Műhelysarok

A PRÍMSZÁMOK KIVÁLASZTÁSA

Olosz Ferenc tanár, Szatmárnémeti

Gyakran előfordul, hogy egy számról feltétlen tudnunk kell, hogy az prímszám-e vagy sem. A kisebb prímszámokat kívülről tudjuk, nagyobb számok esetén pedig vagy prímszámtáblázatot használunk, vagy utánaszámolunk. Az A természetes számról számítással úgy döntjük el, hogy prímszám-e vagy sem, hogy megnézzük, osztható-e a szám a $\sqrt{A}$-nál kisebb prímszámok valamelyikével. Ha nem osztható egyikkel sem, akkor A prímszám, ellenkező esetben összetett szám.

Egy adott számnál kisebb prímszámok kiválasztásának több mint két évezredes módszere az Eratoszthenész-féle szita, amely a már ismertté vált prímszámok többszöröseinek eltávolításával keresi az újabb prímszámokat. Lévén, hogy e módszer közismert, ezért nem térünk ki a részletes ismertetésre, csupán csak annyit jegyzünk meg, hogy ha az induló táblázatba a 2 mellé csak a páratlan számokat írjuk be (sőt az 5-ön kívül a többi 5-ben végződő számot is kihagyjuk), akkor valamivel kevesebbet kell dolgozzunk.

Az eddig látottak alapján egy nagy szám teszteléséhez szükségünk van az illető szám négyzetgyökénél kisebb prímszámokra és az ezekkel való oszthatóság vizsgálatára, így csak nagyon sok munkával lehet eldönteni, hogy az prímszám-e vagy sem.

Az évszázadok során a prímszámok kiválasztására sokan próbáltak hatékonyabb módszereket találni, de napjainkig se történt e téren lényeges javulás.

Az 1770-ben felfedezett Wilson-tétel (amely kimondja, hogy egy adott p szám akkor és csak akkor prímszám, ha $(p-1)!+1$ osztható p-vel) a prímszámok kiválasztására teljesen alkalmatlan, viszont az elméleti bizonyításokban jól használható.

Mint érdekességet mutatjuk be S. P. Sudar hindu matematikus által szerkesztett táblázatot, amellyel egy adott nagyságig a páratlan összetett számokat lehet kiválasztani (azért csak a páratlanokat, mert a 2 kivételével minden páros számról eleve tudjuk, hogy összetett szám). A táblázatot a számtani haladványok segítségével állítjuk össze, és a kiválasztás helyességének bizonyításánál a számtani haladvány általános tagját használjuk, így e módszer ismertetésével a haladványok alkalmazásának egy újabb lehetőségét tárjuk fel.

Tudjuk, hogy a számtani haladvány az $a_{n+1} = a_n + r$ rekurzióval értelmezett sorozat, bármely $n \in \mathbb{N}^*$ esetén, ahol a_1 és r adott számok. A számtani haladvány általános tagja $a_n = a_1 + (n-1)r$.

Egy olyan táblázatot készítünk, amelyben soronként és oszloponként számtani haladványokat írunk. Az első sorban, illetve oszlopban a kezdő tag $a_1 = 4$, és az állandó különbség (ráció) $r_1 = 3$. A többi sorban (oszlopban) a kezdő tag az illető sorban (oszlopban) szereplő első szám, és a ráció soronként (oszloponként) az előző sorhoz (oszlophoz) viszonyítva 2-vel növekszik (tehát ez is számtani haladvány).

Tétel: *Ha valamely A természetes szám megtalálható e táblázatban, akkor $2A+1$ összetett szám, ha pedig az A szám nem található meg e táblázatban, akkor $2A+1$ prímszám.*

Bizonyítás: A számtani haladvány általános tagja alapján az n-edik sorban (oszlopban) az első tag $4 + (n-1)\cdot 3 = 3n+1$, és a ráció $r_n = 3 + (n-1)\cdot 2 = 2n+1$.

Ezek alapján az n-edik sorban és k-adik oszlopban található elem a következőképpen néz ki: $a_{nk} = (3n+1) + (k-1)\cdot r_n = 3n+1+(k-1)(2n+1) = n + k(2n+1)$, $n, k \in \mathbb{N}^*$.

Ha az A szám a táblázatunkban megtalálható, akkor $A = n + k(2n + 1)$ alakú, így $2A + 1 = 2[n + k(2n + 1)] + 1 = 2n + 2k \cdot 2n + 2k + 1 = (2n + 1)(2k + 1)$, ami azt jelenti, hogy $2A + 1$ összetett szám. Tehát a táblázatból vett bármely A szám esetén $2A + 1$ összetett szám.

