{\log(x-2)} > A'\frac{x}{\log x}$. □

3.7. Következmény. *Létezik olyan $a > 0$ konstans, amelyre $p_n < a \cdot n \log n$.*

Bizonyítás. Világos, hogy $n = \pi(p_n)$. Az előző tétel alapján tudjuk, hogy minden n esetén

$$n = \pi(p_n) > A\frac{p_n}{\log(p_n)},$$

melyből az alábbi következik:

$$p_n < \frac{1}{A} n \log(p_n). \tag{1}$$

Mivel $p_n \leq 2^{2^{n-1}}$, ezért, ha n elég nagy, akkor

$$p_n < \frac{1}{A} n \log(p_n) \leq \frac{1}{A} n 2^{n-1} \log 2 < 4^n.$$

Ezt az (1) -es egyenlőtlenségbe behelyettesítve kapjuk, hogy ha n elég nagy, akkor

$$p_n < \frac{1}{A} n \log(p_n) < \frac{1}{A} n \cdot \log 4n < n^3.$$

Újra behelyettesítve (1) -be az alábbi következik:

$$p_n < \frac{1}{A} n \log(p_n) < \frac{3}{A} n \log n.$$

Végül legyen $a = \frac{3}{A}$, így megkapjuk az állításban szereplő egyenlőtlenséget. □

4. Riemann cikke

Riemann 1859-es cikkében [11] formulát ad $\pi(x)$-re végtelen sor alakban, melynek domináns tagja $\mathrm{Li}(x)$. Ennek bizonyítása nem kielégítő, hisz nem látja be, hogy konvergál, sem pedig, hogy $\mathrm{Li}(x)$ a domináns tag. Riemann leírja, hogy a Dirichlet-től tanult Euler-szorzat segítségével a ζ függvény a következőképpen is megadható:

$$\zeta(s) = \sum_n \frac{1}{n^s} = \prod_p \left(1 - \frac{1}{p^s}\right),$$

ahol p a prímeken, n pedig a pozitív egész számokon fut végig. Megemlíti, hogy ζ-nak zérushelye van az $s = -2, -4, -6, \ldots$ helyeken (mindegyik egyszeres), sőt bizonyos értékeit konkrétan meg is adta, mint például

$$\zeta(0) = -\frac{1}{2},\ \zeta(-1) = -\frac{1}{12},\ \zeta(-3) = \frac{1}{120}.$$

Valószínűleg ismerte a $\zeta(-n) = (-1)^n \frac{B_{n+1}}{n+1}$, illetve $\zeta(2n) = \frac{(2\pi)^{2n}(-1)^{n+1}B_{2n}}{2\cdot(2n)!}$ formulákat is – ez utóbbit Euler fedezte fel 1755-ben –, de erről nem tesz említést. Ezekben a formulákban B_n-ek a Bernoulli számokat jelölik.

Ír a ζ függvény analitikus kiterjesztéséről és a kiegészített ζ függvényről – ez utóbbit $\xi(s)$-sel jelölt, és a következőképpen definiálta:

$$\xi(s) = \Gamma\left(\frac{s}{2}\right)(s-1)\pi^{-\frac{s}{2}}\zeta(s),$$

ahol $\Gamma\left(\frac{s}{2}\right)$ miatt a zérushelyek, $s-1$ miatt pedig a pólus tűnik el, és melyre $\xi(s) = \xi(1-s)$, és ha $\xi(s) = 0$, akkor $0 \leq \mathrm{Re}\ s \leq 1$. Nagyon valószínűnek tartotta, hogy ζ zérushelyeinek valós része $\frac{1}{2}$, de ezt nem bizonyította be, mivel nem ez volt a célja ebben a cikkben. Ezt a mai napig be nem bizonyított állítást Riemann-sejtésnek hívják. Ezt a sejtést Hilbert 1900-ban a 23 problémából álló listájára vette, majd 2000-ben a milleniumi problémák közé sorolták. Ez utóbbi miatt bizonyítását egymillió dollárral díjazzák.

