Prímszámok, prímtényezőkre bontás

Az alábbi szöveg Péter Rózsa Játék a végtelennel *című könyvéből származik. Néhány kisebb módosítás, kiegészítés viszont történt.*

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, hiszen $10^3 + 9^3$ is és $12^3 + 1^3$ is 1729.

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. Emlékezzünk csak 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.

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 már láttuk, hogy 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. Rendbe szedve és az egyenlő tényezők szorzatát hatványalakban írva

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

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

Tehát érdemes a számok építőköveivel közelebbről is megismerkedni. 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: $2, 3, 5, 7, 11$.

Gépet is lehetne szerkeszteni, mely az itt adott utasítást végrehajtja, és így hibátlanul ontja a prímszámokat egy bizonyos határig. Beszéltünk is róla, hogy ezzel a módszerrel keresik a prímszámokat a szuperszámítógépekkel. 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: