Prímek, Polignac, Polymath

Harcos Gergely

Rényi Alfréd Matematikai Kutatóintézet
http://www.renyi.hu/∼gharcos/

2016. november 23.
Magyar Tudományos Akadémia

A prímek és a szorzatra bontás

Példa

Vegyünk egy számot, és bontsuk minél kisebb számok szorzatára:

1. $180 = 18 \cdot 10 = 18 \cdot 5 \cdot 2 = 6 \cdot 3 \cdot 5 \cdot 2 = 3 \cdot 2 \cdot 3 \cdot 5 \cdot 2$
2. $180 = 30 \cdot 6 = 30 \cdot 3 \cdot 2 = 10 \cdot 3 \cdot 3 \cdot 2 = 5 \cdot 2 \cdot 3 \cdot 3 \cdot 2$
3. $180 = 45 \cdot 4 = 45 \cdot 2 \cdot 2 = 9 \cdot 5 \cdot 2 \cdot 2 = 3 \cdot 3 \cdot 5 \cdot 2 \cdot 2$
4. $180 = 60 \cdot 3 = 12 \cdot 5 \cdot 3 = 4 \cdot 3 \cdot 5 \cdot 3 = 2 \cdot 2 \cdot 3 \cdot 5 \cdot 3$

A végén mindig ugyanazokat a prímszámokat kapjuk!

Tétel (Eukleidész i.e. 300 körül, Gauss 1801)

Minden 1-nél nagyobb szám felbontható prímszámok szorzatára. A felbontás a tényezők sorrendjétől eltekintve egyértelmű.

Tétel (Eukleidész i.e. 300 körül)

Minden prímszámnál van nagyobb prímszám.

A prímek és a hatványozás

Példa

Vizsgáljuk egy prím kitevőjű hatvány maradékát a prímmel osztva:

1. $2^7 = 128 = 18 \cdot 7 + 2$, *tehát a maradék* 2
2. $2^{11} = 2048 = 186 \cdot 11 + 2$, *tehát a maradék* 2
3. $2^{23} = 8388608 = 364722 \cdot 23 + 2$, *tehát a maradék* 2
4. $3^5 = 243 = 48 \cdot 5 + 3$, *tehát a maradék* 3
5. $3^7 = 2187 = 312 \cdot 7 + 3$, *tehát a maradék* 3
6. $3^{13} = 1594323 = 122640 \cdot 13 + 3$, *tehát a maradék* 3

A maradék mindig megegyezik a hatványalappal!

Tétel (Fermat 1640)

Ha p prímszám és $0 < m < p$, akkor m^p maradéka p-vel osztva m.

A prímek egyre ritkuló sorozata

10-jegyűek	**100-jegyűek**	**1000-jegyűek**
1000000007	$100000\cdots000289$	$100000\cdots000007$
1000000009	$100000\cdots000303$	$100000\cdots000663$
1000000021	$100000\cdots000711$	$100000\cdots002121$
1000000033	$100000\cdots001287$	$100000\cdots002593$
1000000087	$100000\cdots002191$	$100000\cdots003561$
$\vdots$	$\vdots$	$\vdots$
9999999851	$999999\cdots997783$	$999999\cdots981127$
9999999881	$999999\cdots997873$	$999999\cdots988763$
9999999929	$999999\cdots998713$	$999999\cdots990139$
9999999943	$999999\cdots999089$	$999999\cdots993433$
9999999967	$999999\cdots999203$	$999999\cdots998231$
$\Delta \approx 22.3$	$\Delta \approx 229.5$	$\Delta \approx 2301.8$

Az ikerprímek még ritkább sorozata

10-jegyűek	**100-jegyűek**	**1000-jegyűek**
1000000007	$1000\cdots00006001$	$1000\cdots01975081$
1000000009	$1000\cdots00006003$	$1000\cdots01975083$
1000000409	$1000\cdots00028441$	$1000\cdots03142729$
1000000411	$1000\cdots00028443$	$1000\cdots03142731$
$\vdots$	$\vdots$	$\vdots$
9999999017	$9999\cdots99914921$	$9999\cdots95309921$
9999999019	$9999\cdots99914923$	$9999\cdots95309923$
9999999701	$9999\cdots99964781$	$9999\cdots98131919$
9999999703	$9999\cdots99964783$	$9999\cdots98131921$

Ikerprímsejtés

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

Polignac-számok

Definíció

A d pozitív egész *Polignac-szám*, ha a $p - p' = d$ egyenletnek végtelen sok megoldása van prímekben.

