SUJOVÁ Sára **VTI 2020, P2**

4pAIŘ/1 **27.12.2020**

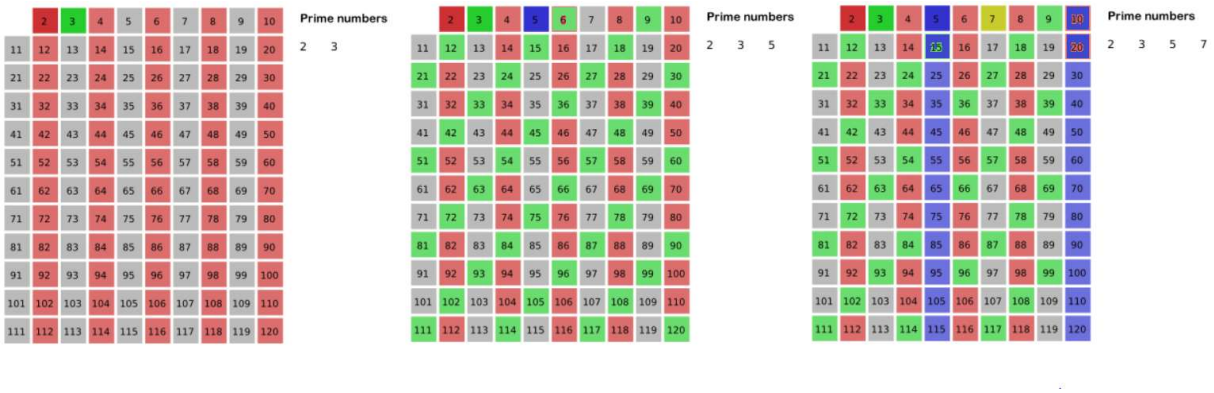
Programy a eseje pro kryptografii

Teorie

Grafické rozložení prvočísel, aneb skrytý řád

Prvočíslo $p \in \mathbf{N}$ je číslo, pre ktoré platí, že $p \geq 2$ a zároveň nemá žiadneho iného deliteľa, než 1 a p. Podľa Euklidovského teorému, ktorý bol vyslovený okolo roku 300 pred našim letopočtom, existuje nekonečne mnoho prvočísel. Zároveň každé číslo, ktoré nie je prvočíslom, može byť rozložené na súčin prvočísel.

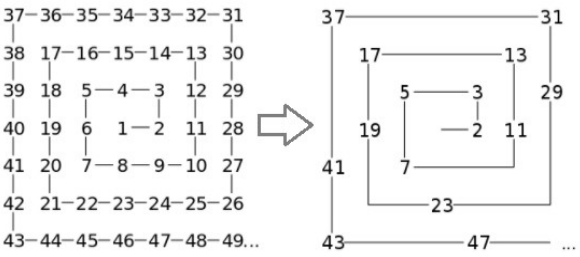
Jedným z najspoľahlivejších sposobov, ako nájsť všetky prvočísla do stanovenej hornej hranice (napr. do čísla 1000, alebo do 100 prvočísel) je Eratosthenesove sito. Jeho princíp spočíva v interaktívnom označovaní a zapisovaní prvočísiel a ich násobkov, ktoré následne "vyradí" zo zoznamu potenciálnych prvočísiel, pretože už nespĺňajú ich definíciu. Postupuje sa zaradom cez všetky neoznačené čísla od 2, tj. keď algoritmus zapíše 2 ako prvočíslo a 4, 6, 8… označí ako jeho násobky (ktoré už z definície nemožu byť prvočíslami), postúpi k ďalšiemu neoznačenému číslu (v tomto prípade číslo 3), ktoré zapíše ako prvočíslo a jeho násobky označí a vychádzajúc z definície "vyradí" z potenciálneho zoznamu prvočísel. Názornejšia ukážka je na obrázku:



Nevýhodou tohto algoritmu je jeho jednoduchosť, ktorá zapríčiňuje dlhé výpočtové časy pri generovaní veľkých objemov prvočísel.

Cieľom tohto projektu je skúmať skrytý systém v množine prvočísel. Pri skúmaní má zmysel kvôli názornosti uvažovať o grafickom spracovaní.

Jedným z najznámejších sposobov zobrazovania prvočísel je prvočíselná špirála, inak aj Ulamova špirála. Bola zostrojená a popísaná v roku 1963 matematikom Stanislawom Ulamom a neskor publikovaná v časopise Scientific American. V tejto špirále sú znázornené okom pozorovateľné usporiadania pri skúmaní vo vertikálnom, horizontálnom aj diagonálnom smere. Vznik týchto usporiadaní pripomínajúcich čiary zodpovedá kvadratickým polynómom, napríklad Eulerovmu prvočíselnému polynómu, ktorý vytvára vysokú hustotu prvočísel. Jej konštrukcia spočíva v zapísaní daného počtu kladných celých čísiel do štvorcovej špirály a označení prvočísiel.



Rovnakým sposobom sa dá vytvoriť špirála pre akýkoľvek tvar, napr. kruh, trojuholník alebo iný mnohouholník, v ktorých vizuálny systém znázorňuje rôzne metódy získavania prvočísiel.

Okrem tvorby pravidelných špirál sa dá systém prvočísiel skúmať napr. na základe vzájomnej vzdialenosti prvočísel od seba navzájom. Týmto spôsobom sa dajú prvočísla nakresliť do rôznych tvarov, nadväzujúce na seba navzájom pod rôznym uhlom, v 2D aj 3D. Vzniknuté útvary vzhľadovo pripomínajú úlohy typu „random walk“.

Uživatelský popis programu

Uvedený program vypočíta na základe užívateľom zadefinovanej hornej hranice programu v okne *Upper limit* všetky prvočísla nachádzajúce sa v tomto intervale. Tieto prvočísla sú následne zobrazené v okne s názvom *List of primes*. Keď uživateľ klikne na tlačítko *Visualise*, je zobrazená grafická metóda, ktorá kreslí čiaru z bodov daných ako celé čísla vzynačené bodmi. Vždy keď je celé číslo zároveň prvočíslom, zlomí čiaru o 90° doľava. Berie teda do úvahy vzdialenosť dvoch po sebe idúcich prvočísiel. Počiatočný bod je vykreslený ako červená hviezdička. Horná hranica programu (*Upper limit*) nemá žiadne obmedzenie. Je možné počítat rádovo veľmi veľké čísla na úkor prehľadnosti a výpočetného času. Tlačidlo *Clear all contents* vymaže všetky zadané a vypočítané údaje. Prostredie aplikácie vyzerá nasledovne: