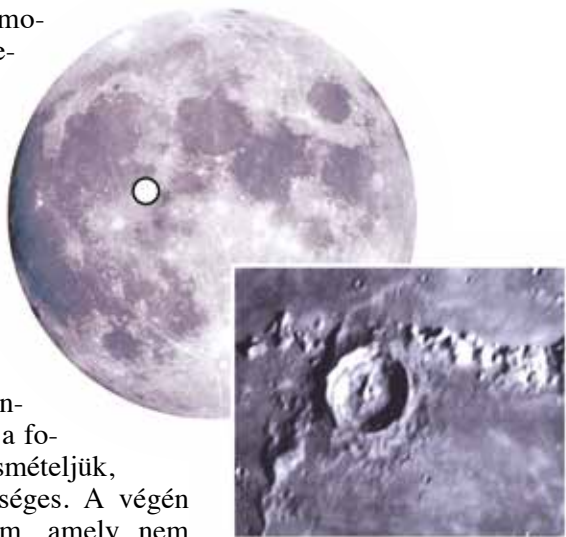


ha ki akarjuk deríteni a 100-nál kisebb prímszámokat, akkor először leírjuk 1-től 100-ig a természetes számok listáját. Megkeressük az 1-től eltérő első számot (2), majd kihúzzuk az összes többszörösét. Ezután megkeressük a következő nem kihúzott számot (3), és annak is kihúzzuk minden többszörösét. Ezt a folyamatot annyiszor ismételjük, ahányszor csak lehetséges. A végén az összes olyan szám, amely nem hullott ki a szítán, prímszám lesz 1 és 100 között. Általánosságban elmondható, hogy az N-nél kisebb összes prímszám megtalálásához nem muszáj elvégezni ezt a hosszadalmas folyamatot az N-ig terjedő összes egész számra. Bizonyítható, hogy elegendő az N-nél kisebb $\sqrt{N}$ nvagy azzal egyenlő egész számokat szűrni. A mi esetünkben elég azokat a számokat vizsgálni, amelyek kisebbek, mint $\sqrt{100} = 10$. Eratoszthenész szitája az egyik leghatékonyabb módszer kis, azaz tízmilliárdnál nem nagyobb prímszámok megkeresésére. Természetesen nem papírral és ceruzával végzett szítalásról van szó. Az informatika korában élünk, és több olyan algoritmus is rendelkezésünkre áll, amely lehetővé teszi,



▲ És mintha tudományos érdemei nem lennének elegendők ahhoz, hogy halhatatlanná tegyék Eratoszthenész nevét, a tudós további elismerésben is részesült: holdkrátert neveztek el róla.

hogy ezt a feladatot számítógépes programokkal végeztessük el. Nem érdemes hosszú prímszámlistákat tárolni, hiszen a program sokkal gyorsabban megtalálja a számokat, mint bármelyik számítógép, amely a listát a merevlemezről olvassa be.

•Végtelen sok prímszám van

A prímszámok végtelenségét már több tucat módon bizonyították. Néhányan alaposan kidolgozva, például Fürstenberg 1955-ben a topologikus terekkel, ugyanakkor a legelegánsabb, merthogy legegyszerűbb bizonyítás Eukleidésztől származik. A gondolatmenet a következő. Tegyük fel, hogy véges számú prímszám létezik. Ebben az esetben van egy, az összes többinél nagyobb szám, nevezzük P-nek. Most szorozzuk meg az összes prímszámot egészen P-ig, és az eredményt nevezzük N-nek: $2 \times 3 \times 5 \times 7 \times 11 \times \dots \times P = N$. Nézzük meg, mi történik az N + 1 számmal. Nyilvánvaló, hogy ez a szám nem osztható 2-vel, mert az az N egyik osztója, így a maradék 1 lenne. Ugyanezen okból nem osztható 3-mal sem, mert az is az N osztója, és megint csak 1 lenne a maradék. Ezzel a gondolatmenettel arra a következtetésre jutunk, hogy N + 1 nem osztható egyetlen P-ig terjedő prímszámmal sem, ami azt jelenti, hogy vagy maga is prímszám, vagy egy P-nél nagyobb prímszámmal osztható. Mivel azt feltételeztük, hogy P-nél nagyobb prímszámok nem léteznek, ugyanakkor N + 1 prímszámnak bizonyult, ez ellentmond annak a feltételezésnek, hogy P a legnagyobb

prímszám. Ez az ellentmondás azt jelenti, hogy a kiinduló feltevés hamis volt.

•Kiszámíthatatlanabb, mint az időjárás

Könnyebb megjósolni, milyen idő lesz két év múlva egy kis faluban, vagy milyen lesz a részvények végső árfolyama, mint a prímszámok előfordulását meghatározni a természetes számok sorában. Például 1 és 100 között több prímszám van, mint 101 és 200 között. 1 és 1 000 között 168 prímszám van, míg a 10^{100} és $10^{100} + 1\,000$ közötti ezer számból csak kettő prímszám. Van azonban egy tétel (ennek megfogalmazását és bizonyítását sok matematikus egészen lenyűgözőnek tartja), amely megadja a prímszámok hozzávetőleges gyakoriságát az egész számok között. Tegyük fel, hogy P(N) az N-nél kisebb prímszámokat jelenti. P(8) például 4, mivel a nyolcas szám előtt négy prímszám található, nevezetesen a 2, a 3, az 5 és a 7. A matematikusok által prímszámtételnek nevezett elgondolás szerint N növekedésével az N / P(N) arány egyre inkább megközelíti N természetes logaritmusát. Ez a látszólagos zűrzavar a következőképpen fordítható le. Tegyük fel, hogy valaki megkérdezi tőlünk, szerintünk hány prímszám létezik az első ezer szám között. Vegyünk elő egy zsebszámológépet, és hajtuk végre a következő lépéseket:

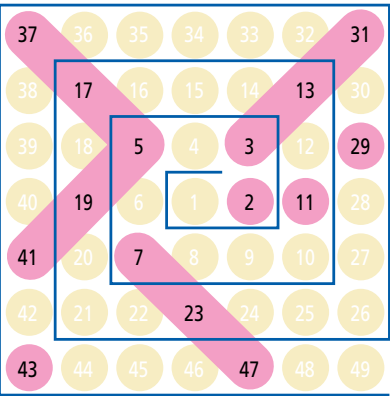
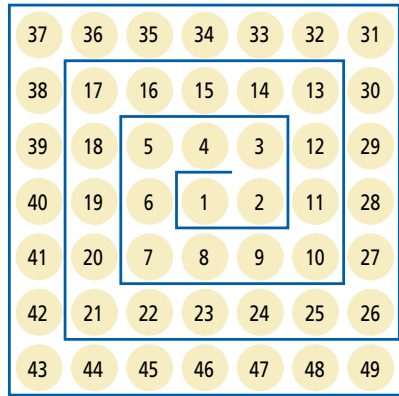
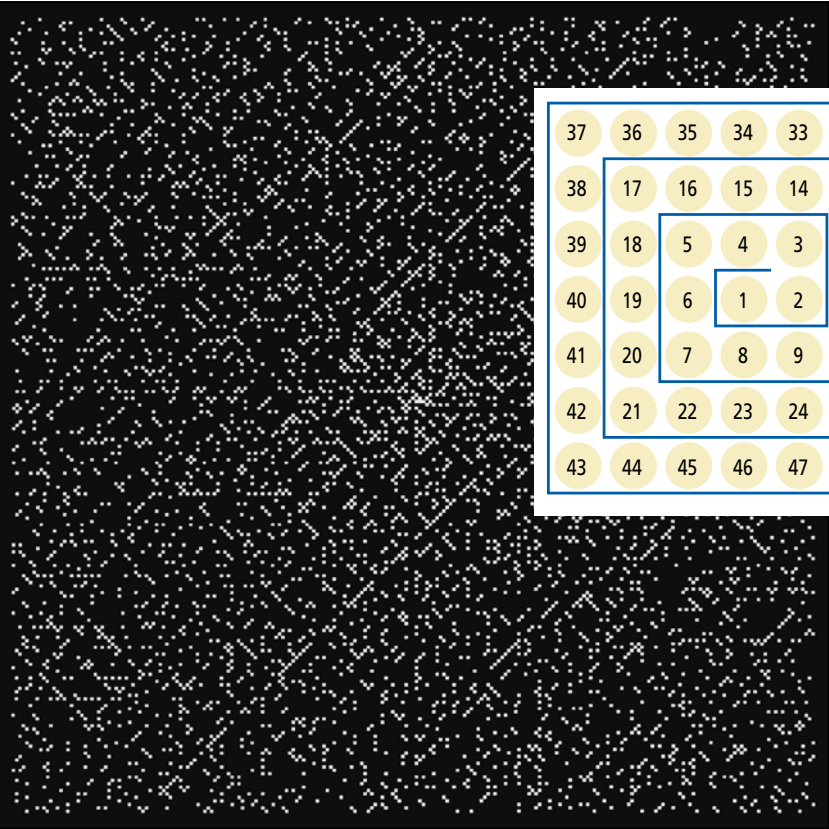
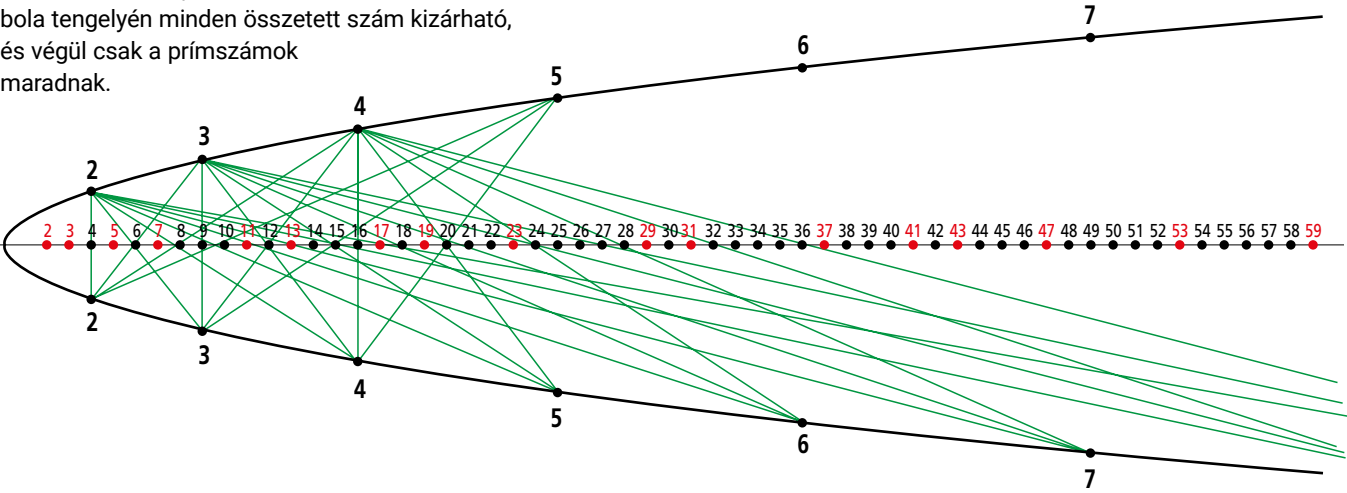
A prímszámtétel táblázata		
N	P (N)	N/ln(N)
1 000	168	145
10 000	1 229	1 089
100 000	9 592	8 696
1 000 000	78 498	72 464
10 000 000	664 579	621 118
100 000 000	5 761 455	5 434 783
1 000 000 000	50 847 478	48 309 185
10 000 000 000	455 052 511	434 782 650

- 1) írjuk be azt, hogy 1 000,
- 2) nyomjuk meg az ln (logaritmus) gombot,
- 3) nyomjuk meg a 1/x gombot,
- 4) szorozzuk meg az eredményt ezerrel.

Az eredmény 144,7648270108394255037630630554 lesz, ami azt jelenti, hogy 1 és 1 000 között körülbelül 145 prímszám található. A hozzávetőleges eredmény nem csoda, hiszen valójában 168 prímszám van. Ne felejtjük el azonban, hogy az eredmény egyre pontosabb lesz, ahogyan N növekszik, és nagy bizonyossággal állíthatjuk, hogy például az első milliárdnak csak 3,6%-a prímszám. Ezt a rendkívüli eredményt először 1792-ben a zseniális német Karl Friedrich Gauss jegyezte fel, mindössze 15 évesen. Több mint

Modern szűrő

A zseniális tudósok képesek meglátni a látszólag egymástól nagyon különböző dolgok közötti szokatlan összefüggéseket. Mi lehet a közös a prímszámokban és a parabolában? Két XX. századi orosz matematikus, Jurij Matijaszevics és Borisz Sztecskin e görbének egy figyelemre méltó tulajdonságát fedezte fel. Az egymást követő egész számok pontokként ábrázolhatók a görbe két ágán, méghozzá úgy, hogy két tetszőleges pontot összekötő szakasz pontosan a szorzatuknak megfelelő pontban metszi a parabola tengelyét. A szakaszok szisztematikus ábrázolásával a parabola tengelyén minden összetett szám kizárható, és végül csak a prímszámok maradnak.