Ebben a cikkében Riemann a prímszámtétel bizonyításáról is ír. Ő egy $J(x)$-szel (eredetileg $f(x)$-szel) jelölt prímszámláló függvényt vett, ami a következőképpen néz ki:

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

és ennek a kapcsolatát tekintette a ζ függvénnyel. Ez a következő:

$$\log\zeta(s) = s\int_0^\infty J(x)x^{-s-1}dx, \tag{2}$$

ha $\mathrm{Re}\, s > 1$. Erre a Fourier inverziós formulát alkalmazva kapta, hogy ha $\sigma > 1$, akkor

$$J(x) = \frac{1}{2\pi i} \int_{\sigma - i\infty}^{\sigma + i\infty} \log \zeta(s) x^s \frac{ds}{s}. \tag{3}$$

Ebből a ξ függvény szorzatalakját felhasználva, melynek bizonyítása hiányos – ezt Hadamard tette teljessé 1893-ban –, kapta $J(x)$ explicit formuláját, mely a következő:

$$J(x) = \mathrm{Li}(x) - \sum_{\mathrm{Im}\rho > 0} \left[\mathrm{Li}(x^\rho) + \mathrm{Li}(x^{1-\rho})\right] + \int_x^\infty \frac{dt}{t(t^2 \log t)} + \log \xi(0), \tag{4}$$

ahol $\mathrm{Li}(x) = \left(\int_0^{1-} + \int_{1+}^x\right) \frac{dt}{\log t}$. A $\sum_{\mathrm{Im}\rho > 0} [\mathrm{Li}(x^\rho) + \mathrm{Li}(x^{1-\rho})]$ egy nem megalapozott tagonkénti integrálással jön ki. Ennek a helyességét Landau igazolta 1908-ban, viszont Mangoldt 1895-ben a problémát megkerülve igazolta a formulát.

Természetesen Riemann célja az volt, hogy $\pi(x)$-re adjon explicit formulát. Ehhez segítségére volt a $J(x)$ és $\pi(x)$ függvények egy kapcsolata, nevezetesen az, hogy

$$J(x) = \pi(x) + \frac{1}{2}\pi(x^{\frac{1}{2}}) + \frac{1}{3}\pi(x^{\frac{1}{3}}) + \ldots + \frac{1}{n}\pi(x^{\frac{1}{n}}) + \ldots \tag{5}$$

Ebből a Möbius-féle inverziós formulával megkapta $\pi(x)$-re az alábbi képletet:

$$\pi(x) = J(x) - \frac{1}{2}J(x^{\frac{1}{2}}) - \frac{1}{3}J(x^{\frac{1}{3}}) - \frac{1}{5}J(x^{\frac{1}{5}}) + \frac{1}{6}J(x^{\frac{1}{6}}) \ldots + \frac{\mu(n)}{n}J(x^{\frac{1}{n}}) + \ldots \tag{6}$$

Az (5) és a (6) összefüggésekből kapott explicit formulát $\pi(x)$-re.

Ezután közel 30 évig szinte semmi eredmény nem volt a prímszámokkal kapcsolatban, egészen addig, míg Hadamard és de la Vallée Poussin be nem bizonyították a prímszámtételt, melyben Riemann ötletei kulcsfontosságúak.

5. Prímszámtétel

Hadamard 1893-ban ξ szorzatformuláját ténylegesen bizonyította. 1895-ben Mangoldt belátta $J(x)$ explicit formuláját, és egyszerűbb alakban is felírta, mert a $\frac{\zeta'}{\zeta}$ hányados szebben viselkedik, mint $\log\zeta$.

Hadamard és de la Vallée Poussin az alábbi tételt bizonyították egymástól függetlenül 1896-ban:

5.1. Tétel (Prímszámtétel)**.** *A $\pi(x)$ számelméleti függvény aszimptotikusan egyenlő az $\frac{x}{\log(x)}$ hányadossal.*

Ők komplex függvénytani segédeszközöket használtak. Mindketten Mangoldt (8) formulájának egy-egy variációját vezették le. Mangoldt és de la Vallée Poussin variánsa azért is különbözött, mert de la Vallée Poussin tévesen azt gondolta, hogy Mangoldt bizonyítása rossz.

Csebisev 1850-ben bevezette az alábbi $\psi(x)$ függvényt.

5.1. Definíció. A $\psi(x)$ számelméleti függvényt a következőképpen definiáljuk:

$$\psi(x) = \sum_{p^k \le x} \log p.$$

5.1. *Megjegyzés.* A $\psi(x)$ számelméleti függvényt a következőképpen is értelmezhetjük:

$$\psi(x) = \sum_{n \le x} \Lambda(n),$$

ahol $\Lambda(n)$ a Mangoldt-féle függvény.

A következő segédtételt és megfordítását Csebisev mutatta meg, melyet egyik 1850-es cikkében adott közre.

