PRÍMEK, POLIGNAC, POLYMATH

HARCOS GERGELY

1. HALÁSZÁS A PRÍMEKRE

A prímszámok rejtélyes viselkedése és a matematikában betöltött központi szerepe az ókori idők óta foglalkoztatja az embereket. Az elmúlt 10 évben több rendkívüli áttörést láttunk ezen a területen, amik korábban elérhetetlennek tűntek [10, 8, 32, 14, 6, 15, 7]. Ebben a cikkben az ikerprímsejtés körüli izgalmas fejleményekre koncentrálunk, hangsúlyozva a tételek mögötti alapgondolatokat.

Euklidész már az *Elemek* című művében (IX. könyv, 20. állítás) leírta a mindannyiunk által tanult bizonyítást, miszerint végtelen sok prímszám van. A szomszédos prímszámok közötti távolságok az első különbségtől eltekintve párosak, és talán már Euklidész megfigyelte, hogy ez a különbség gyakran 2, legalábbis a sorozat elején:

$$(3,5),\ (5,7),\ (11,13),\ (17,19),\ (29,31),\ (41,43),\ (59,61),\ (71,73),\ \dots$$

Az ilyen prímeket *ikerprímeknek* nevezzük, és azt sejtjük, hogy végtelen sok van belőlük:

Ikerprímsejtés. *A $p-p'=2$ egyenletnek végtelen sok megoldása van prímekben.*

Általánosabban, Polignac [19] azt sejtette, hogy minden páros szám végtelen sokszor előfordul két szomszédos prímszám közötti távolságként, ami motiválja a következő fogalmat.

1. definíció. A d pozitív egészt *Polignac-számnak* nevezzük, ha a $p-p'=d$ egyenletnek végtelen sok megoldása van prímekben. A Polignac-számok halmazát jelölje $\mathscr{D}$.

A definícióban nem követeljük meg, hogy p és p' szomszédos prímszámok legyenek. Polignac sejtéséből következik, hogy $\mathscr{D}$ a pozitív páros számok halmaza, de egészen tavalyig azt sem tudtuk, hogy $\mathscr{D}$ nem üres-e.

1. tétel (Zhang [32])**.** *Létezik Polignac-szám, azaz $\mathscr{D}\neq\emptyset$.*

A tétel bizonyítása a probléma egy újszerű megközelítésén alapul, amit eredetileg Goldston, Pintz, Yıldırim [8] fejlesztett ki Heath-Brown [12] egy korábbi ötletére alapozva. A klasszikus megközelítésben egy konkrét d pozitív páros számról (pl. $d=2$) igyekszünk kimutatni, hogy Polignac-szám, azaz hogy végtelen sok n pozitív egészre az n és az $n+d$ is prímszám. Felfoghatjuk ezt egyfajta prímhalászásnak, amiben két kézzel – amik adott távolságra vannak egymástól – próbálunk két prímet fogni úgy, hogy az egész számok különböző helyein próbálkozunk. A [8] cikk alapötlete, hogy a prímhalászást ne puszta kézzel, hanem halászhálóval – egy $\mathscr{H}$ véges halmaz eltoltjaival – végezzük. Ezáltal jobb esélyünk van arra, hogy két egymáshoz közeli prímet fogjunk, de cserébe azok távolsága már nem egy konkrét d lesz, hanem a $\mathscr{H}$-ban fellépő különbségek egyike. A [8] cikk központi észrevétele, hogy a prímszámoknak bizonyos maradékosztályokban való nagyon egyenletes eloszlása mellett a vázolt prímhalászás hatékonnyá tehető. Motohashi és Pintz [16] a szükséges hipotézist jelentősen gyengítette, és Zhang [32] ezt bizonyította bravúrosan.

Az 1. tétel szenzációs bejelentését követően Terence Tao vezetésével elindult a Polymath8 elnevezésű internetes kutatási projekt, amibe bárki szabadon bekapcsolódhatott, pl. magyar részről Pintz János mellett a szerző is részt vett benne. A projekt célja Yitang Zhang munkájának megértése, elemzése és a kvantitatív aspektusainak optimalizálása volt

– ennek eredményeit a [20] cikk tartalmazza. Időközben – újabb drámai fordulatként – Heath-Brown fiatal tanítványa, James Maynard továbbfejlesztette a [8]-ban szereplő szitát – tehát hogy hol érdemes kivetni a hálót –, és ezáltal a [16]-ban megfogalmazott egyenletes eloszlási hipotézisre sem volt szüksége. Ily módon Maynard [14] új bizonyítást adott a Zhang-tételre, sőt azt is belátta, hogy kellően nagy halászhálóval akármilyen előírt véges számú prímet foghatunk, nem csak kettőt. Hasonló észrevételeket tett a blogján Tao is [29], majd a Polymath8 projekt folytatódott a Maynard–Tao-tétel továbbfejlesztésével [21].

2. Milyen hálóval halásszunk?

Az 1. tétel bizonyításának alapötlete a [8] cikkben szerepel:

1. ötlet. *Legyen $\mathscr{H}=\{h_1,\dots,h_k\}$ egy egész számokból álló k elemű halmaz. Próbáljunk végtelen sok n pozitív egészt találni úgy, hogy az $n+\mathscr{H}=\{n+h_1,\dots,n+h_k\}$ eltolt halmaz minél több prímet tartalmazzon.*

A szakirodalomban valóban a $\mathscr{H}$ jelölés terjedt el a fenti halmazra, ezért a halászháló metafora többszörösen helyénvalónak tűnik. A továbbiakban az elemeket nagyságrendi sorrendben számozzuk: $h_1<\dots<h_k$. Persze rögtön látjuk, hogy nem minden k elemű halmaz felel meg egyaránt a prímhalászás céljára. Pl. a $k=2$ esetben $\mathscr{H}=\{0,1\}$ eleve rossz, mert n és $n+1$ közül az egyik mindig páros, tehát $n>2$ esetén csak az egyikük lehet prím. A $\mathscr{H}=\{0,2\}$ jobb ebből a szempontból, hiszen az ikerprímsejtés szerint n és $n+2$ egyszerre prím végtelen sok n-re. Hasonlóan, a $k=3$ esetben a 2 és a 3 szerinti maradékokat nézve látjuk, hogy $\mathscr{H}=\{0,2,3\}$ vagy $\mathscr{H}=\{0,2,4\}$ nem kifejezetten jó háló gyanánt, hiszen ezek eltoltjaiban legfeljebb csak két prím van, ha $n>3$. Ellenben a $\mathscr{H}=\{0,2,6\}$ eltoltjaira nem tudunk semmiféle okot, ami megakadályozná, hogy mindhárom eleme prím legyen végtelen sokszor. Ez motiválja az alábbi fogalmat.

