Algoritmy teorie čísel

Radan Kučera, doplněk, podzimní semestr 2021

Motivace

Někdy (například při řešení diofantických rovnic) potřebujeme pracovat v okruhu R celých algebraických čísel tělesa algebraických čísel K (tj. K je konečné rozšíření $\mathbb{Q}$).
Obecně R není okruh s jednoznačným rozkladem, ale je to Dedekindův okruh, a tedy každý nenulový ideál okruhu R lze jednoznačně rozložit na součin prvoideálů. Místo rozkládání celého algebraického čísla $a \in R$ na součin ireducibilních prvků okruhu R můžeme rozkládat hlavní ideál aR na součin prvoideálů.
Pak ale v jisté chvíli se potřebujeme vrátit zpět od ideálu k číslu, které jej generuje, což je však možné jen v případě, že jde o hlavní ideál. V tom případě je generátor tohoto hlavního ideálu určen až na násobení **jednotkou**. Obstrukce kontrolující, zda je daný ideál hlavní, je skryta v **grupě tříd ideálů** Cl_K, kterou lze definovat jako faktorgrupu grupy všech **lomených ideálů** okruhu R podle podgrupy hlavních lomených ideálů.
Proto potřebujeme popsat následující aritmetické objekty okruhu R: jeho **grupu tříd ideálů** Cl_K a jeho **grupu jednotek** $R^\times$.

Grupa jednotek $R^\times$ je konečně generovaná

Torzní část W_K grupy $R^\times$ je konečná cyklická grupa obsahující všechny odmocniny z jedné patřící do K.

$\mathbb{Z}$-rank grupy $R^\times$ je dán Dirichletovou větou: $R^\times \cong W_K \times \mathbb{Z}^r$, kde $r := \operatorname{rank}_{\mathbb{Z}} R^\times = s + t - 1$, přičemž s je počet reálných vnoření tělesa K a t je počet párů nereálných vnoření tělesa K. Tudíž stupeň $[K : \mathbb{Q}] = s + 2t$.

Tato vnoření mohou být určena například takto: existuje $\alpha \in K$ takové, že $K = \mathbb{Q}(\alpha)$. Minimální polynom $f(X) \in \mathbb{Q}[X]$ čísla α má s reálných kořenů $\alpha_1, \ldots, \alpha_s$ a t dvojic komplexně sdružených kořenů $\alpha_{s+1}, \overline{\alpha_{s+1}}, \ldots, \alpha_{s+t}, \overline{\alpha_{s+t}}$.

Nechť σ_i je vnoření určené $\alpha \mapsto \alpha_i$. Pak σ_i je reálné, právě když $i \leq s$.

Tudíž známe $\mathbb{Z}$-rank r grupy $R^\times$, ale nalezení fundamentálních jednotek, tj. generátorů grupy $R^\times / W_K$, je velmi obtížný problém. Přestože je znám algoritmus, jeho časová náročnost se stupněm $[K : \mathbb{Q}]$ roste velmi rychle.

Geometrie jednotek

Logaritmické zobrazení $\ell : R^\times \to \mathbb{R}^{r+1}$ je definováno předpisem $\ell(\varepsilon) = (\dots, \delta_i \log|\sigma_i(\varepsilon)|, \dots)$, kde $\delta_i = 1$ pro $i \le s$ a $\delta_i = 2$ jinak.

Pak $\ker \ell = W_K$ a $\ell(R^\times) \subset \mathcal{H} = \left\{(x_1, \dots, x_{r+1}) \mid \sum_{i=1}^{r+1} x_i = 0\right\}$.

Pro libovolnou r-tici $\eta_1, \dots, \eta_r \in R^\times$ definujeme regulátor

$$R(\eta_1, \dots \eta_r) = \left|\det(\delta_i \log|\sigma_i(\eta_j)|)_{i,j=1,\dots,r}\right|.$$

Tudíž regulátor $R(\eta_1, \dots \eta_r)$ je dán r-rozměrným objemem rovnoběžnostěnu daného obrazy $\ell(\eta_1), \dots, \ell(\eta_r)$ v $\mathcal{H}$.

Proto $R(\eta_1, \dots \eta_r) = 0$, právě když jednotky $\eta_1, \dots, \eta_r$ jsou (multiplikativně) závislé.

Regulátor R_K tělesa K je definován jako regulátor libovolného systému fundamentálních jednotek (tj. r-tice jednotek generujících spolu s W_K grupu všech jednotek $R^\times$).

Platí $[R^\times : \langle W_k \cup \{\eta_1, \dots, \eta_r\}\rangle] = \frac{R(\eta_1,\dots\eta_r)}{R_K}$, je-li $R(\eta_1, \dots \eta_r) \neq 0$.

Dedekindova ζ-funkce ζ_K tělesa K

Dedekindova ζ-funkce ζ_K tělesa K je definována v oblasti $z \in \mathbb{C}$, $\Re(z) > 1$, absolutně konvergentní řadou

$$\zeta_K(z) = \sum_A (N(A))^{-z},$$

kde A probíhá množinu všech nenulových ideálů okruhu R a $N(A) = |R/A|$ je absolutní norma A.

Protože R je Dedekindův okruh, každý nenulový ideál A je jednoznačně dán jako součin prvoideálů.

Absolutní norma ideálů je multiplikativní, a tedy funkce $\zeta_K(z)$ je dána Eulerovým součinem přes všechny prvoideály okruhu R: je-li $\Re(z) > 1$, pak

$$\zeta_K(z) = \prod_{\mathfrak{P}} (1 - N(\mathfrak{P})^{-z})^{-1}.$$

Grupa tříd ideálů Cl_K je konečná grupa

Erich Hecke dokázal, že funkce $\zeta_K(z)$ má meromorfní prodloužení na celé $\mathbb{C}$ s jediným pólem v $z = 1$. Tento pól je jednoduchý a jeho residuum je

$$\lim_{z\to 1}(z-1)\zeta_K(z) = \frac{2^s(2\pi)^t h_K R_K}{|W_K|\cdot\sqrt{|D_K|}},$$

kde $h_K = |\,\mathrm{Cl}_K\,|$ je počet tříd ideálů a D_K je diskriminant tělesa K, který je definován takto:

Aditivní grupa $(R,+)$ je volná komutativní grupa ranku $\mathrm{rank}_{\mathbb{Z}}\, R = [K:\mathbb{Q}] = s+2t$. Nechť $b_1,\ldots,b_{s+2t}$ je systém nezávislých generátorů grupy $(R,+)$, pak diskriminant D_K je druhá mocnina determinantu

$$\det\Big(\sigma_1(b_j),\ldots,\sigma_{s+t}(b_j),\overline{\sigma_{s+1}(b_j)},\ldots,\overline{\sigma_{s+t}(b_j)}\Big)_{j=1,\ldots,s+2t}.$$

Odhad součinu $h_K R_K$

Speciálně pro těleso $\mathbb{Q}$ je Dedekindova ζ-funkce $\zeta_{\mathbb{Q}}$ rovna Riemannově ζ-funkci a platí $\lim_{z\to 1}(z-1)\zeta_{\mathbb{Q}}(z) = 1$.
Proto

$$\frac{2^s(2\pi)^t h_K R_K}{|W_K|\cdot\sqrt{|D_K|}} = \lim_{z\to 1}\frac{\zeta_K(z)}{\zeta_{\mathbb{Q}}(z)} = \lim_{z\to 1}\prod_p \frac{1-p^{-z}}{\prod_{\mathfrak{P}|pR}(1-N(\mathfrak{P})^{-z})},$$

kde ve vnějším součinu probíhá p všechna prvočísla, zatímco vnitřní součin je vzat přes konečně mnoho prvoideálů $\mathfrak{P}$ vystupujících v rozkladu ideálu pR. Proto spočítáme-li rozklady všech ideálů pR pro všechna prvočísla $p < L$ pro jistou dostatečně velkou hranici L, platí přibližně

$$h_K R_K \doteq \frac{|W_K|\cdot\sqrt{|D_K|}}{2^s(2\pi)^t}\prod_{p<L}\frac{1-p^{-1}}{\prod_{\mathfrak{P}|pR}(1-N(\mathfrak{P})^{-1})}.$$

