Prímszámok

v1.0

Az alábbi szöveg főként Péter Rózsa *Játék a végtelennel* című könyvéből származik. Néhány kisebb módosítás, kiegészítés viszont történt. A taxis történetet a Wikipedia Rámánudzsanról szóló szócikkéből másoltam be. A prímtényezőkre bontás módját Obádovics J. Gyula *Matematika* című könyvéből vettem.

Mik azok a prímszámok?

A hinduk ősidőktől fogva kitűnő matematikusok, és sajátos képességeik vannak ezen a téren. Mikor egyszer Hardy és Rámánudzsan Londonban taxin utazott, Hardy a taxi távozása után vette észre, hogy aktatáskáját a kocsiban felejtette. Kéziratok lévén a táskában, ez kétségbe ejtette, de Rámánudzsan megnyugtatta, hogy a taxi száma 1729. Hardy igen örült ennek, de nem hagyta nyugodni a kérdés, hogyan lehetett megjegyezni egy ilyen érdektelen számot. Nem érdektelen ez a szám, felelte Rámánudzsan: ez a legkisebb olyan egész szám, amely kétféleképpen bontható fel két köbszám összegére.

A hinduknak még a négyjegyű számok is ilyen külön sajátságokkal felruházott személyes ismerőseik. Nálunk a kis számokat kezelik ilyen individuumok módjára: a 2-es nem a sok szürke szám egyike, hanem sok oldalról megismert különálló egyéniség: ő az első páros szám, $1 + 1$, 4-nek a fele stb. De akár 10-ig színezzük így a számokat, akár olyan messzeségekig, mint a hinduk, mindez csak szerény kis töredéke a végtelen számsornak, amely ezen túl szürkén hömpölyög tovább.

Tudjuk ugyan, hogy vannak páros számok, igen, minden második szám páros:

$$1, \underline{2}, 3, \underline{4}, 5, \underline{6}, 7, \underline{8}, 9, \underline{10}, 11, \underline{12}, ...$$

ugyanígy minden harmadik szám osztható 3-mal:

$$1, 2, \underline{3}, 4, 5, \underline{6}, 7, 8, \underline{9}, 10, 11, \underline{12}, ...$$

minden negyedik szám 4-gyel:

$$1, 2, 3, \underline{4}, 5, 6, 7, \underline{8}, 9, 10, 11, \underline{12}, ...$$

s í. t., ezek azonban csak kisebb-nagyobb hullámokat jelentenek, melyek, ha egyszer megindultak, egyhangúan, egyformán gördülnek tovább. Valóban nincs semmi váratlan, semmi egyéni szeszély, ami felélénkíthetné ezt az egyhangúságot?

De van: a prímszámok szeszélyes, szabályokba nem szorítható eloszlása. Gondoljunk az oszthatóságra:

$$\begin{aligned} 10 \text{ összes osztói: } & 1, 2, 5, 10, \\ 12 \text{ összes osztói: } & 1, 2, 3, 4, 6, 12, \\ \text{közben } 11 \text{ összes osztói: } & 1, 11. \end{aligned}$$

1-gyel és önmagával minden szám osztható; vannak számok, amelyek e kettőn kívül semmi mással: ilyen például a 11. Ezeket a számokat nevezik törzsszámoknak vagy prímszámoknak.

Az 1 e szempontból rendellenesen viselkedik; csak egy osztója van: 1, és ez egyszersmind önmaga. Ezért 1-et nem szokás a prímszámok közé sorolni. Az 1 neve *egység*. Eszerint a legkisebb prímszám a 2, ez egyszersmind az egyetlen páros prímszám, mert minden páros szám osztható 2-vel és ez a szám prímszám voltát csak akkor nem rontja el, ha ez a 2-es osztó maga a szám.

Prímtényezőkre bontás

Jelentőséget az ad a prímszámoknak, hogy minden más szám ezekből az építőkövekből rakható össze; éppen ezért nevezik a többi számot összetett számnak. Pontosabban úgy fogalmazható ez meg, hogy minden összetett szám csupa prímszám szorzataként állítható elő.

