Érdekes informatika feladatok

IV. rész

A prímszámok előállítása

A *prímszámok* vagy *törzsszámok* igencsak nagy jelentőséggel bírtak a matematika történetében. A természetes számok vagy az egész számok *atomjainak* is nevezzük őket. A prímszámok fogalmát minden valószínűség szerint már az egyiptomiak és a mezopotámiaiak is ismerték, de tudomásunk szerint első komoly tanulmányozói a püthagoreusok voltak, és pontos meghatározást e fogalomra csak Eukleidésznél (Kr. e. 300 körül) találunk.

A prímszám fogalma szorosan összefügg az *oszthatósággal*. Ha $a = b \cdot c$, akkor b és c az a szám *valódi osztói*. Minden szám felírható mint 1-nek és önmagának a szorzata, ezért az 1 és a szám maga az adott szám *triviális osztói*.

Így a prímszám fogalmára több definíció is adható:

- *Azokat a természetes számokat, amelyeknek csak triviális osztói vannak, prímszámoknak nevezzük.*
- *Azokat a természetes számokat, amelyeknek pontosan két osztója van (1 és önmaga), prímszámoknak nevezzük.*
- *Azokat a természetes számokat, amelyek nem bonthatók fel nála kisebb természetes számok szorzatára, prímszámoknak nevezzük.*

Az 1 és a 0 nem prímszámok, mert az 1-nek egy darab, a 0-nak pedig végtelen sok osztója van. A 2 a legkisebb prímszám, egyben ő az egyetlen páros prímszám. Prímszámok: 2, 3, 5, 7, 11, 13, 17, 19, 23, 31 stb.

A prímszámok a természetes számok „atomjai", vagyis minden természetes vagy prímszám, vagy felbontható prímszámok szorzatára – a számelmélet alaptétele szerint. Azok a számok, amelyek nem prímszámok, összetett számok. Kivételt képez a 0 és az 1, ezek nem prímszámok, de összetett számok sem.

Ha pontosan akarjuk megfogalmazni a definíciót, akkor ezt mondhatjuk: *Összetett számoknak nevezzük azokat a természetes számokat, amelyeknek 2-nél több, de véges számú osztója van.*

Bármely összetett szám, a tényezők sorrendjétől eltekintve, egyértelműen felírható prímszámok szorzataként (prímtényezős felírás).

Vagyis: ha a összetett szám, akkor $a = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_n^{k_n}$, ahol p_1, p_2, ..., p_n prímszámok, k_1, k_2, ..., k_n pedig 0-nál nagyobb hatványkitevők.

Így könnyen kiszámítható egy szám osztóinak is a száma, ez egyenlő $(k_1 + 1) \cdot (k_2 + 1) \cdot \ldots \cdot (k_n + 1)$.

Két vagy több természetes szám *relatív prím*, ha legnagyobb közös osztójuk az 1, vagyis nincs közös prímtényezőjük.

Prímszámokkal kapcsolatban a következő kérdések foglalkoztatják ma is a matematikusokat:

- *prímszámok előállítása*
- *egy szám prímszám-e vagy sem?*
- *prímszámok típusai*
- *minél nagyobb prímszámot keresni*
- *prímszámok eloszlása*

Prímszámok előállítására ma is gyakran használt módszer az úgynevezett Eratoszthenész-szita. Eratoszthenész (Kr. e. 276.-197.) görög matematikus, az észak-

afrikai Kirénében született. Sok évet töltött Athénben, majd Ptolemaiosz egyiptomi király meghívta Alexandriába fia nevelőjének és a könyvtár igazgatójának. Foglalkozott grammatikával és filozófiával, csillagászattal és fizikával, de költészettel is. Ő végezte a Föld felületén az első fokmérést, és az akkori mérési módszerek fejlettségéhez képest elég pontosan kiszámította az egyenlítő hosszát. Idős korában megvakult és önkéntes éhhalált halt.

A nevéhez fűződő módszer lényege az, hogy az 1-nél nagyobb természetes számok közül „kiszitáljuk" az összetett számokat, így a prímszámok maradnak meg.