5.2. Segédtétel. *Ha $\psi(x)$ aszimptotikusan x, akkor $\pi(x)$ aszimptotikusan $\frac{x}{\log x}$.*

Bizonyítás. Tetszőleges p prímre 1 és x között $\left\lfloor \frac{\log x}{\log p} \right\rfloor$ darab p-hatvány van, így

$$\psi(x) = \sum_{p^k \le x} \log p = \sum_{p \le x} \log p \left\lfloor \frac{\log x}{\log p} \right\rfloor.$$

A fenti egyenletben az egészrészt elhagyva a $\psi(x)$ számelméleti függvényt tudjuk felülről becsülni. Ekkor a következőt kapjuk:

$$\psi(x) \le \sum_{p \le x} \log p \frac{\log x}{\log p} = \pi(x) \log x.$$

Ha $\psi(x)$ definíciójában csak a prímeket hagyjuk meg és a prímhatványokat elhagyjuk, akkor alsó becslését kapjuk a függvénynek:

$$\psi(x) \geq \sum_{p \leq x} \log p.$$

Legyen $\varepsilon > 0$ tetszőlegesen kicsi szám. Ekkor $\sum_{p \leq x} \log p$-t a következőképpen becsülhetjük alulról:

$$\sum_{p \leq x} \log p \geq \sum_{x^{1-\varepsilon} < p \leq x} \log p \geq (\pi(x) - \pi(x^{1-\varepsilon})) \log x^{1-\varepsilon}.$$

Mivel $\pi(x^{1-\varepsilon}) \leq x^{1-\varepsilon}$, ezért

$$(\pi(x) - \pi(x^{1-\varepsilon})) \log x^{1-\varepsilon} \geq (1-\varepsilon)\pi(x) \log x - (1-\varepsilon)x^{1-\varepsilon} \log x.$$

A fentiekből következik, hogy

$$\frac{\psi(x)}{x} \leq \frac{\pi(x) \log x}{x} \leq \frac{1}{1-\varepsilon} \frac{\psi(x)}{x} + \frac{\log x}{x^{\varepsilon}}. \tag{7}$$

Mivel $\frac{\psi(x)}{x}$ tart 1-hez, és $\frac{\log x}{x^{\varepsilon}}$ tart 0-hoz, ezért az egyenlőtlenség jobb oldala tart $\frac{1}{1-\varepsilon}$-hoz. Ebből következik, hogy minden pozitív ε-ra

$$1 \leq \liminf \frac{\pi(x) \log x}{x} \leq \limsup \frac{\pi(x) \log x}{x} \leq \frac{1}{1-\varepsilon}.$$

Mivel ε tetszőlegesen kicsi szám lehet, így a fenti összefüggésből következik, hogy

$$1 = \liminf \frac{\pi(x) \log x}{x} = \limsup \frac{\pi(x) \log x}{x} = 1.$$

Ebből következik, hogy létezik a határérték, és annak értéke 1, tehát

$$\lim \frac{\pi(x) \log x}{x} = 1.$$

□

5.2. *Megjegyzés.* A fenti bizonyításból könnyen belátható, hogy a segédtétel megfordítása is igaz, hiszen átrendezve az (7) egyenlőtlenséget, becslést kapunk $\frac{\psi(x)}{x}$-re:

$$\frac{(1-\varepsilon)\pi(x) \log x}{x} - \frac{(1-\varepsilon) \log x}{x^{\varepsilon}} \leq \frac{\psi(x)}{x} \leq \frac{\pi(x) \log x}{x}.$$

Ez alapján mondhatjuk, hogy az az állítás, hogy $\psi(x)$ aszimptotikusan x ekvivalens a prímszámtétellel.

A Riemann által megfogalmazott (2) kapcsolat von Mangoldt féle átfogalmazása a ζ függvény és $\psi(x)$ között, ha $\operatorname{Re} s > 1$, a következő:

$$\frac{-\zeta'(s)}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s} = \int_0^{\infty} \psi(x) \cdot s \cdot x^{-s-1} dx,$$

melyből az első egyenlőséget a 2.5. Lemmában beláttuk. A Fourier inverziós formulát alkalmazva erre Mangoldt az alábbit kapta, mely Riemann (3) formulájának felel meg:

$$\psi(x) = \frac{1}{2\pi i} \int_{\sigma-i\infty}^{\sigma+i\infty} \left(-\frac{\zeta'(s)}{s \cdot \zeta(s)} \cdot x^s \right) ds.$$

