Problema logaritmului discret

Algoritmul Pohlig-Hellman

Ingredientul principal al acestui algoritm îl constitue Lema Chineză a resturilor. Dacă $m = m_1 m_2 \dots m_t$, unde m_i sunt prime între ele două câte două, atunci rezolvarea unei ecuaţii modulo m este mai mult sau mai puţin echivalentă cu rezolvarea ecuaţiilor modulo m_i pentru fiecare i. În cazul problemei logaritmului discret, trebuie să rezolvăm ecuaţia $g^x \equiv h \pmod{p}$. În acest caz, modulul p este prim, fapt ce ne sugerează că nu poate fi folosită Lema Chineză a resturilor. Totuşi, să ne amintim că soluţia x este determinată modulo $p-1$, şi deci trebuie să gândim soluţia ca element al lui $\mathbb{Z}/(p-1)\mathbb{Z}$. Aceasta ne sugerează că descompunerea lui $p-1$ în factori primi ar putea juca un rol important în studiul dificultăţii PLD în $(\mathbb{Z}/p\mathbb{Z})^*$

• Descompunem pe $n = p-1$ în factori primi, adică $n = p-1 = \prod_{i=1}^{k} p_i^{c_i}$, unde p_i sunt numere prime distincte. Notaţia $n = p-1$ a fost făcută pentru uşurinţa în scriere.

• Valoarea $x = d\log_g h$ este determinată unic modulo n.

• Dacă am putea calcula $x_i = x \pmod{p_i^{c_i}}$, pentru fiecare i, $1 \le i \le k$, atunci putem calcula $x \pmod{n}$ folosind Lema Chineză a resturilor.

Sistemul de congruenţe liniare simultane $x \equiv x_i \pmod{p_i^{c_i}}$, $1 \le i \le k$, are soluţie unică modulo $n = p-1$. Aceasta se calculează astfel: definim $N_i = \frac{n}{p_i^{c_i}}$, $1 \le i \le k$. Evident $\gcd(N_i, p_i^{c_i}) = 1$ şi deci există M_i astfel ca $M_i \cdot N_i \equiv 1 \pmod{p_i^{c_i}}$. Se verifică uşor că

$$x = \sum_{i=1}^{k} x_i M_i N_i$$

este soluţie a sistemului de mai sus, unică modulo n.

Fie q un număr prim astfel încât $n \equiv 0 \pmod{q^c}$ şi $n \not\equiv 0 \pmod{q^{c+1}}$.

Să vedem cum se poate calcula valoarea $a = x \pmod{q^c}$, unde $0 \le a \le q^c - 1$. Dezvoltăm mai întâi pe a în baza q:

$$a = \sum_{i=0}^{c-1} a_i q^i,$$

unde $0 \le a_i \le q-1$, pentru $0 \le i \le c-1$. Să mai observăm că putem exprima pe x ca $x = a + sq^c$ pentru un anumit întreg s şi deci

$$x = \sum_{i=0}^{c-1} a_i q^i + sq^c.$$

Vom calcula pe rând coeficienţii a_i. Primul pas al algoritmului este calculul lui a_0.

Principala observaţie folosită în algoritm este

$$h^{n/q} \equiv g^{a_0 n/q} \pmod{p}.$$

Într-adevăr

$$\begin{aligned} h^{n/q} &= (g^x)^{n/q} \\ &= g^{(a_0+a_1q+\cdots+a_{c-1}q^{c-1}+sq^c)n/q} \\ &= g^{(a_0+Kq)n/q}, \text{ unde } K \text{ este un întreg} \\ &= g^{a_0 n/q}(g^n)^K \\ &= g^{a_0 n/q} \pmod{p}. \end{aligned}$$

Folosind această ecuaţie este simplu să-l calculăm pe a_0. De exemplu, calculăm $\gamma = g^{n/q}, \gamma^2, \ldots$ până când găsim un i, $i \leq c-1$, astfel încât $\gamma^i \equiv h^{n/q}$. Acest i va fi a_0.

