1. Prímszámok

Klasszikus megoldatlan problémák (FGy5.1)

Ikerprímek
$(p, p+2)$ párok, ahol mindkettő prím. Pl. $(3,5)$, $(5,7)$, $(11,13)$.

Van-e végtelen sok ikerprím-pár?
Zhang, Tao: Végtelen sok p-re van prím p és $p+246$ között.
Viggo Brun: Az ikerprímek reciprokösszege véges (a prímeké nem).

Goldbach-sejtés
Előáll-e minden 2-nél nagyobb páros szám két prím összegeként?

Vinogradov: Minden elég nagy páratlan szám három prím összege.

Van-e végtelen sok prím az alábbi sorozatokban?
n^2+1, $1111\ldots1$, $3333\ldots31$, Fibonacci-sorozat.

Green, Tao: Van bármilyen hosszú számtani sorozat prímszámokból.

Hézagtétel

Hézagtétel (FGy5.5.1, 5.5.2)
Minden N-re van olyan p prím, hogy p és $p+N$ között már nincs prím, sőt olyan is, amelyre $p-N$ és p között sincs (*izolált* prím).

Bizonyítás
$(N+1)!+k$ összetett, ha $2 \le k \le N+1$, mert k-val osztható. Így a legnagyobb $p \le (N+1)!+1$ prím megfelel az első feltételnek.
Vegyünk $N < p_1, p_2, \ldots, p_{2N}$ különböző prímeket, és tekintsük az
$x \equiv i\ (p_i)$, $x \equiv -i\ (p_{N+i})$ szimultán kongruenciarendszert ($1 \le i \le N$, tehát $2N$ kongruenciából áll).
A kínai maradéktétel szerint ennek van megoldása, ami egy maradékosztály (tehát számtani sorozat) a $d = p_1 \ldots p_{2N}$ modulusra nézve. Nyilván $(d, \pm i) = 1$, hiszen $p_i > N \ge i$. Ezért Dirichlet tétele miatt a megoldások között van p prím, ami nyilván izolált. □

A prímek nagysága
Az f és g valós függvények *aszimptotikusan egyenlőek*,
ha $\frac{f(x)}{g(x)} \to 1$ ha $x \to \infty$. Jele $f \sim g$.
Az x-nél nem nagyobb (pozitív) prímek száma $\pi(x)$. Pl. $\pi(20) = 8$. A logaritmus mindig természetes (vagyis e alapú).

Tétel (FGy5.4.1, 5.4.2, 5.4.5, 5.5.3, 5.6.2, F5.4.4)
Nagy prímszámtétel: $\pi(x) \sim \frac{x}{\log x}$.
Az n-edik prímszám, $p_n \sim n \log n$. (Pl. $p_{10} = 29$.)
Csebisev tétele: n és $2n$ között mindig van prímszám.
$\sum_{p \le n,\ p \text{ prím}} \frac{1}{p} \sim \log\log n$, sőt a két szám eltérése korlátos.
Speciálisan a prímek reciprokösszege végtelen.
$P_n = \prod_{p \le n,\ p \text{ prím}} p < 4^n$, sőt $\log P_n \sim n$, tehát P_n „kb." e^n.

A részletes bizonyítások jórészt megtalálhatók a FGy-könyvben. Most e tételekhez bizonyításvázlatokat, megjegyzéseket fűzünk.

Kapcsolat a Riemann-függvénnyel

Legyen $R_p(s) = 1 + \frac{1}{p^s} + \ldots + \frac{1}{p^{ks}} + \ldots$. Ekkor
$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ prím}} R_p(s)$ (ez az *Euler-formula*).

A végtelen mértani sor összegképlete miatt $R_p(s) = \frac{1}{1-p^{-s}}$.
Az állítás akkor igaz, ha mindkét oldal abszolút konvergens, $s > 1$-re biztosan, de ezzel most nem foglalkozunk.
Heurisztika: Ha n kanonikus alakja $p_1^{\alpha_1} \ldots p_k^{\alpha_k}$, akkor $1/n^s$ a jobb oldali szorzat beszorzásakor pontosan egyszer jelenik meg: amikor $R_{p_i}(s)$-ből $1/p_i^{\alpha_i s}$-et vesszük, a többi tényezőből pedig 1-et. (Azok a szorzatok nullával egyenlők, ahol végtelen sok $R_p(s)$-ből nem 1-et veszünk ki). Az s kitevőre a konvergencia miatt van szükség.
Vagyis ez a képlet *magába sűríti a számelmélet alaptételének állítását az összes pozitív egészre*. A képlet $s = 1$-re nem alkalmazható, de egy véges változata igen, ez vezet el a prímek reciprokösszegének vizsgálatához.

