Historie matematiky a informatiky
Cvičení 3

Doc. RNDr. Alena Šolcová, Ph. D.,
KAM, FIT ČVUT v Praze

2014

Evropský sociální fond
Investujeme do vaší budoucnosti

Výpočet Velikonoc

Gaussův algoritmus

Pro období 1900 – 2099 volíme konstanty

$$m = 24 \text{ a } n = 5.$$

Nechť a, b, c, d, e jsou nejmenší nezáporná čísla, která splňují kongruence

$a \equiv r \pmod{19}$,

$b \equiv r \pmod{4}$,

$c \equiv r \pmod{7}$,

$d \equiv (m + 19a) \pmod{30}$,

$e \equiv (n + 2b + 4c + 6d) \pmod{19}$.

Pak pro $d + e < 10$ připadá velikonoční neděle na březnový den, který výpočteme jako (22 + d + e).

Výpočet Velikonoc 2

- Pro $d + e = 35$ připadá velikonoční neděle

  na $(d + e - 16)$ – tý den v dubnu a ve zbývajících případech měsíce dubna na den

  $(d + e - 9)$.

  Tento algoritmus má však nejméně dvě výjimky, roky 1954 a 2049, kdy velikonoční neděle nepřipadne na 25. dubna.

Řetězové zlomky

- Sofistikovanější metodu tvorby reziduí publikovali v roce 1931 Derrick Henry Lehmer a Ralph Ernest Powers
- Používají k tomu rozvoj $\sqrt{N}$ do řetězového zlomku

Řetězové zlomky

- Řetězový zlomek = zápis čísla x ve tvaru

$$x = b_0 + \cfrac{1}{b_1 + \cfrac{1}{b_2 + \cfrac{1}{\dots}}} = [b_0, b_1, \dots]$$

- Vztahy pro výpočet:

$$x_0 = x,\ b_n = \lfloor x_n \rfloor,\ x_{n+1} = \frac{1}{x_n - b_n}$$

Řetězové zlomky

- x je možné aproximovat konečným počtem hodnot, tj. $x_M = [b_0, b_1, \dots, b_M]$
- To je možné vyjádřit také jako poměr M-tých členů posloupností A a B: $x_M = \frac{A_M}{B_M}$
- Vztahy pro výpočet posloupností:

$$A_{-1} = 1, B_{-1} = 0$$
$$A_0 = b_0, B_0 = 1$$
$$A_n = b_n A_{n-1} + A_{n-2}$$
$$B_n = b_n B_{n-1} + B_{n-2}$$

Řetězové zlomky

- A k čemu nám jsou řetězové zlomky při faktorizaci ???
- Chceme faktorizovat N, označme $x = \sqrt{N}$
- Pro x vytvořme řetězový zlomek, tj. počítejme členy posloupností A a B
- Pro $x = \sqrt{N}$ můžeme k výpočtu hodnot x_n jako alternativu využít posloupností P a Q – jejich definice zde neuvádím, není to důležité

Řetězové zlomky

- Je možné ukázat (důkaz není úplně lehký):

$$A_{i-1}^2 - N \cdot B_{i-1}^2 = (-1)^i \cdot Q_i$$

- Tato rovnost modulo N:

$$A_{i-1}^2 \equiv (-1)^i \cdot Q_i \pmod{N}$$

- Máme kvadratické reziduum – takovou kongruenci jsme hledali ☺
- Také se dá ukázat, že

$$0 < Q_i < 2\sqrt{N}$$

Takže reziduum bude poměrně malé (vzhledem k N) a bude mít ty vlastnosti, které jsme chtěli

Řetězové zlomky - ukázka

- Faktorizujme N = 507. Budeme počítat posloupnosti pro zápis $\sqrt{507}$ do řetězového zlomku.
- $A_0 = 22;\ A_0^2 \equiv 484 \pmod{507}$
- $A_1 = 23;\ A_1^2 \equiv 22 \pmod{507}$
- $A_2 = 45;\ A_2^2 \equiv 504 \pmod{507}$
- $A_3 = 146;\ A_3^2 \equiv 22 \pmod{507}$
- $23^2 \cdot 146^2 \equiv 22^2 \pmod{507}$
- $316^2 - 22^2 \equiv 0 \pmod{507}$
- $294 \cdot 338 \equiv 0 \pmod{507}$
- GCD (294, 507) = 3; GCD (338, 507) = 169
  => $507 = 3 \cdot 169$

Další algoritmy

- Kongruence čtverců je použita i v jiných algoritmech.
- Quadratic Sieve (QS), Carl Pomerance, 1981
- Special Number Field Sieve (SNFS), John Pollard, 1996
- Další vývoj SNFS = General Number Field Sieve (GNFS), nejúčinnější dosud známý faktorizační algoritmus pro obecné případy.