Komplex függvénytani eszközök segítségével a fentiből $\psi(x)$-re a következő négytagú összeget kapta, mely Riemann (4) formulájának felel meg:

$$\psi(x) = x - \sum_{\rho} \frac{x^\rho}{\rho} - \frac{1}{2} \log \left(1 - \frac{1}{x^2} \right) - \log 2\pi, \tag{8}$$

ahol ρ a ζ függvény kritikus sávban levő zérushelyein fut végig. Azt szeretnénk hogy ez az összeg aszimptotikusan egyenlő legyen x-szel, tehát, hogy x legyen a domináns tag. Ehhez korlátozni szeretnénk a $\sum_\rho \frac{x^\rho}{\rho}$ összeget, hogy lassabban tartson végtelenbe x-nél. Ha $\operatorname{Re} \rho < 1$, akkor $|x^\rho| = x^{\operatorname{Re} \rho} < x$, tehát $\frac{|x^\rho|}{x}$ konvergál a 0-hoz. A következő lemma segítségével – melyet Mertens alkalmazott 1898-as cikkében – belátjuk, hogy a $\operatorname{Re} \rho = 1$ egyenesen nincs zérushelye a ζ függvénynek.

5.1. Lemma. *Minden $x \in \mathbb{R}$ számra igaz a következő:*

$$3 + 4\cos x + \cos 2x \geq 0.$$

Bizonyítás. Tekintsük a következő trigonometrikus azonosságot:

$$\cos 2x = \cos^2 x - \sin^2 x = 2\cos^2 x - 1.$$

Ezt behelyettesítve a $3 + 4\cos x + \cos 2x$ kifejezésbe kapjuk, hogy

$$3 + 4\cos x + \cos 2x = 2 + 4\cos x + 2\cos^2 x = 2(1 + \cos x)^2 \geq 0.$$

□

5.3. Segédtétel. *A Riemann-féle ζ függvénynek nem esik zérushelye a* $\operatorname{Re} s = 1$ *egyenletű egyenesre, azaz minden t valós számra*

$$\zeta(1 + it) \neq 0.$$

Bizonyítás. Állításunkat indirekt módon fogjuk bebizonyítani. Ehhez feltesszük, hogy létezik olyan $t_0 \in \mathbb{R}$, amelyre

$$\zeta(1 + it_0) = 0.$$

Legyen $s = \sigma + it$ és tegyük fel, hogy $\operatorname{Re} s > 1$. Mivel a 7.2. Lemma alapján minden w komplex számra $\log |w| = \operatorname{Re} \log w$, ezért

$$\log |\zeta(s)| = \operatorname{Re} \log \zeta(s).$$

Tekintsük a $\zeta(s)$ függvényre az Euler-szorzatot:

$$\zeta(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}.$$

Az előbbiek és a logaritmus azonosságai alapján kapjuk a következőt:

$$\log |\zeta(s)| = \operatorname{Re} \log \zeta(s) = \operatorname{Re} \log \prod_p \left(1 - \frac{1}{p^s}\right)^{-1} = \operatorname{Re} \sum_p (-1) \log \left(1 - \frac{1}{p^s}\right).$$

A logaritmus hatványsora alapján

$$\operatorname{Re} \sum_p (-1) \log \left(1 - \frac{1}{p^s}\right) = \operatorname{Re} \sum_{p,k} \frac{1}{kp^{ks}}.$$

Minden $s = \sigma + it \in \mathbb{C}$ és $n \in \mathbb{N}$ esetén $n^s = n^\sigma(\cos(\log n \cdot t) + i \sin(\log n \cdot t))$. Ezt az $n = p^k$ esetben alkalmazva a fenti összeg tagjaira, a következőt kapjuk:

$$\operatorname{Re} \sum_{p,k} \frac{1}{kp^{ks}} = \sum_{p,k} \frac{1}{kp^{k\sigma}} \cos(t \log p^k).$$

Tehát

$$\log |\zeta(s)| = \sum_{p,k} \frac{1}{kp^{k\sigma}} \cos(t \log p^k). \tag{9}$$

Tekintsük a (9) egyenletet az $s = \sigma$, $s = \sigma + it$, illetve az $s = \sigma + 2it$ helyeken. A logaritmus azonosságait felhasználva kapjuk, hogy

$$\log |\zeta(\sigma)^3 \cdot \zeta(\sigma + it)^4 \cdot \zeta(\sigma + 2it)| = \sum_{p,k} \frac{1}{kp^{k\sigma}} (3 + 4\cos(t \log p^k) + \cos(2t \log p^k)).$$

