Probeklausur

1. a) $(AFFE)_{16} = 10\cdot 16^{3} + \dots + 14\cdot 16^{0}$, also falsch!

b) $ggT(2^2 3^5 5,\ 2^2 3^3 7) = 2^2\cdot 3^3$, also falsch!

c) $10 \in \mathbb{Z}_{25}$ nicht invert., da $ggT(10,25) = 5 \neq 1$.

d) $\bar{3}\cdot\bar{3} = \bar{9} = \bar{4} \neq \bar{1}$ d.h. $\bar{3}^{-1} \neq \bar{3}$.

e) 11 prim $\Rightarrow (\mathbb{Z}_{11}\setminus\{0\},\cdot)$ Gruppe ✓

f) $4x \equiv 2 \mod 25$ eindeutig lösbar mit $x \equiv 4^{-1}\cdot 2$
existiert $ggT(4,25)=1$.

g) $10x + 7y = 6$ lösb. $\Leftrightarrow ggT(10,7) = 1 \mid 6$ ✓

h) $f: \mathbb{Z}_{12} \to \mathbb{Z}_{12}$, $f(x) = 8x \mod 12$

$\neq 8\cdot x$ nicht surj. (da $ggT(8,12) \neq 1$)

nicht inj.

nicht bijektiv

1	2	3	5
8	16 = 4	0	4

($f(x) = 5x \mod 12$ bijektiv: da $\exists$ Umkehrfkt $f^{-1}(x) = 5^{-1}x$)

2. $(P \oplus Q) \Leftrightarrow Q =: P \circ Q$

a)

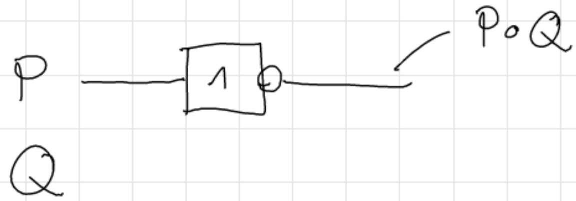
P	Q	$P\oplus Q$	$(P\oplus Q)\Leftrightarrow Q$
0	0	0	1
0	1	1	1
1	0	1	0
1	1	0	0

b) $P \circ Q \overset{DNF}{\Longleftrightarrow}$

$0\circ 0$ $\wedge$ $\neg P \wedge \neg Q \vee$
$0\circ 1$ $\wedge$ $\neg P \wedge Q \vee$
$\underbrace{1\circ 0}_{0}$ $\wedge$ $P \wedge \neg Q \vee$
$\underbrace{1\circ 1}_{0}$ $\wedge$ $P \wedge Q$

$\Leftrightarrow (\neg P \wedge \neg Q) \vee (\neg P \wedge Q)$ ← DNF c)

$$\Leftrightarrow \neg P \wedge \underbrace{(\neg Q \vee Q)}_{1} \Leftrightarrow \underline{\neg P}$$



3. $$\sum_{k=0}^{n} 2^k \doteq 2^{n+1} - 1$$

<u>IA:</u> $n = 0$: LS: $\sum_{k=0}^{0} 2^k = 2^0 = 1$

RS: $2^{0+1} - 1 = 2 - 1 = 1$ ✓

<u>IS:</u> $\underline{n \to n+1}$. ~~zzg~~ $$\sum_{k=0}^{n+1} 2^k \doteq 2^{(n+1)+1} - 1 = \underline{2^{n+2} - 1}$$

$$\sum_{k=0}^{n+1} 2^k = \underbrace{2^0 + 2^1 + 2^2 + \dots + 2^n}_{\sum_{k=0}^{n} 2^k \overset{IV}{=} 2^{n+1} - 1} + 2^{n+1} = 2^{n+1} - 1 + 2^{n+1}$$

$$= 2 \cdot 2^{n+1} - 1 = \underline{2^{n+2} - 1}$$

4. $9x \equiv 3 \mod 150$.

$$\Leftrightarrow 9x = 3 + k \cdot 150 \Leftrightarrow 9x + 150\underbrace{(-k)}_{y} = 3$$

<u>EEA:</u>

$a_i = q_i b_i + r_i$	x_i	y_i	$ggT = a_i x_i + b_i y_i$
$9 = 0 \cdot 150 + 9$	17	−1	$3 = 9 \cdot 17 + 150(-1)$
$150 = 16 \cdot 9 + 6$	−1	17	$3 = 150(-1) + 9 \cdot 17$
$9 = 1 \cdot 6 + \boxed{3}$	1	−1	$3 = 9 \cdot 1 + 6 \cdot (-1)$
$6 = 2 \cdot 3 + 0$	0	1	$3 = 6 \cdot 0 + 3 \cdot 1$

- $x_0 = 17$ ist eine Lösung!
- $X = x_0 + z \cdot \frac{b}{ggT} = \underline{17 + z \cdot 50}$.

