EGCD-Übung

extended greatest common divisor

$a = 43 \quad b = 31 \quad \gcd(a,b) = 1$

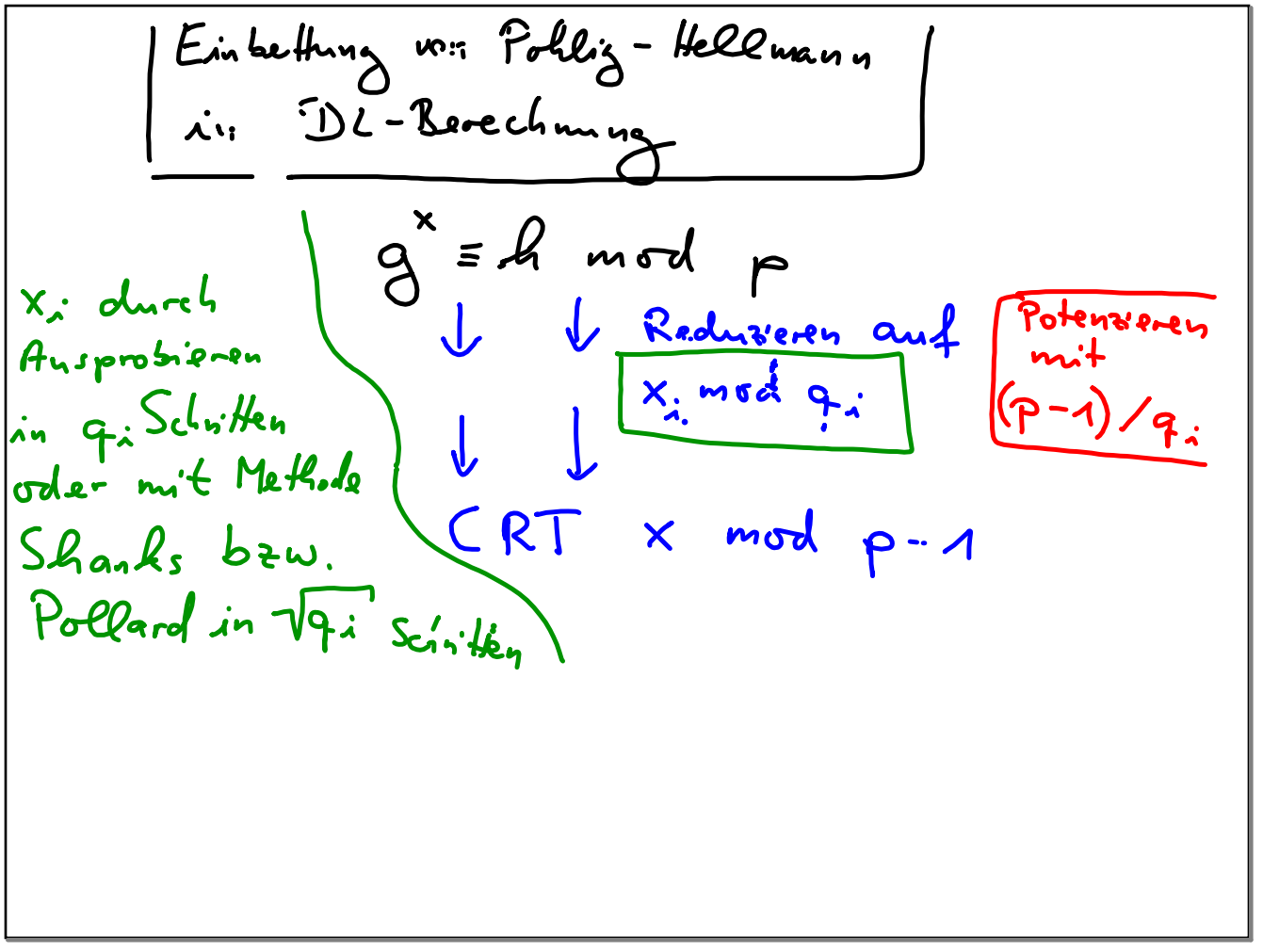
$a \cdot x + b \cdot y = 1$

$43 \cdot 13 - 31 \cdot 18 = 1 \xrightarrow{\text{mod } 43} -31 \cdot 18 \equiv 1 \bmod 43$

