I

$3 \odot_9 (\underbrace{2 \oplus_9 5}_{=7}) = 21 \bmod 9 = 3$

$\underbrace{3 \odot_{10} 2}_{=6} \oplus_{10} 8 = 14 \bmod 10 = 4$

$(3 \oplus_{12} 9) \odot_{12} (3 \oplus_{12} 9) = 0$

$=0$

$7 \odot_9 2 \oplus_9 4 \odot_9 6 = 5 \oplus_9 5 = 11 \bmod 9 = 2$

$=5 \qquad =6$

$(\underbrace{(\underbrace{3 \oplus_9 6}_{=0}) \odot_9 3}_{=0}) \ominus_9 8 = 0 \ominus_9 8 = -8 \equiv 1$

$\underbrace{\underbrace{3 \odot_8 6}_{=2} \ominus_8 2 \ominus_8 3}_{=0} = -3 \bmod 8 = -3$

II

$\oplus_7$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

$\odot_7$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	1	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

b) $\mathbb{Z}_7$ $\odot_7$ invertierbar

ggT(1,7) = 1

ggT(2,7) = 1

ggT(3,7) = 1

ggT(4,7) = 1

ggT(5,7) = 1

ggT(6,7) = 1

1, 2, 3, 4, 5, 6

wenn ggT(x, $\odot_7$) = 1,
dann ist modular invers

III.

$3^{13} \not\equiv 13 = 3$

$13 = (1101)_2$

1 1 0 1

QMQMQQM → QMQQM

$3 \xrightarrow{Q} 9 \equiv 9 \xrightarrow{M} 27 \equiv 1 \xrightarrow{Q} 1 \equiv 1 \xrightarrow{Q} 1 \equiv 1 \xrightarrow{M} 3 \equiv \underline{3}$

IV $n = 15$, $\mathbb{Z}^*_{15} = \{1, 2, 4, 7, 8, 11, 13, 14\}$

x	1	2	4	7	8	11	13	14
$x \odot_{15} x$	1	4	1	4	4	1	4	1

a	1	2	4	7	8	11	13	14
$\sqrt{a} \not\equiv 15$	1, 4, 11, 14		2, 7, 8, 13					

V.

k	1	2	3	4	5	6	7	8	9	10
$k^2 \bmod 11$	1	4	9	5	3	3	5	9	4	1

k^2:

a	1	2	3	4	5	6	7	8	9
$\sqrt{a} \bmod 11$	1, 10	[redacted]	5, 6	2, 9	4, 7	[redacted]	[redacted]	[redacted]	3, 8

$QR = 1, 3, 4, 5, 9$ $\quad NR = 2, 6, 7, 8, 10$

Rest, der aus einer Quadrierung entsteht

Rest, der nicht aus einer Quadrierung entsteht

VI

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$k^2 \% 21$	1	4	9	16	4	15	7	1	18	16	16	18	1	7	15	4	16	9	4	1

Zeile 8, 13, 20 aus Menge nehmen

$QR = 1, 4, 16$ $\quad NR = 7, 9, 15, 18$

Quadratwurzeln von 1 sind $1, 8, 13, 20$

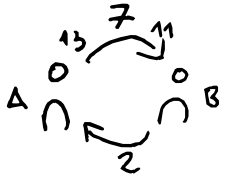
VII. $n=13$, $g=11$ — Diffie – Hellmann

$a=5$, $b=7$

Alice	Bob
$11^5 \bmod 13$	$11^7 \bmod 13$
101	111
QMQQM	QMQMQM
→ QQM	→ QMQM

Alice: $11 \xrightarrow{Q} 121 \equiv 4 \xrightarrow{Q} 16 \equiv 3 \xrightarrow{M} 33 \equiv 7$ ← A

Bob: $11 \xrightarrow{Q} 121 \equiv 4 \xrightarrow{M} 44 \equiv 5 \xrightarrow{Q} 25 \equiv 12 \xrightarrow{M} 132 \equiv 2$ ← B



a private = 5	b private = 7
A public = 7	B public = 2
$B^a \,\%\, n$	$A^b \,\%\, n$
$2^5 \,\%\, 13 = \underline{\underline{6}}$	$7^7 \,\%\, 13 = \underline{\underline{6}}$