5.
$$x \equiv 2 \mod 3$$
$$x \equiv 3 \mod 5$$
$$x \equiv 5 \mod 11$$

$ggT(3,5) = 1$, $ggT(3,11) = 1$, $ggT(5,11) = 1$
d.h. Module sind paarw. teilerfremd!

$\rightarrow$ CRT:

$$m = 3\cdot 5\cdot 11 = 165$$

$$k_1 = \cancel{3}\cdot 5\cdot 11 = 55 \qquad x_1\cdot \overbrace{55}^{1} \equiv 1 \mod 3 \Rightarrow x_1 = 1$$
$$k_2 = 3\cdot \cancel{5}\cdot 11 = 33 \qquad x_2\cdot \overbrace{33}^{3} \equiv 1 \mod 5 \Rightarrow x_2 = 2$$
$$k_3 = 3\cdot 5\cdot \cancel{11} = 15 \qquad x_3\cdot \underbrace{15}_{4} \equiv 1 \mod 11 \Rightarrow x_3 = 3$$

$$x = \sum_{i=1}^{3} a_i k_i x_i = 2\cdot 55\cdot 1 + 3\cdot 33\cdot 2 + 5\cdot 15\cdot 3$$
$$= 110 + 198 + 225 = \underline{\underline{533}} \equiv 38 \mod 165 \checkmark$$

$$\boxed{y = 38 + z\cdot 165}$$

6. $5x + 7y = 3$

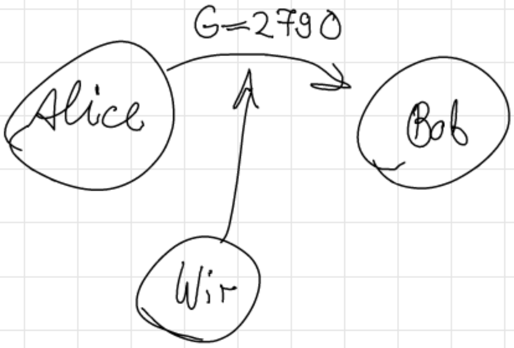
- Zuerst löse $5x + 7y = ggT(5,7)$ mit EEA:

$a_i = q_i b_i + r_i$	x_i	y_i	$ggT = a_i x_i + b_i y_i$
$5 = 0\cdot 7 + 5$	3	-2	$1 = 5\cdot 3 + 7(-2)$
$7 = 1\cdot 5 + 2$	-2	3	$1 = 7\cdot(-2) + 5\cdot 3$
$5 = 2\cdot 2 + \boxed{1}$	1	-2	$1 = 5\cdot 1 + 2\cdot(-2)$
$2 = 2\cdot 1 + 0$	0	1	$1 = 2\cdot 0 + 1\cdot 1$

$(x_0, y_0) = (3, -2)$

- Lsg. von $5x + 7y = 3$: $\quad 3\cdot(3,-2) = (9,-6)$
- Allg. Lsg: $(x,y) = (9 + z\cdot 7,\ -6 - z\cdot 5)$
- $-10 \le x,y \le 10$:
  - ~~$z = -3 \quad (x,y) = (-12, 9)$~~
  - $z = -2 \quad (x,y) = (-5, 4)$ ✓
  - $z = -1 \quad (x,y) = (2, -1)$ ✓
  - $z = 0 \quad (x,y) = (9, -6)$ ✓
  - ~~$z = 1 \quad (x,y) = (16, -11)$~~

7. $(N, e) = (3233, 17)$



Wir brauchen: d zum Entschl. $\qquad \underbrace{e}_{17} \cdot d \equiv 1 \mod \underbrace{\varphi(N)}_{\varphi(p \cdot q) = (p-1)(q-1)}$

Wir brauchen: p, q mit $N = p \cdot q$. $\qquad p = 61$, $q = 53$ (Testen!)

$$\varphi(N) = 60 \cdot 52 = \underline{3120}.$$

also $\quad 17 \cdot d \equiv 1 \mod 3120$

$$\Leftrightarrow 17 \cdot d = 1 + k \cdot 3120 \qquad \underline{\text{EEA}}: d = 2753.$$

$$G^d = 2790^{2753} \equiv \ldots \equiv \underline{65} \mod 3233$$