Maturita 2023

Tento dokument slouží jako podpůrný materiál pro maturanty v roce 2023. Obsahuje užitečné informace ke složitějším maturitním otázkám. Koukejte si to pořádně pročíst!

Otázka 1: Césarova šifra

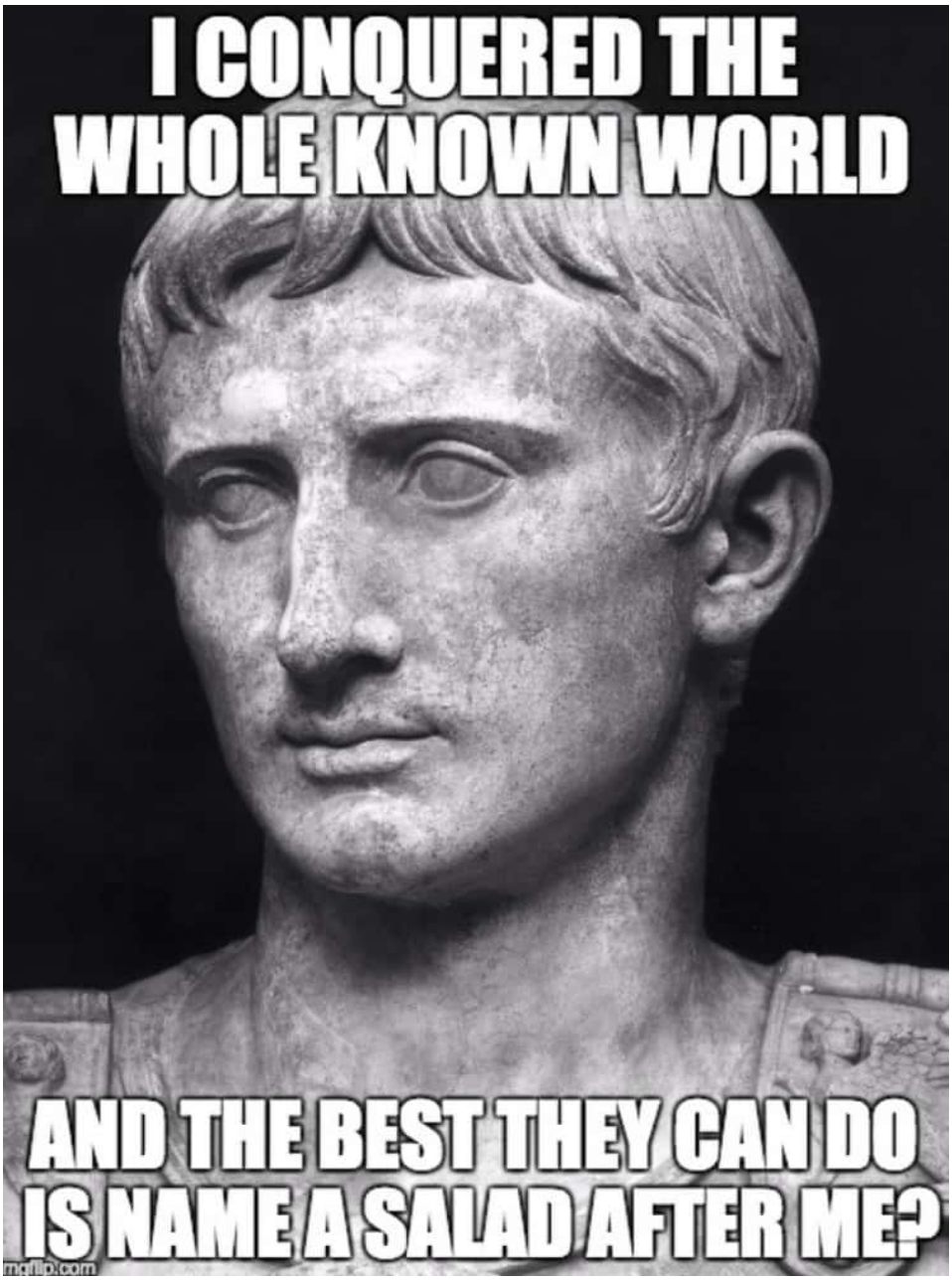
`Cézarova šifra` je starověká metoda kódování zpráv pomocí posunu písmen o určitý počet míst v abecedě. Například, pokud si zvolíme posun o 3 místa, písmeno `A` se nahradí písmenem `D`, písmeno `B` písmenem `E` atd. Tento způsob kódování se používal již v době Římské říše. V programovacím jazyce C# můžeme implementovat Cézarovu šifru jednoduše pomocí cyklu a jednoduchých matematických operací.

