Pedagogická fakulta,Katolícka Univerzita v Ružomberku

Prvočísla
(Práca z Histórie matematiky)

Pisarčíková Viera
4. ročník
M/Nv

PRVOČÍSLA

Číslo, ktoré má práve dvoch deliteľov, a to 1 a samo seba (nemá teda vlastné delitele), nazývame prvočíslo. Všetky prirodzené čísla, ktoré majú vlastné delitele (teda odlišné od 1 a čísla samého), nazývame zložené čísla.

Príklad: $360 = 2^3 \ . \ 3^2 \ . \ 5$

Číslo 1 má osobiné postavenie, nepovažujeme ho ani za prvočíslo, ani za zložené číslo. Takto definovali prvočísla už slávni matematici Aristoteles a Euklides. Ich definície sa nepodstatne líšili iba slovosledom.

Už viac ako 300 rokov pred n. l. Euklides dokázal veľmi dôležirý výsledok: prvočísel je nekonečne veľa (neexistuje teda najväčšie prvočíslo) a každé prirodzené číslo možno vyjadriť súčinom prvočísel (tzv. Prvočíselný rozklad daného čísla). Úlohou – vytriediť všetky prvočísla z množiny prirodzených čísel - riešil ako prvý Eratostenes (ktorý je ale známejší tým, že ako prvý a vcelku veľmi presne určil priemer Zeme). Metóda sa preto nazýva Eratostenovo sito na jeho početnosť.

Eratostenovo sito je jednoduchý algoritmus pre nájdenie všetkých prvočísel menších ako zadaná horná hranica. Algoritmus je pomenovaný po gréckom matematikovi Eratostenovi, ktorý žil v rokoch 276–194 pred Kr.

Algoritmus funguje na postupnom „presievaní“ zoznamu čísel – na začiatku zoznam obsahuje všetky čísla v danom rozsahu (2, 3, 4, …, zadané maximum). Potom sa opakovane prvé číslo zo zoznamu vyberie, toto číslo je prvočíslom; zo zoznamu sa potom odstránia všetky násobky tohto čísla (to sú zložené čísla). Tak sa pokračuje až dovtedy, kým sa zo zoznamu neodstráni posledné číslo (alebo dovtedy, keď je ako prvočíslo označené číslo vyššie ako odmocnina najvyššieho čísla – v tomto prípade všetky zostávajúce čísla v zozname sú určite prvočísla).

Príklad

Pre nájdenie prvočísel medzi prvými 20 číslami :

Krok 1: Zoznam obsahuje všetky čísla v rozsahu 2–20:

Zoznam: 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20

Krok 2: Odoberieme prvé číslo zo zoznamu a označíme ho ako prvočíslo:

Známe prvočísla: 2

Zoznam: 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20

Krok 3: Odoberieme zo zoznamu všetky násobky práve odobratého prvočísla:

Známe prvočísla: 2

Zoznam: 3 5 7 9 11 13 15 17 19

Krok 4: Pokračujeme opäť bodom 2, pokiaľ ostávajú nejaké čísla :

Známe prvočísla: 2 3

Zoznam: 5 7 11 13 17 19

Známe prvočísla: 2 3 5

Zoznam: 7 11 13 17 19

5 je vyšší než √19, takže ostávajú už iba prvočísla.

Výsledný zoznam prvočísel v rozsahu 2–20: 2, 3, 5, 7, 11, 13, 17, 19

Eratostenovo sito sa môže v čase počítačov javiť ako niečo ťažkopádne. Počítačové programy na hľadanie prvočísel sú však založené práve na tejto metóde. Má to svoj praktický význam - pomocou veľkých prvočísel je možné zašifrovať tajné správy tak, že rozlúštenie je praktický nemožné. Sú softvérové firmy, ktoré na tento účel používajú výkonné počítače a matematické vedomosti svojich zamestnancov, pričom výsledky výhodne speňažia. Až doteraz (stav ku koncu r. 1997) bolo najväčšie prvočíslo nájdené pomocou jedného z najvýkonnejších superpočítačov vôbec. V desiatkovom zápise by malo 895 932 číslic. V exponenciálnom (mocninovom) tvare ho možno zapísať ako ($2^{2976221}$ - 1). Získame ho, ak číslo 2 vynásobíme sebou samým 2 976 221-krát a od výsledku odčítame 1.

