

PAL cv. 9

November 24, 2021

10/2. Máte jednu hrací kostku. Popište, jak využijte házení kostkou tak, abyste měli generátor náhodných celých čísel v rozmezí 0..10. Všechna čísla 0, 1, 2, ..., 10 musí být generována se stejnou pravděpodobností.

10/3. Vysvětlete, jak pomocí generátoru náhodných čísel zamícháte do náhodného pořadí seřazené pole čísel. Akce musí proběhnout v čase úměrném délce pole.

10/4. Ověřte, zda lineární kongruenční generátor s danými parametry má maximální možnou délku periody.

- ▶ A) $x_{n+1} = (91x_n + 49) \bmod 600$
- ▶ B) $x_{n+1} = (8x_n + 80) \bmod 49$
- ▶ C) $x_{n+1} = (37x_n + 55) \bmod 144$
- ▶ D) $x_{n+1} = (99x_n + 81) \bmod 113$

10/5. Určete délku periody v Lehmerově generátoru, který je dán předpisem $x_{n+1} = ((M - 1) * x_n) \bmod M$, kde M je prvočíslo.

10/6. Určete, kolik přibližně prvočísel leží v intervalu

- ▶ A) $[0, 10^9]$
- ▶ B) $[10^9, 2 * 10^9]$
- ▶ C) $[2 * 10^9, 3 * 10^9]$

10/7. Řekneme, že přirozené číslo je poloprvočíslo, pokud je buď prvočíslem nebo celou mocninou prvočísla. Popište modifikaci Eratosthenova síta, která bude generovat právě poloprvočísla. Napište pseudokód.

10/9. Vygenerujeme všech 168 prvočísel menších než 1000 (2, 3, 5, ..., 991, 997) a dále ze seznamu $S = (1000, 1001, \dots, 999999)$ všech celých čísel větších než 999 a menších než 1000000 vyškrtáme všechny násobky uvedených prvočísel. Kolik čísel zbyde v S a kolik z nich budou prvočísla? Uveďte co nepřesnější odhad.

10/10. Určete, jaký je maximální možný počet prvočísel v kterémkoli z intervalů $[30k, 30k + 29]$, $k = 1, 2, 3, 4, \dots$.

10/14. Uvedený kód počítá celočíselnou mocninu x^n . Popište, jak jej upravíte, aby počítal $x^n \bmod m$, pro kladné celé m .

Minimalizujte riziko přetečení.

```
BinPower(int x, int n) {
    int r = 1, y = x;
    while (n > 1) {
        if (n % 2 == 1) r *= y;
        y *= y;
        n /= 2;
    }
    return r*y;
}
```