# Mathematik 1 – AI

Blatt 4

**A31**

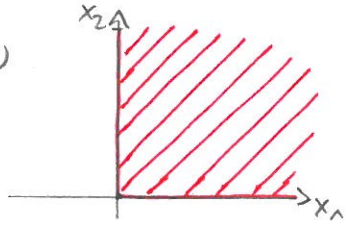
a) falsch  b) falsch  c) wahr

d) falsch  e) wahr  f) wahr

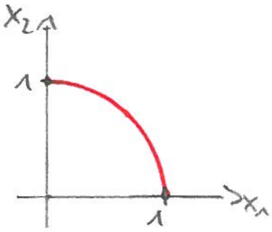
g) wahr  h) wahr  k) wahr

**A32**

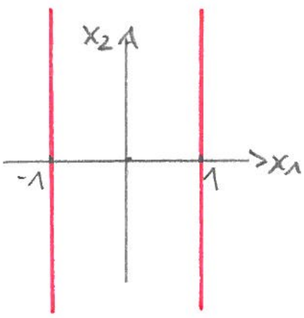
a)



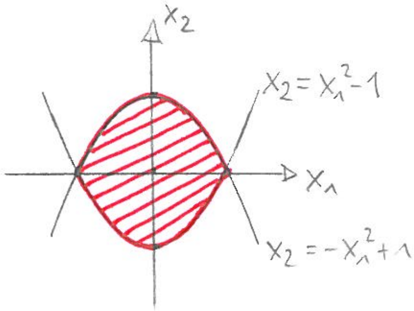

b)



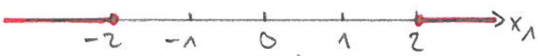

c)




d)

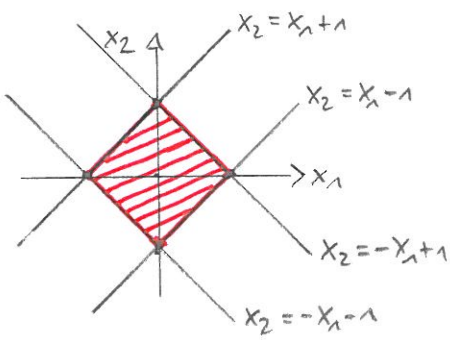



e)

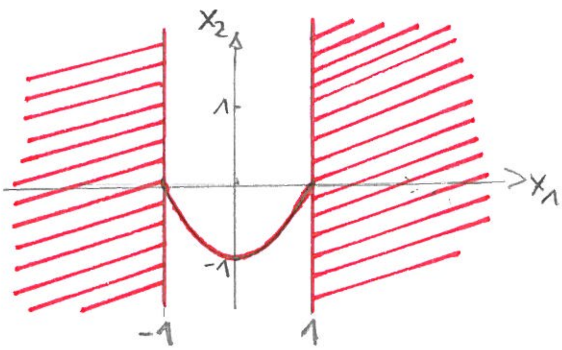



f)


g)

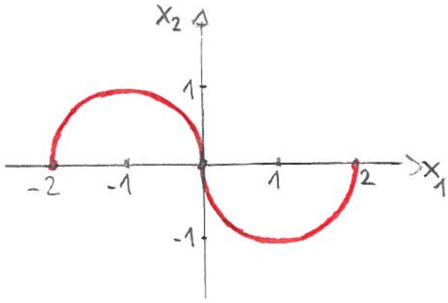



h)



A32 Fortsetzung

e)