Ukázka implementace šifry

```
string message = "Tajna zprava"; // zpráva, kterou chceme zašifrovat
int shift = 3; // počet míst, o které se mají posunout písmena v abecedě
string encryptedMessage = ""; // inicializace prázdného řetězce pro zašifrovanou zprávu

foreach (char letter in message)
{
    int asciiCode = (int)letter; // převod písmene na ASCII kód
    int shiftedAsciiCode = asciiCode + shift; // posunutí ASCII kódu o zvolený počet míst
    char shiftedLetter = (char)shiftedAsciiCode; // převod posunutého ASCII kódu zpět na
písmeno
    encryptedMessage += shiftedLetter; // přidání posunutého písmene do zašifrované zprávy
}

Console.WriteLine(encryptedMessage); // výpis zašifrované zprávy
```



Nějaký humřík na uvolnění :D

Otázka 3: Vigenèrova šifra

`Vigenèrova šifra` je typ šifrování, který používá `klíč` složený z řetězce písmen k zakódování zprávy. Každé písmeno zprávy je posunuto o určitý počet míst na základě odpovídajícího písmene v klíči. Tento posun se opakuje pro každé písmeno v zprávě, dokud není celá zpráva zakódována.

Vigenèrova šifra je podobná Cézarově šifře, ale namísto pevného posunu používá proměnlivý posun pro každé písmeno v zprávě, což ji činí mnohem bezpečnější.

Otázka 5: Metoda Monte Carlo

Metoda `Monte Carlo` v programování je způsob, jak přibližně vypočítat výsledek nějakého problému, aniž bychom museli použít přesné matematické rovnice. **Namísto toho používáme náhodná čísla a statistickou analýzu, abychom získali odhad výsledku**. Tento přístup se používá v mnoha různých oblastech, kde je těžké nebo nemožné najít přesné matematické řešení.

Jako příklad si ukážeme program, který aproximuje hodnotu čísla `π` pomocí náhodně vygenerovaných bodů v čtverci a kruhu:

Metoda Monte Carlo

```
using System;

class MonteCarloPi
{
    static void Main(string[] args)
    {
        int n = 1000000; // počet náhodných bodů
        int count = 0;

        Random rnd = new Random();

        for (int i = 0; i < n; i++)
        {
            double x = rnd.NextDouble(); // náhodná hodnota x od 0 do 1
            double y = rnd.NextDouble(); // náhodná hodnota y od 0 do 1
            if (x * x + y * y <= 1) // bod je uvnitř kruhu
            {
                count++;
            }
        }

        double pi = 4.0 * count / n; // aproximace hodnoty pi

        Console.WriteLine("Approximation of pi: " + pi);
    }
}
```

> Aproximace je matematický postup, při kterém se snažíme najít hodnotu nebo řešení daného problému, aniž bychom museli použít přesné matematické vztahy nebo algoritmy. Namísto toho používáme jednodušší a rychlejší metody, které nám umožňují dosáhnout přibližného výsledku, který je dostatečně přesný pro naše účely.

Otázka 6: Eratostenovo síto

Eratostenovo síto je matematická metoda pro nalezení všech prvočísel menších nebo rovných zadanému číslu. Princip spočívá v tom, že se nejprve vytvoří seznam všech čísel od 2 do zadaného čísla a postupně se odstraňují čísla, která nejsou prvočísly.