Az állítás fordítva is igaz, mert minden $2A + 1$ páratlan összetett szám felírható két páratlan természetes szám szorzataként, és ha $2A + 1 = (2n + 1)(2k + 1)$, akkor

$$A = \frac{(2n + 1)(2k + 1) - 1}{2} = \frac{2k(2n + 1) + 2n}{2} = n + k(2n + 1) = a_{nk},$$

ami azt jelenti, hogy A megtalálható a táblázatunk n-edik sorában és k-adik oszlopában.

	$r_1 = 3$	$r_2 = 5$	$r_3 = 7$	$r_4 = 9$	$r_5 = 11$	$r_6 = 13$	$r_7 = 15$	$r_8 = 17$	...
$r_1 = 3$	4	7	10	13	16	19	22	25	...
$r_2 = 5$	7	12	17	22	27	32	37	42	...
$r_3 = 7$	10	17	24	31	38	45	52	59	...
$r_4 = 9$	13	22	31	40	49	58	67	76	...
$r_5 = 11$	16	27	38	49	60	71	82	93	...
$r_6 = 13$	19	32	45	58	71	84	97	110	...
$r_7 = 15$	22	37	52	67	82	97	112	127	...
$r_8 = 17$	25	42	59	76	93	110	127	144	...
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	

E tétel értelmében, ha egy páratlan B számról el akarjuk dönteni, hogy prímszám-e vagy sem, akkor megnézzük, hogy $\frac{B-1}{2}$ szerepel-e a táblázatban. Ha igen, akkor B összetett szám, ha nem, akkor prímszám. Például 39 esetén $\frac{39-1}{2} = 19$ megtalálható a táblázatban, tehát 39 összetett szám. Ha 47-et teszteljük, akkor $\frac{47-1}{2} = 23$-at nem találjuk a táblázatban, tehát prímszám. Vigyázzunk, mert a fent elkészített 8×8-as táblázattal csak 51-ig lehet meghatározni a prímszámokat, ugyanis az első sorban (oszlopban) a legnagyobb szám 25. A táblázat egy ilyen kis részéből még nem lehet tudni, hogy egy $\frac{B-1}{2} > 25$ szám megjelenik-e majd valamelyik lassabban növekvő sorban (oszlopban). Például 118-at formálisan nem látjuk a táblázat fent elkészített részében, de ha több sort és oszlopot is felírunk, akkor ez a szám meg fog jelenni az első sor 39-edik oszlopában, tehát $2 \cdot 118 + 1 = 237$ összetett szám.

Mint a fenti példákból is láttuk e táblázat használata kényelmes, könnyű számításokat igényel, azonban a táblázat terjedelmes volta itt is nagy nehézségeket okoz, számítógépes szűrésre alkalmatlan.

Napjainkban az információk titkosításában (a kriptográfiában) szükségünk van nagyon nagy prímszámokra. Például az egyik legtöbbet használt titkosító rendszer, az 1976-ban bevezetett RSA-eljárás, egy nyílt (mindenki számára ismert) és egy titkos kulcsot használ. A nyílt kulccsal kódolt információt, csak a titkos kulccsal lehet dekódolni (megfejteni).

A kulcsok készítéséhez két nagy (több száz számjegyű) prímszám szorzatából indulnak ki, és egy e szorzat tényezőit jellemző számmal és két szabadon választott szám segítségével szerkesztik meg több lépésben a titkos kulcsot. A titkosítás folyamatát azért vázoltuk, hogy kihangsúlyozzuk a nagy prímszámok keresésének szükségességét, valamint a nagy összetett számok prím tényezőkre bontásának fontosságát (aki a nyílt kulcs ismeretében szeretné megfejteni, hogy mi lehet a titkos kulcs, annak csak akkor van erre némi esélye, ha egy óriási nagy számot gyorsan fel tud két prímszám szorzatára bontani, ez viszont napjainkban, még a leggyorsabb számítógépek használatával is, nagyon sok időbe telik).

Ahhoz, hogy a véletlenszerűen generált nagy számok közül ki lehessen választani a prímszámokat, prímtesztekre van szükség. Ezért többféle prímteszt is napvilágot látott. Ezek a tesztek általában nem határozzák meg az összetett számok osztóit. A determinisztikus tesztek nem használnak véletlen számokat, és e teszteknél biztos eredményre lehet számítani. A véletlen számokat használó úgynevezett nem determinisztikus (más szóval véletlen) tesztek esetén elfogadunk minimális valószínűségű hibás döntést is.

A számítógépen futtatott prímszámtesztek több változata is ismeretes, és ezek mindegyike lényegében az Euler–Fermat-tételen alapszik.

A legnagyobb ismert prímszám $2^{82589933} - 1$ (az ötvenegyedik Mersenne-prímszám), amely 24862048 számjegyből áll.

Szakirodalom

[1] Kiss Ernő: A törzsszámok néhány tulajdonsága, *Matematikai és Fizikai Lapok* 1957/4, 162-172. old.