A prímek reciprokösszege divergens

Tétel (FGy5.6.1)
$\sum_{p \le n} \frac{1}{p} \ge \log\log n - \log 2$. Így $\sum_p \frac{1}{p}$ divergens.
(A p az ilyen összegzésekben ezentúl prímszámot jelöl.)

Felhasználjuk, hogy $\sum_{i=1}^{n} \frac{1}{i^2} < 2$ és $\sum_{d=1}^{n} \frac{1}{d} \ge \log n$,
továbbá hogy $\log(1+x) \le x$, ha $x > -1$. (Ezek elemiek.)

A $P = \prod_{p \le n} \left(1 + \frac{1}{p}\right) \ge \sum_{m \le n,\ m \text{ négyzetmentes}} \frac{1}{m} = N$
összefüggés közvetlen beszorzással látható.
Mivel minden $d \ge 1$ egyértelműen bontható egy négyzetszám és egy négyzetmentes szám szorzatára, így $\sum_{d=1}^{n} \frac{1}{d} \le N \sum_{i=1}^{n} \frac{1}{i^2}$.
Tehát $P \ge N \ge (1/2)\log n$. Másrészt $\log(1+x) \le x$ miatt
$\log P = \sum_{p \le n} \log\left(1 + \frac{1}{p}\right) \le \sum_{p \le n} \frac{1}{p}$. Az eddigieket összegezve
$\sum_{p \le n} \frac{1}{p} \ge \log\left((1/2)\log n\right) = \log\log n - \log 2$. □

A binomiális együtthatók prímhatvány-osztói

Tétel (FGy5.4.4)
Az $\binom{n}{k}$ minden prímhatvány-osztója legfeljebb n.

Állítás: $\lfloor x+y\rfloor - \lfloor x\rfloor - \lfloor y\rfloor$ értéke 0 vagy 1 (x, y valós).

Valóban, legyen $x = n+t$ és $y = m+s$, ahol $0 \le t, s < 1$. Ekkor $\lfloor x\rfloor = n$, $\lfloor y\rfloor = m$, és mivel $x+y = (n+m)+(t+s)$, ezért $\lfloor x+y\rfloor$ értéke $n+m$ vagy $n+m+1$ lehet csak aszerint, hogy $t+s<1$ vagy $1 \le t+s < 2$. Az első esetben $\lfloor x+y\rfloor - \lfloor x\rfloor - \lfloor y\rfloor$ értéke 0, a másodikban 1. □

Egy p prím kitevője $\binom{n}{k} = \frac{n!}{k!(n-k)!}$-ban a Legendre-formula szerint

$m = \sum_{i=1}^{t} \left(\lfloor \frac{n}{p^i}\rfloor - \lfloor \frac{k}{p^i}\rfloor - \lfloor \frac{n-k}{p^i}\rfloor\right)$, ahol t a legnagyobb egész, amelyre még $p^t \le n$. Az Állítás szerint az összeg minden tagja 0 vagy 1, ezért $m \le t$, így $p^m \le p^t \le n$. □

$\pi(x)$ alsó becslése

Tétel (FGy5.4.3)
Alkalmas c konstansra $\pi(x) \ge c\frac{x}{\log x}$, ha $x \ge 2$.

Valóban, írjuk föl $\binom{n}{k}$-t prímhatványok szorzataként. Láttuk, hogy mindegyik legfeljebb n, és persze a megfelelő prímek is, ezért $\binom{n}{k} \le n^{\pi(n)}$. Ezt összegezve $k = 1$-től $n-1$-ig, a binomiális tétel szerint $2^n \le (n-1)n^{\pi(n)} + 2 \le n^{\pi(n)+1}$. Logaritmust véve $\pi(n) \ge (\log 2)\frac{n}{\log n} - 1 \ge (\log 2 - 0{,}4)\frac{n}{\log n}$. □

A Nagy Prímszámtétel szerint minden 1-nél kisebb c megfelelő, ha x elegendően nagy. Sőt, az is igaz, hogy $c = 1$ is választható elég nagy x-re. Itt a $\log(2) - 0{,}4$ azért szerepel, hogy a bizonyítás már $x \ge 2$-től működjön. A Nagy Prímszámtétel szerint $\pi(x) \le c\frac{x}{\log x}$ is teljesül elég nagy x-re minden $c > 1$ esetén. Ezért a fenti alsó becslésben semmilyen $c > 1$ érték nem választható.

A prímek szorzata

Tétel (FGy5.4.5)
$P_n = \prod_{p \le n} p < 4^n$.