2. definíció. A $\mathscr{H}=\{h_1,\dots,h_k\}$ egész számokból álló k elemű halmaz *megengedett*, ha semmilyen $m\geqslant 2$ egészre nézve nem tartalmaz teljes maradékrendszert.

Persze rögtön látjuk, hogy ha egy k elemű $\mathscr{H}$ halmaz tartalmaz teljes maradékrendszert valamilyen $m\geqslant 2$ egészre nézve, akkor $m\leqslant k$, vagyis $\mathscr{H}$ tartalmaz teljes maradékrendszert valamilyen $p\leqslant k$ prímszámra nézve is – nevezetesen az m bármely prímosztójára nézve. Tehát a fenti definícióban nem vesztünk semmit, ha feltesszük, hogy $m\leqslant k$ prímszám. Ez mutatja, hogy minden k-ra van megengedett k elemű halmaz, pl. a k utáni első k darab prímszám halmaza.

Az 1. ötletnek komoly támogatást ad Dickson [2] egy sejtése, illetve annak Hardy-tól és Littlewoodtól származó kvantitatív formája [11]:

Dickson–Hardy–Littlewood-sejtés. *Legyen $\mathscr{H}$ egy megengedett halmaz. Ekkor végtelen sok n pozitív egészre az $n+\mathscr{H}$ eltolt halmaz minden eleme prímszám.*

A sejtés persze nem mondja meg, az n-et miként válasszuk meg, hogy az $n+\mathscr{H}$ összes eleme, vagy akár csak két eleme prím legyen. A metaforánkkal élve: hiába van hálónk, ha nem tudjuk, hova vessük ki, tehát hol gazdag halban a víz. Pl. ha az n-et valamilyen nagy x körül az egyenletes eloszlás szerint véletlenszerűen választjuk, akkor az $n+\mathscr{H}$ halmazba átlagosan csak kb. $|\mathscr{H}|/\log x$ prímszám fog esni, mert ebben a tartományban átlagosan kb. $\log x$ távolságra vannak a prímszámok egymástól. Tehát ha x nagy, akkor ezen a naiv módon átlagosan közel nulla darab prímet fogunk kihalászni, nemhogy kettőt vagy többet. Itt és a továbbiakban $\log x$ a természetes logaritmust jelöli, az analitikus számelméletben megszokott módon. Az n ügyes megválasztásával, avagy a rossz n-ek „kiszitálásával” kell ellensúlyozni azt a tényt, hogy a prímszámok sorozata egyre ritkul. Ennek módja már Goldston, Pintz, Yıldırım [8] cikkében szerepel, de Zhang [32] bizonyította először, hogy így legalább két prímszám garantálható egy alkalmas megengedett halmaz végtelen sok eltoltjában. Maynard [14] még ügyesebben szitálja az n-et, ami által akár száz prímet is tud garantálni végtelen sok $n+\mathscr{H}$ alakú eltoltban.

2. tétel (Zhang [32]). *Létezik egy k pozitív egész az alábbi tulajdonsággal. Ha $\mathscr{H}$ egy k elemű megengedett halmaz, akkor végtelen sok n pozitív egészre az $n+\mathscr{H}$ eltolt halmazba legalább két prímszám esik.*

A tételből azonnal következik, hogy ha $\mathscr{H} = \{h_1, \dots, h_k\}$ egy megfelelő halmaz, akkor a fellépő $h_j - h_i$ $(i < j)$ különbségek egyike Polignac-szám, hiszen $n+h_i$ és $n+h_j$ különbsége $h_j - h_i$. Tehát ha az a cél, hogy $\mathscr{D}$-ben minél kisebb elem létezését garantáljuk, akkor a tételbeli $\mathscr{H}$-t kell minél kisebb átmérőjűnek választani. Ehhez első lépésben a tételbeli k-t kell minimalizálni, majd ahhoz kell megtalálni a legjobb $\mathscr{H}$-t. Ilyen típusú optimalizálással telt a Polymath8 projekt jelentős része [20, 21]. Az alábbi táblázatban összefoglaljuk, hogy az 1-2. tételek numerikus variánsai miként fejlődtek.

forrás	$k=$	$\min \mathscr{D} \leqslant$
Zhang [32]	3.5×10^6	7×10^7
Polymath8a [20]	632	4680
Maynard [14]	105	600
Polymath8b [21]	50	246

A táblázat utolsó sora szerint van egy 50 elemű $\mathscr{H} \subset \{0, 2, \dots, 246\}$ megengedett halmaz, aminek eltoltjaiban végtelen sokszor található két prímszám. Az 50 elem részletesen fel van sorolva a [21] cikk 76. oldalán. Tehát $\mathscr{D}$-ben mindenképpen van legfeljebb 246 nagyságú páros szám, de konkrét elemet megnevezni nem tudunk. Ilyen konkrét elem megtalálása a jelenlegi módszerekkel reménytelennek tűnik: a probléma valószínűleg az ikerprímsejtéssel megegyező nehézségű. Mindazonáltal a $\mathscr{D}$-ről a fenti eredmények jóval többet elmondanak, amint az a következő fejezetből kiderül.

3. A Polignac-számok sűrűsége

Pintz János ismerte fel a 2. tétel azon következményét, hogy a Polignac-számok a természetes számok egy – csak a k-tól függő – pozitív hányadát elfoglalják, továbbá a szomszédos Polignac-számok közötti távolság korlátos. Az eredményt a közelmúltban finomította Granville, Kane, Koukoulopoulos, Lemke Oliver, és mi ebben a formában mondjuk ki és bizonyítjuk.

