Pollard-ρ-Methode

probabilistisch, kaum Hauptspeicherbedarf

Situation: reduziertes DL-Problem $G \to g$, $H \to h$

$$g^x \stackrel{!}{\equiv} h \mod p \qquad x \in \{0,1,2,\dots,q-1\}$$

$x \mod q$ gesucht

$q \mid p-1$

Idee:

Zahlenfolge konstruieren

$y_i \equiv g^{k_i} h^{l_i} \mod p$,

falls

$y_i = y_j$ für $i \neq j$

dann ist das DL-Problem gelöst.

$$g^x \equiv h \mod p$$

$$y_i = y_j$$

$$g^{k_i} h^{l_i} \equiv g^{k_j} \cdot h^{l_j} \mod p$$

$$g^{k_i} \cdot (g^x)^{l_i} \equiv g^{k_j} \cdot (g^x)^{l_j} \mod p$$

$$g^{k_i + x \cdot l_i} \equiv g^{k_j + x \cdot l_j} \mod p$$

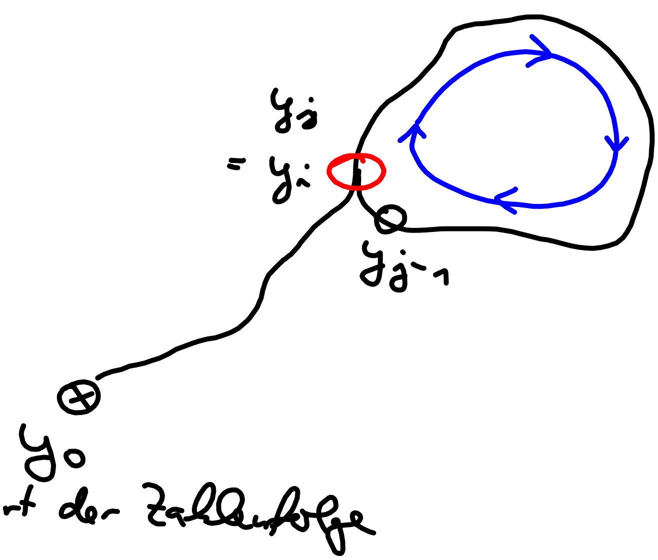
$x \mod q$ eindeutig:

$$k_i + x \cdot l_i \equiv k_j + x \cdot l_j \mod q.$$

$$\Rightarrow \quad x \cdot (l_i - l_j) \equiv k_j - k_i \mod q$$

$$\Rightarrow \quad x \equiv \frac{k_j - k_i}{l_i - l_j} \mod q$$

graphische Darstellung



Pollard-Definition der y_i-Zahlenfolge:

Startwert $y_0 \equiv g^1 \cdot h^1 \bmod p$

$$y_{i+1} \equiv \begin{cases} g \cdot y_i \bmod \overset{k+1}{p}, & \text{falls } \quad y_i \equiv 0 \bmod 3 \\ h \cdot y_i \bmod \overset{\ell+1}{p}, & \text{"} \quad y_i \equiv 1 \bmod 3 \\ y_i^2 \bmod \underbrace{p}_{2k,\, 2\ell}; & \text{"} \quad y_i \equiv 2 \bmod 3 \end{cases}$$