Próbáljuk például 60-at szorzatként írni fel:

$$60 = 6 \cdot 10$$

Itt 6 és 10 is tovább bontható tényezőkre:

$$6 = 2 \cdot 3 \quad \text{és} \quad 10 = 2 \cdot 5,$$

ezeket beírva 6 és 10 helyére:

$$60 = 2 \cdot 3 \cdot 2 \cdot 5$$

és itt már minden tényező prímsszám.

Másképp is hozzáfoghattunk volna ehhez, hiszen a 60-at nagyon sokféleképpen lehet két szám szorzataként felírni. Ha ebből indulunk ki:

$$\begin{aligned} & 60 = 4 \cdot 15, \\ \text{itt} \quad & 4 = 2 \cdot 2 \quad \text{és} \quad 15 = 3 \cdot 5, \\ \text{tehát} \quad & 60 = 2 \cdot 2 \cdot 3 \cdot 5, \end{aligned}$$

ha pedig ezt a felbontást választjuk:

$$\begin{aligned} & 60 = 2 \cdot 30, \\ \text{akkor} \quad & 30 = 5 \cdot 6 \quad \text{és itt} \quad 6 = 2 \cdot 3, \quad \text{tehát} \quad 30 = 5 \cdot 2 \cdot 3, \\ \text{vagy} \quad & 30 = 2 \cdot 15 \quad \text{és itt} \quad 15 = 3 \cdot 5, \quad \text{tehát} \quad 30 = 2 \cdot 3 \cdot 5, \\ \text{vagy} \quad & 30 = 3 \cdot 10 \quad \text{és itt} \quad 10 = 2 \cdot 5, \quad \text{tehát} \quad 30 = 3 \cdot 2 \cdot 5; \end{aligned}$$

látjuk tehát, hogy 30 mindenképpen a 2, 3 és 5 prímszámok szorzatára bomlik; e szorzatot írva 30 helyébe

$$60 = 2 \cdot 2 \cdot 3 \cdot 5.$$

Bármi módon fogunk is hozzá, csak ugyanazon prímszámokra esik szét 60, legfeljebb más sorrendben lépnek fel ezek. Ugyanilyen könnyű bármely más összetett számot is felbontani ,,prímtényezőire'' (és be lehet bizonyítani, hogy mindig csak egyféle felbontásra juthatunk). Ha első pillanatra megakadunk azon, hogyan is fogjunk hozzá, gondoljuk meg, hogy a szám legkisebb osztója (1-en kívül) biztosan prímszám, mert ha az is összetett szám volna, akkor kellene önmagánál kisebb osztójának lenni, és ez persze az eredeti számban is megvolna maradék nélkül. Tehát mindig a legkisebb osztót keresve, szépen legöngyölíthetők bármely szám prímtényezői, például:

$$\begin{aligned} 90 &= 2 \cdot 45 \\ &= 2 \cdot \overbrace{3 \cdot 15} \\ &= 2 \cdot 3 \cdot \overbrace{3 \cdot 5} \end{aligned}$$

Egy ilyen felbontás jól bevilágít a szám szerkezetébe, pl. kiolvasható belőle, hogy 90 osztói 1-en kívül:

egytényezősök: $2, 3, 5,$

kéttényezősök: $2 \cdot 3 = \underline{6}, \quad 2 \cdot 5 = \underline{10}, \quad 3 \cdot 3 = \underline{9}, \quad 3 \cdot 5 = \underline{15},$

háromtényezősök: $2 \cdot 3 \cdot 3 = \underline{18}, \quad 2 \cdot 3 \cdot 5 = \underline{30}, \quad 3 \cdot 3 \cdot 5 = \underline{45},$

négytényezős: $2 \cdot 3 \cdot 3 \cdot 5 = \underline{90}.$

A prímtényezőkre bontás javasolt módja az, hogy az adott számot elosztjuk a legkisebb számmal, amelyik a számnak az osztója. A hányadost ismét elosztjuk a benne található legkisebb prímszámmal és ezt addig ismételjük, amíg a hányados 1 lesz. Az így előállított prímszámok az adott szám prímtényezői. Az eljárás áttekinthető, ha az adott számot leírjuk és a szám mellé húzunk egy függőleges vonalat, majd mellé írjuk az első prímszámosztót. A hányadost a szám alá írjuk, s az előbbi lépést addig ismételjük, míg hányadosul 1-et nem kapunk.