$x = 13, \quad y = -18 \quad \Rightarrow \frac{1}{31} \equiv -18 \bmod 43$

Bemerkungen:

- effizient, weil EGCD Laufzeit $\mathcal{O}(\log(b)^3)$
- EGCD kann vermieden werden
  - mod p, $p \in \mathbb{P}$
    $a^{p-1} \equiv 1 \bmod p \Rightarrow \frac{1}{a} \equiv a^{p-2} \bmod p$
  - mod m, m klein $\rightarrow$ Ausprobieren


Einbettung von Pohlig-Hellman in DL-Berechnung
$g^x \equiv h \mod p$
Reduzieren auf $x_i \bmod q_i$
Potenzieren mit $(p-1)/q_i$
x_i durch Ausprobieren in q_i Schritten oder mit Methode Shanks bzw. Pollard in $\sqrt{q_i}$ Schritten
CRT $x \bmod p-1$

Shanks Methode: Baby-Step-Giant-Step

Situation:

Gleichung $g^x = h$ ($g^x \equiv h \bmod p$) nach der Reduktion

mit $x \in \{0, 1, 2, \ldots, q-1\}$

Idee:

$$g^x = g^{x_1 \cdot m + x_0} = h \qquad m = \lceil \sqrt{q} \rceil$$

in Hasse: $0 \le x_0 \le m-1$, $0 \le x_1 \le m-1$

$$g^{x_1 \cdot m + x_0} = h$$

$$(g^m)^{x_1} \cdot g^{x_0} = h$$

$$(g^m)^{x_1} = \underbrace{h \cdot g^{-x_0}}$$

Paare $(x_0, h \cdot g^{-x_0})$ in Hashtabelle

Beispiel: $p = 47$, $G = 5$, $H = 23$

$47 - 1 = 2 \cdot 23$

$$5^x \equiv 23 \mod 47$$

$q = 23$, Pohlig-Hellman

$$\left(5^{\frac{47-1}{23}}\right)^x \equiv 23^{\frac{47-1}{23}} \mod 47$$

$$25^x \equiv 12 \mod 47$$

Shanks: $g^x = h$

Hashtabelle aufbauen:

$h \cdot g^{-x_0}$ für $0 \le x_0 \le m = \lceil \sqrt{q} \rceil$

$q = 23$

$12 \cdot 25^{-x_0} \bmod 47$, $0 \le x_0 \le 5$

x_0	$12 \cdot 25^{-x_0} \bmod 47$
0	12
1	8
2	21
3	14
4	25
5	1

$(g^m)^{x_1} \bmod p$

$(25^5)^0 \equiv 1 \bmod 47$

$x = x_1 \cdot m + x_0 = 0 \cdot 5 + 5 = 5$

$\Rightarrow 25^5 = 12 \bmod 47$

Übung: Shanks anwenden für:

$G = 5$, $H = 33$, $p = 47$

$p - 1 = 2 \cdot 23$ (q)

5 ↓ g — 33 ↓ h (Pohlig-Hellman)

$25^x \equiv 8 \bmod 47$

$\vdots$

Hashtabelle ↓ mit x_0 — $0 \le x_0 \le 5$, $m = \lceil \sqrt{q} \rceil$

Ausprobieren ↓ mit x_1 — $x_1 \ge 0$

$\rightarrow x = x_1 \cdot m + x_0$

Lösung:

$$5^x \equiv 33 \mod 47$$

$$p-1 = 47-1 = 2 \cdot 23$$

$x \bmod 2$

$x \bmod 23$

q

$q = 2$: $\frac{p-1}{2}$ $\frac{p-1}{2}$.

