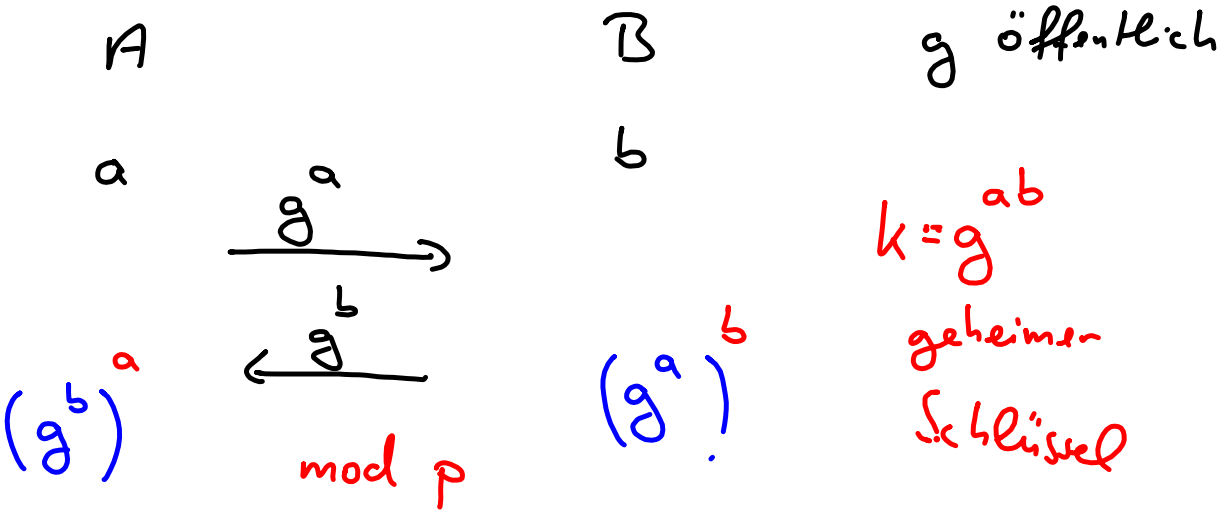
Diffie-Hellman



Beispiel:

Alice $a = 37$ Bob $b = 373$

Primzahl $p = 2^{16} + 1 = 65537$

Erzeuger $g = 2053$

$39981^{373} \bmod p \rightarrow 55440$

$g^a \bmod p = 39981 \rightarrow$ Bob $\rightarrow 55440$

$g^b \bmod p = 13933 \rightarrow$ Alice $\rightarrow 13933^{37} \bmod p$

Sicherheit des DH-Protokolls

- Länge von p, Bitlänge ≥ 2048 Bit
- p sichere Primzahl
- Ordnung von g

Ordnung von g

Beispiel:

$p = 65521$, $g = 65520$

$g^1 \equiv 65520 \equiv -1 \pmod{p}$

$g^2 \equiv 1 \pmod{p}$

$g^3 \equiv -1 \pmod{p}$

$\vdots$

g hat Ordnung 2

Ordnungen berechnen mod p

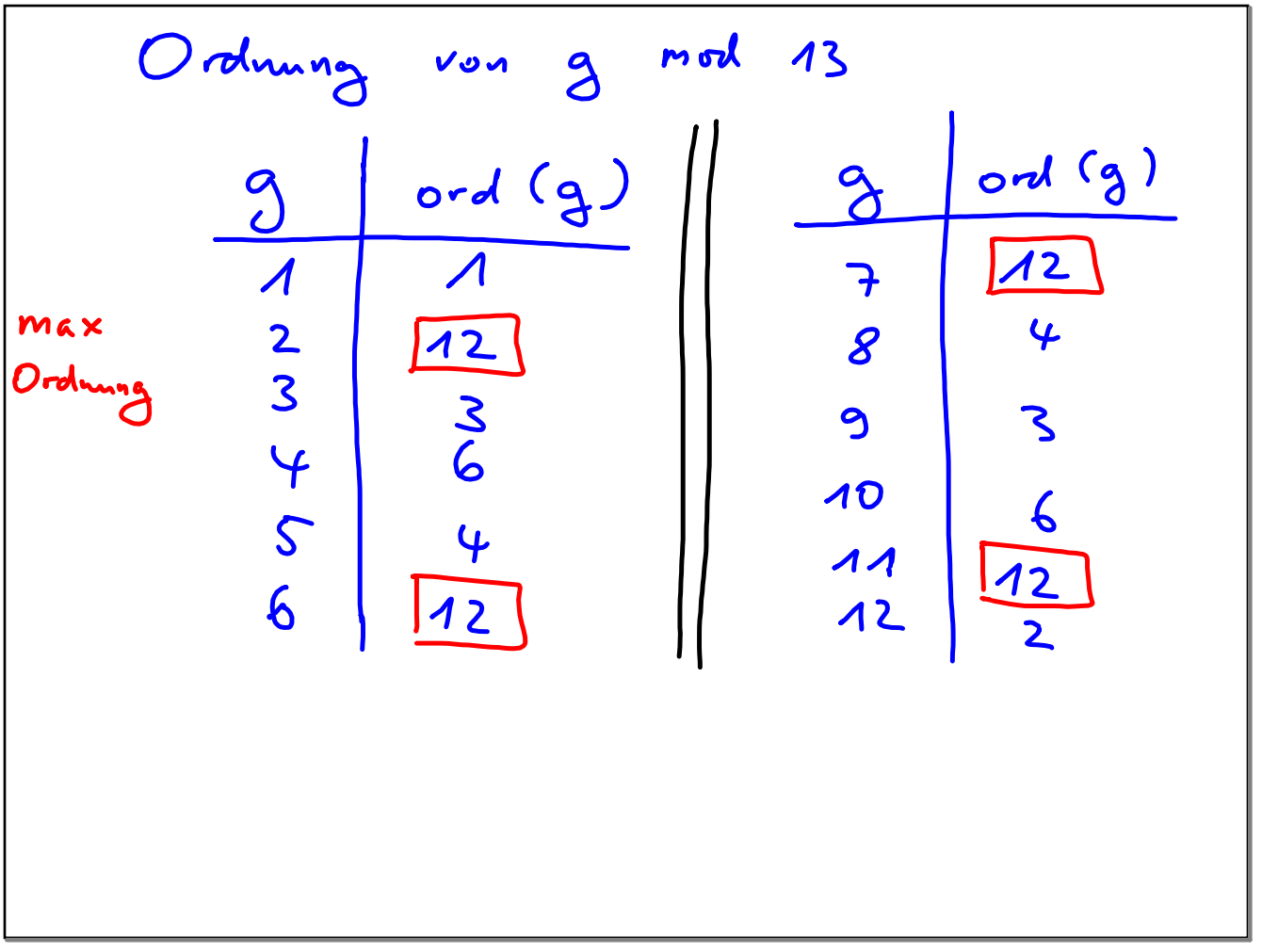
für jedes Element g mod p

finde kleinsten Exponenten $i \in \mathbb{N}$

für den $g^i \equiv 1 \bmod p$

gilt.

Beispiel: $p = 13$


Ordnung von g mod 13
g
ord (g)
1 1
2 12
3 3
4 6
5 4
6 12
g
ord (g)
7 12
8 4
9 3
10 6
11 12
12 2
max Ordnung

Wieviele g mit max. Ordnung gibt es?

wenn g max. Ordnung hat,

dann hat auch $g^j \bmod p$ max. Ordnung, falls

$$ggT(j, p-1) = 1$$

Das sind $\varphi(p-1)$ Stück.

Im Beispiel $p = 13$

$\Rightarrow \varphi(13-1)$ Elemente mit max Ordnung

$$\varphi(12) = \varphi(2^2) \cdot \varphi(3)$$

$$= (2^2 - 2^1) \cdot (3-1) = 4$$

$\Rightarrow$ 4 Elemente mod 13 mit max. Ordnung

ERZEUGER

Satz:

für eine Primzahl p
und ein Element g mod p
mit $ggT(g, p) = 1$
gilt $ord(g) \mid p-1$.

Erzeugerkriterium

Für $p \in \mathbb{P}$ und $g \in \mathbb{N}$ mit $ggT(g,p)=1$

zerlege $p-1$ in Primfaktoren

$$p-1 = q_1^{e_1} q_2^{e_2} \cdots q_k^{e_k}$$

und prüfe

$$g^{\frac{p-1}{q_i}} \not\equiv 1 \bmod p, \quad 1 \le i \le k$$

$12 = 2^2 \cdot 3$

Übung: (mit PARI/gp)

drei Erzeuger finden für

$p = 11$, $p = 101$, $p = 397$

und $p = 65521$