

PRVOČÍSLA JSOU ZÁKLADNÍ STAVEBNÍ KAMENY VŠECH Kladných celých čísel.

MATEMATICI POUŽÍVAJÍ VÝKONNÉ POČÍTAČE, ABY SE DOSTALI DO VZDÁLENÝCH KONČIN,

V NICHŽ PŘEBÝVAJÍ TYTO PODIVUHODNÉ A NEPŘEDVÍDATELNÉ ABSTRAKTNÍ OBJEKTY.



• Prvočísla Atomy aritmetiky

Některá čísla lze dělit jinými čísly. Například číslo 8 je dělitelné číslem 2 a také číslem 4, číslo 15 je dělitelné číslem 3 a číslem 5. Existují však čísla, která nelze dělit žádným jiným číslem, například 13 nebo 17. První z nich lze vyjádřit jako součin jiných čísel ($8 = 2 \times 4$, $27 = 3 \times 9$), a proto se jim říká složená čísla. Druhá čísla lze vyjádřit pouze jako součin ve tvaru $11 = 11 \times 1$ nebo $17 = 17 \times 1$. Z tohoto důvodu je nazýváme prvočísla.

Přesnou definici prvočísla se učíme v prvních letech školní docházky: „Prvočíslo je číslo jiné než 1 dělitelné pouze číslem 1 a sebou samým.“ Označujeme tak čísla 2, 3, 5, 7, 11... Tři tečky na konci této věty znamenají, jak tomu tak bývá, že řada pokračuje. Možná se však jedná o jedno z nejméně vhodných míst na světě, kde je použít, jelikož nijak nenaznačují, jak má řada pokračovat. Řekneme-li, že sudá čísla jsou ta, která lze dělit číslem 2, a zapíšeme



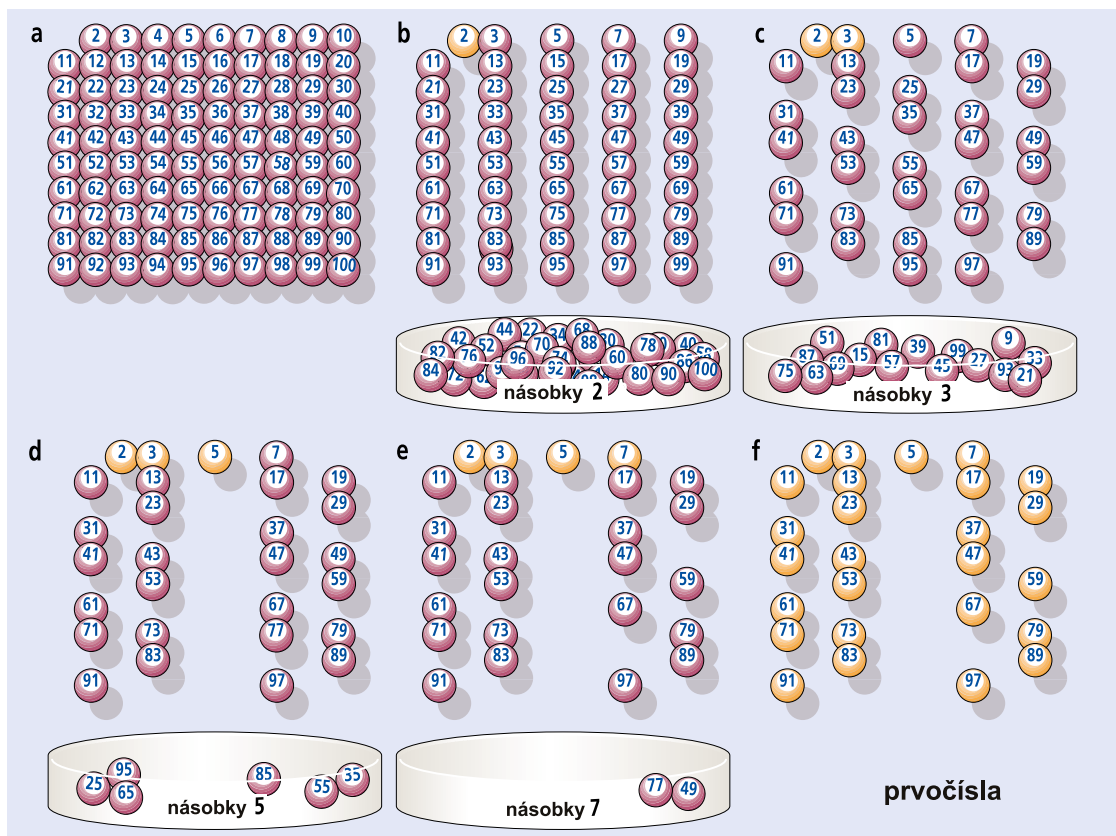
▲ Velkému řeckému učenci Eratosthenovi z Kyrény (273–194 př. n. l.), někdejšímu řediteli Alexandrijské knihovny, vdčíme nejen za síto prvočísel, ale také za brilantní určení průměru Země.

2, 4, 6, 8..., jsou zřejmé dvě věci: zaprvé, že kdokoli může bezproblémově pokračovat v psaní čísel, a zadruhé, že jich je příliš mnoho (ve skutečnosti nekonečně mnoho) na to, aby bylo možné je všechna vypsát. Máme ale zákon pro výskyt prvočísel? Existuje jich nekonečně mnoho? Na druhou otázku lze jednoznačně odpovědět ano. Prvočísel je nekonečně mnoho. Pokud jde o první otázku, odpověď je ano i ne. Existují určité metody, jako například Eratosthenovo síto, které umožňují najít prvočísla menší než dané číslo, a máme také vzorce pro nalezení zvláštních prvočísel, neexistuje však žádné pravidlo, které by umožňovalo vypočítat všechna z nich.