3. tétel (Pintz et al. [18, 9]). *Végtelen sok Polignac-szám létezik. Pontosabban:*

(a) *A $\mathscr{D} \subset \mathbb{N}$ halmaz aszimptotikus alsó sűrűsége*

$$\underline{d}(\mathscr{D}) \geqslant \frac{1}{k-1} \prod_{p \leqslant k} \left(1 - \frac{1}{p}\right),$$

ahol k mint a 2. tételben, és a szorzás a prímeken fut végig.

(b) *Létezik $m \in \mathbb{N}$ úgy, hogy minden $n \in \mathbb{N}$ esetén $\mathscr{D} \cap \{n, n+1, \dots, n+m\} \neq \emptyset$.*

Bizonyítás. A jelzett becslés a k csökkentésével erősödik, ezért feltehető, hogy k a legkisebb egész, ami a 2. tételbeli állítást kielégíti. Ekkor persze $k \geqslant 2$, és a feltétel szerint létezik egy $k-1$ elemű $\mathscr{H} = \{h_1, \dots, h_{k-1}\}$ megengedett halmaz, aminek $n+\mathscr{H}$ eltoltjában legfeljebb csak egy prímszám van, ha n kellően nagy. Legyen most $h > h_{k-1}$ olyan egész, amivel $\mathscr{H} \cup \{h\}$ egy k elemű megengedett halmaz, ekkor végtelen sok $n + (\mathscr{H} \cup \{h\})$ eltoltban található két prímszám. A $\mathscr{H}$ tulajdonsága miatt szükségszerű, hogy valamilyen $1 \leqslant j \leqslant k-1$ indexre és végtelen sok n-re az $n+h_j$ és az $n+h$ egyszerre prím, vagyis $h - h_j \in \mathscr{D}$. A $h > h_{k-1}$ egészre tett feltevés csak annyi megkötést jelent, hogy ha egy $p \leqslant k$ prímszámra nézve $\mathscr{H}$ mod p már tartalmaz $p-1$ különböző maradékot, akkor h mod p is ezen $p-1$ maradékok egyike kell, hogy legyen. A kínai maradéktétel alapján tehát megadható $\prod_{p \leqslant k}(p-1)$ darab maradékosztály modulo $\prod_{p \leqslant k} p$ úgy, hogy ha $h > h_{k-1}$

ezek uniójából való, akkor a $h-h_1,\dots,h-h_{k-1}$ különbségek egyike Polignac-szám. Innen már könnyű meggondolással következik az (a) és a (b) állítás, pl. az utóbbiban vehető $m:=h_{k-1}-h_1+\prod_{p\leqslant k}p$. □

Ahogy a [9] cikk szerzői is megjegyzik, az (a) állításban vehető a már igazolt $k=50$ érték [21], és ezzel a $\underline{d}(\mathscr{D})>\frac{1}{354}$ becslést kapjuk a Polignac-számok aszimptotikus alsó sűrűségére. Tehát átlagosan minden 354 egymás utáni számra jut egy Polignac-szám, míg az első Polignac-szám legfeljebb 246. Ezzel szemben a szomszédos Polignac-számok közötti legnagyobb távolságra a fentihez hasonló formális érveléssel nem tudunk konkrét értéket szolgáltatni, aminek oka a következő. Adott M pozitív egészre van olyan $\mathscr{E}\subset\mathbb{N}$ halmaz, amiben az M végtelen sokszor fellép két szomszédos elem távolságaként, miközben bármely megengedett $\{h_1,h_2,h_3\}$ hármas esetén az $\mathscr{E}$ tartalmazza a h_2-h_1, h_3-h_2, h_3-h_1 különbségek egyikét. Pl. $\mathscr{E}$-nek vehetjük azon természetes számok halmazát, amik modulo $3M$ kongruensek egy legfeljebb M abszolút értékű egész számmal. Tehát ha a 2. tételből csak annyit használunk fel, hogy minden k elemű megengedett $\mathscr{H}$ halmazra a $\mathscr{D}$ tartalmazza két $\mathscr{H}$-beli elem különbségét, akkor még $k=3$ esetén is szóba jön a $\mathscr{D}=\mathscr{E}$ lehetőség, amikor is a (b) állítás csak $m\geqslant M$ mellett igaz.

4. A HALÁSZÁS MŰVÉSZETE

Mint láttuk, a 2. tételből következik az 1. tétel, illetve sok egyéb értékes információ a Polignac-számok eloszlására vonatkozóan. A 2. tétel bizonyításának alapötlete szintén a [8] cikkben szerepel, és elnagyoltan annyit tesz, hogy megpróbáljuk előre megtippelni, hogy mely $n+\mathscr{H}$ alakú eltolt halmazokban várható az átlagosnál jóval több prímszám. Ezt jól csinálni egyfajta művészet, hiszen egyensúlyozni kell aközött, ami igaz és amit bizonyítani tudunk. Ha túl direkt módon választjuk ki a potenciálisan jó eltoltakat, akkor a várakozásunkat nem fogjuk tudni igazolni, ha pedig túl megengedőek vagyunk, akkor az eltoltakba nem esik majd elég prímszám. Formálisan az 1. ötlet egy valószínűségi finomításáról van szó:

2. ötlet. *Legyen $\mathscr{H}=\{h_1,\dots,h_k\}$ egy k elemű megengedett halmaz. Minden elég nagy $x>0$ számra találjunk olyan valószínűségi mértéket az $x\leqslant n\leqslant 2x$ egészeken, amire nézve az $n+\mathscr{H}=\{n+h_1,\dots,n+h_k\}$ eltolt halmazba eső prímek számának várható értéke egynél nagyobb.*

A gyakorlatban ez annyit tesz, hogy olyan $\nu(n)\geqslant 0$ súlyokat keresünk, amikre bizonyíthatóan fennáll

$$\sum_{x\leqslant n\leqslant 2x}\nu(n)\sum_{i=1}^{k}1_{n+h_i\text{ prím}}>\sum_{x\leqslant n\leqslant 2x}\nu(n). \tag{1}$$

Vegyük észre, hogy az egyenlőtlenség csak úgy teljesülhet, ha a jobb oldali összeg pozitív, és akkor ezzel az összeggel leosztva a $\nu(n)$ súlyok egy valószínűségi mértékké normálódnak. Az egyenlőtlenségből következik, hogy valamilyen $x\leqslant n\leqslant 2x$ egészre a belső összeg egynél nagyobb, tehát az $n+\mathscr{H}$ eltolt halmazba legalább két prímszám esik. Ha ez minden elég nagy $x>0$ számra fennáll, akkor a 2. tételbeli állítás igaz a $\mathscr{H}$-ra.