Mivel az előző lemma alapján $3 + 4\cos(t \log p^k) + \cos(2t \log p^k) \geq 0$, ezért a fenti összeg nemnegatív lesz. Ebből következik, hogy ha $\sigma > 1$, akkor

$$|\zeta(\sigma)^3 \cdot \zeta(\sigma + it)^4 \cdot \zeta(\sigma + 2it)| \geq 1.$$

Legyen $t = t_0$ és σ tartson felülről 1-hez, és szorozzuk meg majd pedig osszuk el a fenti egyenlőtlenség bal oldalát $|\sigma - 1|^4$-nel. Ekkor rendezve kapjuk a következőt:

$$|(\sigma-1)(\zeta(\sigma)(\sigma-1))^3\left(\frac{\zeta(\sigma+it_0)}{\sigma-1}\right)^4\zeta(\sigma+2it_0)| \geq 1. \tag{10}$$

Ekkor, ha $\sigma \to 1$, akkor kapjuk a következő határértékeket:

(i) $(\sigma - 1) \to 0$,

(ii) mivel az $s = 1$ helyen a ζ függvénynek egyszeres pólusa van, és ott reziduuma egyenlő 1-gyel, így

$$\zeta(\sigma)(\sigma-1) \to 1.$$

A következő két pontban felhasználjuk, hogy a $\zeta(s)$ függvény analitikus folytatással kiterjeszthető az egész síkra kivéve az $s = 1$ helyen.

(iii) Tekintsük a következő hányadost: $\frac{\zeta(\sigma+it_0)}{\sigma-1}$. Ez valójában egy differenciahányados, hiszen a $\zeta(1 + it_0) = 0$ indirekt feltevést felhasználva kapjuk, hogy

$$\lim_{\sigma\to1}\frac{\zeta(\sigma+it_0)-0}{\sigma-1} = \lim_{\sigma\to1}\frac{\zeta(\sigma+it_0)-\zeta(1+it_0)}{\sigma-1} = \zeta'(1+it_0),$$

mely alapján

$$\left(\frac{\zeta(\sigma+it_0)}{\sigma-1}\right)^4 \to (\zeta'(1+it_0))^4,$$

(iv) végezetül pedig

$$\zeta(\sigma+2it_0) \to \zeta(1+2it_0).$$

Ez alapján a (10)-beli kifejezés tart $|0 \cdot 1 \cdot (\zeta'(1+it_0))^4 \cdot \zeta(1+2it_0)| = 0$-hoz, ami ellentmondáshoz vezet, tehát az indirekt feltevésünk hamis. Ebből következik, hogy az $1 + it$ egyenesen a ζ függvénynek nincs zérushelye. □

6. Érdekességek

A 17. században a matematikusok felfedeztek egy tesztet, amivel úgy gondolták, hogy egyértelműen el lehet dönteni egy n számról, hogy az prím-e vagy sem. Ehhez ki kell számítani, hogy mivel kongruens 2^n modulo n. Ha ez a szám 2, tehát

$$2^n \equiv 2 \pmod{n},$$

akkor az n szám prímszám. Viszont ez az elgondolás 1819-ben megbukott, hiszen bár 340-ig jól működik, 341-ről azt mondja hogy az prím, miközben $341 = 11 \cdot 31$.

Szintén ebben a században Fermat úgy gondolta, hogy minden n természetes számra $2^{2^n} + 1$ prím lesz, de ezúttal tévedett, ami ritka esetnek számított. Ezt a tévedést Euler vette észre először. Ő 1732-ben bebizonyította, hogy ez a képlet nem prímszámot ad, ha $n = 5$. Fermat a prímek egy másik nagyon különleges tulajdonságának feltárásában már jóval nagyobb sikerrel járt. 1640-ben Mersenne-nek levelet írt arról a felfedezéséről, hogy azok a prímek, melyek 4-gyel osztva 1-et adnak maradékul felírhatók két négyzetszám összegeként. Bár azt állította, hogy van rá bizonyítása, azt nem hagyta meg az utókornak.

Az alábbi tétel Wilsontól származik, de Edward Waring publikálta először 1770-ben és Lagrange bizonyította 1773-ban a megfordítással együtt.

