Poznámky a umění výpočtů

prof. RNDr. Miroslav Vlček, DrSc.

vlcek@fd.cvut.cz

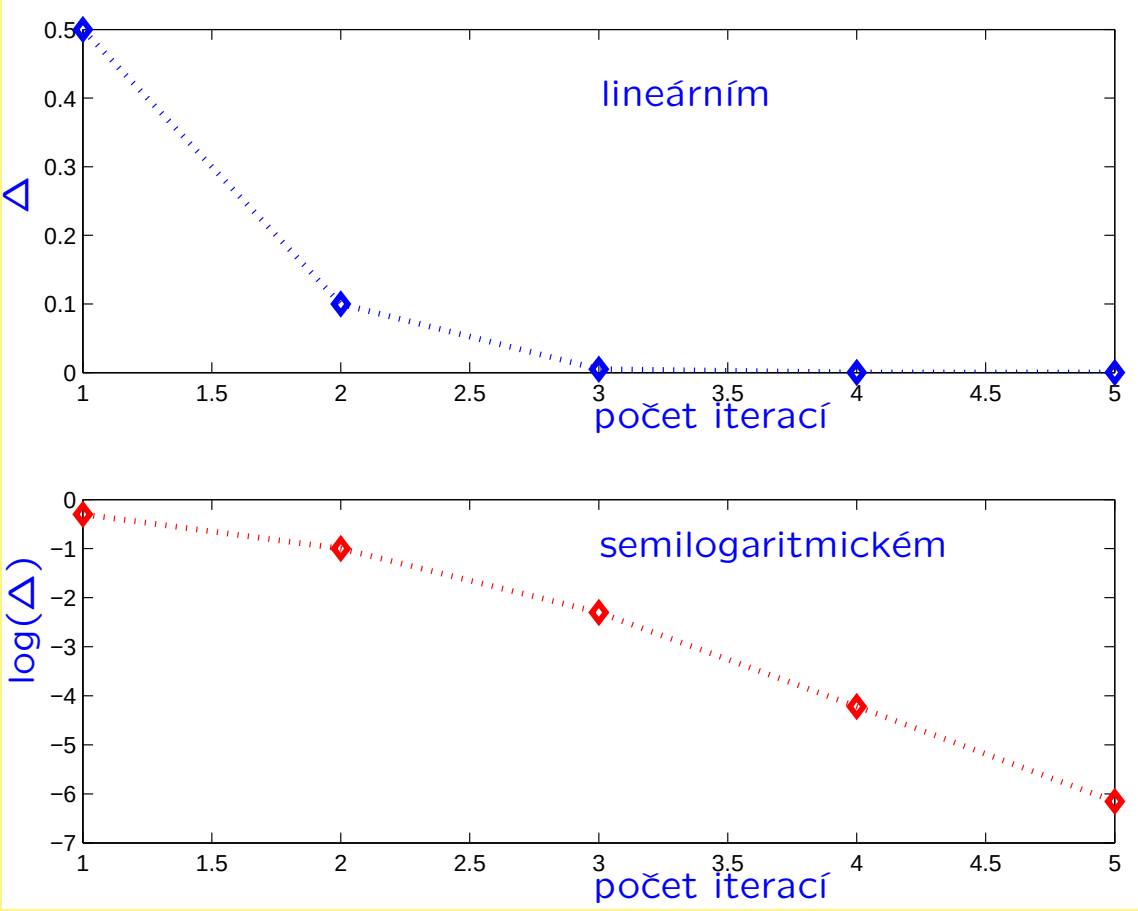
3. ledna 2008

K domácímu úkolu č. 1

Algoritmus pro výpočet odmocniny

$$y(n) = \frac{1}{2}\left[y(n-1) + \frac{x_0}{y(n-1)}\right]$$

a zobrazování dat v měřítku...



Modulární umocňování

Společný problém mnohých kryptografických systému spočívá v rychlosti výpočtu $x^n (mod\, m)$ pro velké hodnoty x a n.

Příklad: Nalezněte $17^{73} (mod\, 19)$.

Zapíšeme binárně exponent

$$73 = 1\times1+1\times8+1\times64 = 1\times2^0+1\times2^3+1\times2^6$$

- Paralelní algoritmus

$$\begin{aligned} 17^{73}(mod\,19) &= (17)^1 \times (17)^8 \times (17)^{64}(mod\,19) \\ &= 17 \times 9 \times 17 \equiv 17(mod\,19) \end{aligned}$$

- Sériový algoritmus

$$\begin{aligned} 17^{73}(mod\,19) &= (17)^1 \times (17 \times (17)^8)^8(mod\,19) \\ &= 17 \times (17 \times 9)^8(mod\,19) \\ &\equiv 17(mod\,19) \end{aligned}$$

K domácímu úkolu č. 3

Platí

$$\begin{aligned} 3 &\equiv 3 (\mathrm{mod}\, 4), \\ 3^2 &\equiv 1 (\mathrm{mod}\, 4), \\ &\vdots \\ 3^{76} &\equiv 1 (\mathrm{mod}\, 4), \\ 3 \times 3^{76} &\equiv 3 (\mathrm{mod}\, 4), \\ 3^{77} - 1 &\equiv 2 (\mathrm{mod}\, 4), \\ (3^{77} - 1)/2 &\equiv 1 (\mathrm{mod}\, 2). \end{aligned}$$

Odtud již plyne, že číslo $\dfrac{3^{77} - 1}{2}$ je liché.

Co můžeme říci o číslech $\dfrac{3^{77} - 1}{2}$ a $\dfrac{3^7 - 1}{2}$, jestliže platí

$$\begin{aligned} \frac{3^{77} - 1}{3^7 - 1} &= 3^{70} + 3^{63} + 3^{56} + 3^{49} + 3^{42} + 3^{35} \\ &+ 3^{28} + 3^{21} + 3^{14} + 3^7 + 1 = \sum_{m=0}^{10} (3^7)^m ? \end{aligned}$$

Čísla $\frac{3^{77}-1}{2}$ a $\frac{3^{7}-1}{2}$ jsou soudělná !!

Bez použití algoritmů faktorizace

http://www.alpertron.com.ar/ECM.HTM

lze dokázat, že číslo $\frac{3^{77}-1}{2}$ je složené.

Diskrétní logaritmus

Inverzí výpočtu mocnin v modulární aritmetice je výpočet diskrétního logaritmu, tj. čísla x z kongruence

$$a^x \equiv b(mod\, n).$$

Řešení kongruence $2^x \equiv 3(mod\, 13)$ hrubou silou.

$$\begin{aligned} x = 1,\ \ 2^1 &\equiv\ \ 2(mod\, 13) \\ x = 2,\ \ 2^2 &\equiv\ \ 4(mod\, 13) \\ x = 3,\ \ 2^3 &\equiv\ \ 8(mod\, 13) \\ x = 4,\ \ 2^4 &\equiv\ \ 3(mod\, 13) \end{aligned}$$

Hledaným rešením je $x = 4$.

Řešení problému diskrétního logaritmu hrubou silou je pro velká n nesmírně obtížné. Proto je na tomto problém založeno několik kryptografických algoritmů veřejného klíče.

Redukovaná množina reziduí

Pro kladné celé číslo n označuje symbol $\phi(n)$ **Eulerovu funkci**, která udává počet kladných celých čísel menších než n, která jsou s n nesoudělná.

Například $\phi(10) = 4$, protože $1, 3, 7, 9$ jsou s číslem 10 nesoudělná.

Množina kladných celých čísel $< n$ a nesoudělných s n tvoří **redukovanou množinu residuí**, tj. zbytkovou třídu $mod\, n$.

Proto $\{1, 3, 7, 9\}$ je redukovaná množina residuí $mod\, 10$.

Vlastnosti $\phi(n)$

- $\phi(p) = p - 1$ pro prvočíslo p.
- $\phi(p \times q) = (p-1)(q-1)$ pro různá prvočísla p a q.
- Nechť $n = p_1^{e1} \times p_2^{e2} \ldots p_\mu^{e_\mu}$, kde p_i jsou různá prvočísla. Potom $\phi(n) = \prod_i^\mu p_i^{e_i - 1} \times (p_i - 1)$.
- Eulerův teorém: pro $\gcd(a, p) = 1$ platí
$$a^{\phi(p)} \equiv 1 (mod\, p)$$
- Malá Fermatova věta: Jestliže p je prvočíslo, které není dělitelem a, potom platí
$$a^{p-1} \equiv 1 (mod\, p).$$

Příklady:

- $\phi(13) = 12$
- $\phi(10) = \phi(2 \times 5) = 1 \times 4 = 4$
- $\phi(15) = 2 \times 4 = 8$
- $\phi(24) = \phi(2^3 \times 3^1) =$
- $= 2^2 \times (2-1) \times 3^0 \times (3-1) = 8$

Výpočet inverzí $mod\, n$

Nechť $0 < a < n$. Potom existuje x takové, že $ax \equiv 1 (mod\, n)$, jestli-že $\gcd(a, n) = 1$. Číslo x se nazývá inverzí čísla a a zapisuje se jako a^{-1}.

Příklady:

$$3 \times 7 \equiv 1 (mod\, 10), \;\; 3^{-1} = 7 \;\; \text{a} \; 7^{-1} = 3$$
$$9 \times 9 \equiv 1 (mod\, 10), \;\; 9^{-1} = 9$$
$$1 \times 1 \equiv 1 (mod\, 10), \;\; 1^{-1} = 1$$

Problém
Je dáno $\gcd(a, n) = 1$. Hledáme x takové, aby $ax \equiv 1 (mod\, n)$.

Metoda hrubé síly
Počítáme

$$a^1, a^2, a^3 \ldots a^k (mod\, n),$$

až najdeme

$$a^r \equiv 1(mod\, n) \Leftrightarrow a \times a^{r-1} \equiv 1(mod\, n) \Leftrightarrow a \times x \equiv 1(mod\, n) \Rightarrow x = a^{r-1}$$

Eulerův teorém

Pokud známe $\phi(n)$, pak

$$a^{\phi(n)} \equiv 1(mod\, n) \Rightarrow x = a^{\phi(n)-1}$$

Příklad: Máme najít $29^{-1}(mod\, 181)$.

Protože modul 181 je prvočíslo, je $\phi(181) = 180$ a musí platit

$$\begin{aligned} x &= a^{\phi(n)-1}(mod\, 181) \\ x &= 29^{180-1}(mod\, 181) \\ x &= 29^{128+32+16+2+1}(mod\, 181) \\ x &= (29^{128} \times 29^{32} \times 29^{16} \times 29^2 \times 29^1)(mod\, 181) \\ x &= (145 \times 117 \times 29 \times 117 \times 29)(mod\, 181) \\ x &= 25(mod\, 181) \end{aligned}$$

Čínský teorém o zbytcích

Nechť $n_1, n_2, \ldots, n_k$ jsou čísla párově nesoudělná. Pak systém simultánních kongruencí

$$\begin{aligned} x &\equiv a_1 (mod\, n_1) \\ x &\equiv a_2 (mod\, n_2) \\ &\vdots \\ x &\equiv a_k (mod\, n_k) \end{aligned}$$

má jediné řešení modulo $n = n_1 n_2 \ldots n_k$ pro daná celá čísla a_i za podmínky $0 < x < n$.

Gaussův algoritmus

Řešením je

$$x = \sum_{i=1}^{k} a_i \times N_i \times M_i (mod\, n),$$

kde $N_i = n/n_i$ a $M_i = N_i^{-1} (mod\, n_i)$.

Příklad: Nalezněte řešení kongruencí

$$\begin{aligned} x &\equiv 5 (mod\, 6) \\ x &\equiv 33 (mod\, 35) \end{aligned}$$

Protože $\gcd(35, 6) = 1$ je $n = 6 \times 35 = 210$. Dále platí

$$a_i \qquad N_i = \frac{N}{n_i} \qquad M_i = N_i^{-1} (mod\, n_i)$$

$$a_1 = 5 \quad N_1 = \frac{210}{6} = 35 \quad M_1 = 35^{-1} (mod\, 6) = 5$$

$$a_2 = 33 \quad N_2 = \frac{210}{35} = 6 \quad M_2 = 6^{-1} (mod\, 35) = 6$$

$$\begin{aligned} x &\equiv \{a_1 N_1 M_1 + a_2 N_2 M_2\} (mod\, n) \\ &\equiv \{5 \times 35 \times 5 + 33 \times 6 \times 6\} (mod\, 210) \\ &\equiv \{875 + 1188\} (mod\, 210) \\ x &\equiv 173 (mod\, 210) \end{aligned}$$