A súlyokat úgy érdemes megválasztani, hogy $\nu(n)$ várhatóan akkor legyen nagy, amikor az $n+h_1,\dots,n+h_k$ számok között sok a prím vagy legalábbis kevés prímosztójuk van együttesen. A legnaivabb választást a már említett Dickson–Hardy–Littlewood-sejtés adja:

$$\nu(n):=1_{n+h_1,\dots,n+h_k\text{ prím}}.$$

Ezek a súlyok a gyakorlatban nemigen használhatók, mert ha tudnánk, hogy az (1) jobb oldala minden elég nagy x-re pozitív, akkor rögtön a Dickson–Hardy–Littlewood-sejtést is igazoltuk volna. Vezessük be a

$$P(n):=(n+h_1)\dots(n+h_k)$$

jelölést, ekkor a [8]-beli súlyokhoz közelebb álló, de még mindig naiv változat a

$$\nu(n) := 1_{P(n) \text{ prímosztóinak száma legfeljebb } k+\ell},$$

ahol $0 \leqslant \ell \leqslant k$ egy szabadon választható paraméter. Ennek egy analitikus variánsa

$$\nu(n) := \sum_{d|P(n)} \mu(d) \log^{k+\ell}\left(\frac{P(n)}{d}\right), \tag{2}$$

ahol a $\mu(d)$ ún. *Möbius-függvény* a logikai-szitából jól ismert ± 1 súlyok megjelenése a prímszámok elméletében (vö. Eratosztenész-szita):

$$\mu(d) := \begin{cases} +1, & \text{ha } d \text{ páros sok különböző prímszám szorzata;} \\ -1, & \text{ha } d \text{ páratlan sok különböző prímszám szorzata;} \\ 0, & \text{ha } d \text{ nem négyzetmentes.} \end{cases}$$

Nem triviális, de a (2)-beli súlyokra teljesül

$$0 \leqslant \nu(n) \leqslant \log^{k+\ell}(P(n)),$$

továbbá $\nu(n)$ akkor és csak akkor pozitív, ha $P(n)$ különböző prímosztóinak száma legfeljebb $k+\ell$.

Goldston, Pintz, Yıldırım [8] és ezáltal Zhang [32] sikere nagy részben a (2)-beli naiv súlyok egy megfelelő finomításán múlik, ami lehetővé teszi az (1) két oldalának aszimptotikusan pontos kiszámítását. A finomítás Selberg [25] úttörő munkájának gyümölcse, amit a [8] merőben újszerű módon használ, bár a szerzők elismerik, hogy az ötlet részben Heath-Browntól [12] származik. A Selberg-szita abból indul ki, hogy ne az összes, hanem csak a $d \leqslant R$ feltételt kielégítő négyzetmentes számokkal szitáljunk, ahol R egy szabadon választható „levágási paraméter". A $d \leqslant R$ megszorítással a súlyok nemnegativitása már nehezen garantálható, ezért azokat még négyzetre is emeljük. A [8, 32] dolgozatokban konkrétan használt súlyfüggvény

$$\nu(n) := \left(\sum_{d|P(n)} \mu(d) \log_+^{k+\ell}\left(\frac{R}{d}\right)\right)^2, \tag{3}$$

ahol $R := x^{\theta/2}$ valamilyen rögzített $\theta > 0$ mellett. Itt $\log_+ t := \max(\log t, 0)$, tehát az összegben csak a $d \leqslant R$ osztók vesznek részt. Ezeket a súlyokat érdemes megszorítani azokra az n-ekre, amikre $P(n)$ mentes a nagyon kicsi prímosztóktól. Ennek egyik oka, hogy az ilyen n-ekre az $n+h_1, \ldots, n+h_k$ tényezők páronként relatív prímek, másrészt így az (1) két oldalának aszimptotikus kiszámításában a kis prímekből származó ún. lokális faktorok elhagyhatók. Mi a továbbiakban feltesszük, hogy $P(n)$ minden prímosztója legalább $\log\log\log x$, a többi n-re a $\nu(n)$-t nullának vesszük. A (3)-beli súlyfüggvény egy arányossági tényezőtől eltekintve nem más, mint

$$\nu(n) := \left(\sum_{d|P(n)} \mu(d) \left(1 - \frac{\log d}{\log R}\right)_+^{k+\ell}\right)^2, \tag{4}$$

ahol értelemszerűen $(1-t)_+ := \max(1-t, 0)$. Egy fontos általánosítást javasolt és vizsgált először Soundararajan [27, 28]:

$$\nu(n) := \left(\sum_{d|P(n)} \mu(d) g\left(\frac{\log d}{\log R}\right)\right)^2, \tag{5}$$

ahol $g : \mathbb{R} \to \mathbb{R}$ egy kellően sima függvény, ami a $[0,1]$ intervallumon kívül nulla. Ezek az általánosabb súlyok lehetővé tették a [8, 32]-beli eredmények jelentős élesítését [5, 20], és megnyitották az utat az újabb felfedezések felé [14, 21].