▲◀ A prímszámok eloszlásáról még mindig sok mindent nem tudunk. 1963-ban Stanisław Ulam lengyel származású amerikai matematikus azzal az ötlettel állt elő, hogy az egész számokat spirálba rendezi, egy rács közepéből kiindulva. Ezután észrevette, hogy a prímszámok nem teljesen véletlenszerűen jelennek meg, hanem gyakran furcsa sugarakat vagy átlókat alkotnak (a képen rózsaszínnel jelölve). A bal oldalon ezek az érdekes struktúrák egy 399 x 399 méretű rácson láthatók.



egy évszázaddal később, 1896-ban Jacques Hadamard és Charles de la Vallée Poussin be is bizonyította.

•Feltételezések világa

A nehezen megfogható prímszámok számos egyszerű megfigyelésre vezetnek, amelyek nehéz feltevések elé állították a matematika világát. Például megfigyelhetjük, hogy:

$$\begin{aligned} 4 &= 2 + 2 \\ 6 &= 3 + 3 \\ 8 &= 3 + 5 \\ 10 &= 5 + 5 \\ 12 &= 5 + 7 \\ 14 &= 7 + 7 \end{aligned}$$

Egy kis türelemmel még meglepőbb eredményeket is kaphatunk, mint például $374 = 151 + 223$.

Goldbach, Euler levelezőtársa fogalmazta meg azt a feltételezést, hogy minden páros szám, amely nagyobb kettőnél, két prímszám összegeként írható fel. Eddig senkinek sem sikerült ezt alátámasztania. 1937-ben Vinogradov bebizonyította, hogy bármely „elég nagy” szám három prímszám összegeként írható fel. Később kiderült, hogy az „elég nagy” mintegy 7 000 000 számjegyet jelent, mégis, ez kétségtelenül nagy előrelépésnek számított. Számítógépek révén bebizonyosodott, hogy Goldbach feltevése minden 2×10^6 -nál kisebb páros számra igaz. 2 000 és 2002 között 1 000 000 dolláros jutalmat tűztek ki annak, aki ezt a hipotézist megerő-

► Goldbach 1742. június 7-én írt levele Eulernek, amelyben először mutatta be híres feltevését a prímszámokról. Christian Goldbach (1690–1764) az orosz kormány magas rangú tisztviselője és II. Péter cár tanítója volt, mindemellett pedig kiemelkedő matematikus.



Az aritmetika alaptétele

A nem prímszámok, vagyis azok a számok, amelyeket összetettnek nevezünk, különböző módon fejezhetők ki. Például a 12 összetett szám, amelyet 3×4 -ként, 2×6 -ként vagy $3 \times 2 \times 2$ -ként fejezhetünk ki. Ezzel szemben a 11-et csak 1×11 -ként tudjuk leírni. A 12-es számot kifejező három mód közül csak az utolsó áll prímszámokból, és van egy fontos tulajdonsága: ez az egyetlen módja annak, hogy a 12-es számot prímszámok szorzataként fejezzük ki. Ezt a tulajdonságot bármely számra kiterjeszthetjük. Például: $18 = 2 \times 3 \times 3$ az egyetlen lehetséges írásmódja a 18-nak prímszámok szorzataként. Ezt az egyik legfontosabb eredményt, amelyet az aritmetika alaptételeként ismerünk, Euklidész bizonyította be. Pontos megfogalmazása szerint „minden egynél nagyobb pozitív egész szám egyértelműen kifejezhető prímszámok szorzataként”.“

síti. Senki sem jelentkezett, és biztosan nem a szándék hiányzott hozzá.

Egy másik feltevés, amely még bizonyításra vár, az úgynevezett ikerprímek hipotézise. Végtelenül sok olyan prímpár létezik, amelyek különbsége 2, például 17 és 19, 41 és 43, valamint 59 és 61 (a legnagyobb ilyen ismert pár $835\,335^{39\,014}$ és $(835\,335^{39\,014} + 2)$). Más esetekben azonban két egymást követő prímszámot több százmilliárd egyéb egész szám választhat el (bebizonyosodott, hogy bármely adott K egész szám esetén létezik egész számok olyan K hosszúságú sorozata, amely egyetlen prímszámot sem tartalmaz).