Például határozzuk meg ily módon 1512 prímtényezőit:

1512	2
756	2
378	2
189	3
63	3
21	3
7	7
1	

Az adott szám prímszámtényezőkre bontva tehát:

$$1512 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 3 \cdot 7.$$

Mivel gyakran előfordul több közös tényező, ezért a prímtényezős alakban való felírás rövidíthető, ha az egyenlő tényezőket *hatvány* kifejezésként írjuk fel. Erre a következő

jelölés szolgál: $2{\cdot}2{\cdot}2 = 2^3$ (olv.: kettő a harmadikon vagy kettő a köbön); $3{\cdot}3{\cdot}3 = 3^3$. A közös tényezőt, pl. a 2-t vagy a 3-at a hatvány *alapjának*, a fölé írt számot, amely megmutatja, hogy az alapot hányszor kell tényezőül venni, *kitevőnek* nevezzük. Ezzel a rövidített írásmóddal az 1512 prímtényezős alakja:

$$1512 = 2^3 \cdot 3^3 \cdot 7.$$

Most már fel tudjuk írni szép formában a már korábban felbontott 60-as számot is:

$$60 = 2^2 \cdot 3 \cdot 5.$$

Olvasd: hatvan egyenlő kettő a másodikon[1] szorozva hárommal szorozva öttel.

Ha ezek után leírom Hardy és Rámánudzsan taxijának számát két köbszám összegeként kétféle módon, akkor ezt a felírást már tudjuk értelmezni:

$$1729 = 10^3 + 9^3 \quad \text{és} \quad 1729 = 12^3 + 1^3.$$

Eratosztenész szitája

Próbáljuk felírni rendre a prímszámokat. Már tudjuk, hogy a legkisebb prímszám a 2, és innen kezdve a páros számokat nyugodtan át lehet ugrani, hiszen ezek mind oszthatók 2-vel. 3 is, 5 is, 7 is prímszám; az ember szeretné rámondani, hogy a 9 is, de ez nem igaz, hiszen 9 osztható 3-mal. Most azt gondolnók, hogy innen kezdve ritkulnak a prímszámok; ez megint nem igaz, mert 11 és 13 is prímszám.

Még a régi görögöktől maradt ránk egy szellemes ötlet, amely tévedés lehetősége nélkül, gépiesen állítja elő ezt a szeszélyes sorozatot: az ún. Eratosztenész-féle rosta. Írjuk fel a számokat 2-től 50-ig; e sorozat első tagja látatlanban is biztosan prímszám, hiszen minden valódi osztója kisebb volna nála s így (1-en kívül) előtte szerepelne a sorozatban, előtte azonban nincs semmi. Most nézzük meg, hogy mi ez az első szám: 2. Minden második szám 2-nek többszöröse és így 2 kivételével nem prímszám, tehát innen kezdve húzzunk ki minden második számot:

$$\textcircled{2}, 3, \cancel{4}, 5, \cancel{6}, 7, \cancel{8}, 9, \cancel{10}, 11, \cancel{12}$$

A legelső szám, ami 2 után épségben maradt, ismét csak prímszám lehet, hiszen csak előtte szereplő számnak lehetne többszöröse, előtte pedig csak olyan szám van, melynek többszöröseit kihúztuk. Nézzük meg ezt a számot: 3. Minden harmadik szám 3-nak többszöröse, tehát húzzunk ki innen kezdve minden harmadik számot (nem baj, hogy így egyes számokat kétszeresen is áthúzunk):

$$\textcircled{2}, \textcircled{3}, \cancel{4}, 5, \cancel{6}, 7, \cancel{8}, \cancel{9}, \cancel{10}, 11, \cancel{12}$$