• Eratosthenovo síto

Eratosthenés z Kyrény vymyslel chytrou a efektivní metodu k nalezení prvočísel menších než dané číslo. Například chceme-li nalézt všechna prvočísla menší než 100, nej-

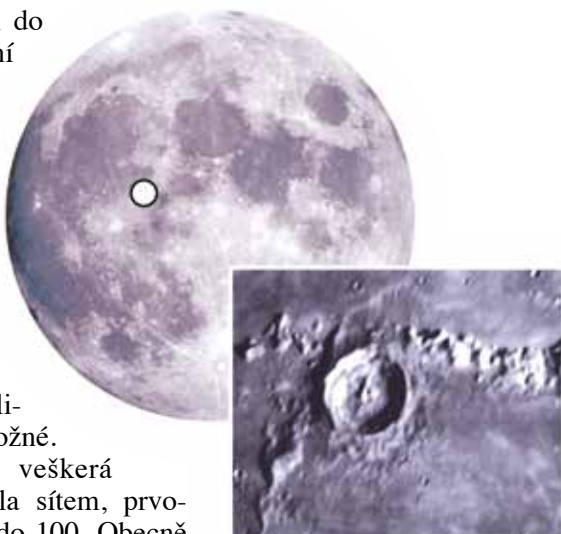
► Eratosthenovo síto je příkladem algoritmu, metody, která umožňuje systematicky dosáhnout požadovaného výsledku pomocí konečného počtu kroků. Zde je zobrazeno prosévání čísel do 100. V krocích od a do f se prosévají násobky 2 a poté 3, 5 a 7. Není třeba pokračovat, protože násobky 11 menší než 100 jsou také násobky čísla menšího než 10 a tato operace již byla dokončena v předchozích krocích.



prve sepišeme seznam všech přirozených čísel od 1 do 100. Najdeme první číslo jiné než 1 (2) a poté vyškrtneme všechny jeho násobky. Následně vyhledáme první číslo, které není přeškrtnuto (3) a které se liší od prvního, a přeškrtneme i všechny jeho násobky. Tento proces se opakuje tolikrát, kolikrát je to možné.

Na konci budou veškerá čísla, která nepropadla sítem, prvočísla v rozmezí od 1 do 100. Obecně platí, že k nalezení všech prvočísel menších než číslo N není nutné provádět tento zdoluhavý proces pro všechna celá čísla až do N . Lze dokázat, že stačí prosít celá čísla menší než $\sqrt{N}$ nebo jemu rovná. V našem příkladu tedy stačí prosit čísla menší než $\sqrt{100} = 10$.

Eratosthenovo síto je jednou z efektivních metod pro hledání malých prvočísel, tj. prvočísel menších než deset miliard. Samozřejmě se nejedná o prosévání pomocí papíru a tužky. Žijeme v éře informatiky a máme k dispozici několik algoritmů, které nám umožňují použít tuto metodu v počítačovém programu s takovou rychlostí, že se nevyplatí ukládat dlouhé seznamy prvočísel,



▲ Aby toho nebylo málo, Eratosthenés se stal nesmrtelným nejen díky svým objevům, je také po něm pojmenován kráter na Měsíci.

neboť program najde čísla mnohem rychleji než jakýkoliv počítač čtoucí seznam na pevném disku.

•Prvočísel je nekonečně mnoho

Existují desítky důkazů nekonečnosti prvočísel. Některé z nich jsou důkladně propracované, jako například ten, který v roce 1955 předvedl Fürstenberg za pomoci topologických prostorů, avšak s nejelegantnějším, tedy nejjednodušším, přišel už Eukleidés. Zní takto: předpokládejme, že existuje konečný počet prvočísel. V takovém případě bude existovat jedno větší než všechna ostatní, které můžeme nazvat P . Nyní vynásobíme všechna prvočísla až do P a jako N označíme výsledek $N = 2 \times 3 \times 5 \times 7 \times 11 \times \dots \times P$.

Podívejme se, co se stane s číslem $N + 1$. Je zřejmé, že toto číslo nelze dělit číslem 2, protože se jedná o jeden z dělitelů N , tudíž by nám zbylo číslo 1. Z téhož důvodu jej nelze dělit číslem 3, protože se opět jedná o dělitele N a opět by nám zbylo číslo 1. Tímto uvažováním dojdeme k závěru, že $N + 1$ není dělitelné žádným prvočíslem až do P , což znamená, že buď je číslo samo prvočíslem, nebo je dělitelné prvočíslem větším než P . Jelikož předpokládáme že neexistují žádná prvočísla větší než P , vyplývá z toho, že $N + 1$ je prvočíslo, což je v rozporu s předpokladem, že P bylo největším prvočíslem. A to, že jsme dospěli k sporu, znamená, že výchozí hypotéza byla nepravdivá.

Moderní síto

Geniální vědci dokážou vidět neobvyklé souvislosti mezi objekty, které se od sebe zdánlivě velmi liší. Co mohou mít společného prvočísla s parabolou? Ruští matematici Jurij Matijasevič a Boris Stečkin objevili ve 20. století následující pozoruhodnou vlastnost této křivky. Po sobě jdoucí celá čísla lze znázornit body na jejich dvou větvích tak, že úsečka spojující libovolné dva body protíná osu paraboly v bodě, který přesně odpovídá jejich součinu. Systematickým vynášením úseček na osu paraboly se vyloučí všechna složená čísla a nakonec zůstanou pouze prvočísla.