5. Az átlagos kapás

Egy $\mathscr{H}$ megengedett halmazra az (1) bal és jobb oldalának hányadosa adja meg, hogy az $n+\mathscr{H}$ $(x\leqslant n\leqslant 2x)$ eltoltakba átlagosan hány prímszám esik, ha az átlagolást a $\nu(n)$ súlyokkal végezzük. Ez a hányados hatékonyan kiszámítható az (5) alakú súlyokra, feltéve, hogy a prímszámok bizonyos maradékosztályokban kellően egyenletesen oszlanak el. Az egyenletes eloszlás az (1) bal oldalának számítása közben merül fel, mégpedig a következőképpen. Az (5)-öt használva az (1) bal oldala

$$\sum_{i=1}^{k}\sum_{d,d'\leqslant R}\mu(d)\mu(d')g\left(\frac{\log d}{\log R}\right)g\left(\frac{\log d'}{\log R}\right)\sum_{\substack{x\leqslant n\leqslant 2x\\ [d,d']\mid P(n)}}1_{n+h_i\text{ prím}},$$

ahol $[d,d']$ a d és a d' legkisebb közös többszöröse, tehát a $[d,d']\mid P(n)$ reláció annyit tesz, hogy d és d' a $P(n)$ osztója. Pontosabban itt csalunk egy kicsit, de ez a lényeget nem érinti: a belső összegben csak azok az n-ek szerepelnek, amikre $P(n)$ minden prímosztója legalább $\log\log\log x$. A belső összeg olyan – nagyjából x és $2x$ közötti – prímek számát adja meg, amik modulo $q:=[d,d']$ egy nem túl nagy számú adott maradékosztályba esnek. A külső összegzésben a négyzetmentes $d,d'\leqslant R$ számok vesznek részt, ezért $q\leqslant R^2=x^\theta$ is négyzetmentes. A továbblépéshez célszerű feltenni, hogy az x és $2x$ közötti prímszámok maradékai a legtöbb szóba jövő q modulusra nézve nagyon egyenletesen oszlanak el:

$EH(\theta)$ **hipotézis.** *Minden $A>0$ számhoz található egy $C>0$ konstans, hogy $x\geqslant 2$ esetén*

$$\sum_{\substack{q\leqslant x^\theta\\ q\text{ négyzetmentes}}}\max_{(a,q)=1}\left|\sum_{\substack{x\leqslant p\leqslant 2x\\ p\equiv a\,(\mathrm{mod}\,q)}}1-\frac{1}{\varphi(q)}\int_x^{2x}\frac{dt}{\log t}\right|<C\frac{x}{\log^A x}.$$

Az egyenlőtlenségben szereplő integrál az x és $2x$ közötti prímek számát adja meg jó közelítéssel, $\varphi(q)$ a modulo q redukált maradékosztályok száma. A hipotézist a $\theta<1/2$ értékekre Bombieri és Vinogradov igazolta egymástól függetlenül [1, 30], míg a $\theta<1$ értékekre Elliott és Halberstam sejtette [3]. Mindezek után elmondhatjuk a számolás végeredményét, amit eredetileg Goldston, Pintz, Yıldırım [8] talált a $g(t):=(1-t)_+^{k+\ell}$ esetben (vö. (4)) és Soundararajan [27, 28] az általános esetben (vö. (5)).

4. tétel ([8, 27, 28])**.** *Legyen $\mathscr{H}$ egy k elemű megengedett halmaz. Legyen $g:\mathbb{R}\to\mathbb{R}$ egy k-szor folytonosan differenciálható függvény, ami a $[0,1]$ intervallumon kívül nulla. Az $EH(\theta)$ hipotézis mellett van olyan valószínűségi mérték az $x\leqslant n\leqslant 2x$ egészeken, amire nézve az $n+\mathscr{H}$ eltolt halmazba eső prímek számának várható értéke*

$$\frac{\theta}{2}\cdot\frac{k\int_0^1 g^{(k-1)}(t)^2\,\frac{t^{k-2}}{(k-2)!}\,dt}{\int_0^1 g^{(k)}(t)^2\,\frac{t^{k-1}}{(k-1)!}\,dt}+o(1).$$

A tételben $g^{(j)}$ a g függvény j. deriváltját jelöli, míg $o(1)$ egy nullához tartó mennyiség $x\to\infty$ mellett. Meglepő módon a fenti „átlagos prímkapás” mértéke nem éri el az egyet, de azt a k növelésével tetszőlegesen meg tudja közelíteni. Pontosabban az $EH(\theta)$ hipotézist egyelőre csak a $\theta<1/2$ értékekre sikerült bizonyítani, míg [5, Theorem 16] szerint a második tört szuprémuma a lehetséges g-k felett kifejezhető a J_{k-2} Bessel-függvény első pozitív gyökéből mint

$$\sup_g\frac{k\int_0^1 g^{(k-1)}(t)^2\,\frac{t^{k-2}}{(k-2)!}\,dt}{\int_0^1 g^{(k)}(t)^2\,\frac{t^{k-1}}{(k-1)!}\,dt}=\frac{4k(k-1)}{j_{k-2,1}^2}\approx 4-\frac{14.8461}{k^{2/3}}.$$

Mindenesetre a fenti tételből már következik, hogy ha $EH(\theta)$ fennáll bármilyen $\theta>1/2$ értékre, akkor létezik a 2. tételt kielégítő k, tehát létezik Polignac-szám is. Például a [8] dolgozat fontos megállapítása, hogy az Elliott–Halberstam-sejtés mellett vehető $k=6$, amikor is $\min\mathscr{D}\leqslant 16$.

6. HOGYAN FOGJUNK TÖBB PRÍMET?

A 4. tétel a határán van annak, hogy Polignac-szám létezése következzék belőle, ezért a megjelenésekor természetes kérdésként merült fel, hogy a benne szereplő várható érték megnövelhető-e valamiképpen. A szóban forgó várható érték a $o(1)$ hibatagot leszámítva két pozitív tényező szorzataként van megadva, ezért – ha kissé banálisak akarunk lenni – valamelyik tényezőt kell megnövelni úgy, hogy a másik tényező legfeljebb csak keveset változzék. A dolog azért bonyolultabb, mint hangzik, olyannyira, hogy a szakértők körében elterjedt volt a nézet, miszerint a meglévő eszközökkel ilyesfajta javítás nem várható. Mégis, a későbbi fejleményekben pontosan ez történt, mégpedig mindkét lehetséges irányban. Zhang [32] és Polymath8a [20] az első tényező megnövelésére koncentrált, míg Maynard [14] és Polymath8b [21] a második tényező megnövelésére.