Generátory grupy tříd ideálů Cl_K

Grupa Cl_K je generována třídami obsahujícími prvoideály $\mathfrak{P}$, jejichž norma

$$N(\mathfrak{P}) \leq (\tfrac{4}{\pi})^t \frac{(s+2t)!}{(s+2t)^{s+2t}} \sqrt{|D_K|}.$$

Je třeba najít relace mezi třídami obsahujícími tyto prvoideály, tj. jejich součiny, které jsou rovny hlavnímu ideálu. Přitom dokázat, že daný ideál je hlavní, je možné nalezením jeho generátoru. Ale dokázat, že daný ideál hlavní není, znamená dokázat, že jistá diofantická rovnice nemá řešení, což může být velmi obtížné (nemáme-li štěstí, že vede na nějakou kongruenci, která nemá řešení).

Využití odhadu $h_K R_K$ pro určení Cl_K a fundamentálních jednotek

Za bázi faktorizace se vezme množina prvoideálů dělících prvočísla $p < L$, hledají se relace mezi nimi tvaru „součin několika z nich je hlavní ideál, přitom generátor α tohoto hlavního ideálu je nalezen“. Tyto relace se uchovávají jako vektory, jejichž složky jsou celá čísla udávající exponenty tohoto součinu a v posledních $s + t$ složkách jsou komplexní logaritmy

$$(\log \sigma_1(\alpha), \ldots, \log \sigma_{s+t}(\alpha)).$$

Z nich se Gaussovou eliminací odvodí relace, které určí vztahy mezi generátory grupy Cl_K, a také vektory mající jen nuly ve složkách udávajících exponenty, které odpovídají jednotkám.
Je nutné kontrolovat, zda už máme nalezeny generátory grupy jednotek a všechny relace mezi generátory Cl_K.
Určíme počet prvků $\tilde{h}_K$ nalezené faktorgrupy a spočítáme regulátor $\tilde{R}_K$ generátorů dosud nalezené grupy jednotek a zjistíme, je-li součin $\tilde{h}_K \tilde{R}_K$ přibližně roven nalezenému odhadu $h_K R_K$ (chybí-li jednotky nebo relace, jde o celočíselný násobek $h_K R_K$).

Praktická využití faktu, že rozklad daného velkého přirozeného čísla na prvočinitele je obtížný

RSA (Rivest-Shamir-Adleman, 1977) - nejšířeji užívaný asymetrický kryptosystém založený na obtížnosti rozkladu čísla získaného jako součin dvou velkých prvočísel.

Většina kryptosystémů užívajících eliptické křivky je založena na tzv. problému diskrétního logaritmu (Koblitz, Miller, 1985).

KMOV (Koyama-Maurer-Okamoto-Vanstone, 1991) - první kryptosystém užívající eliptické křivky založený na obtížnosti rozkladu čísla získaného jako součin dvou velkých prvočísel.

Existují další podobné kryptosystémy; ukážeme si kryptosystém, který navrhli Hamad Alshehhi a Abderrahmane Nitaj (2021).

RSA

Generování klíčů: Je nutné zvolit dvě velká prvočísla p, q (přibližně stejně velká, např. $p < q < 2p$, ale s velkým rozdílem $q - p$), $n = pq$, λ je nejmenší společný násobek čísel $p-1$ a $q-1$ (je však možná i volba $\lambda = \varphi(n) = (p-1)(q-1)$).

Dále je nutné zvolit $e \in \mathbb{Z}$, $e > 1$, $(e, \lambda) = 1$, $(e-1, \lambda) = 1$ (doporučuje se $e > 2^{16}$) a spočítat $f \in \mathbb{Z}$, $f > 0$, $ef \equiv 1 \pmod{\lambda}$.

Veřejný klíč: n, e.

Tajný klíč: f (také p, q, pomocí nichž lze f snadno spočítat).

Šifrování: Zpráva je $m \in \mathbb{Z}$, $1 < m < n$. Odesílající použije veřejný klíč a odešle zbytek po dělení čísla m^e číslem n, tj. odešle $x \in \mathbb{Z}$, $0 < x < n$, $x \equiv m^e \pmod{n}$.

Dešifrování: Příjemce použije tajný klíč, zpráva m je zbytek po dělení čísla x^f číslem n, neboť $m \equiv x^f \pmod{n}$. Protože příjemce zná prvočísla p, q, může výpočet zrychlit tím, že postupně najde zbytky po dělení čísla x^f čísly p a q a pak m určí pomocí Čínské zbytkové věty.

Okruh $\mathbb{Z}[i]$

$\mathbb{Z}[i] = \{a + bi; a, b \in \mathbb{Z}\}$ je okruh s jednoznačným rozkladem (dokonce eukleidovský vzhledem k normě $N(a + bi) = a^2 + b^2$).
Grupa jednotek $\mathbb{Z}[i]^\times = \{1, i, -1, -i\}$.
Libovolný ideál je hlavní, nenulové prvoideály jsou generovány ireducibilními prvky. Každý ireducibilní prvek se vyskytne v rozkladu právě jednoho prvočísla.
Prvočíslo $2 = -i(1 + i)^2$, $N(1 + i) = 2$.
Prvočísla $q \equiv 3 \pmod 4$ jsou ireducibilní prvky, $N(q) = q^2$.
Prvočísla $p \equiv 1 \pmod 4$ se rozkládají na součin dvou nesoudělných ireducibilních prvků: $p = \pi\overline{\pi}$, $N(\pi) = N(\overline{\pi}) = p$.
Ireducibilní prvek λ se nazývá primární, jestliže $\lambda \equiv 1 \pmod{2+2i}$.
Pro každý ireducibilní prvek $\lambda \nmid 2$ existuje jediný asociovaný prvek, který je primární.
Pro libovolný ireducibilní prvek $\lambda \nmid 2$ a libovolné $\alpha \in \mathbb{Z}[i]$, $\lambda \nmid \alpha$ definujme čtvrtý mocninný symbol $(\frac{\alpha}{\lambda})_4$ čísla α vzhledem k λ podmínkou

$$(\tfrac{\alpha}{\lambda})_4 \in \{1, i, -1, -i\}, \qquad (\tfrac{\alpha}{\lambda})_4 \equiv \alpha^{(N(\lambda)-1)/4} \pmod \lambda.$$

Zákon bikvadratické reciprocity v okruhu $\mathbb{Z}[i]$

Ireducibilní prvek λ se nazývá primární, jestliže $\lambda \equiv 1 \pmod{2+2i}$.
Pro libovolný ireducibilní prvek $\lambda \nmid 2$ a libovolné $\alpha \in \mathbb{Z}[i]$, $\lambda \nmid \alpha$ definujeme čtvrtý mocninný symbol $(\frac{\alpha}{\lambda})_4$ čísla α vzhledem k λ podmínkou $(\frac{\alpha}{\lambda})_4 \in \{1, i, -1, -i\}$, $(\frac{\alpha}{\lambda})_4 \equiv \alpha^{(N(\lambda)-1)/4} \pmod{\lambda}$.

Existence a jednoznačnost mocninného symbolu $(\frac{\alpha}{\lambda})_4$ plyne z toho, že $\mathbb{Z}[i]/(\lambda)$ je těleso mající $N(\lambda)$ prvků, v němž polynom $x^4 - 1$ má čtyři různé kořeny (třídy obsahující čísla $1, i, -1, -i$). Z $\lambda \nmid \alpha$ plyne $\alpha^{N(\lambda)-1} \equiv 1 \pmod{\lambda}$, a tedy $\alpha^{(N(\lambda)-1)/4}$ je jeden z kořenů.