Ha 12-ig bezárólag vagyunk kíváncsiak a prímszámokra, akkor tovább már nem is kell mennünk, mert az első fennmaradó szám 5, és ennek a 3-szorosánál nagyobb többszörösei már túl vannak 12-n, kisebb többszörösei pedig már mind a kihúzott számok közt szerepelnek. 12-ig tehát a következő prímszámokat találtuk: $2, 3, 5, 7, 11$.

[1] vagy kettő a négyzeten

Gépet is lehetne szerkeszteni, mely az itt adott utasítást végrehajtja, és így hibátlanul ontja a prímszámokat egy bizonyos határig.[2] Ez azonban mit sem változtat azon, hogy a prímszámok minden határon túl a legszeszélyesebben bukkannak fel újra meg újra.

Így például meg lehet mutatni, hogy bármilyen nagy réseket találhatunk köztük, ha elég messzire megyünk a számsorban. Például egy legalább 6 egységnyi rést, azaz hat egymást követő olyan számot, amelyek egyike sem prímszám, adnak a következő műveletek eredményei:

$$\underline{2}\cdot 3\cdot 4\cdot 5\cdot 6\cdot 7+2,\quad 2\cdot \underline{3}\cdot 4\cdot 5\cdot 6\cdot 7+3,$$
$$2\cdot 3\cdot \underline{4}\cdot 5\cdot 6\cdot 7+4,\quad 2\cdot 3\cdot 4\cdot \underline{5}\cdot 6\cdot 7+5,$$
$$2\cdot 3\cdot 4\cdot 5\cdot \underline{6}\cdot 7+6,\quad 2\cdot 3\cdot 4\cdot 5\cdot 6\cdot \underline{7}+7,$$

mert ezek valóban egymást követő számok: mindegyik éppen 1-gyel több az előzőnél, és egyik sem prímszám, hiszen $2\cdot 3\cdot 4\cdot 5\cdot 6\cdot 7$ minden egyes tényezőjével osztható, tehát az első közülük olyan összeg, melynek mindkét tagja osztható 2-vel, a második hasonló okokból 3-mal osztható, a harmadik 4-gyel, a negyedik 5-tel, az ötödik 6-tal és a hatodik 7-tel. Kiszámítva

$$2\cdot 3\cdot 4\cdot 5\cdot 6\cdot 7=5040,$$

tehát itt a következő hat számról van szó:

$$5042, 5043, 5044, 5045, 5046, 5047.$$

Ezek elég nagy számok, elég messze kell mennünk a számsorban, hogy ezen a módon 6-tagú rést találjunk a prímszámok közt (persze lehetséges, hogy már jóval előbb van közöttük ilyen rés).[3] De ha nem sajnálunk jó messzire menni, legalább 100 tagú rést is találhatunk ugyanígy, ha 2-től 101-ig terjedő számok

$$2\cdot 3\cdot 4\cdot 5\cdot\cdots 101,$$

szorzatához adunk hozzá sorra 2-t, 3-at, ... végül 101-et. Ezen a módon találhatunk bármilyen hosszú réseket is.

Mindamellett, ameddig csak megvizsgálták a számsort, újra meg újra, bármilyen hosszú réseken túl is, találtak szomszédos páratlan számokat, amelyek prímszámnak bizonyultak, mint például a számsor elején 11 és 13, vagy 29 és 31. A matematikusok azt sejtik, hogy ilyen ,,ikerprímszámok'' minden távolságban előfordulnak, a számsor megvizsgált részén túl is; de ezt ilyen általánosságban mindmáig nem sikerült bebizonyítani.

Mennyi prímszám van?