Zhang [32] bizonyítása Motohashi és Pintz [16] egy fontos észrevételére épül: a 4. tételhez vezető számolásban nem vesztünk sokat, ha az $EH(\theta)$ hipotézist megszorítjuk azokra a négyzetmentes $q \leqslant x^\theta$ számokra, amiknek minden prímosztója legfeljebb x^δ valamilyen $\delta > 0$ konstanssal. Az ilyen számokat x^δ-simáknak nevezzük, és sok előnyös tulajdonságuk van, pl. két egymás utáni osztójuknak a hányadosa legfeljebb x^δ, továbbá bármely osztójuk maga is x^δ-sima. Egy másik fontos észrevétel, hogy a számolásban csak azok az $a \bmod q$ maradékosztályok vesznek részt, amiket bármilyen $p \mid q$ prímosztó szerint redukálva a $h_j - h_i \bmod p$ $(i \neq j)$ maradékosztályok egyikét kapjuk. Zhang [32] az ily módon gyengített $EH(\theta,\delta)$ hipotézist igazolta valamilyen $\theta > 1/2$ és $\delta > 0$ paraméterekkel, és ebből adódott következésként a 2. tétel. A Polymath8a [20] projekt jelentősen bővítette a megfelelő (θ,δ) párok halmazát, minden ilyen párra csökkentette a megfelelő k értékét, és egyszerűsítette a bizonyítást. Pl. a θ felső határa Zhang [32] dolgozatában $1/2+1/584$, a Polymath8a [20] cikkben $1/2+7/300$.

Maynard [14] és Tao [29] az (5) helyett a

$$\nu(n) := \left(\sum_{d_1 \mid n+h_1} \dots \sum_{d_k \mid n+h_k} \mu(d_1)\dots\mu(d_k) f\left(\frac{\log d_1}{\log R}, \dots, \frac{\log d_k}{\log R} \right) \right)^2 \tag{6}$$

súlyokat használja, ahol $f : \mathbb{R}^k \to \mathbb{R}$ egy kellően sima függvény, ami a

$$\Delta_k := \{(t_1,\dots,t_k) \in \mathbb{R}^k : \ t_1,\dots,t_k \geqslant 0 \text{ és } t_1+\dots+t_k \leqslant 1\}$$

szimplexen kívül nulla. Ez a definíció jobban megfelel az eredeti célkitűzésnek, mert az $n+\mathscr{H}$ elemeiről külön-külön próbálja elérni, hogy kevés prímosztójuk legyen, nem csak a szorzatukat, a $P(n)$-t tartja szem előtt. Valójában az (5) a (6)-nak azon speciális esete, amikor $f(t_1,\dots,t_k)$ csak a változók összegétől függ, nevezetesen

$$f(t_1,\dots,t_k) = g(t_1+\dots+t_k). \tag{7}$$

Ennek oka, hogy a megállapodásunk szerint csak olyan n-ekkel dolgozunk, amikre az $n+h_1,\dots,n+h_k$ számok páronként relatív prímek, vagyis a (6)-beli $d_1,\dots,d_k$ változók kölcsönösen egyértelműen meghatároznak egy $d \mid P(n)$ osztót a $d = d_1\dots d_k$ utasítással. Ezek után kimondhatjuk a 4. tétel megfelelőjét, ami a (6) súlyokkal való átlagolással következik. Először is bevezetünk egy jelölést a Δ_k szimplex $t_i = 0$ egyenlettel definiált lapjára:

$$\Delta_{k,i} := \{(t_1,\dots,t_k) \in \Delta_k : \ t_i = 0\}, \qquad i = 1,\dots,k.$$

5. tétel ([14, 29]). *Legyen $\mathscr{H}$ egy k elemű megengedett halmaz. Legyen $f : \mathbb{R}^k \to \mathbb{R}$ egy k-szor folytonosan differenciálható függvény, ami a Δ_k szimplexen kívül nulla. Az $EH(\theta)$ hipotézis mellett van olyan valószínűségi mérték az $x \leqslant n \leqslant 2x$ egészeken, amire nézve az $n+\mathscr{H}$ eltolt halmazba eső prímek számának várható értéke*

$$\frac{\theta}{2} \cdot \frac{\sum_{i=1}^k \int_{\Delta_{k,i}} \left(\frac{\partial^{k-1} f}{\partial t_1 \dots \partial t_{i-1} \partial t_{i+1} \dots \partial t_k} \right)^2}{\int_{\Delta_k} \left(\frac{\partial^k f}{\partial t_1 \dots \partial t_k} \right)^2} + o(1).$$

A (7) alakú függvényekre a fenti állítás a 4. tételbe megy át, mert a $t_1+\cdots+t_k=t$ affin hipersík a Δ_k-t egy $\frac{t^{k-1}}{(k-1)!}$ térfogatú $(k-1)$-szimplexben metszi, a $\Delta_{k,i}$-t pedig egy $\frac{t^{k-2}}{(k-2)!}$ térfogatú $(k-2)$-szimplexben. Általában véve is megmutatható [21, Lemma 41], hogy a tétel nem gyengül, ha szimmetrikus $f:\mathbb{R}^k\to\mathbb{R}$ függvényekre szorítkozunk: ilyenkor az $n+\mathscr{H}$ eltolt halmazba eső prímek számának várható értéke

$$\frac{\theta}{2}\cdot\frac{k\int_{\Delta_{k,k}}\left(\frac{\partial^{k-1}f}{\partial t_1\dots\partial t_{k-1}}\right)^2}{\int_{\Delta_k}\left(\frac{\partial^k f}{\partial t_1\dots\partial t_k}\right)^2}+o(1).$$