Věta 1. *Nechť $\lambda \in \mathbb{Z}[i]$ je ireducibilní, $\lambda \nmid 2$, $\alpha, \beta \in \mathbb{Z}[i]$, $\lambda \nmid \alpha\beta$. Pak*

- $x^4 \equiv \alpha \pmod{\lambda}$ *má řešení v* $\mathbb{Z}[i]$ $\iff$ $(\frac{\alpha}{\lambda})_4 = 1$,
- $(\frac{\alpha\beta}{\lambda})_4 = (\frac{\alpha}{\lambda})_4 (\frac{\beta}{\lambda})_4$,
- $\alpha \equiv \beta \pmod{\lambda}$ $\implies$ $(\frac{\alpha}{\lambda})_4 = (\frac{\beta}{\lambda})_4$.

Věta 2. *Jestliže π a λ jsou nesoudělné primární ireducibilní prvky, pak*

$$(\tfrac{\pi}{\lambda})_4 = (\tfrac{\lambda}{\pi})_4 \cdot (-1)^{(N(\pi)-1)(N(\lambda)-1)/16}.$$

Počet bodů na eliptické křivce $y^2 = x^3 - ax$ nad $\mathbb{Z}_p$

Věta 3. *Nechť p je prvočíslo, $a \in \mathbb{Z}$, přičemž $p \neq 2$, $p \nmid a$. Nechť N je počet bodů na eliptické křivce $y^2 = x^3 - ax$ nad $\mathbb{Z}_p$.*

- *Je-li $p \equiv 3 \pmod 4$, pak $N = p + 1$.*
- *Je-li $p \equiv 1 \pmod 4$ a $p = \pi\overline{\pi}$ je rozklad čísla p na součin dvou primárních ireducibilních prvků v $\mathbb{Z}[i]$, pak*

$$N = p + 1 - \overline{\left(\frac{a}{\pi}\right)_4} \cdot \pi - \left(\frac{a}{\pi}\right)_4 \cdot \overline{\pi}.$$

Dokažme větu jen pro lehčí první případ: je-li $p \equiv 3 \pmod 4$, pak Legendreův symbol $\left(\frac{-1}{p}\right) = -1$. Na eliptické křivce leží nevlastní bod O a bod $[0, 0]$. Pro každé $u = 1, \ldots, \frac{p-1}{2}$ spočítejme počet bodů, jejichž x-ová souřadnice je $\pm u$. Označme $v = u^3 - au$.
Je-li $v = 0$, máme dva body $[u, 0]$, $[-u, 0]$.
Je-li $v \neq 0$, je právě jedno z čísel v, $-v$ kvadratický zbytek modulo p, a tedy z kongruencí $y^2 \equiv v \pmod p$ a $y^2 \equiv -v \pmod p$ má jedna dvě řešení a druhá žádné. Proto opět dostáváme dva body, jejichž x-ová souřadnice je $\pm u$.

Příklad: eliptická křivka $y^2 = x^3 - 2x$ nad $\mathbb{Z}_{101}$

Rozložme $p = 101$ v $\mathbb{Z}[i]$.
Platí $p = 101 = (10 + i)(10 - i) = (1 + 10i)(1 - 10i)$. Označme $\pi = -1 + 10i$, pak π je primární. Víme, že

$$(\tfrac{2}{\pi})_4 \in \{1, i, -1, -i\}, \qquad (\tfrac{2}{\pi})_4 \equiv 2^{(N(\pi)-1)/4} = 2^{25} \pmod{\pi}.$$

Protože $2^{25} \equiv 10 \pmod{101}$, je

$$(\tfrac{2}{\pi})_4 \equiv 10 \equiv 100i \equiv -i \pmod{\pi},$$

a tedy $(\frac{2}{\pi})_4 = -i$. Podle věty 3 pro počet N bodů na eliptické křivce $y^2 = x^3 - 2x$ nad $\mathbb{Z}_{101}$ platí

$$N = p + 1 - \overline{(\tfrac{2}{\pi})_4} \cdot \pi - (\tfrac{2}{\pi})_4 \cdot \overline{\pi} = 102 - i \cdot \pi + i \cdot \overline{\pi} = 122.$$

Okruh $\mathbb{Z}[\omega]$, kde $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$

$\mathbb{Z}[\omega] = \{a + b\omega; a, b \in \mathbb{Z}\}$ je okruh s jednoznačným rozkladem (dokonce eukleidovský vzhledem k $N(a + b\omega) = a^2 - ab + b^2$).
Grupa jednotek $\mathbb{Z}[i]^\times = \{1, \omega, \omega^2, -1, -\omega, -\omega^2\}$.
Libovolný ideál je hlavní, nenulové prvoideály jsou generovány ireducibilními prvky. Každý ireducibilní prvek se vyskytne v rozkladu právě jednoho prvočísla.
Prvočíslo $3 = -\omega^2(1 - \omega)^2$, $N(1 - \omega) = 3$.
Prvočísla $q \equiv 2 \pmod 3$ jsou ireducibilní prvky, $N(q) = q^2$.
Prvočísla $p \equiv 1 \pmod 3$ se rozkládají na součin dvou nesoudělných ireducibilních prvků: $p = \pi\overline{\pi}$, $N(\pi) = N(\overline{\pi}) = p$.
Ireducibilní prvek λ se nazývá primární, jestliže $\lambda \equiv 2 \pmod 3$.
Pro každý ireducibilní prvek $\lambda \nmid 3$ existuje jediný asociovaný prvek, který je primární.
Pro libovolný ireducibilní prvek $\lambda \nmid 6$ a libovolné $\alpha \in \mathbb{Z}[\omega]$, $\lambda \nmid \alpha$ definujme šestý mocninný symbol $(\frac{\alpha}{\lambda})_6$ čísla α vzhledem k λ podmínkou

$$(\tfrac{\alpha}{\lambda})_6 \in \{\pm 1, \pm\omega, \pm\omega^2\}, \qquad (\tfrac{\alpha}{\lambda})_6 \equiv \alpha^{(N(\lambda)-1)/6} \pmod \lambda.$$

Zákon kubické reciprocity v okruhu $\mathbb{Z}[\omega]$

Ireducibilní prvek λ se nazývá primární, jestliže $\lambda \equiv 2 \pmod 3$.
Pro libovolný ireducibilní prvek $\lambda \nmid 6$ a libovolné $\alpha \in \mathbb{Z}[\omega]$, $\lambda \nmid \alpha$ definujeme šestý mocninný symbol $(\frac{\alpha}{\lambda})_6$ čísla α vzhledem k λ podmínkou $(\frac{\alpha}{\lambda})_6 \in \{\pm 1, \pm\omega, \pm\omega^2\}$, $(\frac{\alpha}{\lambda})_6 \equiv \alpha^{(N(\lambda)-1)/6} \pmod \lambda$.

Existence a jednoznačnost mocninného symbolu $(\frac{\alpha}{\lambda})_6$ plyne z toho, že těleso $\mathbb{Z}[\omega]/(\lambda)$ má $N(\lambda)$ prvků a polynom $x^6 - 1$ v něm má šest různých kořenů (třídy obsahující čísla $\pm 1, \pm\omega, \pm\omega^2$). Z $\lambda \nmid \alpha$ plyne $\alpha^{N(\lambda)-1} \equiv 1 \pmod \lambda$, a tedy $\alpha^{(N(\lambda)-1)/6}$ je jeden z kořenů.