Pokúsme sa, hoci čiastočne, predstaviť si „obrovskú" veľkosť uvedeného čísla pomocou dávnej legendy o vzniku šachovej hry: na prvé políčko šachovnice položme dve doštičky 2 mm hrubé, na druhé políčko 4 také doštičky, na ďalšie 8, potom 16, 32 doštičiek atď.
Na poslednom poličku šachovnice vyrastie veža z 2^{64} doštičiek. Či veríme, či nie, jej výška bude skoro rovnaká ako vzdialenosť k najbližšej hviezde Proxime Centauri. Tá je vzdialená približne 4 svetelné roky, teda svetlo od nej k nám putuje vesmírnym priestorom asi 4 roky! Číslo ($2^{2976221}$ - 1) je ale nepredstaviteľne veľké oproti 2^{64}.Naša myseľ jednoducho neobsiahne tak veľké čísla. Nemáme ich s čím porovnať, nevieme si ich predstaviť.

Hoci definícia prvočísel je jednoduchá, teória zaoberajúca sa nimi je mimoriadne zložitá a je v nej veľa stále nevyriešených problémov. Celé matematické školy začínajúc Euklidom sa zaoberali a zaoberajú štúdiom prvočísel, zisťovaním a dokazovaním ich vlastností. Niektoré domnienky o prvočíslach sa doteraz nepodarilo dokázať – uveďme napríklad známu Goldbachovu hypotézu. Roku 1724 Christian Goldbach v liste svojmu priateľovi Leonhardovi Eulerovi vyslovil dve domnienky: po prvé, že každé prirodzené číslo väčšie ako 2 sa dá vyjadriť súčtom dvoch prvočísel a po druhé, že podobne každé prirodzené číslo väčšie ako 6 možno vyjadriť súčtom troch prvočísel.

$$6 = 3 + 3,\ 8 = 3 + 5,\ 11 = 3 + 3 + 5$$

Hoci prvá hypotéza bola potvrdená pre všetky párne čísla až do 100 000 000 previerkou na počítači, všeobecný dôkaz doteraz stále nie je známy. Veľa ďalších problémov okolo prvočísel znepokojuje matematikov. Bolo by, napríklad, veľmi žiaduce mať vzorec umožňujúci nájsť prvočíslo podľa jeho polohy na zozname, teda povedzme 500-té alebo 1 998-me prvočíslo. Dnes sa väčšina matematikov nazdáva (hoci v matematike to nemusí nič znamenať), že šanca takýto všeobecný vzorec objaviť je malá, a že pravdepodobne neexistuje. Podľa ďalšej podobnej hypotézy existuje nekonečne veľa prvočíselných dvojčiat, čiže prvočísel líšiacich sa o 2:

3,5 – 5,7 – 11,13 – 17,19 – 29,31 - ...

Testovacie výpočty to potvrdzujú, ale všeobecný dôkaz chýba. Poľský matematik Stanislav M. Ulam sa na jednom stretnutí nudili a z dlhej chvíle si začal kresliť usporiadanie prirodzených čísel v tvare špirály. Potom podčiarkol všetky prvočísla a zbadali, že väčšina z nich sa nachádza na rovnobežkách s uhlopriečkami výsledného štvorca. Neskôr nakreslil pomocou počítača rovnaký obrazec prvých 56 000 prirodzených čísel, na ktorom bolo rozmiestnenie prvočísel ešte výraznejšie. Obrazec dostal názov Ulamov rubáš.