Ötlet: Ha $k+2 \le p \le 2k+1$, akkor $p \mid \binom{2k+1}{k}$. Valóban, p osztja a $(2k+1)!$ számlálót, de a $k!(k+1)!$ nevezőt nem. □

Erdős Pál és Kalmár László bizonyítása: indukció n-re. $n \le 3$ esetén nyilvánvaló. Ha n páros, akkor $P_n = P_{n-1} \le 4^{n-1}$.
Ha $n = 2k+1$ páratlan, akkor $P_n = P_{k+1}\prod_{k+2\le p\le 2k+1} p$. Az első tényező az indukciós feltevés miatt legfeljebb 4^{k+1}. A második a fenti Ötlet miatt osztója $\binom{2k+1}{k}$-nak. Ezért elég belátni, hogy $\binom{2k+1}{k} \le 4^k$.

A binomiális tétel szerint $\sum_{i=0}^{2k+1}\binom{2k+1}{i} = 2^{2k+1} = 2\cdot 4^k$. Az összeg két egyenlő tagja $d = \binom{2k+1}{k} = \binom{2k+1}{k+1}$, így $d \le 4^k$. □

$\pi(x)$ felső becslése

Tétel (FGy5.4.3)
Alkalmas c konstansra és x_0-ra $\pi(x) \le c\frac{x}{\log x}$, ha $x \ge x_0$.

Erdős Pál bizonyítása. A $P_n = \prod_{p\le n} p < 4^n$ szorzatot vágjuk ketté $\sqrt{n}$-nél. Az alsó felét hagyjuk el, a többi tényező helyére írjunk $\sqrt{n}$-et.
Így $4^n \ge \sqrt{n}^{\left(\pi(n)-\pi(\sqrt{n})\right)} \ge \sqrt{n}^{\left(\pi(n)-\sqrt{n}\right)}$, hiszen $\pi\left(\sqrt{n}\right) \le \sqrt{n}$. Logaritmust véve $(\log 4)n \ge \left(\pi(n)-\sqrt{n}\right)\log\sqrt{n}$, ahonnan $\pi(n) \le \frac{(4\log 2)n}{\log n} + \sqrt{n}$. Mivel $\frac{\sqrt{n}}{n/\log n} = \frac{\log n}{\sqrt{n}} \to 0$ ha $n \to \infty$, ezért elég nagy n-re $\sqrt{n} \le 0{,}01\frac{n}{\log n}$. Ezzel beláttuk, hogy elég nagy x-re $\pi(x) \le c\frac{x}{\log x}$, ahol $c = 4\log 2 + 0{,}01$. □

Ez a konstans körülbelül 2,78. Elsőként Csebisev bizonyította be $\pi(x)$-nek ilyen alsó és felső becslését.

Csebisev tétele

Erdős Pál bizonyításának vázlata. Ha $n < p \le 2n$,
akkor p kitevője a $\binom{2n}{n} = (2n)!/(n!)^2$ binomiális együtthatóban 1.
Valóban, $2p$ már nem osztója $(2n)!$-nak, ezért p kitevője a számlálóban 1, a nevező viszont nem osztható p-vel. □
Állítás: Ha $2n/3 < p \le n$, akkor p nem osztója $\binom{2n}{n}$-nek.
Valóban, ilyenkor p kitevője a számlálóban és a nevezőben is 2. □
Állítás: Ha $\sqrt{2n} < p \le 2n/3$, és $p^t \mid \binom{2n}{n}$, akkor $t \le 1$.
Valóban, láttuk, hogy $p^t \le 2n$, ezért $p > \sqrt{2n}$ miatt $t \le 1$. □

Stratégia: Legyen $\binom{2n}{n} = ABC$ aszerint, hogy a prímosztók melyik intervallumban vannak $[1, \sqrt{2n}]$, $(\sqrt{2n}, (2/3)n]$, $(n, 2n]$ közül. A tétel állítása: $C > 1$. Így A, B-re felső, $\binom{2n}{n}$-re alsó becslés kell.

$\binom{2n}{n}$ számlálójában a $2k+1 > 1$ tényezők helyére írjunk $2k$-t, emeljünk ki 2-t minden tényezőből, majd egyszerűsítsünk $n!(n-1)!$-al. Az eredmény $2^{2n-1}/n$. Ezért $\binom{2n}{n} \ge \frac{4^n}{2n}$.