Mindezek fényében kézenfekvőnek tűnik egy f szimmetrikus polinomot keresni, amire a második tört 4-nél nagyobb, mert akkor alkalmas $\theta<1/2$ értékkel új bizonyítást kapunk a 2. tételre. Más szóval, ha M_k jelöli a második tört szuprémumát a lehetséges f-ek felett, akkor $M_k>4$ kimutatása a cél. A gyakorlatban célszerűbb az f helyett a nevezőben szereplő

$$F(t_1,\dots,t_k):=\frac{\partial^k f}{\partial t_1\dots\partial t_k}$$

parciális deriváltat megadni, ami szintén szimmetrikus polinom. Maynard [14] az első két hatványösszeg, $t_1+\cdots+t_k$ és $t_1^2+\cdots+t_k^2$ polinomjaival kísérletezve talált egy 11-edfokú példát, amiből $M_{105}>4$ következett. Polymath egy 23-adfokú F szimmetrikus polinommal demonstrálta az $M_{54}>4$ egyenlőtlenséget [21, Theorem 23]. Másfelől belátható [21, Corollary 37], hogy M_k legfeljebb $\frac{k}{k-1}\log k$, amiért $M_{50}<4$. Tehát a 2. tételben mindenképp vehető $k=54$, de a $k=50$ értékhez az 5. tétel nem elegendő. Ugyanakkor az 5. tételnek vannak olyan variánsai [21, Theorems 26 & 28], amikben $f:\mathbb{R}^k\to\mathbb{R}$ a Δ_k szimplexen kívül is lehet nullától különböző: ezek segítségével a 2. tétel állítása a $k=50$ értékre igazolható, és egy Elliott–Halberstam-típusú sejtés mellett $k=3$ is megfelelő. Tehát bizonyításunk van arra, hogy $\min\mathscr{D}\leqslant 246$, és jó okunk van hinni abban, hogy $\min\mathscr{D}\leqslant 6$.

Mit ad az 5. tétel nagy k-ra? Már említettük az $M_k\leqslant\frac{k}{k-1}\log k$ felső becslést. A másik irányban Maynard [14] igazolta minden elég nagy k-ra, hogy $M_k\geqslant\log k-\log\log k-2$. Valójában ez az alsó becslés minden $k\geqslant 2$ értékre teljesül [21, 48. oldal], és a $\log\log k$ helyett egy alkalmas abszolút konstanssal is igaz [21, Theorem 23]. Tehát a Bombieri–Vinogradov-tétel [1, 30] alapján kb. $\frac{1}{4}\log k$ darab prímet tudunk garantálni végtelen sok $n+\mathscr{H}$ eltoltban, és a Zhang-féle iránnyal kombinálva az $\frac{1}{4}$ együttható javítható $\frac{157}{600}$-ra [21, Theorem 6]. Ez a Dickson–Hardy–Littlewood-sejtés egy gyenge formája, és igen figyelemre méltó eredmény.

7. Történeti megjegyzések

A kis prímhézagok terén az egyik első fontos eredmény Erdős Páltól [4] származik: létezik egy $c<1$ konstans úgy, hogy a

$$0<p-p'<c\log p$$

egyenlőtlenségnek végtelen sok megoldása van prímekben. A $c<1$ feltételnek az a jelentősége, hogy a prímszámtétel szerint az x körüli prímszámok átlagosan $\log x$ távolságra vannak egymástól, vagyis $c>1$ esetén a fenti állítás egyszerű következmény, míg $c=1$ esetén nem túl meglepő. A c-re többen próbáltak minél jobb értéket megadni, de az igazi áttörést Goldston, Pintz, Yıldırım [8] érte el, amikor sikerült belátniuk, hogy minden $c>0$ konstans megfelelő. A [8]-ban kifejlesztett módszer fontos szerepet játszott Erdős két másik kedvenc problémájának megoldásában: van-e tetszőlegesen hosszú számtani sorozat a prímek között, illetve megjavítható-e a nagy prímhézagokra vonatkozó Rankin-becslés [23] egy végtelenhez tartó faktorral. Az elsőre ad választ a híres Green–Tao-tétel [10], a másodikat pedig néhány hónapja oldotta meg egymástól függetlenül Ford–Green–Konyagin–Tao [6] és Maynard [15]. A Rankin-becslés további javítását tartalmazza a napokban megjelent

[7] preprint. A prímhézagokról és a kapcsolódó Landau-problémák történetéről részletes áttekintést nyújt a [17] dolgozat.

A Bombieri–Vinogradov-tétel [1, 30] két alappillére a Siegel–Walfisz-tétel [26, 31] és a Linnyik [13] által felfedezett ún. nagy szita egy letisztult formája. A nagy szita valószínűségszámítási jellegét az elsők között ismerte fel Rényi Alfréd [24], és a segítségével áttörést ért el az ikerprímsejtés és a hozzá szorosan kapcsolódó Goldbach-sejtés megközelítésében. Könnyen lehet, hogy már a Linnyik–Rényi-féle első verziókból következik az $EH(\theta)$ hipotézis valamilyen pozitív θ-val, legalábbis erre enged következtetni Bombieri egy megjegyzése [1, (1.12) alatt]. Mindez különösen érdekes az 5. tétel fényében, hiszen az itt szereplő várható érték bármilyen $\theta > 0$ mellett tetszőleges naggyá tehető a k és az $f : \mathbb{R}^k \to \mathbb{R}$ alkalmas megválasztásával.

A Polymath projekteket Timothy Gowers kezdeményezte 2009 elején a matematikai kutatás egy újfajta formájaként. A kutatás nyilvánosan, egy internetes felületen keresztül történik, és bárki kötetlenül – akár névtelenül is – csatlakozhat. A prímhézagokra vonatkozó Polymath8 projekt egy intenzív évet ölelt fel 2013 nyarától 2014 nyaráig, és különösen sikeresnek mondható. Az Európai Matematikai Társulat (EMS) felkérésére több résztvevő – köztük a szerző is – leírta az idevágó személyes tapasztalatait, és ezek megjelentek az EMS Newsletter legfrissebb számában [22].

8. Köszönetnyilvánítás

A cikk a Fazekas Mihály Gimnáziumban, a Közép-európai Egyetemen és a Helvetic Algebraic Geometry Seminar-on tartott előadásaimra épül. Köszönöm a megtisztelő felkéréseket, ahogyan különböző grantok – OTKA K101855 és K104183, ERC AdG-228005 és AdG-321104 – támogatását is. Hálával tartozom Pintz Jánosnak, aki a kéziratot gondosan átnézte és értékes megjegyzéseivel ellátta.

