Quadratische Reste und das Legendre Symbol

Definition Quadratischer Rest

Sei p prim. Ein Element $a \in \mathbb{Z}_p$ heißt *quadratischer Rest* in $\mathbb{Z}_p^*$, falls es ein $b \in \mathbb{Z}_p^*$ gibt mit $b^2 \equiv a \bmod n$. Wir definieren

$$QR_p = \{a \in \mathbb{Z}_p^* \mid a \text{ ist ein quadratischer Rest }\} \text{ und } QNR_p = \mathbb{Z}_p^* \setminus QR.$$

Definition Legendre Symbol

Sei $p > 2$ prim und $a \in \mathbb{N}$. Das *Legendre Symbol* ist definiert als

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{falls } p|a \\ 1 & \text{falls } (a \bmod p) \in QR_p \\ -1 & \text{falls } (a \bmod p) \in QNR_p. \end{cases}$$

Berechnung von $\mathrm{dlog}_\alpha(\beta) \bmod 2$

Satz Berechnung des niederwertigsten Bits

Sei p prim, α Generator von $\mathbb{Z}_p^*$ und $\beta \equiv \alpha^a \bmod p$. Dann gilt

$$\left(\frac{\beta}{p}\right) \equiv \beta^{\frac{p-1}{2}} \bmod p = \begin{cases} 1 & \text{falls } a \equiv 0 \bmod 2 \\ -1 & \text{falls } a \equiv 1 \bmod 2 \end{cases}.$$

Beweis:

- Es gilt $\mathbb{Z}_p^* = \{\alpha, \alpha^2, \ldots, \alpha^{p-1}\}$. Damit folgt

$$QR_p = \{\alpha^2, \alpha^4, \ldots, \alpha^{2\cdot\frac{p-1}{2}}, \underbrace{\alpha^{2\cdot\frac{p+1}{2}}}_{\alpha^2}, \underbrace{\alpha^{2\cdot\frac{p+3}{2}}}_{\alpha^4}, \ldots, \underbrace{\alpha^{2(p-1)}}_{\alpha^{p-1}}\}$$

- D.h. β ist ein quadratischer Rest gdw a gerade ist.
- Es gilt $\beta^{\frac{p-1}{2}} = \pm 1$, da die 1 in $\mathbb{Z}_p^*$ Quadratwurzeln ± 1 besitzt.
- Ferner ist $\beta^{\frac{p-1}{2}} = \alpha^{\frac{a(p-1)}{2}} = 1$ gdw $\frac{a(p-1)}{2}$ Vielfaches von $p-1$.
- D.h. $\beta^{\frac{p-1}{2}} = 1$ gdw a gerade ist.

Korollar: Wir können $\mathrm{dlog}_\alpha(\beta) \bmod 2$ in Zeit $\mathcal{O}(\log^2 p)$ berechnen.

Lernen von $\mathrm{dlog}_\alpha(\beta)$ modulo Teiler von $p-1$

Idee des Pohlig Hellman Algorithmus:

- Wir nehmen an, dass die Zerlegung $p-1=\prod_{i=1}^{k} p_i^{e_i}$ bekannt ist.
- Bestimmen $a = a_i \bmod p_i^{e_i}$ für alle i. Wir ermitteln a mittels CRT.
- Zur Bestimmung von a_i verwenden wir die p_i-adische Zerlegung

  $$a_i = a_{i0} + a_{i1}p_i + a_{i2}p_i^2 + \ldots + a_{ie_i-1}p_i^{e_i-1} \text{ mit } 0 \leq a_{ij} < p_i.$$
- Die a_{ij} werden sukzessive für $j = 0, \ldots, e_i - 1$ berechnet.

Elemente in der p_i-adischen Entwicklung

Bestimmung von a_{i0}:

- Es gilt

$$\beta^{\frac{p-1}{p_i}} \equiv \alpha^{a\cdot\frac{p-1}{p_i}} = \alpha^{(a \bmod p_i)\cdot\frac{p-1}{p_i}} \cdot \underbrace{\alpha^{\lfloor\frac{a}{p_i}\rfloor\cdot p_i\cdot\frac{p-1}{p_i}}}_{1}$$

$$\equiv \alpha^{(a \bmod p_i)\cdot\frac{p-1}{p_i}} \equiv \alpha^{(a_i \bmod p_i)\cdot\frac{p-1}{p_i}} = \alpha^{a_{i0}\cdot\frac{p-1}{p_i}} \bmod p.$$

- Wir berechnen $\alpha^{\ell\cdot\frac{p-1}{p_i}}$ für $\ell = 0, \ldots, p_i - 1$ und vergleichen mit $\beta^{\frac{p-1}{p_i}}$.

Bestimmung von a_{ij}:

- Angenommen, wir haben bereits $a_{i0}, \ldots, a_{ij-1}$ bestimmt.
- Setze $r = a_0 + \ldots + a_{ij-1}p_i^{j-1}$ und $\beta' := \beta \cdot \alpha^{-r}$.
- Analog zum obigen Fall berechnen wir

$$\beta'^{\frac{p-1}{p_i^{j+1}}} \equiv \alpha^{(a-r)\cdot\frac{p-1}{p_i^{j+1}}} \equiv \alpha^{(a-r \bmod p_i^{j+1})\cdot\frac{p-1}{p_i^{j+1}}} \equiv \alpha^{(a_i-r \bmod p_i^{j+1})\cdot\frac{p-1}{p_i^{j+1}}} = \alpha^{a_{ij}\cdot\frac{p-1}{p_i}}.$$

- Durch Vergleich mit $\alpha^{\ell\cdot\frac{p-1}{p_i}}$, $\ell = 0, \ldots, p_i - 1$ bestimmen wir a_{ij}.

Pohlig-Hellman Algorithmus

Algorithmus Pohlig-Hellmann

EINGABE: p, α, $\beta' \equiv \alpha^a \bmod p$ und $p-1 = \prod_{i=1}^{k} p_i^{e_i}$

1. FOR $i = 1, \ldots, k$ und $\ell = 0, \ldots, p_i - 1$ berechne $c_{i\ell} = \alpha^{\ell \cdot \frac{p-1}{p_i}}$.
2. FOR $i = 1, \ldots, k$
   1. Setze $\beta := \beta'$.
   2. FOR $j = 0, \ldots, e_i - 1$
      1. Bestimme $c_{i\ell}$ mit $c_{i\ell} = \beta^{\frac{p-1}{p_i^{j+1}}}$. Setze $a_{ij} = \ell$ und $\beta := \beta \cdot \alpha^{-a_{ij} p_i^j}$.
3. Für $i = 1, \ldots, k$ berechne $a_i = a_{i0} + a_{i1} p_i + \ldots + a_{ie_i-1} p_i^{e_i-1}$.
4. Bestimme $a = CRT(a_1, \ldots, a_k) \bmod p - 1$.

AUSGABE: $a = \mathrm{dlog}_\alpha \beta$

Laufzeit:

- Schritt 1: $T_1 = (p_1 + \ldots + p_k) \cdot \mathcal{O}(\log^3 p)$.
- Schritt 2,3,4: $T_2 = (e_1 + \ldots + e_k) \cdot \mathcal{O}(\log^3 p) = \mathcal{O}(\log^4 p)$.
- D.h. wir erhalten Gesamtlaufzeit $\mathcal{O}(T_1 + T_2)$.
- Damit ist unsere Laufzeit polynomiell falls $p_i = \mathcal{O}(\log p)$ für alle i.