**Téma 01 – prvočísla**

**Prvočíslo je prirodzené číslo väčšie ako 1, ktoré nemá žiadnych kladných deliteľov okrem 1 a seba samého. Prirodzené číslo väčšie ako 1 ktoré nie je prvočíslo sa nazýva zložené číslo.**

Napríklad, 5 je prvočíslo, pretože iba 1 a 5 ho delí, zatiaľ čo 6 je zložené číslo z dôvodu, že má deliteľov 2 a 3, okrem 1 až 6. Základná teória aritmetiky stanovuje ústrednú úlohu prvočísel v teórii čísel: ľubovoľné celé číslo väčšie ako 1 možno vyjadriť ako súčin prvočísel, ktorý je jedinečný. Jedinečnosť tejto vety vyžaduje počítanie s číslom 1 ako s prvočíslom.

Vlastnosť bytia prvočíslom sa nazýva prvočíselnosť. Jednoduchá, ale pomalá metóda na overenie či je dané číslo *n* prvočíslom je známa ako **skúšobná divízia**. ***Pozostáva z testovania, či n je násobkom všetkých kladných čísel medzi číslom 2 a druhou odmocninou čísla n.*** Algoritmy, ktoré sú oveľa účinnejšie ako skúšobná divízia boli navrhnuté na testovanie prvočíselnosti veľkých čísel. Zvlášť rýchle metódy sú k dispozícii pre prvočísla špeciálnych foriem, ako je napríklad Mersennovo prvočíslo. V súčasnosti je najväčšie známe prvočíslo rovné 257,885,161 − 1 s 17 425 170 ciframi.

Existuje niekoľko druhov prvočísel, pre ich obrovské množstvo uvádzam len niekoľko z nich:

1. Spojené prvočísla: ich ciferný súčet je tiež prvočíslo

2. Párne prvočíslo: jediné je 2 . Iné neexistuje.

3. Faktoriálové prvočísla: n!-1 alebo n!+1 je prvočíslo

4. Fibonacciho prvočísla: prvočísla z Fibonacciho postupnosti

Šťastné prvočísla: šťastné čísla ktoré sú prvočíslami – Šťastné číslo je v matematike definované nasledujúcim spôsobom: vezmime ľubovoľné kladné celé číslo, nahradíme ho súčtom druhých mocnín jeho cifier a tento proces opakujeme až kým sa nedostaneme k číslu jedna (kde sa proces zastaví) alebo kým sa nám v postupnosti neobjaví niektoré číslo dvakrát (tzn. Postupnosť sa zacyklí). Tie čísla, ktoré týmto spôsobom skončí jednotkou, nazývame šťastné, ostatné potom nešťastné.

5. Mersennove prvočísla: v matematike, sú Mersennove prvočísla v tvare Mn = 2n-1. Sú pomenované podľa francúzskeho mnícha Marina Mersenna, ktorý študoval na začiatku 17. storočia. Je známe, že ak *n* je zložené číslo tak potom aj 2n - 1 je zložené číslo. Definícia je preto nezmenená , keď Mp = 2p-1, kde *p* sa predpokladá, že je prvočíslo. V súčasnosti je známych 48 Mersennových prvočísel. Najväčšie z nich je 257,885,161 − 1 .

6. Palindromické prvočísla: čítajú sa rovnako spredu aj zozadu.

7. Wall–Sun–Sun prvočísla: prvočísla väčšie ako 5, ktorých druhá odmocnina delí n-té Fibonacciho číslo, kde *n* je dané prvočíslo mínus 1, ak zvyšok po delení tohto prvočísla číslom 5 je rovný číslu jedna a -1, ak je rovný číslu 2. Je avšak veľmi zaujímavé že dodnes takéto prvočíslo nebolo nájdene.