Věta 4. *Nechť $\lambda \in \mathbb{Z}[\omega]$ je ireducibilní, $\lambda \nmid 3$, $\alpha, \beta \in \mathbb{Z}[\omega]$, $\lambda \nmid \alpha\beta$. Pak*

- $x^6 \equiv \alpha \pmod \lambda$ *má řešení v* $\mathbb{Z}[\omega]$ $\iff$ $(\frac{\alpha}{\lambda})_6 = 1$,
- $x^3 \equiv \alpha \pmod \lambda$ *má řešení v* $\mathbb{Z}[\omega]$ $\iff$ $(\frac{\alpha}{\lambda})_6 = \pm 1$,
- $(\frac{\alpha\beta}{\lambda})_6 = (\frac{\alpha}{\lambda})_6 (\frac{\beta}{\lambda})_6$,
- $\alpha \equiv \beta \pmod \lambda$ $\implies$ $(\frac{\alpha}{\lambda})_6 = (\frac{\beta}{\lambda})_6$.

Věta 5. *Jestliže π a λ jsou primární ireducibilní prvky takové, že $N(\pi) \neq N(\lambda)$, pak $(\frac{\pi}{\lambda})_6 = \pm(\frac{\lambda}{\pi})_6$.*

Počet bodů na eliptické křivce $y^2 = x^3 + b$ nad $\mathbb{Z}_p$

Věta 6. *Nechť p je prvočíslo, $b \in \mathbb{Z}$, přičemž $p > 3$, $p \nmid b$. Nechť N je počet bodů na eliptické křivce $y^2 = x^3 + b$ nad $\mathbb{Z}_p$.*

- *Je-li $p \equiv 2 \pmod 3$, pak $N = p + 1$.*
- *Je-li $p \equiv 1 \pmod 3$ a $p = \pi\overline{\pi}$ je rozklad čísla p na součin dvou primárních ireducibilních prvků v $\mathbb{Z}[\omega]$, pak*

$$N = p + 1 + \overline{(\tfrac{4b}{\pi})_6} \cdot \pi + (\tfrac{4b}{\pi})_6 \cdot \overline{\pi}.$$

Dokažme větu jen pro lehčí první případ: je-li $p \equiv 2 \pmod 3$, pak zobrazení $f : \mathbb{Z}_p \to \mathbb{Z}_p$ určené předpisem $f(t) = t^3$ je bijekce, neboť na nulu se zobrazí jen nula a zúžení f na $\mathbb{Z}_p^\times$ je homorfismus grup s triviálním jádrem. Proto pro každé $y \in \mathbb{Z}_p$ existuje jediné $x \in \mathbb{Z}_p$ splňující $f(x) = y^2 - b$. Pro každé $y \in \mathbb{Z}_p$ tedy existuje jediné $x \in \mathbb{Z}_p$ tak, že $[x, y]$ leží na eliptické křivce. Kromě nevlastního bodu O existuje na eliptické křivce tedy právě p bodů.

Příklad: eliptická křivka $y^2 = x^3 + 2$ nad $\mathbb{Z}_{103}$

Rozložme $p = 103$ v $\mathbb{Z}[\omega]$.
Hledáme tedy $u, v \in \mathbb{Z}$, aby $u^2 - uv + v^2 = p$.
Pak $4p = (2u - v)^2 + 3v^2$, lze tedy postupovat dosazováním malých přirozených čísel za v. V našem případě $4p = 412 = 20^2 + 3 \cdot 2^2$. Proto $11 + 2\omega$ je ireducibilní prvek dělící p, není však primární. Je třeba jej vynásobit vhodnou mocninou ω, abychom dostali koeficient u ω dělitelný třemi. Platí $(11 + 2\omega)\omega = 11\omega + 2(-1 - \omega) = -2 + 9\omega$, což také není primární, ale vynásobením -1 dostaneme hledaný primární ireducibilní prvek $\pi = 2 - 9\omega$.

Potřebujeme spočítat $(\frac{4b}{\pi})_6$, v tomto případě je $4b = 8$ třetí mocnina, a tak můžeme použít Legendreův symbol $8^{(p-1)/6} = 2^{(p-1)/2} \equiv (\frac{2}{p}) \pmod{p}$. Je tedy $(\frac{8}{\pi})_6 = (\frac{2}{103}) = 1$.

Podle věty 6 pro počet N bodů na eliptické křivce $y^2 = x^3 + 2$ nad $\mathbb{Z}_{103}$ platí

$$N = p+1+\overline{(\tfrac{8}{\pi})_6}\cdot\pi+(\tfrac{8}{\pi})_6\cdot\overline{\pi} = 104+\pi+\overline{\pi} = 104+4-9\omega-9\omega^2 = 117.$$

KMOV – základní myšlenka

Nechť $n = pq$ pro velká prvočísla $p \neq q$, kde $p \equiv q \equiv 2 \pmod 3$. Libovolnou dvojici $A = [u, v]$, kde $u, v \in \mathbb{Z}$ jsou taková, že $b = v^2 - u^3$ je nesoudělné s n, lze interpretovat jako bod ležící současně na dvou eliptických křivkách daných rovnicí $y^2 = x^3 + b$, totiž na $\mathcal{E}_p$ nad $\mathbb{Z}_p$ a na $\mathcal{E}_q$ nad $\mathbb{Z}_q$. Podle věty 6 platí $|\mathcal{E}_p| = p + 1$ a $|\mathcal{E}_q| = q + 1$.

I v případě, že neznáme p a q, lze pomocí výpočtů prováděných modulo n takové dvojice reprezentující body na obou křivkách sčítat, problémy vzniknou jen v případě, že výsledný bod je neutrální prvek na právě jedné z těchto dvou křivek. Avšak jsou-li prvočísla p, q opravdu velká, nalezení takového bodu je krajně nepravděpodobné (víme, že znalost takového bodu znamená znalost rozkladu n na součin prvočísel).

Nechť λ je společný násobek čísel $p + 1$ a $q + 1$. Pak pro každé přirozené číslo $t \equiv 1 \pmod \lambda$ platí $t \cdot A = A$.

KMOV – použití

Generování klíčů: Je nutné zvolit velká prvočísla $p \equiv q \equiv 2 \pmod 3$ (přibližně stejně velká, např. $p < q < 2p$, ale s velkým rozdílem $q - p$), $n = pq$, λ je (nejmenší) společný násobek čísel $p + 1$ a $q + 1$ (je možné vzít $\lambda = (p + 1)(q + 1)$). Dále je nutné zvolit $e \in \mathbb{Z}$, $e > 1$, $(e, \lambda) = 1$, $(e - 1, \lambda) = 1$ a spočítat $f \in \mathbb{Z}$, $f > 0$, $ef \equiv 1 \pmod \lambda$.

Veřejný klíč: n, e.

Tajný klíč: f (také p, q, pomocí nichž lze f snadno spočítat).

Šifrování: Zpráva je dvojice $[m_1, m_2]$, kde $m_1, m_2 \in \mathbb{Z}$, $1 < m_1 < n$, $1 < m_2 < n$. Odesílající interpretuje dvojici $A = [m_1, m_2]$ jako bod ležící současně na eliptických křivkách $\mathcal{E}_p$ nad $\mathbb{Z}_p$ a na $\mathcal{E}_q$ nad $\mathbb{Z}_q$ daných rovnicí $y^2 = x^3 + b$, kde $b = m_2^2 - m_1^3$ (případ b soudělného s n je nepravděpodobný). Použije veřejný klíč a spočítá bod $B = e \cdot A$, který pak odešle (výpočty provádí modulo n).

Dešifrování: Příjemce použije tajný klíč a spočítá zprávu $A = f \cdot B$ (výpočty může provádět modulo n, anebo postup zrychlit tak, že počítá postupně modulo p a modulo q, pak užije Čínskou zbytkovou větu).

Kryptosystém Alshehhi-Nitaj – základní myšlenka

Nechť pro přirozená čísla r, s je $p = (4r+3)^2 + (4s+2)^2$ prvočíslo. Pak $p \equiv 5 \pmod 8$ a p se v $\mathbb{Z}[i]$ rozkládá na součin $p = \pi\overline{\pi}$, kde $\pi = (4r+3) + (4s+2)i$ je primární ireducibilní prvek.

