Übung:

$$5^x \equiv 12 \mod 23$$

$q = 2$ $\qquad$ $q = 11$

$$(5^x)^{\frac{23-1}{2}} \equiv 12^{\frac{23-1}{2}} \mod 23$$

$$22^x \equiv 1 \mod 23$$

$\Rightarrow x \equiv 0 \mod 2$

$$(5^x)^{\frac{23-1}{11}} \equiv 12^{\frac{23-1}{11}} \mod 23$$

$$2^x \equiv 6 \mod 23$$

$x \equiv 9 \mod 11$

CRT $\quad x \equiv 0 \mod 2$, $\quad x \equiv 9 \mod 11$

$a_1 \quad m_1$

$a_2 \quad m_2$

$$m_1' \equiv \frac{1}{m_1} \mod m_2$$

$$6 \equiv \frac{1}{2} \mod 11$$

$$m_2' \equiv \frac{1}{m_2} \mod m_1$$

$$\equiv \frac{1}{11} \mod 2$$

$$\equiv \frac{1}{1} \equiv 1 \mod 2$$

$z \equiv \frac{1}{2} \mod p$

$2 \cdot z \equiv 1 \mod p$

$z = \frac{p+1}{2}$ $\quad 1, \quad p+1, \quad 2p+1$

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

$$0 \cdot 11 \cdot 1 + 9 \cdot 2 \cdot 6 = 108 \equiv 20 \mod 22$$

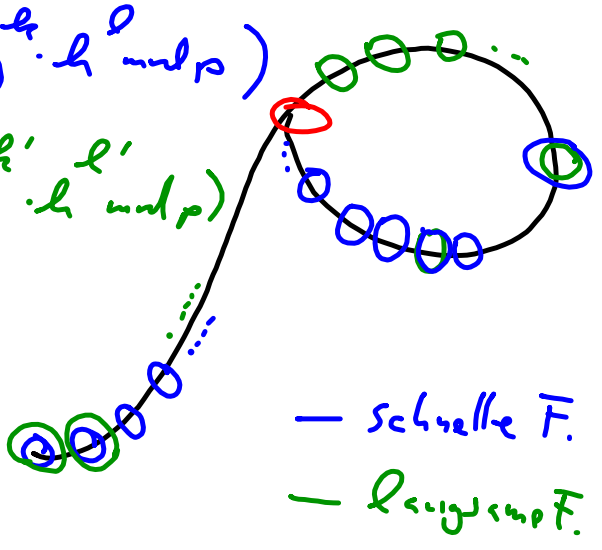
Erkennen der Kollision in der Zahlenfolge

Ziel: Speichern der Folge vermeiden

$y \quad k \quad l \qquad (y \equiv g^k \cdot h^l \bmod p)$

$y' \quad k' \quad l' \qquad (y' \equiv g^{k'} \cdot h^{l'} \bmod p)$

$y \equiv y'$



Laufzeit

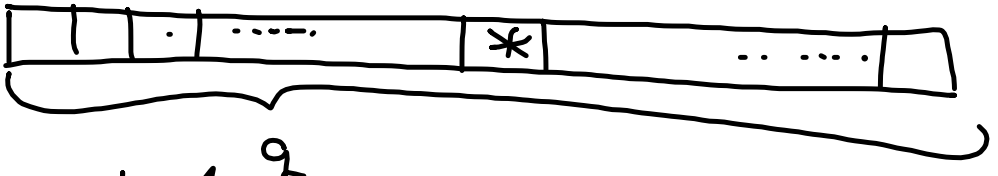
Anzahl Schritte bis Kollision

q verschiedene Werte für x bzw y

Folge verhält sich "wie zufällig"

Wahrscheinlichkeitsbetrachtung
⇒ erwartete Laufzeit

Frage: mit welcher Wahrscheinlichkeit wiederholt sich y beim 2. Schritt



q

Antwort $\frac{1}{q}$

Also wird mit Wahrscheinlichkeit $\frac{q-1}{q}$ weitergerechnet.

Beim 3. Schritt sind 2 Werte vorhanden,

d.h. Weiterrechnen mit W. $\frac{q-2}{q}$

Insgesamt werden i Schritte gerechnet

$$P(i) = \frac{q-1}{q} \cdot \frac{q-2}{q} \cdot \frac{q-3}{q} \cdots \frac{q-i}{q}$$

Ergebnis erwartet wenn $P(i) < \frac{1}{2}$

$$\left(1-\frac{1}{q}\right)\cdot\left(1-\frac{2}{q}\right)\cdots\left(1-\frac{i}{q}\right) < \frac{1}{2}$$

Trick: $1+x < e^x = 1 + x + \frac{x^2}{2} + \ldots$

$$\square < e^{-\frac{1}{q}} \cdot e^{-\frac{2}{q}} \cdots e^{-\frac{i}{q}}$$

$$= e^{-\frac{1}{q}-\frac{2}{q}-\frac{3}{q}-\cdots-\frac{i}{q}}$$

$$= e^{-\frac{1}{q}(1+2+\ldots+i)}$$

$$= e^{-\frac{1}{q}\left(\frac{i(i+1)}{2}\right)} < \frac{1}{2}$$

$$-\frac{1}{q} \cdot i \cdot \frac{i+1}{2} < \ln\left(\frac{1}{2}\right) = -\ln(2)$$

$$\underbrace{i\cdot(i+1)}_{\approx i^2} > \underbrace{q \cdot 2 \cdot \ln(2)}_{c_1 \cdot q}$$

$$i \in \Theta(\sqrt{q})$$

gleiche Laufzeit wie bei Shanks, ohne Platzverbrauch, aber nicht deterministisch

Übung:

Implementierung in bel. Programmiersprache

Pollard-Folge

$(y, k, \ell) \longrightarrow (y, k, \ell)$

$(y, k, \ell) \rightarrow (y, k, \ell) \rightarrow (y, k, \ell)$

(y, k'', ℓ)

Eingabe: g, h, p, q

Programm löst $g^x \equiv h \mod p$

q Teiler von $p-1$

$\Rightarrow (g^x)^{\frac{p-1}{q}} \equiv h^{\frac{p-1}{q}} \mod p$

$G^x \equiv H \mod p$

Pollard-Folge mit G, H, p

Ausgabe y, k, ℓ

y, k, ℓ

Schritte