•Óriási prímszámok

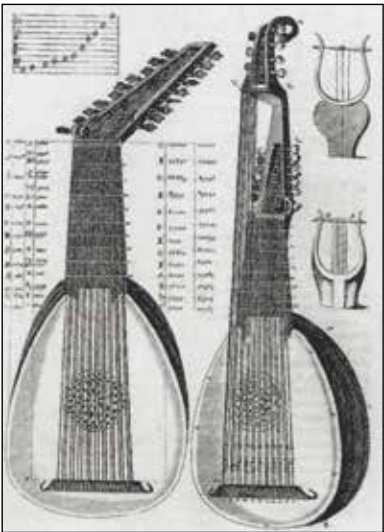
1644-ben Marin Mersenne, a nagyszerű tudós, Descartes, Galilei és Fermate levele-



► Postai bélyegző Urbana városából (Egyesült Államok) a Mersenne-prímek felfedezésének tiszteletére.

zőtársa, azt a számtípust tanulmányozta, amelyet később róla neveztek el. A Mersenne-szám (M_p) egy $2^p - 1$ alakú szám, ahol p prímszám. Például $M_2 = 2^2 - 1 = 4 - 1 = 3$ és $M_3 = 2^3 - 1 = 8 - 1 = 7$. Ha folytatjuk, akkor $M_5 = 31$ és $M_7 = 127$ lesz, mindkettő prímszám. Ugyanakkor $2^{11} - 1 = 2\,047 = 23 \times 89$, így M_{11} már nem prímszám. Mersenne feltételezte, hogy p = 257-ig $2^p - 1$ csak akkor lesz prímszám, ha p = 2, 3, 7, 13, 17, 19, 31, 67, 127 és 257. Kiderült, hogy a lista hibákat tartalmaz, és fontos tények hiányoznak belőle. Például 5 000-ig $2^p - 1$ prímszám p = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1 279, 2 203, 2 281, 3 217, 4 253 és 4 423 esetén.

Felmertülhet a kérdés, hogy mire jó az ilyen bonyolult számok meghatározása. A válasz az, hogy a nagy teljesítményű számítógépek korát éljük, és a Mersenne-számokkal végezhető teszt alkalmas a számítógépes felhasználásra. A Lucas-teszt megmondja nekünk, hogy a Mersenne-szám prímszám-e. Létezik egy szervezet, a GIMPS (Great Internet Mersenne Prime Search), amely a Mersenne-prímek átfogó internetes keresését koordinálja. Ennek köszönhetően találták meg az $M_3\,021\,377$, $M_6\,972\,593$, $M_{30}\,402\,457$ és $M_{32}\,582\,657$ számo-



▲ A Harmonie Universelle című mű egyik oldala. Szerzője, Marin Mersenne (1588–1648) pap, matematikus, fizikus és filozófus volt. Aktívan kutatta a zenei jelenségeket is, elemzésüknek legalább hat művet szentelt.

Mersenne-szám	Számjegyek	Év	Számítógép
M_{521}	157	1952	SWAC
M_{607}	183	1952	SWAC
$M_{1\,279}$	386	1952	SWAC
$M_{2\,203}$	664	1952	SWAC
$M_{3\,021\,377}$	909.526	1998	Pentium (200 Mhz)
$M_{6\,972\,593}$	2 098 960	1999	Pentium (350 Mhz)
$M_{30\,402\,457}$	9 152 052	2005	Itanium 2 (1,5 Ghz)
$M_{32\,582\,657}$	9 808 358	2006	Itanium 2 (1,6 Ghz)

a prímszámok listája, nyugodtan kipróbálhatjuk őket egymás után. Ez egyszerűnek látszik, mint ahogy a keverékeket alkotó színeket megtalálni sem volna nehéz, ha a raktárban legfeljebb egy tucat alapszín lenne. De nem ez a helyzet, pláne nem a prímszámok esetében. Kideríteni például azt, hogy az 1 409 305 684 859 két prímszám, a 705 967 és a 1 996 277 szorzatának eredménye, mindenki türelmét próbára teheti, különösen, ha figyelembe vesszük, hogy mindkét prímszámot olyan listából választották ki, amely az 1 és 2 millió közötti összes prímszámot tartalmazza (ez körülbelül

◀ Mersenne szivacsként szívta magába a tudást, gyakorlatilag nem volt olyan korabeli tudományág, amely ne érdekelt volna. A matematikában természetesen a számelmélet iránt érdeklődött, de geometriával, konkrétan a cikloidok tanulmányozásával is foglalkozott.