6.1. Tétel (Wilson-tétel). *Az n szám akkor és csak akkor prím, ha*

$$(n-1)! \equiv -1 \pmod{n}.$$

Euler 1772-ben észrevette, hogy ha 0-tól 39-ig beírja az egész számokat az $x^2 + x + 41$ kifejezésbe, akkor prímszámok egy listáját kapja. Elkezdte érdekelni, hogy 41 helyett mely számok beírásával kap még ilyen sorozatot. Rájött, hogy a 41 mellett $r = 2, 3, 5, 11$ és 17 is választható és az $x^2 + x + r$ kifejezés csupa prímszámot ad, ha 0 és $r - 2$ közötti számokat írunk be. Szintén 1772-ben felfedezte, hogy az $x^2 - x + 1$ kifejezés prímet ad az $1, 2, 3, \ldots, 40$ helyeken. Legendre 1798-ban a következő lemmát mondta ki:

6.1. Lemma. *Az $x^2 - 79x + 1601$ polinom prímet ad az $0, 1, 2, \ldots, 79$ helyeken.*

1751-ben Euler így ír arról, hogy még neki sem sikerült megadnia olyan egyszerű képletet, mely az összes prímszámot megadná:

> „Vannak rejtélyek, amelyekbe az emberi elme sosem lesz képes behatolni. Bizonyságul elég egyetlen pillantást vetni a prímek táblázatára; látnunk kell, hogy abban nincs se rend, se semmiféle szabályosság.”

A következő tétel 1837-ből származik:

6.2. Tétel (Diriclet-tétel)**.** *Minden $a, a+b, a+2b, \ldots$ számtani sorozat, ahol a és b relatív prímek, végtelen sok prímszámot tartalmaz.*

Terence Tao 2004-ben Ben Greennel belátta, hogy a prímek sorozatában létezik tetszőlegesen hosszú számtani sorozat. Ez a Green-Tao-tétel. 8 évvel később, 2012-ben Tao igazolta a „gyenge" Goldbach-sejtés egy gyengített változatát, ami kimondja, hogy minden 5-nél nagyobb páratlan szám előáll legfeljebb öt prímszám összegeként. 2013-ban Harald Helfgott belátta apáratlan Goldbach-sejtést, vagyis, hogy minden 5-nél nagyobb páratlan szám előáll legfeljebb három prímszám összegeként

Valószínűleg már Euklidészben is megfogalmazódott az ikerprím-sejtés, mely kimondja, hogy végtelen sok olyan prímszámpár létezik, melyek között 2 a különbség. Ennek bizonyításában 2013 tavaszán nagy áttörés történt, melyet Yitang Zhang-nak köszönhetünk. Ő belátta, hogy a szomszédos prímek közötti távolság végtelen sokszor kisebb 70 milliónál. Ezt a korlátot a PolyMath8 nevezetű kutatócsoport, mely az interneten szerveződik Terence Tao vezetésével, 5000 alá csökkentette. Később pedig a PolyMath8b projekt keretében ezt a számot 246-ra csökkentették

7. Függelék (segédtételek és lemmák)

7.1. Definíció. A $\nu_p(n)$-nel jelölt függvény megadja a p prímszám kitevőjét n prímfelbontásában.

7.1. Segédtétel. *Bármely $n \in \mathbb{N}$-re igaz a következő:* $\nu_p(n!) = \sum_{i=1}^{\infty} \lfloor \frac{n}{p^i} \rfloor$.

Bizonyítás. Az első n természetes szám között a p-vel osztható számok száma összesen $\lfloor \frac{n}{p} \rfloor$. Minden p^2-edik szám osztható p második hatványával. Ezek száma összesen $\lfloor \frac{n}{p^2} \rfloor$, és így tovább. Ebből következik, hogy

$$\nu_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + ... = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor.$$

Ez az összeg pedig véges, mivel létezik $0 < j_0$ küszöbszám úgy, hogy minden $j > j_0$-ra a $\frac{n}{p^j}$ hányados kisebb lesz, mint egy, tehát egészrésze 0. □

7.2. Segédtétel. *Bármely $x \in \mathbb{R}$-re igaz a következő:* $\lfloor 2x \rfloor - 2\lfloor x \rfloor = \begin{cases} 1, & ha\ \{x\} \geq \frac{1}{2}; \\ 0, & ha\ \{x\} < \frac{1}{2}. \end{cases}$

Bizonyítás. Legyen $f(x) = \lfloor 2x \rfloor - 2\lfloor x \rfloor$. Először tegyük fel, hogy $\{x\} < \frac{1}{2}$. Ekkor $2x = 2\lfloor x \rfloor + 2\{x\}$, ahol $2\lfloor x \rfloor \in \mathbb{Z}$ és $2\{x\} \in [0,1)$, mivel $\{x\} \in [0, \frac{1}{2})$. Ebből következik, hogy $\lfloor 2x \rfloor = 2\lfloor x \rfloor$, tehát $f(x) = 0$, ha $\{x\} < \frac{1}{2}$.