Az algoritmus egyszerű:

1. Felírjuk a természetes számokat 2-től *n*-ig.
2. Bekarikázzuk az első számot, a 2-est, ezután kihúzzuk az összes többszörösét.
3. Megkeressük az utolsó bekarikázott számnál nagyobb első ki nem húzott számot, bekarikázzuk, majd *n*-ig kihúzzuk az összes többszörösét.
4. A 3.as lépést addig folytatjuk, ameddig minden szám be lesz karikázva vagy ki lesz húzva.
5. A kihúzott számok az összetett számok, a bekarikázott számok a prímszámok.

A fenti algoritmust a következőképpen lehet javítani:

- Ha *n*-ig keressük a prímszámokat, a ciklus elegendő ha csak *round*($\sqrt{n}$)-ig megy.
- Amit már egyszer kihúztunk, még egyszer nem kell kihúzzuk.
- A számok felírásából már eleve elhagyhatjuk a 2-nél nagyobb páros számokat, négyzetszámokat stb. – így a szita sokkal kisebb lesz.

Ha azt akarjuk megmondani egy számról, hogy prímszám-e vagy sem, akkor úgy járhatunk el, hogy megkeressük a szám osztóit, és ha 1-en és önmagán kívül van más osztója is, akkor nem prímszám (kivétel 0 és 1). Természetesen itt is elegendő ha csak *round*($\sqrt{n}$)-ig vizsgáljuk meg az osztókat.

A fent említett algoritmusok azonban nagy prímek esetében nagyon hosszú ideig futnak. Ha gyors prímtesztet akarunk, akkor más matematikai meglátásokat is segítségül kell hívni.

Például a *kis-Fermat tételt*. A második, vagy kis-Fermat tétel a következőt mondja ki: Ha *p* prímszám, *a* pedig egy olyan tetszőleges egész szám, amely nem osztható *p*-vel, akkor az a^{p-1}-t *p*-vel osztva 1-t ad maradékul. Ezen az eredményen alapszik az úgynevezett AKS-algoritmus, amelyet Indiában dolgoztak ki 2002 nyarán, és amelyik polinomiális időben meg tudja mondani egy számról, hogy prím-e vagy sem. Sajnos, e páratlanul szép elméleti eredményt nagyon körülményes a gyakorlatban leprogramozni, a program amennyit nyer a prím-teszten, kb. annyit veszít a más adatstruktúrák és algoritmusok nagysága és lassúsága miatt.

Sok matematikus próbált a prímszámok előállítására képletet találni, de ezek a kísérletek nem jártak gyakorlati sikerrel, elméletileg viszont prímszám típusokat, osztályokat tudtak felállítani.

Milyen típusú prímszámok léteznek?

Euler a következő képlettel kísérletezett: $p(n) = n^2 + n + 41$. Ez a képlet prímszámokat ad n = 1-től n = 39-ig, viszont n = 40 illetve n = 41 esetén a kapott szám már összetett.

A páratlan prímszámok két osztályba sorolhatók:

- $4n + 1$ alakú, ahol n természetes szám. Pl.: 5, 13, 17, stb.
- $4n - 1$ alakú prímek, ahol n természetes szám. Pl.: 3, 7, 11, stb.

Viszont az is igaz, hogy nem minden n-re adnak a fenti képletek prímszámokat.

Fermat tétele szerint (a tétel bizonyítását Fermat nem közölte, jóval később Euler bizonyította be még egyszer) a $4n + 1$ alakú prímek előállíthatók két négyzetszám összegeként (Pl. $5 = 1^2 + 2^2$, $13 = 2^2 + 3^2$, $17 = 1^2 + 4^2$), a $4n - 1$ alakúak viszont sohasem állíthatók elő két négyzetszám összegeként.

Hasonlóan a 3-nál nagyobb prímszámok:

- $6n + 1$ vagy
- $6n - 1$ alakúak, ahol n természetes szám,

de itt is az ilyen alakú természetes számok között vannak összetettek is (Pl. $49 = 6 \cdot 8 + 1$, $35 = 6 \cdot 6 - 1$).