Označme $u = 4r+3$, $v = 4s+2$, tedy $\pi = u + iv$, najdeme $c \in \mathbb{Z}$, aby $cv \equiv u \pmod p$. Protože $c^2v^2 \equiv u^2 \equiv -v^2 \pmod p$, je $c^2 \equiv -1 \pmod p$. Zvolme libovolně $a \in \mathbb{Z}$, $p \nmid a$. Podle věty 3 pro počet N bodů na eliptické křivce $y^2 = x^3 - ax$ platí

$$N = p + 1 - \overline{\left(\tfrac{a}{\pi}\right)_4} \cdot \pi - \left(\tfrac{a}{\pi}\right)_4 \cdot \overline{\pi}.$$

Víme, že $\left(\frac{a}{\pi}\right)_4 \in \{1, i, -1, -i\}$, $\left(\frac{a}{\pi}\right)_4 \equiv a^{(p-1)/4} \pmod \pi$. Rozlišme

- $a^{(p-1)/4} \equiv 1 \pmod p$, pak $\left(\frac{a}{\pi}\right)_4 = 1$ a $N = p + 1 - 2u$.
- $a^{(p-1)/4} \equiv -1 \pmod p$, pak $\left(\frac{a}{\pi}\right)_4 = -1$ a $N = p + 1 + 2u$.
- $a^{(p-1)/4} \equiv c \pmod p$, pak $\left(\frac{a}{\pi}\right)_4 \equiv c \pmod \pi$, a tedy $\overline{\left(\frac{a}{\pi}\right)_4} \cdot \pi + \left(\frac{a}{\pi}\right)_4 \cdot \overline{\pi} \equiv c(u - iv) \equiv 2cu \equiv 2c^2v \equiv -2v \pmod \pi$. Protože $\overline{\left(\frac{a}{\pi}\right)_4} \cdot \pi + \left(\frac{a}{\pi}\right)_4 \cdot \overline{\pi} \in \mathbb{Z}$, je $\overline{\left(\frac{a}{\pi}\right)_4} \cdot \pi + \left(\frac{a}{\pi}\right)_4 \cdot \overline{\pi} \equiv -2v \pmod p$. Platí $|\pi| = |\overline{\pi}| = \sqrt{p} < \frac{p}{4}$, $|2v| < 2\sqrt{p} < \frac{p}{2}$, tedy $\overline{\left(\frac{a}{\pi}\right)_4} \cdot \pi + \left(\frac{a}{\pi}\right)_4 \cdot \overline{\pi} = -2v$, a proto $N = p + 1 + 2v$.
- $a^{(p-1)/4} \equiv -c \pmod p$, pak analogicky $N = p + 1 - 2v$.

Kryptosystém Alshehhi-Nitaj – použití

Generování klíčů: Je nutné zvolit velká přirozená čísla r_1, s_1, r_2, s_2, aby pro $u_1 = 4r_1 + 3$, $v_1 = 4s_1 + 2$, $u_2 = 4r_2 + 3$, $v_2 = 4s_2 + 2$ byla $p_1 = u_1^2 + v_1^2$ a $p_2 = u_2^2 + v_2^2$ různá prvočísla. Pak $n = p_1 p_2$. Dále je nutné zvolit $e \in \mathbb{Z}$, $e > 1$, tak, aby čísla e i $e - 1$ byla nesoudělná s každým z čísel $(p_i + 1)^2 - 4u_i^2$, $(p_i + 1)^2 - 4v_i^2$, $i = 1, 2$.

Veřejný klíč: n, e.

Tajný klíč: u_1, v_1, u_2, v_2, p_1, p_2.

Šifrování: Zpráva je číslo $m \in \mathbb{Z}$, $0 < m < n$. Odesílající zvolí náhodné $r \in \mathbb{Z}$, $0 < r < n$ (je možné toto r použít k podpisu zprávy), může ověřit, že $(m, n) = 1$, $(r, n) = 1$, $(m^2 - r^3, n) = 1$, což skoro jistě platí, jinak by „uhádl“ rozklad n (s výjimkou případu $n \mid m^2 - r^3$) a spočítá $a \in \mathbb{Z}$ splňující $ra \equiv m^2 - r^3 \pmod{n}$. Platí $(a, n) = 1$ a lze interpretovat dvojici $A = [r, m]$ jako bod ležící současně na eliptických křivkách $\mathcal{E}_{p_1}$ nad $\mathbb{Z}_{p_1}$ a na $\mathcal{E}_{p_2}$ nad $\mathbb{Z}_{p_2}$ daných rovnicí $y^2 = x^3 + ax$. Odesílající pak spočítá bod $B = e \cdot A$, který odešle (výpočty provádí modulo n).

Kryptosystém Alshehhi-Nitaj – dešifrování

Příjemce použije tajný klíč a najde zbytky po dělení obou souřadnic bodu B prvočísly p_1 a p_2, tím získá bod $B_1 = [x_1, y_1]$ na $\mathcal{E}_{p_1}$ a bod $B_2 = [x_2, y_2]$ na $\mathcal{E}_{p_2}$. Díky podmínkám při volbě e je násobení číslem e automorfismem na obou křivkách, a proto body B_1, B_2 nemají řád 2, a tedy obě souřadnice těchto bodů jsou nenulové. Pro každé $i = 1, 2$ určí a_i z kongruence $a_i x_i \equiv y_i^2 - x_i^3 \pmod{p_i}$. Toto $a_i \equiv a \not\equiv 0 \pmod{p_i}$. Spočítá $a_i^{(p_i-1)/4}$ modulo p_i, čímž získá počet N_i bodů na eliptické křivce $\mathcal{E}_{p_i}$, neboť

- Je-li $a_i^{(p_i-1)/4} \equiv \pm 1 \pmod{p_i}$, pak $N_i = p_i + 1 \mp 2u_i$.
- Je-li $v_i \cdot a_i^{(p_i-1)/4} \equiv \pm u_i \pmod{p_i}$, pak $N_i = p_i + 1 \pm 2v_i$.

Najde f_i, aby $e \cdot f_i \equiv 1 \pmod{N_i}$ a spočítá bod $C_i = f_i \cdot B_i$ na $\mathcal{E}_{p_i}$. Pak užije Čínskou zbytkovou větu, aby našel bod C, jehož souřadnice modulo p_1 dávají C_1 a modulo p_2 dávají C_2. Platí $C = A$ (pro získání zprávy m stačí spočítat y-ovou souřadnici, pro případné ověření podpisu je nutné určit i x-ovou).

Kryptosystém Alshehhi-Nitaj – možnost podpisu

Možností, jak podepsat zprávu, je hodně, probereme jednu z nich.
Obě strany se předem dohodnou na metodě, jak vhodně odvodit číslo $z \in \mathbb{Z}$ ze znalosti n, aby $z^2 > n > 2z$, například $z = [100\sqrt{n}]$.

Předpokládejme, že odesílatel si vytvořil veřejný a tajný klíč pro RSA, jehož modul $\tilde{n} = \tilde{p} \cdot \tilde{q}$ splňuje $2z < \tilde{n} < n$. Tajný klíč $\tilde{f}$, $\tilde{p}$, $\tilde{q}$ zná jen odesílatel, veřejný klíč $\tilde{n}$, $\tilde{e}$ zná i příjemce (a je si jist, že skutečně patří odesílateli, tj. že klíč není podvržen).

Odesílatel vyjádří zprávu m v z-adické poziční soustavě jako $m = tz + s$ a užitím svého tajného klíče spočítá zbytek w po dělení čísla $(t + s + 1)^{\tilde{f}}$ číslem $\tilde{n}$. Při šifrování volí náhodně celé číslo $g \geq 0$ tak, aby $r = g\tilde{n} + w < n$. Pak $r \equiv (t + s + 1)^{\tilde{f}} \pmod{\tilde{n}}$.

Příjemce tím, že spočítá bod C, najde čísla r, m.
Určí pak z, t, s stejným postupem jako odesílatel a zjistí, zda $r^{\tilde{e}} \equiv t + s + 1 \pmod{\tilde{n}}$.
Pokud ano, uvěří, že zpráva pochází opravdu od odesílatele, neboť jen on znal číslo $\tilde{f}$ (platí $1 < t + s + 1 < \tilde{n}$).

Diskrétní logaritmus

Nechť $(G, \cdot)$ je konečná grupa, $g \in G$ prvek řádu n. Pak pro každé $h \in \langle g \rangle$ existuje $c \in \mathbb{Z}$ tak, že $h = g^c$. Toto celé číslo c je určeno jednoznačně modulo n a dotyčná zbytková třída $[c]_n$ se nazývá diskrétní logaritmus prvku h o základu g, píšeme

$$[c]_n = \log_g h$$

(někdy se diskrétním logaritmem rozumí celé číslo c, pak je nutno mít na paměti, že je určeno jen modulo n).

Přestože jsou všechny n-prvkové cyklické grupy izomorfní, v některých grupách je úloha nalezení diskrétního logaritmu snadná, v jiných obtížná. Záleží totiž na tom, jak jsou označeny jednotlivé prvky dané grupy.

Příklad. V grupě $(\mathbb{Z}_m, +)$ je $g = [a]_m$, $h = [b]_m$. Při hledání diskrétního logaritmu řešíme kongruenci $ax \equiv b \pmod{m}$, pomocí Eukleidova algoritmu nalezneme Bezoutovu rovnost, což dá hledaný diskrétní logaritmus (jde o algoritmus kvadratické časové náročnosti).

Diskrétní logaritmus v grupě $(\mathbb{Z}_p^\times, \cdot)$ pro prvočíslo p

Grupa $(\mathbb{Z}_p^\times, \cdot)$ je cyklická; označme g primitivní kořen modulo p. Ve starší literatuře bývají definována celá čísla g_i podmínkou

$$g_i \equiv g^i \pmod{p}, \qquad 0 < g_i < p,$$

pak $\log_{[g]_p}[g_i]_p = [i]_{p-1}$, proto se dříve diskrétnímu logaritmu v této grupě říkalo index. Nejrychlejší známý algoritmus na počítání diskrétních logaritmů v této grupě je proto nazýván „index calculus“. Má subexponenciální časovou náročnost.

Tento algoritmus si popíšeme podrobněji, některé jeho části jsou podobné metodě kvadratického síta. V roce 2001 A. Joux a R. Lecier ukázali, že tento algoritmus lze užít k počítání diskrétních logaritmů v grupě $(\mathbb{Z}_p^\times, \cdot)$, kde p je 120-ciferné prvočíslo (v bázi faktorizace měli milión nejmenších prvočísel).

Analogický algoritmus je možné použít i pro výpočet diskrétního logaritmu v multiplikativní grupě libovolného konečného tělesa.

Index calculus

Nechť $p_1, \ldots, p_r$ je báze faktorizace složená z „malých“ prvočísel. Hledáme kongruence tvaru

$$g^{a_i} \equiv (-1)^{e_{i,0}} \cdot \prod_{j=1}^{r} p_j^{e_{ij}} \pmod{p},$$

které znamenají (pro jednoduchost pišme čísla místo zbytkových tříd)

$$a_i \equiv e_{i,0} \cdot \tfrac{p-1}{2} + \sum_{j=1}^{r} e_{ij} \cdot \log_g p_j \pmod{p-1}.$$

Máme-li takových kongruencí dost, určíme z nich $\log_g p_j$ pro každé $j = 1, \ldots, r$. Pak stačí jediná kongruence tvaru

$$h \cdot g^b \equiv (-1)^{f_0} \cdot \prod_{j=1}^{r} p_j^{f_j} \pmod{p},$$

odkud $$\log_g h \equiv -b + f_0 \cdot \tfrac{p-1}{2} + \sum_{j=1}^{r} f_j \cdot \log_g p_j \pmod{p-1}.$$

Algoritmy pro hledání diskrétního logaritmu v obecné grupě

Předchozí algoritmus „index calculus“ využíval toho, že každou zbytkovou třídu reprezentuje celé číslo, jehož absolutní hodnotu můžeme jednoznačně rozložit na součin prvočísel.

Nyní vysvětlíme následující algoritmy, které je možné použít na výpočet $\log_g h$ v libovolné konečné grupě:

- Shanksova metoda „Baby steps, giant steps“,
- Pollardova ρ-metoda,
- Pollardova λ-metoda.

Všechny tři metody mají exponenciální časovou náročnost $O(\sqrt{n})$.

Shanksova metoda je deterministická, vyžaduje však uložit $O(\sqrt{n})$ informace do paměti. Není nutné znát řád n základu g diskrétního logaritmu, postačí horní odhad tohoto řádu. Je schopna zjistit, že $h \notin \langle g \rangle$.

Pollardovy metody jsou nedeterministické, jde tedy o odhadovanou časovou náročnost. Nejsou náročné na paměť, vyžadují však, aby $h \in \langle g \rangle$ a aby řád n základu g diskrétního logaritmu byl znám.

Shanksova metoda „Baby steps, giant steps“

Předpokládejme, že řád n prvku g v grupě $(G, \cdot)$ splňuje $n \leq m^2$ pro známé celé číslo $m > 0$. Pro dané $h \in G$ chceme zjistit, zda $h \in \langle g \rangle$, a pokud ano, chceme najít $c \in \mathbb{Z}$, pro které $h = g^c$. Není nutné znát přesnou hodnotu n, pokud nám stačí najít jen jedno řešení c a ne všechna.

Každé $c = 0, 1, \ldots, n-1$ můžeme psát ve tvaru $c = um + v$, kde $u, v \in \{0, 1, \ldots, m-1\}$. Je-li tedy $h = g^c$, pak $h \cdot g^{-um} = g^v$.

Nejprve spočítáme $g^0, g, g^2, \ldots, g^m$ (postupným násobením prvkem g) a uložíme $g^0, g, g^2, \ldots, g^{m-1}$ tak, abychom mohli v tomto seznamu rychle vyhledávat.

Pak postupně hledáme, zda v našem seznamu je h, $h \cdot g^{-m}$, $h \cdot g^{-2m}$, …, $h \cdot g^{-(m-1)m}$ (postupným násobením inverzním prvkem g^{-m} k již spočítanému prvku g^m).

Jakmile v seznamu objevíme první z nich, můžeme skončit, neboť z rovnosti $h \cdot g^{-um} = g^v$ plyne $h = g^{um+v}$.

Úprava Shanksovy metody pro eliptické křivky

Je-li dána eliptická křivka E nad konečným tělesem $\mathbb{F}_q$, pak z Hasseho věty plyne $|E| \leq q + 1 + 2\sqrt{q}$.

Proto pro výpočet diskrétního logaritmu $\log_P Q$ o základu $P \in E$ lze volit přirozené číslo m s vlastností $q + 1 + 2\sqrt{q} \leq m^2$.

Protože body a jejich inverze na eliptické křivce mají stejnou x-ovou souřadnici a opačnou y-ovou souřadnici, stačí v seznamu mít jen body $O, P, 2P, \ldots, tP$, kde $t = [\frac{m}{2}]$, a testovat, zda $Q - umP = \pm vP$.

Pak $Q = cP$ pro $c = um \pm v$. Na rozdíl od obvyklého $c \geq 0$ nyní platí jen $c \geq -t$, ale to ve většině aplikací nevadí (je-li dokonce řád bodu P znám, je to nepodstatné).

Pollardova ρ-metoda výpočtu $\log_g h$ pro $h \in \langle g \rangle$

Tuto metodu jsme už poznali při hledání netriviálního dělitele. Potřebujeme znát řád n základu g diskrétního logaritmu a vědět, že $h \in \langle g \rangle$. Označme $G = \langle g \rangle$.
Sestrojíme zobrazení $f : G \to G$, pro které by mohlo platit, že se chová jako náhodné, abychom mohli odhadnout, že rekurentní posloupnost určená předpisem $x_i = f(x_{i-1})$ má pro libovolné počáteční x_0 předperiodu i periodu délky $O(\sqrt{n})$.
Vhodnou funkci můžeme definovat například takto: grupu G rozložíme na několik tříd $C_1, \ldots, C_t$. Zvolíme náhodná čísla $a_0, a_1, \ldots, a_t, b_0, b_1, \ldots, b_t \in \{1, 2, \ldots, n-1\}$. Položíme $y_j = g^{a_j} \cdot h^{b_j}$ a definujeme posloupnost předpisem $x_0 = y_0$,

$$x_i = f(x_{i-1}), \qquad \text{kde } f(x) = x \cdot y_j, \qquad \text{je-li } x \in C_j.$$

Pak každé vypočtené x_i je tvaru $x_i = g^{u_i} \cdot h^{v_i}$, přitom celá čísla u_i, v_i počítáme modulo n.

Pollardova ρ-metoda výpočtu $\log_g h$ pro $h \in \langle g \rangle$

$y_j = g^{a_j} \cdot h^{b_j}$, $x_0 = y_0$, $x_i = f(x_{i-1})$, $f(x) = x \cdot y_j$ pro $x \in C_j$.

Při výpočtu neuchováváme hodnoty všech už vypočtených členů posloupnosti, ale jen dvojici x_i, x_{2i} spolu s u_i, v_i, u_{2i}, v_{2i}.
Jestliže platí $x_i = x_{2i}$, což by mělo nastat po $O(\sqrt{n})$ krocích, máme rovnost $g^{u_i} \cdot h^{v_i} = g^{u_{2i}} \cdot h^{v_{2i}}$, tedy $g^{u_i - u_{2i}} = h^{v_{2i} - v_i}$.
Pro hledaný diskrétní logaritmus $\log_g h$ tedy platí

$$(v_{2i} - v_i) \cdot \log_g h \equiv u_i - u_{2i} \pmod{n}.$$

Je-li $v_{2i} - v_i$ nesoudělné s n, je touto kongruencí $\log_g h$ určen.
Je-li největší společný dělitel $d = (v_{2i} - v_i, n)$ malý, můžeme vyzkoušet všech d řešení této kongruence. Je-li d velké, můžeme začít znovu s jinými a_j, b_j (získanou informaci o hodnotě $\log_g h$ modulo $\frac{n}{d}$ uchováme, abychom ji mohli využít, pokud ani další podobná kongruence neurčí $\log_g h$ jednoznačně).

V kryptografických aplikacích však bývá n prvočíslo.

Pollardova λ-metoda výpočtu $\log_g h$ pro $h \in \langle g \rangle$

Jde o metodu počítanou paralelně na několika počítačích.

Používá funkci f definovanou stejně jako u Pollardovy ρ-metody.

Několik počítačů počítá hodnoty rekurentních posloupností daných stejnou funkcí f pro různé počáteční hodnoty x_0.

Hodnoty x_i splňující jistou zvolenou podmínku (například patří do třídy C_1) jsou hlášeny do centrálního počítače (spolu s jejich vyjádřením ve tvaru součinu mocnin prvků g a h).

Centrální počítač nahlášené hodnoty ukládá a porovnává.

Vyhodnotí, pokud obdržel stejnou hodnotu podruhé, a následně ze dvojího vyjádření této hodnoty získá stejně jako u Pollardovy ρ-metody informaci o $\log_g h$.

Metoda Pohlig-Hellman výpočtu $\log_g h$ pro $h \in \langle g \rangle$

Tato metoda vysvětluje, proč v kryptografických aplikacích diskrétního logaritmu mívá generátor g prvočíselný řád n.

Jestliže řád n generátoru g není prvočíslo a známe jeho rozklad na součin mocnin různých prvočísel $n = \prod_i q_i^{e_i}$, můžeme hledaný diskrétní logaritmus $\log_g h$ nalézt pomocí Čínské zbytkové věty poté, co pro každé i určíme jeho zbytek po dělení číslem $q_i^{e_i}$.

Nechť $k = \log_g h$ a pro prvočíslo $q \mid n$ platí $q^e \mid n$, $q^{e+1} \nmid n$; v q-adické poziční soustavě zapišme $k = k_0 + k_1 q + k_2 q^2 + \ldots$, kde $0 \leq k_i < q$. Postupně nalezneme k_i pro $i = 0, 1, \ldots, e-1$.

Označme $\tilde{g} = g^{n/q}$. Pak $k_0 = \log_{\tilde{g}} h^{n/q}$ a pro každé $i = 1, \ldots, e-1$ platí $k_i = \log_{\tilde{g}} \left(h \cdot g^{-k_0 - q k_1 - \cdots - q^{i-1} k_{i-1}}\right)^{n/q^{i+1}}$.

Přitom $\tilde{g}$ má řád q a logaritmy o základu $\tilde{g}$ můžeme nalézt Shanksovou metodou „Baby steps, giant steps“ v $O(\sqrt{q})$ krocích.

Praktická využití faktu, že výpočet diskrétního logaritmu na eliptické křivce je obtížný

Pokud na eliptické křivce nad konečným tělesem dán bod P, jehož řád n je velké prvočíslo, výpočet diskrétního logaritmu v grupě $\langle P \rangle$ bývá obtížný. Na tom jsou založeny následující kryptosystémy pro komunikaci odposlouchávatelným kanálem, při kterých je předem (veřejně) dohodnuta eliptická křivka a bod na ní:

- Diffie-Hellman – výroba společného tajemství,
- Massey-Omura – přenos tajné zprávy (je poslána třikrát: tam, zpět a znovu tam) pomocí tajných klíčů příjemce i odesílatele,
- El Gamal – přenos tajné zprávy pomocí tajného a veřejného klíče, které vytvořil příjemce zprávy.

Kryptosystém Diffie-Hellman

Obě strany se (veřejně) dohodnou na eliptické křivce nad konečným tělesem a bodu P na ní tak, aby problém diskrétního logaritmu o základu P byl obtížný (obvykle jsou křivka a bod zvoleny tak, aby řád bodu P bylo velké prvočíslo).

- Strana A zvolí své tajné přirozené číslo a, spočítá bod $P_a = aP$, který odešle straně B.
- Strana B zvolí své tajné přirozené číslo b, spočítá bod $P_b = bP$, který odešle straně A.
- Strana A použije číslo a k výpočtu bodu aP_b.
- Strana B použije číslo b k výpočtu bodu bP_a.
- Protože $aP_b = abP = bP_a$, sdílí obě strany týž tajný bod.

Problém Diffie-Hellman: Ze znalosti bodů P, aP, bP nalezni abP.

Je jasné, že výpočet diskrétního logaritmu $a = \log_P(aP)$ nebo $b = \log_P(bP)$ tento problém vyřeší. Neví se, zda existuje metoda, která by vyřešila tento problém bez výpočtu diskrétního logaritmu.

Kryptosystém Massey-Omura

Tento kryptosystém by se dal popsat následovně: Alice chce Bobovi poslat tajnou zprávu. Tak ji sepsanou dá do krabice, na kterou umístí svůj zámek, a pošle Bobovi. Ten na krabici připevní ještě svůj zámek, a odešle zpět. Alice odemkne svůj zámek a krabici zamknutou pouze zámkem Boba odešle Bobovi, aby si mohl krabici odemknout a přečíst zprávu.

Jak to implementovat matematicky?

Alice se s Bobem (veřejně) dohodnou na eliptické křivce nad konečným tělesem tak, aby problém diskrétního logaritmu byl na ní obtížný (křivka může být například zvolena tak, že její řád je velké prvočíslo nebo dvojnásobek velkého prvočísla). Dále se dohodnou, jak reprezentovat zprávu jako bod na této křivce.

Jeden způsob, jak snadno přiřadit zprávě bod na dané eliptické křivce, aby bylo možné ze znalosti tohoto bodu zprávu zpětně zrekonstruovat, si později vysvětlíme.

Kryptosystém Massey-Omura

Alice se s Bobem dohodli na eliptické křivce nad konečným tělesem i na postupu, jak libovolné zprávě přiřadit bod na této křivce.

Označme n řád dohodnuté eliptické křivky.

- Alice svou zprávu reprezentuje jako bod M na dohodnuté eliptické křivce.
- Alice zvolí své tajné přirozené číslo u nesoudělné s n, spočítá bod $M_1 = uM$, který odešle Bobovi.
- Bob zvolí své tajné přirozené číslo v nesoudělné s n, spočítá bod $M_2 = vM_1$, který odešle Alici.
- Alice najde celé číslo $\tilde{u}$, které je řešení kongruence $ux \equiv 1 \pmod{n}$, a spočítá bod $M_3 = \tilde{u}M_2$, který odešle Bobovi.
- Bob najde celé číslo $\tilde{v}$, které je řešení kongruence $vx \equiv 1 \pmod{n}$, a spočítá bod $M_4 = \tilde{v}M_3$. Protože $M_4 = \tilde{v}\tilde{u}vuM$, přičemž platí $\tilde{v}\tilde{u}vu \equiv 1 \pmod{n}$ a $nM = O$, je $M_4 = M$.

Jak přiřadit zprávě bod na dané eliptické křivce

Jde-li o křivku danou rovnicí $y^2 = x^3 + ax + b$ nad $\mathbb{Z}_p$ pro prvočíslo $p \equiv 3 \pmod 4$, lze postupovat například takto:

Nechť zprávou je celé číslo m, kde $0 \leq m < \frac{p}{100}$.

Pro $j = 0, 1, \ldots, 99$ označme $x_j = 100m + j$, $s_j = x_j^3 + ax_j + b$.

Protože s_j vznikají v podstatě náhodně, lze jevy $(\frac{s_j}{p}) = 1$ považovat za nezávislé, přičemž pravděpodobnost každého z nich je $\frac{1}{2}$.

Rychle lze najít j tak, že $(\frac{s_j}{p}) = 1$, a spočítat $y_j \equiv s_j^{(p+1)/4} \pmod p$.

Pak $y_j^2 \equiv s_j^{(p+1)/2} \equiv (\frac{s_j}{p}) \cdot s_j \pmod p$.

Proto bod $[x_j, y_j]$ leží na dané křivce.

Ze znalosti tohoto bodu získáme zprávu m výpočtem $m = [\frac{x_j}{100}]$.

Kryptosystém El Gamal

Alice chce poslat zprávu Bobovi, Bob si proto nachystá tajný a veřejný klíč.

Bob zvolí eliptickou křivku E nad konečným tělesem $\mathbb{F}_q$ a bod P na ní tak, aby problém diskrétního logaritmu o základu P byl obtížný (obvykle jsou křivka a bod zvoleny tak, aby řád bodu P bylo velké prvočíslo). Bob zvolí své tajné přirozené číslo v nesoudělné s řádem bodu P a na E spočítá bod $B = vP$.

Veřejný klíč: eliptická křivka E nad $\mathbb{F}_q$, body P, B.

Tajný klíč: číslo v (které je diskrétním logaritmem $v = \log_P B$).

Alice si zjistí Bobův veřejný klíč a vyjádří svou zprávu jako bod M na E. Dále zvolí své tajné přirozené číslo u. Pak na E spočítá body $M_1 = uP$, $M_2 = M + uB$. Alice se ujistí, že $uP \neq O$ (tj. u není dělitelné řádem bodu P) a odešle body M_1, M_2 Bobovi.

Bob spočítá $M_2 - vM_1 = (M + uB) - v(uP) = M$ a tím určí zprávu, kterou odesílala Alice.

Podepisování zprávy kryptosystémem El Gamal

Alice chce poslat podepsanou zprávu Bobovi, pro jednoduchost předpokládejme, že tuto zprávu není nutné utajit šifrováním. Alice si proto nachystá tajný a veřejný klíč.

Alice zvolí eliptickou křivku E nad konečným tělesem $\mathbb{F}_q$ a bod P na ní tak, aby problém diskrétního logaritmu o základu P byl obtížný (obvykle jsou křivka a bod zvoleny tak, aby řád n bodu P bylo velké prvočíslo). Alice zvolí své tajné přirozené číslo u nesoudělné s n a na E spočítá bod $B = uP$.
Dále zvolí funkci $f : E \to \mathbb{Z}$, aby $f(E) \cap n\mathbb{Z} = \emptyset$.
Například, je-li q prvočíslo (a ne mocnina prvočísla), $q < n$, může $f(C)$ být nejmenší přirozené číslo ze zbytkové třídy modulo q, která je x-ovou souřadnicí daného bodu C.

Veřejný klíč: eliptická křivka E nad $\mathbb{F}_q$, body P, B, funkce $f : E \to \mathbb{Z}$.

Tajný klíč: číslo u (které je diskrétním logaritmem $u = \log_P B$).

Podepisování zprávy kryptosystémem El Gamal

Veřejný klíč: eliptická křivka E nad $\mathbb{F}_q$, body P, B, funkce $f : E \to \mathbb{Z}$.
Tajný klíč: číslo u (které je diskrétním logaritmem $u = \log_P B$).

Zpráva, kterou chce Alice podepsat, je přirozené číslo $m \leq n$ (kde n je řád bodu P). Alice pro tuto zprávu zvolí tajné přirozené číslo k nesoudělné s n, spočítá bod $R = kP$ a najde celé číslo s, které je řešení kongruence $kx \equiv m - u \cdot f(R) \pmod{n}$.

Alice Bobovi odešle trojici (m, R, s).

Bob na E spočítá body $V = f(R) \cdot B + sR, \quad W = mP$.

Jestliže platí $V = W$, uvěří Bob, že je zpráva skutečně od Alice, neboť $f(R) \cdot B + sR = f(R) \cdot uP + skP = (f(R) \cdot u + sk)P = mP$.

Je třeba si uvědomit, že pro výpočet podpisu s bylo třeba využít nejen tajného klíče u (a tedy mohl podpis s spočítat jen ten, kdo tajný klíč znal), ale i zprávy m (a tedy nelze podpis s podvrhnout podpisem jiné zprávy).

MOV útok na kryptosystémy využívající obtížnost výpočtu diskrétního logaritmu na eliptické křivce

Menezes, Okamoto a Vanstone navrhli, jak užít tzv. Weilovo párování na zrychlení výpočtu diskrétního logaritmu na eliptické křivce E nad konečným tělesem $\mathbb{F}_q$.

Protože jsme nevysvětlili, co je to Weilovo párování, zmiňme jen, že jejich metoda převádí výpočet diskrétního logaritmu na E na výpočet diskrétního logaritmu v multiplikativní grupě tělesa $\mathbb{F}_{q^m}$, kde je možné použít zobecnění metody „index calculus“. To může tento výpočet zrychlit v případě, kdy m je malé.

Pro křivky splňující $|E| = q + 1$ dokonce stačí vzít $m = 2$.
To je v jistém smyslu škoda, protože právě pro tyto křivky existuje metoda výpočtu násobku bodu, která je rychlejší než obvyklá metoda rychlého umocňování v grupě (kterou lze použít pro všechny eliptické křivky).