Zápočtový program – Generátor velkých prvočísel

Jan Oupický

1. Zadání

Program má za úkol vygenerovat prvočísla zadané délky dle počtu cifer v desítkové soustavě.

Největší možné prvočíslo bude mít 200 cifer v desítkové soustavě.

Uživatel si může zvolit kolik prvočísel chce vygenerovat.

Vygenerovaná prvočísla budou postupně vypsána do souboru „vystup.txt“ na samostatný řádek v desítkové soustavě.

1. Uživatelský manuál

Po spuštění programu bude uživatel otázán kolik cifer mají mít vygenerovaná prvočísla. Stačí zadat celé číslo v rozmezí 1-200 a stisknout Enter.

Dále se program uživatele zeptá, kolik prvočísel má vygenerovat. Jako v minulém kroku, stačí zadat jakékoliv kladné celé číslo. Po stisknutí Enter program začne generovat prvočísla.

O skončení procesu program uživatele informuje a v souboru „vystup.txt“ budou vygenerovaná prvočísla.

1. Jak program funguje (algoritmus)

V dnešní době se pro generování velkých prvočísel používaných v kryptografii obvykle používá tento algoritmus:

1. Vygeneruj náhodné číslo *n* zadané délky, které není sudé (dělitelné 2) a nekončí 5 (dělitelné 5).
2. Vygenerované číslo otestuj zda *n* je prvočíslo.

Intuitivně se může nejprve zdát, že u velkých čísel bude takové náhodné generování velice neefektivní. Naštěstí prvočísla nejsou tak vzácná. Dle prvočíselné věty pravděpodobnost, že dané číslo *x* je prvočíslo, je zhruba . Tedy například pokud *x* je číslo s 100 ciframi – 10^99 = *x*. Pravděpodobnost, že *x* je prvočíslo bude . Tedy jedno z čísel bude pravděpodobně prvočíslo. A pokud odebereme sudá tak to vyjde na 114 čísel, což není tak špatné.

Nejhlavnější algoritmus je ten, který testuje zda je *n* prvočíslo. Nejpoužívanější je tzv. Millerův-Rabinův test prvočíselnosti. Tento algoritmus