Általában a prímszámok $a \cdot n + b$ alakúak, ahol n egész szám, a és b pedig relatív prímek. Ha n végigfut a természetes számokon, akkor ezek a számok adott a és b esetén számtani sorozatot alkotnak. Ebben az esetben is a számtani sorozat tagjai között találunk összetett számokat is.

Nem ad mindig prímszámot az $n^2 + 1$ képlet sem.

Fermat-féle prímeknek nevezzük a $2^{2^n} + 1$ alakú prímszámokat, viszont nem minden prímszám ilyen alakú és ez a képlet sem eredményez mindig prímszámokat. Fermat csak az első öt ilyen prímszámot számította ki, Euler viszont kimutatta, hogy a hatodik ($4\,294\,967\,297 = 641 \cdot 6\,700\,417$) már nem prímszám. Gauss alig 19 évesen egy érdekes geometriai összefüggést bizonyított be. E szerint körzővel és vonalzóval csak azok a páratlan oldalú szabályos n-oldalú sokszögek szerkeszthetők meg, amelyekre n Fermat-féle prím, vagy különböző Fermat-féle prímek szorzatával egyenlő.

Mersenne-féle prímeknek nevezzük a $2^p - 1$ alakú prímszámokat, ahol p prímszám. Mersenne (1588-1648) francia matematikus Descartes osztálytársa volt és a prímszámok szerelmese. Eddig mindössze 38 darab Mersenne-féle prím ismert, és a talált legnagyobb prímszámok mind ilyen alakúak. Sajnos a Mersenne képlet szerint előállítható számok között is nagyon sok összetett van, és nem mindegyik prímszám írható fel ilyen alakban.

A sok próbálkozás dacára most már jól látjuk, hogy a prímszámok előállításához szükséges általános képlet vagy nem létezik, vagy felfedezése még várat magára!

Eukleidész már bebizonyította azt is, hogy *a prímszámok sorozata végtelen*. A tétel bizonyítása nagyon egyszerű. Tegyük fel, hogy véges számú prímszám van: $p_1, p_2, ..., p_n$, de ebben az esetben a $p_1 \cdot p_2 \cdot ... \cdot p_n + 1$ természetes szám nem osztható a $p_1, p_2, ..., p_n$ prímek egyikével sem, hanem 1 maradékot adna. Ez viszont ellentmond a számelmélet alaptételének.

A kezdetektől fogva a matematikusok között heves versengés alakult ki, hogy ki talál minél nagyobb prímszámot. A számítógépek megjelenése csak fokozta ezt a versenyt, hisz segítségével nagyon nagy számokról meg lehet állapítani, hogy prímek-e vagy sem.

A legkisebb prímszám a 2, de vajon melyik az eddig ismert legnagyobb prím?

Az ókorban csak kevés prímszámot ismertek. Nagyon nagy számokról megállapítani, hogy prím-e jóval meghaladta képességüket. Euler 1750-ben megállapította, hogy $2^{31} - 1$ prímszám. Jó száz éven keresztül ez volt a legnagyobb ismert prímszám: 2 147 483 647. 1876-ban Lucas bebizonyította, hogy $2^{127} - 1$ prímszám: 170 141 183 460 469 231 731 687 303 715 884 105 727.

A számítógépek megjelenésével rohamosan kerültek elő a következő nagy prímek is: $2^{521} - 1$, $2^{607} - 1$, $2^{1279} - 1$, $2^{2203} - 1$, $2^{2281} - 1$, $2^{3217} - 1$, $2^{4253} - 1$, $2^{4423} - 1$, $2^{9941} - 1$, $2^{11\,231} - 1$, amelyet az Illinois-i Egyetem számítógépén számítottak ki.

1991. előtt a legnagyobb ismert prímszám: $2^{216\,091} - 1$ volt, amelyet David Slowinski talált egy Cray X-MP szuperszámítógép segítségével.