Dacă $c = 1$ algoritmul se termină. Altfel $c > 1$ şi calculăm $a_1, \ldots, a_{c-1}$. Aceştia se calculează la fel ca a_0. Presupunem că am calculat deja coeficienţii $a_0, a_1, \ldots, a_{j-1}$. Notăm $h_0 = h$ şi definim $h_j = hg^{-(a_0+a_1q+\cdots+a_{j-1}q^{j-1})}$, pentru $1 \leq j \leq c-1$. Vom folosi acum observaţia

$$h_j^{n/q^{j+1}} \equiv g^{a_j n/q} \pmod{p}.$$

Identitatea se demonstrează analog:

$$\begin{aligned} h_j^{n/q^{j+1}} &= (g^{x-(a_0+a_1q+\cdots+a_{j-1}q^{j-1})})^{n/q^{j+1}} \\ &= (g^{a_jq^j+\cdots+a_{c-1}q^{c-1}+sq^c})^{n/q^{j+1}} \\ &= g^{(a_jq^j+K_jq^{j+1})n/q^{j+1}}, \text{ unde } K_j \text{ este un întreg} \\ &= g^{a_j n/q}(g^n)^{K_j} \\ &= g^{a_j n/q} \pmod{p}. \end{aligned}$$

Pentru a completa descrierea algoritmului să observăm că h_{j+1} se poate calcula recursiv din h_j de îndată ce îl ştim pe a_j:

$$h_{j+1} = h_j \cdot g^{-a_jq^j}.$$

Exemplul 1. *Fie $p = 29$ şi $g = 2$ o rădăcină primitivă modulo 29. Vrem să rezolvăm PLD $2^x \equiv 18$ mod 29.*

Fie $n = p - 1 = 28$. Descompunem pe 28 în factori primi: $28 = 2^2 \cdot 7^1$.

Mai întâi luăm $q = 2$ şi $c = 2$.

Atunci $\gamma_1 = \gamma = g^{n/q} = 2^{28/2} = 2^{14} = 28$ (mod 29).

Pe de altă parte calculăm $h^{(p-1)/q} = 18^{28/2} = 18^{14} = 28$ (mod 29). Am găsit $a_0 = 1$.

Determinăm acum pe a_1.

Calculăm $h_1 = h_0 g^{-a_0} = hg^{-a_0} = 18 \cdot 2^{-1} = 18 \cdot 15 = 9$ (mod 29).

Atunci $h_1^{(p-1)/q^2} = h_1^{28/4} = 9^7 = 28$ (mod 29).

Cum $\gamma_1 \equiv 28$ (mod 29), găsim $a_1 = 1$, adică $x \equiv 1 + 2 \cdot 2 = 3$ (mod 4).

Punem acum $q = 7$ şi $c = 1$.

Calculăm acum $h^{(p-1)/q} = h^{28/7} = 18^4 = 25$ (mod 29).

Pe de altă parte $\gamma = g^{n/q} = 2^{28/7} = 16$ *(mod* 29*). Se mai calculează* $\gamma^2 = 24$, $\gamma^3 = 7$ *şi* $\Gamma^4 = 25$. *Gă sim* $a_0 = 4$ *şi deci* $x \equiv 4$ *(mod* 7*).*

În final, folosind Lema Chineză a resturilor, se rezolvă sistemul $x \equiv 3$ *(mod* 4*),* $x \equiv 4$ *(mod* 7*).*

$N_1 = \frac{28}{4} = 7$. $N_1 \cdot M_1 \equiv 1$ *(mod* 4*). Rezultă* $N_1 = 3$.

$N_2 = \frac{28}{7} = 4$. $N_2 \cdot M_2 \equiv 1$ *(mod* 7*). Rezultă* $N_2 = 2$.

În final se găseşte soluţia $x = 3 \cdot 7 \cdot 3 + 4 \cdot 4 \cdot 2 = 11$ *(mod* 28*), adică* $2^{11} \equiv 18$ *(mod* 29*).*