Sejtés (Polignac 1849)

Minden pozitív páros szám Polignac-szám.

Tétel (Zhang 2014)

A $2, 4, 6, \ldots, 70000000$ *számok egyike Polignac-szám.*

Theorem (Pintz 2013*, Granville et al. 2015, Polymath 2014)

- *A* $2, 4, 6, \ldots, 246$ *számok egyike Polignac-szám.*
- *A Polignac-számok alsó sűrűsége nagyobb, mint* $1/354$*.*
- *A Polignac-számok közötti hézagok korlátosak.*

Halászás a prímekre (1/2)

Ötlet

Legyen $\mathcal{H} = \{h_1, \ldots, h_k\}$ *egy egészekből álló* k *elemű halmaz. Próbáljunk végtelen sok* n *pozitív egészt találni úgy, hogy az* $n + \mathcal{H}$ *eltolt halmaz minél több prímet tartalmazzon.*

Példák

- $\mathcal{H} = \{0, 1\}$ *problémás modulo* 2
- $\mathcal{H} = \{0, 2\}$ *esetében nincs kongruencia-probléma*
- $\mathcal{H} = \{0, 2, 3\}$ *problémás modulo* 2
- $\mathcal{H} = \{0, 2, 4\}$ *problémás modulo* 3
- $\mathcal{H} = \{0, 2, 6\}$ *esetében nincs kongruencia-probléma*

Definíció

A $\mathcal{H} = \{h_1, \ldots, h_k\}$ egészekből álló k elemű halmaz *megengedett*, ha semmilyen $m \geqslant 2$ egész számra nézve nem tartalmaz teljes maradékrendszert. (Feltehető, hogy m prímszám és legfeljebb k.)

Halászás a prímekre (2/2)

Sejtés (Dickson 1904, Hardy–Littlewood 1923)

Legyen $\mathcal{H}$ egy megengedett halmaz. Ekkor végtelen sok n pozitív egészre az $n+\mathcal{H}$ eltolt halmaz minden eleme prímszám.

Tétel (Zhang 2014)

Létezik egy k pozitív egész az alábbi tulajdonsággal. Ha $\mathcal{H}$ egy k elemű megengedett halmaz, akkor végtelen sok n pozitív egészre az $n+\mathcal{H}$ eltolt halmazba legalább két prímszám esik.

forrás	k értéke	becslés Polignac-számra
Zhang	3500000	70000000
Polymath8a	632	4680
Maynard	105	600
Polymath8b	50	246

A halászás művészete (1/2)

Ötlet

Legyen $\mathcal{H} = \{h_1, \dots, h_k\}$ egy k elemű megengedett halmaz. Minden $x > x_0$ számra találjunk olyan valószínűségi mértéket az $x \leqslant n \leqslant 2x$ egészeken, amire nézve az $n + \mathcal{H}$ eltolt halmazba eső prímek számának várható értéke egynél nagyobb.
Más szóval, találjunk nemnegatív $\nu(n)$ súlyokat úgy, hogy

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

Naiv súlyok

Legyen $P(n) := (n + h_1) \dots (n + h_k)$, továbbá legyen $0 \leqslant \ell \leqslant k$.

- $\nu(n) := 1_{n + h_1, \dots, n + h_k \text{ prím}}$
- $\nu(n) := 1_{P(n) \text{ prímosztóinak száma legfeljebb } k + \ell}$
- $\nu(n) := \sum_{d \mid P(n)} \mu(d) \log^{k+\ell} \left(\frac{P(n)}{d} \right)$

A halászás művészete (2/2)

A $d \mid P(n)$ osztókat vágjuk meg az $R := x^{\theta/2}$ paraméternél:

Goldston–Pintz–Yıldırım súlyai

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

Soundararajan súlyai

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

ahol $g : \mathbb{R} \to \mathbb{R}$ kellően sima függvény, ami a $[0,1]$-en kívül nulla.

Technikai okokból ezeket a súlyokat megszorítjuk azon $x \leqslant n \leqslant 2x$ számokra, amikre $P(n)$ minden prímosztója legalább $\log\log\log x$.