1998. január 27-én Roland Clarkson floridai programozó George Woltman számítógépes programjával talált egy ennél nagyobb, 909 526 számjegyű prímszámot.

1999-ben ez a rekord is megdőlt, Nayan Hajratwala 2 098 960 számjegyű Mersenne-féle prímet talált. A program egy Pentium II 350 MHz-es számítógépen futott 111 napig. A prímszám: $2^{6\,972\,593} - 1$.

A következő prímszámot, a $2^{13\,466\,917} - 1$-et, 2001-ben találta meg a 20 éves kanadai Michael Cameron egy több résztvevős internetes prímszámkereső projekt keretében (*Nagy Internetes Mersenne-féle Prímkutatás* [GIMPS]). Ez a szám 4 053 946 számjegyet tartalmaz, és egy embernek három hétig kellene egyfolytában írnia, hogy a végére érjen. Cameron egy egyszerű otthoni számítógépet használt, amely 45 napig futtatta a programot.

Két év múlva, tavaly, 2003-ban megdőlt ez a rekord is. A következő eddigi legnagyobb prímszámot, $2^{20\,996\,011} - 1$-et, Michael Shafernek, a michigani állami egyetem 26 éves végzős vegyészmérnök hallgatójának sikerült megtalálnia. Ez a prímszám 6 320 430 számjegyből áll, több mint 2 000 000 számjeggyel haladja meg az előzőleg megtalált prímszámot. A kereső-program az egyetem 2 GHz-es Pentium 4-es számítógépén futott 19 napig.

A GIMPS projekt mintegy 211 000 számítógépet használ, ezek hálózatba vannak kötve és ugyanaz a prímszámkereső program fut rajtuk egyidejűleg. A projektben mintegy 60 000 önkéntes, diák, iskolás, egyetemista, kutató, tanár és cég alkalmazott vesz részt. Láthattuk, hogy a résztvevők csupán két év eltelte után újabb prímet találtak, ez egyetlen számítógépen 25 ezer évbe telt volna.

A versenynek tétje is van: az első tízmillió számjegyből álló prím megtalálóját az amerikai *Electronic Frontier Foundation* 100 000 dollárral jutalmazza.

Végül szóljunk érdekességképpen egy pár szót a prímszámok eloszlásáról is. Mint már említettük, a prímszámok sorozata végtelen. Korán felvetődött az a kérdés is, hogy a prímszámok miként oszlanak el a természetes számok között. Láthattuk, hogy 10-ig 4 darab, 100-ig 25 darab, 1000-ig 168 darab, 10 000-ig viszont 1239 darab prímszám van. Ha Eratoszthenész szitáját vizsgáljuk, akkor azt vesszük észre, hogy a szita elején sokkal több prímszám van. Tehát minél nagyobb számokból álló intervallumban keresünk, annál kevesebb számú prímet találunk.

Gauss már 15 éves korában megsejtette azt, hogy a prímszámok száma fordítottan arányos a számok logaritmusával, de igazolni nem tudta sejtését.

A prímszámok gyakoriságával foglalkozott Legendre és Csebisev is. Csebisev (1821-1894) orosz matematikus bebizonyította Bertrand (1822-1900) francia matematikus sejtését, azt hogy minden n természetes számra n és $2n$ között létezik prímszám.

Gauss sejtését csak 1896-ban sikerült igazolni Poussin belga és Hadamard francia matematikusoknak.

Ma sem bizonyított sejtés, hogy két négyzetszám között mindig van prímszám, viszont bizonyított az, hogy a prímszámok között tetszőleges hézagok vannak. Például *ikerprímeknek* nevezzük azokat a prímszám-párokat, amelyeknek különbsége 2. Pl. 3 és 5, 11 és 13, 5 971 847 és 5 971 849. Úgy tűnik, hogy végtelen sok ikerprím van, de ezt sem sikerült még a mai napig sem bizonyítani. A prímszámok még egy jó ideig megmaradnak tehát matematikai és informatikai kuriózumoknak!

Kovács Lehel István