Dehát vannak-e egyáltalán prímszámok minden távolságban? Nemcsak a számsor elejét színezik-e ezek egy darabon? Erre a kérdésre már van válaszunk, méghozzá

[2] Beszéltünk is róla, hogy ezzel a módszerrel keresik a prímszámokat a szuperszámítógépekkel.

[3] Valójában elég venni a $2\cdot 3\cdot 5\cdot 7+2$-t és az azt követő 5 számot. De ez a módszer sem adja meg az első legalább 6 egymást követő összetett számot $(90, 91, ..., 96)$.

2000 év óta: Euklidész közölt egy igen elegáns bizonyítást arra, hogy végtelen sok törzsszám van.

Bárhol is mondja valaki, hogy itt a vége, nem futhat el véle, mert meg tudom mutatni, hogy van prímszám azon túl is.

Elég ezt egy esetben megmutatni; minden más esetben ugyanígy megy. Csak azt kell ehhez meggondolnunk, hogy 2-vel minden második szám osztható, 3-mal minden harmadik s í. t., tehát egy 2-vel osztható szám közvetlen rákövetkezője nem lehet osztható 2-vel, egy 3-mal osztható szám közvetlen rákövetkezője nem lehet osztható 3-mal s í. t. Ha mármost valaki azt állítaná, hogy a prímszámok a következők:

$$2, 3, 5, 7$$

és itt a vége, akkor én azonnal megcáfolom, hiszen a felsorolt törzsszámokból megalkothatom a következő számot:

$$2 \cdot 3 \cdot 5 \cdot 7 + 1.$$

$2 \cdot 3 \cdot 5 \cdot 7$ osztható 2-vel is, 3-mal is, 5-tel is, 7-tel is. A közvetlenül rákövetkező $2 \cdot 3 \cdot 5 \cdot 7 + 1$ szám tehát ezek egyikével sem lehet osztható. Dehát valamilyen prímszámmal csak oszthatónak kell lennie szegénynek, ő is csak szám, ő is prímszámokra bontható, vagy esetleg maga is prímsszám és önmagával mindenesetre osztható. Az illető tehát tévedett: kell lenni prímszámnak 7-en túl is. És ugyanígy minden prímszámon túl is.

Számítsuk csak ki ezt a $2 \cdot 3 \cdot 5 \cdot 7 + 1$ számot: az eredmény 211. Egy kis próbálgatás megmutatja, hogy ez 1-en és önmagán kívül mással nem osztható, vagyis véletlenül törzsszám. Tehát ő maga az a 7-en túli törzsszám, aminek a létezését állítottam. Persze szó sincs róla, hogy ez a 7-et közvetlenül követő törzsszám volna: az egy pillanatig sem volt várható, hogy az egymást követő törzsszámokat ilyen szabályszerűen lehetne megszerkeszteni.

Módszerünk pontosabban azt az eredményt adja, hogy 7-től legfeljebb $2 \cdot 3 \cdot 5 \cdot 7 + 1$-ig, ugyanígy 11-től legfeljebb $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1$-ig s í. t. kell menni, hogy újabb törzsszámot találjunk. Ezek azonban elég nagy távolságok; nem lehetne-e szűkebb határok közt törzsszámokat találni?

Sokan foglalkoztak ezzel a kérdéssel. Hogy csak egy szép eredményt említsek: Csebisev orosz matematikus bebizonyította, hogy 2-től kezdve bármely szám és a kétszerese között is mindig van prímszám:

2 és 4 közt	3
3 és 6 közt	5
4 és 8 közt	5 is, 7 is
5 és 10 közt	csak 7

bár ebben semmi szabályszerűség sem látszik, ez mégis minden messzeségben bekövetkezik; sőt ha elég messzire megyünk, elég nagy számokat választunk, akárhány prímszám is esik a számok és kétszereseik közé. Íme mégis valami szabályféle a féktelennek látszó prímszámok számára: bármennyire mégsem rugaszkodhatnak el egymástól.