Elliott és Halberstam sejtése

$EH(\theta)$ hipotézis

Minden $A > 0$ számhoz található egy $C > 0$ konstans úgy, hogy bármely $x \geqslant 2$ esetén fennáll

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

Megjegyzések

- $\theta < 1/2$ *esetén Bombieri (1965) és Vinogradov (1966) tétele*
- $\theta < 1$ *esetén Elliott és Halberstam (1970) sejtése*

Az átlagos kapás

Theorem (Goldston–Pintz–Yıldırım 2009, Soundararajan 2007)

Legyen $\mathcal{H}$ egy k elemű megengedett halmaz, és tegyük fel az $EH(\theta)$ hipotézist. A Soundararajan-súlyok által meghatározott valószínűségi mértékre nézve az $n+\mathcal{H}$ eltolt halmazba eső prímek számának várható értéke

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

Sajnos az $EH(\theta)$ hipotézist csak a $\theta < 1/2$ értékekre sikerült igazolni, miközben a második tört értéke mindig kisebb 4-nél:

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

Hogyan fogjunk több prímet? (1/3)

- Zhang az $EH(\theta)$ hipotézis egy gyengített változatát igazolta a $\theta < 1/2 + 1/584$ értékekre, aminek segítségével az átlagos kapást 1 fölé tudta emelni egy 3500000 elemű megengedett halmaz eltoltjaiban.

- A gyengített $EH(\theta)$ hipotézisben csak kis prímosztókkal rendelkező q modulusok szerepelnek, továbbá csak nagyon speciális q szerinti maradékosztályok. Ezt az ötletet Motohashi és Pintz már évekkel Zhang előtt publikálta.

- A Polymath8a kutatócsoportban enyhítettük a q-ra vonatkozó megszorítást, illetve csökkentettük ennek a k-ra gyakorolt negatív hatását. A technikai részleteket is egyszerűsítettük, így a végén a $\theta < 1/2 + 7/300$ értékekig fel tudtunk menni, ami által a megengedett halmaz szükséges mérete lement 632-re.

Hogyan fogjunk több prímet? (2/3)

Maynard és Tao súlyai

$$\nu(n) := \left(\sum_{\forall i: d_i | n+h_i} \mu(d_1) \dots \mu(d_k) f\left(\frac{\log d_1}{\log R}, \dots, \frac{\log d_k}{\log R} \right) \right)^2,$$

ahol $f : \mathbb{R}^k \to \mathbb{R}$ egy szimmetrikus és kellően sima függvény, ami a $\{(t_1, \dots, t_k) \in \mathbb{R}^k_{\geqslant 0} : t_1 + \dots + t_k \leqslant 1\}$ szimplexen kívül nulla.

Theorem (Maynard 2015, Tao 2013*)

Legyen $\mathcal{H}$ egy k elemű megengedett halmaz, és tegyük fel az $EH(\theta)$ hipotézist. A fenti súlyok által meghatározott valószínűségi mértékre nézve az $(n + \mathcal{H})$-ba eső prímek számának várható értéke

$$\frac{\theta}{2} \cdot \frac{k \int_{\mathbb{R}^{k-1} \times \{0\}} \left(\frac{\partial^{k-1} f}{\partial t_1 \dots \partial t_{k-1}} \right)^2}{\int_{\mathbb{R}^k} \left(\frac{\partial^k f}{\partial t_1 \dots \partial t_k} \right)^2} + o(1).$$

Hogyan fogjunk több prímet? (3/3)

- Az $f(t_1, \ldots, t_k) := g(t_1 + \cdots + t_k)$ speciális esetben Maynard és Tao súlyai Soundararajan súlyait adják vissza.

- Optimális paraméterekkel az átlagos kapás $\approx (\log k)/4$.

- Az f tartójának megnövelésével, illetve Zhang/Polymath8a ötleteinek bevonásával az eredmény tovább javítható.

- A Maynard/Polymath8b által számítógép segítségével talált szimmetrikus polinomok alapján Zhang tétele már viszonylag kis k értékekkel is működik. A jelenlegi rekord $k = 50$.

- Az $EH(\theta)$ hipotézis egy kiterjesztésével Polymath8b a $k = 3$ értéket is be tudta állítani, megjavítva ezzel Maynard és Goldston–Pintz–Yıldırım korábbi értékeit ($k = 5$ és $k = 6$).