Skúšobná divízia

Číslo ***n>1*** je teda prvočíslo ak nemá v intervale ***[2,n)*** žiadnych deliteľov. Úplne triviálny prístup je teda skúsiť všetky čísla v tomto intervale, a ak žiadne nenájdeme, potvrdíme že je to prvočíslo:

**bool** je\_prvocislo(**int** n)

{

**for**(**int** i=2; i<n; i++)

{

**if**(n % i == 0)

**return** **false**;

}

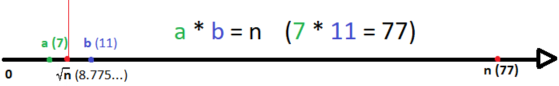
**return** (n>1); //kontrola či zadané číslo je vačšie ako 1

}

V prípade, že je *n* prvočíslo, však spravíme až n−2 = ***O(n)*** krokov. Toto je príliš pomalé pre *n* rádovo 109, alebo viacero *n* okolo 106.

Tu prichádza na rad prvé dôležité pozorovanie. Povedzme, že ***n*** nie je prvočíslo. Potom vieme ***n*** zapísať ako ***n=a\*b***, kde platí (BUNV[[1]](#footnote-1) ***a≤b***) potom platí ***a≤√n***. Ak by totiž ***b ≥ a > √n***, tak ***a\*b > n***.

Inak sa na to dá pozerať aj tak, že každý deliteľ väčší rovný √n má svoju dvojicu, ktorá je menšia rovná ako ***√n*** (a naopak).



Ak teda nenájdeme deliteľa čísla ***n*** v intervale ***[2, √n]***, nemusíme ďalej hľadať - určite ho nemá ani v intervale ***(√n, n)***. Úplne jednoducho teda zrýchlime našu funkciu na overovanie prvočíslenosti - budeme hľadať len po odmocninu n.

**bool** je\_prvocislo(**int** n)

{

**for**(**int** i=2; i\*i<=n; i++) // i\*i<=n

{

**if**(n % i == 0)

**return** **false**;

}

**return** (n>1); //kontrola či zadané číslo je vačšie ako 1

}

V najhoršom prípade teda spravíme ***O(√n)*** operácií, ak je číslo prvočíslo alebo súčinom dvoch čísel blízko jeho odmocnine. To je slušné vylepšenie (z obrázku môžete vidieť, o koľko menej čísel overíme už pre relatívne malé n=77); ak by sme takto skúsili overiť všetky čísla od ***1*** po ***n*** v snahe nájsť všetky prvočísla, zabralo by nám to ***O(n√n) = O(n3/2)*** času.

Ďalšie vylepšenie môžeme teda spraviť pozorovaním, že ak ***n*** je zložené číslo a teda má deliteľov, tak má zaručene aj prvočíselných deliteľov - nemusíme teda skúšať všetky čísla ***≤√n***, ale len všetky prvočísla ***≤√n***, ktorých je ***π(√n)***. Samozrejme, toto urýchlenie overovania jednotlivých čísel prichádza s cenou - ***musíme si najprv predpočítať všetky dostatočne malé prvočísla***. Toto sa oplatí, ak budeme chcieť overovať viacero čísel, alebo ak našim cieľom nájsť všetky prvočísla do n - vtedy to sú predsa dve muchy jednou ranou.

******

vector<**int**> prvocisla;

**void** najdi\_prvocisla(**int** n)

{

**for**(**int** i=2;i<=n;i++)

{

**bool** ok = **true**;

**for**(**int** j=0; j<prvocisla.size() && prvocisla[j]\*prvocisla[j] <= i; ++j)

{

**if**(i % prvocisla[j] == 0)

{

ok = **false**;

**break**;

}

}

**if**(ok)

{

prvocisla.push\_back(i);

}

}

}

Tento prístup má teda časovú zložitosť , a pamäťovú .

Algoritmy na hľadanie prvočísel v intervale 1-n.

**1. Eratostenovo sito**

**2. Atkinovo sito**

**3. Sundaramovo sito**

Testovanie ci dane cislo je prvocislo

#### THE LUCAS–LEHMER TEST

...

Literatúra:

<https://matinfo.estranky.sk/clanky/co-su-to-prvocisla--.html>

<https://www.ksp.sk/kucharka/eratosten/>

1. Bez ujmy na všeobecnosti  
    [↑](#footnote-ref-1)