Ezek után tegyük fel, hogy $\{x\} \geq \frac{1}{2}$. Ekkor $2x = 2\lfloor x \rfloor + 2\{x\}$, ahol $2\lfloor x \rfloor \in \mathbb{Z}$ és $2\{x\} \in [1,2)$, mivel $\{x\} \in [\frac{1}{2}, 1)$. Átalakítással kapjuk, hogy $2x = (2\lfloor x \rfloor + 1) + (2\{x\} - 1)$, ahol $(2\lfloor x \rfloor + 1) \in \mathbb{Z}$ és $(2\{x\} - 1) \in [0,1)$. Ebből $\lfloor 2x \rfloor = 2\lfloor x \rfloor + 1$, tehát $f(x) = 1$, ha $\{x\} \geq \frac{1}{2}$. □

7.3. Segédtétel. *Bármely $k \in \mathbb{N}$-re* $\binom{2k+1}{k} < \frac{2^{2k+1}}{2}$.

Bizonyítás. A Pascal háromszög $2k+1$-edik sorának összege

$$\binom{2k+1}{0} + \binom{2k+1}{1} + \ldots + \binom{2k+1}{k} + \binom{2k+1}{k+1} + \ldots + \binom{2k+1}{2k+1} = 2^{2k+1}.$$

A $\binom{2k+1}{i} = \binom{2k+1}{2k+1-i}$ azonosság szerint a fenti összeg fele

$$\binom{2k+1}{0} + \binom{2k+1}{1} + \ldots + \binom{2k+1}{k} = \frac{2^{2k+1}}{2}.$$

Ezt az összeget alulról becsülve az utolsó tagjával, azaz $\binom{2k+1}{k}$-val, kapjuk a bizonyítandó egyenlőtlenséget. □

7.4. Segédtétel. *Bármely $n \in \mathbb{N}$-re* $\binom{2n}{n} \geq \frac{2^{2n}}{2n}$.

Bizonyítás. Becsüljük a Pascal háromszög $2n$-edik sorának összegét felülről a következő módon: a sor két szélén levő 1-est hagyjuk meg, a többi elemét pedig cseréljük ki a sor legnagyobb számára, tehát $\binom{2n}{n}$-re. Így a következőt kapjuk:

$$\frac{2^{2n}}{2n} \leq \frac{1+1+(2n-1)\binom{2n}{n}}{2n} = \frac{2+(2n-1)\binom{2n}{n}}{2n}.$$

Tehát elegendő belátni, hogy

$$\frac{2+(2n-1)\binom{2n}{n}}{2n} \leq \binom{2n}{n}.$$

A fenti egyenlőtlenség ekvivalens azzal, hogy

$$2 \leq \binom{2n}{n},$$

ami minden $n \geq 1$-re igaz. □

7.1. Lemma.

(1) Ha $x > e$, akkor $\frac{x}{\log x}$ szigorúan monoton növő.

(2) Ha $x \to \infty$, akkor $\frac{x}{\log x} \to \infty$.

(3) Ha $x \to \infty$, akkor minden $\delta > 0$-ra

$$\frac{\frac{x}{\log x}}{\frac{x+\delta}{\log(x+\delta)}} \to 1.$$

Bizonyítás. (1) Deriváljuk a függvényt:

$$\left(\frac{x}{\log x}\right)' = \frac{\log x - x\frac{1}{x}}{\log^2 x} = \frac{\log x - 1}{\log^2 x}.$$

Ha a derivált pozitív, akkor az eredeti függvény monoton növő. A nevező mindig pozitív, így csak a számlálót kell megvizsgálnunk, az pedig akkor lesz pozitív, ha $x > e$. Ebből következik, hogy $\frac{x}{\log x}$ monoton növő, ha $x > e$.