Algoritmus funguje takto:

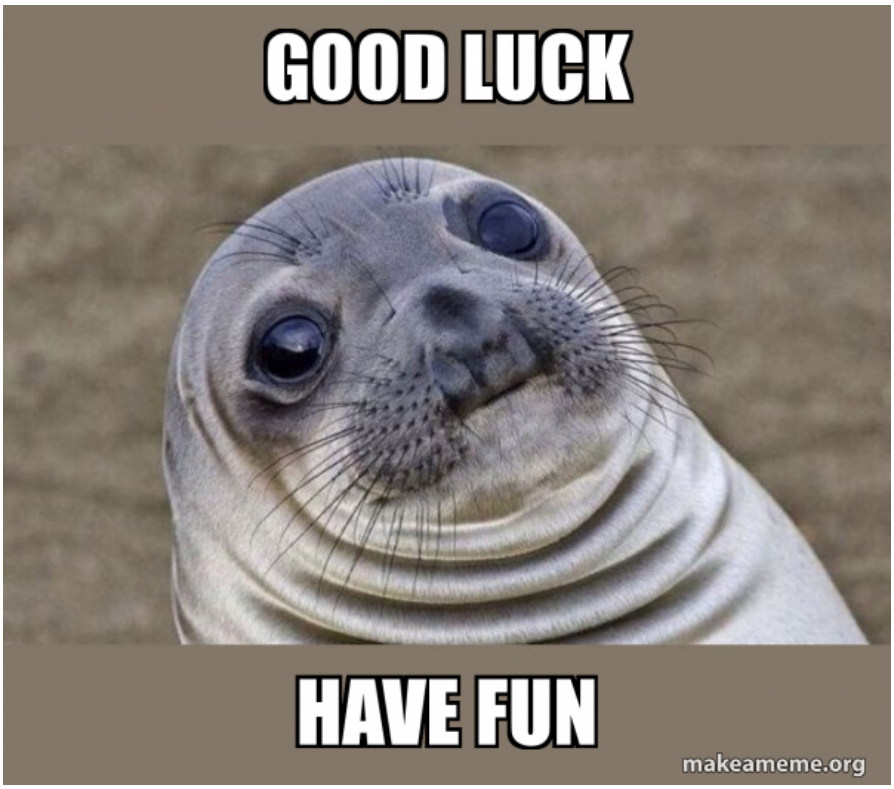
- Vytvoř seznam všech čísel od 2 do zadaného čísla.
- Začni s prvním prvočíslem (tj. číslem 2) a vyškrtni z seznamu všechna násobky tohoto čísla (tj. čísla 4, 6, 8 atd.).
- Přejdi na další nevyškrtnuté číslo v seznamu a opakuj krok 2 až do konce seznamu.
- Zbývající nevyškrtnutá čísla jsou všechna prvočísla menší nebo rovna zadanému číslu.

Například, pokud chceme najít všechna prvočísla menší nebo rovna číslu 30, postupujeme následovně:

- Vytvoříme seznam všech čísel od 2 do 30: 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30.
- Vyškrtneme všechny násobky čísla 2 (tj. 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30).
- Přejdeme na další nevyškrtnuté číslo v seznamu (tj. 3) a vyškrtneme všechny jeho násobky (tj. 9, 15, 21, 27).
- Přejdeme na další nevyškrtnuté číslo (tj. 5) a vyškrtneme všechny jeho násobky (tj. 25).
- Postupujeme takto až do konce seznamu.
- Zbývající nevyškrtnutá čísla jsou všechna prvočísla menší nebo rovna číslu 30: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29.

Závěr

Je důležité ke každé otázce znát alespoň teorii! Hodně štěstí!



:-)

Revision #1
Created 2025-05-21 13:31:45 UTC by Magdalena Dobešová
Updated 2025-05-21 13:37:35 UTC by Magdalena Dobešová