Hivatkozások

[1] E. Bombieri, On the large sieve, *Mathematika* **12** (1965), 201–225. 6, 8, 9
[2] L. E. Dickson, A new extension of Dirichlet's theorem on prime numbers, *Messenger of Math.* **33** (1904), 155–161. 2
[3] P. D. T. A. Elliott, H. Halberstam, A conjecture in prime number theory, In: *Symposia Mathematica*, Vol. IV (INDAM, Rome, 1968/69), 59–72, Academic Press, London, 1970. 6
[4] P. Erdős, The difference of consecutive primes, *Duke Math. J.* **6**, (1940), 438–441. 8
[5] B. Farkas, J. Pintz, Sz. Révész, On the optimal weight function in the Goldston-Pintz-Yıldırım method for finding small gaps between consecutive primes, In: *Number theory, analysis, and combinatorics*, 75–104, De Gruyter Proc. Math., De Gruyter, Berlin, 2014. 5, 6
[6] K. Ford, B. Green, S. Konyagin, T. Tao, Large gaps between consecutive prime numbers, arXiv:1408.4505 1, 8
[7] K. Ford, B. Green, S. Konyagin, J. Maynard, T. Tao, Long gaps between primes, arXiv:1412.5029 1, 9
[8] D. A. Goldston, J. Pintz, C. Y. Yıldırım, Primes in tuples I, *Ann. of Math. (2)* **170** (2009), 819–862. 1, 2, 4, 5, 6, 8
[9] A. Granville, D. M. Kane, D. Koukoulopoulos, R. J. Lemke Oliver, Best possible densities of Dickson m-tuples, as a consequence of Zhang-Maynard-Tao, arXiv:1410.8198 3, 4
[10] B. Green, T. Tao, The primes contain arbitrarily long arithmetic progressions, *Ann. of Math. (2)* **167** (2008), 481–547. 1, 8
[11] G. H. Hardy, J. E. Littlewood, Some problems of 'Partitio numerorum'; III: On the expression of a number as a sum of primes, *Acta Math.* **44** (1923), 1–70. 2
[12] D. R. Heath-Brown, Almost-prime k-tuples, *Mathematika* **44** (1997), 245–266. 1, 5
[13] Y. V. Linnik, The large sieve (Russian), *Dokl. Akad. Nauk SSSR* **30** (1941), 292–294. 9
[14] J. Maynard, Small gaps between primes, *Ann. of Math. (2)*, **181** (2015), 383–413. 1, 2, 3, 5, 7, 8
[15] J. Maynard, Large gaps between primes, arXiv:1408.5110 1, 8
[16] Y. Motohashi, J. Pintz, A smoothed GPY sieve, *Bull. Lond. Math. Soc.* **40** (2008), 298–310. 1, 2, 7
[17] J. Pintz, Landau's problems on primes, *J. Théor. Nombres Bordeaux* **21** (2009), 357–404. 9
[18] J. Pintz, Polignac numbers, conjectures of Erdős on gaps between primes, arithmetic progressions in primes, and the bounded gap conjecture, arXiv:1305.6289 3
[19] M. A. de Polignac, Recherches nouvelles sur les nombres premiers, *Comptes rendus hebdomadaires des séances de l'Académie des sciences* **29** (1849), 397–401. 1

[20] D. H. J. Polymath, New equidistribution estimates of Zhang type, *Algebra & Number Theory* **8** (2014), 2067–2199. 2, 3, 5, 7
[21] D. H. J. Polymath, Variants of the Selberg sieve, and bounded intervals containing many primes, *Res. Math. Sci.* **1** (2014), no. 12, 83 oldal 2, 3, 4, 5, 7, 8
[22] D. H. J. Polymath, The "Bounded gaps between primes" Polymath project - A retrospective analysis, *EMS Newsletter*, no. 94, December 2014, 13–23. 9
[23] R. A. Rankin, The difference between consecutive prime numbers, *J. London Math. Soc.* **13** (1938), 242–244. 8
[24] A. Rényi, On the representation of an even number as the sum of a single prime and single almost-prime number (Russian), *Izv. Akad. Nauk SSSR Ser. Mat.* **12**, (1948), 57–78. 9
[25] A. Selberg, Lectures on sieves, In: *Collected papers, Vol. II*, Springer-Verlag, Berlin, 1991. 5
[26] C. L. Siegel, Über die Classenzahl quadratischer Zahlkörper, *Acta Arith.* **1** (1935), 83–86. 9
[27] K. Soundararajan, Notes on Goldston-Pintz-Yıldırım, 2005, publikálatlan 5, 6
[28] K. Soundararajan, Small gaps between prime numbers: the work of Goldston-Pintz-Yıldırım, *Bull. Amer. Math. Soc. (N.S.)* **44** (2007), 1–18. 5, 6
[29] T. Tao, Polymath8b: Bounded intervals with many primes, after Maynard, 2013, blogbejegyzés, http://terrytao.wordpress.com/2013/11/19/polymath8b-bounded-intervals-with-many-primes-after-maynard/ 2, 7
[30] A. I. Vinogradov, The density hypothesis for Dirichet L-series (Russian), *Izv. Akad. Nauk SSSR Ser. Mat.* **29** (1965), 903–934; Correction (Russian), *ibid.* **30** (1966), 719–720. 6, 8, 9
[31] A. Walfisz, Zur additiven Zahlentheorie. II., *Math. Z.* **40** (1936), 592–607. 9
[32] Y. Zhang, Bounded gaps between primes, *Ann. of Math. (2)* **179** (2014), 1121–1174. 1, 2, 3, 5, 7

MTA Rényi Alfréd Matematikai Kutatóintézet, 1053 Budapest, Reáltanoda u. 13-15.
E-mail address: gharcos@renyi.hu

Közép-európai Egyetem, 1051 Budapest, Nádor u. 9.
E-mail address: harcosg@ceu.hu