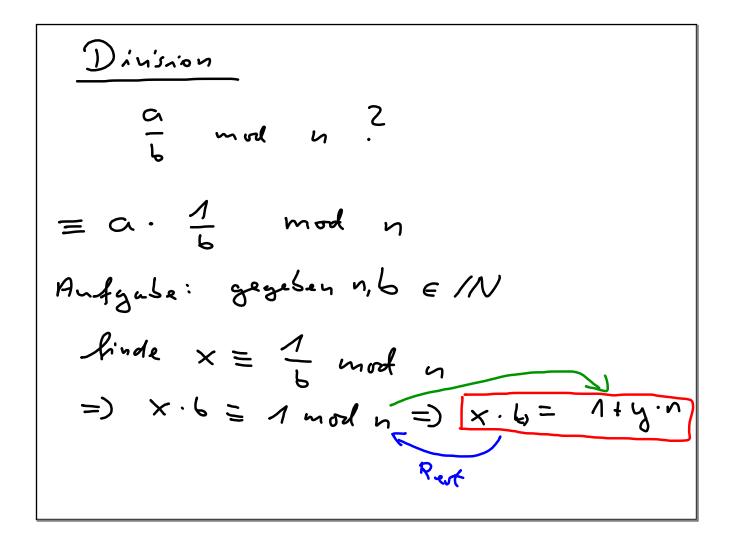
Grundrechenarten

$$7+7 \equiv 1 \mod 13$$

 $1 \mod 13$
 $1 \mod 13$
 $2 \mod 2 = 2 \mod 13$
 $7+7 \equiv -12 \mod 13$
 $7+7 \equiv 10 \mod 13$
 $7+x \equiv 3 \mod 13$
 $x \equiv 3-7 \equiv -4 \equiv 9 \mod 13$



$$x \cdot b = \Lambda + y \cdot n$$

$$x \cdot b - y \cdot n = \Lambda$$
Beisniel:
a)
$$x \cdot 2 - y \cdot 3 = \Lambda \Rightarrow (2, \Lambda)$$

$$(5, 3) (8, 5)$$

$$(5) \overline{x \cdot 6} - y \cdot 8 = \Lambda$$
Heine lösung

$$L_{3} (o''sung nur, wenn ggT(b, n) = \Lambda$$

Lösen der Gleichung

$$x \cdot b - y \cdot n = \Lambda$$

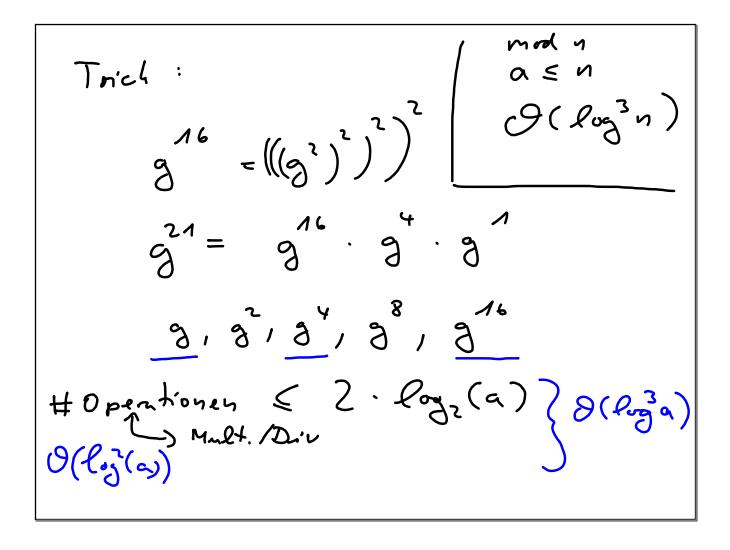
mrit Eußlidtischem Algonikluns
2.8. $b = \Lambda 9$, $n = 23$, $\Lambda = 5 \cdot 23 - 6 \cdot \Lambda 9$
 $\Lambda = 5 \cdot (23 - \Lambda \cdot n9) - \Lambda \cdot 9$
 $\Lambda = 5 \cdot (23 - \Lambda \cdot n9) - \Lambda \cdot 9$
 $\Lambda = 5 \cdot (4 - \Lambda \cdot \Lambda 9)$
 $\Lambda = 4 - (\Lambda 9 - 4 \cdot 4)$
 $\Lambda = 4 - (\Lambda 9 - 4 \cdot 4)$
 $\Lambda = 4 - 1 \cdot 3$

$$\begin{array}{l}
 1 = 5 \cdot 23 - 6 \cdot 19 \\
 y & n \times 6 \\
 l \mod n \\
 1 = 5 \cdot 23 - 6 \cdot 19 \mod 23 \\
 = 17 \mod 23 \\
 Probe : 17 \cdot 19 = 323 = 93 = 1 \mod 23 \\
 \end{array}$$

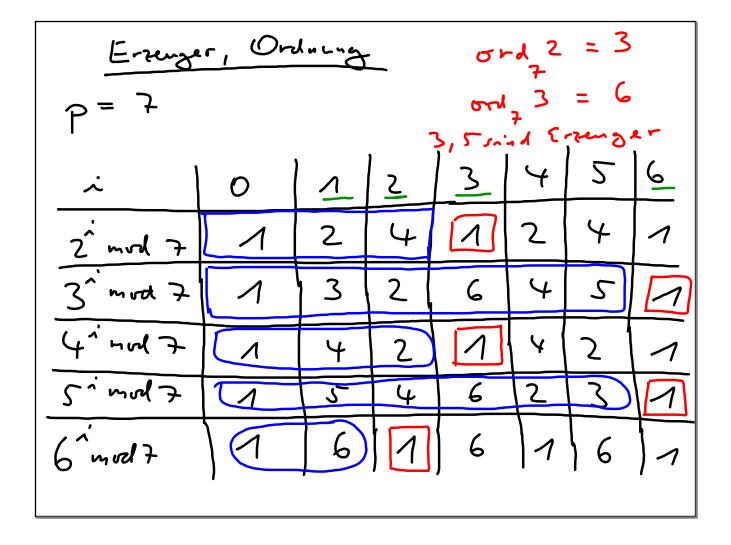
Г

Alternative Methode für laleine" Rahlen
Ausprobrieren !

$$\frac{1}{7}$$
 mood 12
 $7 \cdot 1 \equiv 1 \mod 12$? nein
 $7 \cdot 2$
 $7 \cdot 3$
 $7 \cdot 7 \equiv 49 \equiv 1 \mod 12$ $\frac{1}{7} \equiv 7 \mod 12$



Parameter wahl für Diffie-Hellura. , Standards beginnen bei 2048 Brit sollte ein Erzenger sein જ (order große Ordnung mod p haben p soll eine sichere Primzahl sein



kryptrymphisch relevant: · Erenger = max. Ordnung = p-1 · "große" Ordnung, Z.B. P-1 Z ("Lungo anfgabe : Wieviele Schlüssel kann man · auf 10.000 CPUs/(ores . mit 3,6 GHz · in A Jah- ansprobienen, falls das Ergebnis in A Takt berechnet wäre

Beispiel:

$$p = 7, g = 3 = 3 = 3^{2} = 3^{2} = 1 \mod 7$$

 $p = 21, g = 5$
 $5^{21-1} = 5^{20} = 4 \neq 1 \mod 7$
 $p = 1 \mod 7$
 $heine Princehl = 1 \mod 7$