A bizonyítás folytatása

A minden prímhatvány-osztója legfeljebb n, ezért $A \le (2n)^{\sqrt{2n}}$. □
$B \le \prod_{\sqrt{2n}<p\le 2n/3} p < 4^{2n/3}$ az Erdős–Kalmár-tétel alapján. □
Összegezve $C = \binom{2n}{n}/(AB) \ge \dfrac{4^n}{(2n)\cdot(2n)^{\sqrt{2n}}\cdot 4^{2n/3}}$.
(Látjuk, miért fontos a $2n/3$ és n közötti prímektől megszabadulni.)
Logaritmust véve $\log C \ge (n/3)\log 4 - (\sqrt{2n}+1)\log(2n)$. Mivel $\sqrt{n}/\log n \to \infty$, ha $n \to \infty$, ezért C is végtelenhez tart.

Konkrétan $n = 474$-re már $C > 1$. Az ennél kisebb számokra úgy ellenőrizhetjük Csebisev tételét, hogy tekintjük a következő sorozatot: $2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631$. Ezek mind prímek, és mindegyik kisebb az előző kétszeresénél. Ezért minden $n \le 500$ egészre valamelyikük n és $2n$ között van. □

(Ezt a sorozatot Csebisev tétele miatt akármeddig lehet folytatni.)
Nem ismeretes, hogy n és $n+\sqrt{n}$ között mindig van-e prím.
Tétel(FGy5.5.4): n és $n+n^{0,54}$ között van prím elég nagy n-re.

A prímszámtétel következményei
A prímszámtételből következik, hogy nemcsak n és $2n$ között, hanem n és cn között is van prím minden $c>1$ esetén (FGy5.5.5).

Valóban, $\frac{\pi(cx)}{\pi(x)} \sim c\frac{\log x}{\log cx} \sim c > 1$, hiszen $\frac{\log cx}{\log x} = \frac{\log c+\log x}{\log x} \to 1$, ha $x \to \infty$. Ezért elég nagy x-re $\pi(cx) > \pi(x)$, azaz van prím x és cx között. □

Tétel (FGy5.4.2): Az n-edik prímszám, $p_n \sim n\log n$.

Valóban, definíció szerint $\pi(p_n) = n$. A prímszámtétel miatt
$n = \pi(p_n) \sim \frac{p_n}{\log p_n}$. De $\frac{\log p_n}{p_n^{\varepsilon}} \to 0$ minden $\varepsilon > 0$ esetén, ezért összeszorozva $\frac{p_n^{(1-\varepsilon)}}{n} \to 0$, azaz ≤ 1 elég nagy x-re.
Innen $(1-\varepsilon)\log p_n \le \log n$, és így $1-\varepsilon \le \frac{\log n}{\log p_n} \le 1$.
Mivel ε tetszőlegesen kicsi lehet, $\frac{\log n}{\log p_n} \sim 1$. Megszorozva $\frac{n\log p_n}{p_n} \to$ 1-gyel $\frac{n\log n}{p_n} \to 1$ adódik. □

Az $ak+b$ alakú prímek száma

Dirichlet tételének kvantitatív változata (FGy, F6.4.8)
A prímek közel egyenletesen helyezkednek el a számtani sorozatokban. Vagyis ha $(a,b)=1$, akkor az x-nél nem nagyobb $ak+b$ alakú prímek száma aszimptotikusan $\pi(x)/\varphi(a)$.

Tehát például $6k+1$ és $6k+5$ alakú prímből is kb. $(1/2)\frac{x}{\log x}$ darab van x-ig (ami sokkal több, mint a négyzetszámok $\sqrt{x}$ száma).

A Dirichlet-tétel bizonyítása hasonló a prímszámtételéhez, csak a ζ-függvény helyett egy olyan $L(s,\chi) = \sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}$ Dirichlet-függvényt használ, ahol χ egy mod a periodikus, komplex értékű, szorzattartó leképezés (úgynevezett csoportkarakter).

A prímszámtételt Gauss és Legendre is megsejtette. Riemann munkássága nyomán Hadamard és de la Vallée-Poussin bizonyította be 1896-ban. Erdős Pál és Atle Selberg 1949-ben komplex analízis nélküli bizonyítást adott.

A 30. előadás összefoglalása

Fogalmak
Ikerprímek, Goldbach-sejtés, további nevezetes problémák (FGy5.1).

Tételek
Hézagtétel (FGy5.5.1, 5.5.2).
Prímszámtétel, alsó és felső becslés a prímek számára (FGy5.4.1, 5.4.3, 5.4.4).
Az n-edik prím nagysága (FGy5.4.2). Csebisev tétele (FGy5.5.3).
A prímek reciprokösszege végtelen (FGy5.6.1).
A prímek szorzatának becslése (FGy5.4.5, F5.4.4).
A prímek eloszlása számtani sorozatokban (FGy, F6.4.8).