$$(5^x) \equiv 33 \mod p$$

$$46^x \equiv 46 \mod 47 \Rightarrow x \equiv 1 \bmod 2$$

$q = 23$:

$$\left(5^x\right)^{\frac{p-1}{23}} \equiv 33^{\frac{p-1}{23}} \mod 47$$

(5: G, 33: H)

$$25^x \equiv 8 \mod 47$$

(25: g, 8: h)

→ Lösung $x \bmod 23$

$x \in \{0, 1, 2, \ldots, 22\}$

Shanks: $m = \lceil \sqrt{q} \rceil = \lceil \sqrt{23} \rceil = 5$

$x = x_1 \cdot m + x_0 = 5x_1 + x_0$

$0 \leq x_i \leq 5$

Einschub:

mit x_i muss nur der Bereich $0, 1, \ldots, m-1$ abgedeckt werden

$m = \lceil \sqrt{q} \rceil$

$m^2 \geq q$

$x = x_1 \cdot m + x_0$

$(m-1) \cdot m + m - 1$

$m^2 \underbrace{- m + m} - 1$

$\geq q - 1$

$$25^{x} \equiv 8 \mod 47$$

$$25^{x_1 \cdot m + x_0} \equiv 8 \mod 47$$

$$\left(25^{m}\right)^{x_1} \equiv \underline{8 \cdot 25^{-x_0}} \mod 47$$

$m = 5$, $\underline{0 \leq x_0 \leq 5}$ (Einschränkung $x_0 \leq 4$ reicht)

in Hashtabelle speichern

x_0	$8 \cdot 25^{-x_0} \bmod 47$
0	8
1	21
2	14
3	25
4	1
5	32

Treffer

Baby-Steps füllen Hashtabelle (mit x_0)

Giant-Steps (x_1)

$(25^m)^{x_1} \bmod 47$

$x_1 \geq 0$ bis Treffer in Tabelle

Beispiel:

$8 \cdot 25^{-1} \equiv \frac{8}{25} \bmod 47$

$\frac{1}{25} \bmod 47$? Euklid.

$47 = 1 \cdot 25 + 22$

$25 = 1 \cdot 22 + 3$

$22 = 7 \cdot 3 + 1$

$1 = 22 - 7 \cdot 3$

$= 22 - 7 \cdot (25 - 1 \cdot 22)$

$= 8 \cdot 22 - 7 \cdot 25$

$= 8 \cdot (47 - 1 \cdot 25) - 7 \cdot 25$

$= 8 \cdot 47 - 15 \cdot 25$

$32 \equiv 1/25 \bmod 47$

$8 \cdot 32 \equiv 2 \cdot 4 \cdot 32 = 2 \cdot (-15) = -26 \equiv 21 \bmod 47.$

$(2_5{}^5)^{x_1} \mod 47$

$12^{x_1} \mod 47$

$x_1 = 0 \quad : \quad 12^0 \equiv 1 \mod 47$

↳ Treffer: $x = x_1 \cdot m + x_0$

$x = 0 \cdot 5 + 4$

$x \equiv 4 \mod 23$

$25^4 \equiv 8 \mod 47$

Teillösungen:

$$\left.\begin{aligned} x &\equiv 1 \bmod 2 \\ x &\equiv 4 \bmod 23 \end{aligned}\right\} \quad x \bmod (2 \cdot 23)$$

CRT: $a_1 = 1,\ m_1 = 2,\ a_2 = 4,\ m_2 = 23$

$$x = a_1 \cdot m_2 \cdot m_2' + a_2 \cdot m_1 \cdot m_1'$$

$$m_2' \equiv \frac{1}{m_2} \bmod m_1 \qquad m_1' \equiv \frac{1}{m_1} \bmod m_2$$

$$\equiv \frac{1}{23} \bmod 2 \qquad \equiv \frac{1}{2} \bmod 23$$

$$\equiv 1 \bmod 2 \qquad \equiv 12 \bmod 23$$

$$x = 1 \cdot 23 \cdot 1 + 4 \cdot 2 \cdot 12 = 119$$

$$x \equiv 27 \bmod 46$$

$$\Rightarrow \quad G^x \equiv H \bmod p$$

$$5^{27} \equiv 33 \bmod 47$$