(2) Tekintsük $\frac{x}{\log x}$ határértékét, ha $x \to \infty$. Mivel $\frac{x}{\log x}$ ilyenkor $\frac{\infty}{\infty}$ alakú, így a L'Hopital-szabályt alkalmazva

$$\lim_{x\to\infty} \frac{x}{\log x} = \lim_{x\to\infty} \frac{1}{\frac{1}{x}} = \lim_{x\to\infty} x = \infty.$$

(3) Legyen $\delta > 0$ tetszőlegesen kicsi pozitív szám. Tekintsük $\frac{\frac{x}{\log x}}{\frac{x+\delta}{\log(x+\delta)}}$ határértékét ha $x \to \infty$. Ehhez alakítsuk át a törtet a következő módon:

$$\frac{\frac{x}{\log x}}{\frac{x+\delta}{\log(x+\delta)}} = \frac{x \log(x+\delta)}{(x+\delta)\log x}.$$

Mivel a fenti tört $\frac{\infty}{\infty}$ alakú, így a L'Hopital-szabályt alkalmazva kapjuk a következőt:

$$\lim_{x\to\infty} \frac{x \log(x+\delta)}{(x+\delta)\log x} = \lim_{x\to\infty} \frac{\log(x+\delta) + \frac{x}{x+\delta}}{\log x + \frac{x+\delta}{x}}.$$

Ez még mindig $\frac{\infty}{\infty}$ alakú, így a L'Hopital-szabály újbóli alkalmazásával az alábbi következik:

$$\lim_{x\to\infty} \frac{\log(x+\delta) + \frac{x}{x+\delta}}{\log x + \frac{x+\delta}{x}} = \lim_{x\to\infty} \frac{\frac{x+2\delta}{(x+\delta)^2}}{\frac{x-\delta}{x^2}} = \lim_{x\to\infty} \frac{(x+2\delta)x^2}{(x+\delta)^2(x-\delta)} = 1.$$

□

7.2. Lemma. *Legyen $s = \sigma + it$ egy tetszőleges komplex szám, és legyen $w = e^s$. Ekkor igazak a következők:*

(i) $w = e^{\sigma}(\cos t + i \sin t)$, *melyből következik, hogy* $|w| = e^{\sigma}$,

(ii) *minden* $n \in \mathbb{N}$*-re* $n^s = e^{\log n \cdot s} = n^{\sigma}(\cos(\log n \cdot t) + i \sin(\log n \cdot t))$,

(iii) $s = \log w = \sigma + it = \log|w| + i \arg w$, *amiből következik, hogy* $\log|w| = \operatorname{Re}\log w$.

Hivatkozások

[1] Csebisev, P. L.: *Sur la fonction qui détermine la totalité des nombres premiers inferieurs à une limite donnée.* J. Math. Pures Appl., **17**, 1848

[2] Csebisev, P. L.: *Mémoire sur les nombres premiers.* J. Math. Pures Appl., **17**, 1852

[3] Edwards, H. M.: *Riemann's Zeta Function.* Dover Publications, Inc., Mineola, New York, 1974

[4] Erdős Pál: *Beweis eines Satzes von Tschebyschef.* Acta Litt. Sci., Szeged, **5**, 194-198, 1932

[5] Euler, L.: *Variae observationes circa series infinitas.* Comm. Acad. Sci. Petropolitanae, **9**, 222-236, 1737

[6] Euler, L.: *Introductio in Analysin Infinitorum.* Chapter 15. Bousquet and Socios., Lausanne, 1748 („Opera" (1), Vol. 8.)

[7] C. F. Gauss levele Enke-nek, 1849. December 24. „Werke," Vol. II, pp. 444-447.

[8] Hadamard, J.: *Sur la distribution des zeros de la fonction $\zeta(s)$ et ses consequences arithmétiques.* Bull. Soc. Math. France, **24**, 199-220, 1896

[9] Legendre, A. M.: *Théorie des Nombres.* 4th ed., Vol. 2, 4th Pt., §VIII Paris, 1830

[10] von Mangoldt, H.: *Zu Riemann's Abhandlung 'Ueber die Anzhal der Primzahlen unter einer gegebenen Grösse'.* J. Reine Angew. Math., **114**, 255-305, 1895

[11] Riemann, B.: *Ueber die Anzahl der Primzahlen unter einer gegebenen Grösse.* 1859

[12] du Sautoy, M: *A prímszámok zenéje.* Park Könyvkiadó, 2014

[13] de la Vallée Poussin, C.-J.: *Recherches analytiques sur la théorie des nombres (premiére partie).* Ann. Soc. Sci. Bruxelles, $\mathbf{20}_2$, 183-256, 1896

Alulírott Szabó Lilla kijelentem, hogy a szakdolgozatban foglaltak a saját munkám eredményei, és csak a hivatkozott forrásokat (szakirodalom, eszközök, stb.) használtam fel. Tudomásul veszem, hogy szakdolgozatomat a Szegedi Tudományegyetem könyvtárában a kölcsönözhető könyvek között helyezik el, és az interneten is nyilvánosságra hozhatják.

2014. december 01. Szabó Lilla