A33

a) $\varphi(x,y) = (x \geq 0) \wedge (y \geq 0) \wedge (y \leq -x+1)$

b) $\varphi(x,y) = (x^2 + y^2 \geq 1) \wedge (x^2 + y^2 \leq 4)$

c) $\varphi(x,y) = (x \geq 1) \wedge (x \leq 3) \longrightarrow (y = -x+4)$

d) $\varphi(x,y) = \big[(x \geq -1) \wedge (x \leq 1) \wedge$
$\wedge \big((y=1) \vee (y=-1) \vee (x=1) \vee (x=-1) \vee (y=x) \vee (y=-x)\big)\big] \vee$
$\vee \big[(x \geq -1) \wedge (x \leq 0) \wedge (y = x+2)\big] \vee$
$\vee \big[(x \geq 0) \wedge (x \leq 1) \wedge (y = -x+2)\big]$

e) $\varphi(x,y) = \big[(x \geq -1{,}57) \wedge (x \leq 1{,}57) \wedge (y \leq \sin x + 1) \wedge (y \geq \sin x - 1)\big] \vee$
$\vee \big[(x = 1{,}57) \wedge (y \leq 0) \wedge (y \geq -2)\big]$

f) $\varphi(x,y) = \big[(x \geq -2) \wedge (x \leq 2) \wedge (y \geq 0) \wedge (y^2 \leq 1 - \frac{1}{4}x^2)\big] \vee$
$\vee \big[(x \geq -1) \wedge (x \leq 1) \wedge (y \geq -2) \wedge (y \leq 0)\big]$

A34 a) Die ersten $n$ ungeraden Zahlen $1, 3, 5, \ldots$ erhält man mit dem Term $2k-1$, $k = 1, 2, 3, \ldots, n$

z.z. $\sum_{k=1}^{n} 2k-1 = n^2$ (per Induktion nach $n$)

Ind.anfang: $n=1$

l.S. $\sum_{k=1}^{1} 2k-1 = 2\cdot 1 - 1 = 1$

r.S. $1^2 = 1$ ✓

Induktionsschritt: $n \to n+1$

$$\sum_{k=1}^{n+1} 2k-1 = \underbrace{\sum_{k=1}^{n} 2k-1}_{n^2 \text{ nach I.V.}} + 2(n+1) - 1 \overset{\text{I.V.}}{=} n^2 + 2(n+1) - 1 =$$

$$= n^2 + 2n + 1 = (n+1)^2.$$

b) Die ersten $n$ geraden Zahlen $2, 4, 6, \ldots$ erhält man mit dem Term $2k$, $k = 1, 2, 3, \ldots, n$.

z.z. $\sum_{k=1}^{n} 2k = n^2 + n$ (per Induktion nach $n$)

Ind.anfang: $n=1$

l.S. $\sum_{k=1}^{1} 2k = 2 \cdot 1 = 2$

r.S. $1^2 + 1 = 2$ ✓

Induktionsschritt: $n \to n+1$

$$\sum_{k=1}^{n+1} 2k = \underbrace{\sum_{k=1}^{n} 2k}_{n^2+n \text{ nach I.V.}} + 2(n+1) = n^2 + n + 2(n+1) = n^2 + 2n + 1 + n + 1$$

$$= (n+1)^2 + n + 1$$

A34 c) z.z. $\sum_{i=0}^{n-1} 2^i = 2^n - 1$

Ind. anfang: $n=1$

l.S. $\sum_{i=0}^{0} 2^i = 2^0 = 1$

r.S. $2^1 - 1 = 2 - 1 = 1$

Induktionsschritt: $n \to n+1$

$$\sum_{i=0}^{n} 2^i = \underbrace{\sum_{i=0}^{n-1} 2^i}_{2^n-1 \text{ nach I.V.}} + 2^n = 2^n - 1 + 2^n = 2 \cdot 2^n - 1 = 2^{n+1} - 1$$

d) z.z. $\sum_{k=0}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$

Ind. anfang: $n=0$

l.S. $\sum_{k=0}^{0} k^2 = 0^2 = 0$

r.S. $\frac{0(0+1)\cdot(2\cdot 0+1)}{6} = 0$

Induktionsschritt: $n \to n+1$

$$\sum_{k=0}^{n+1} k^2 = \underbrace{\sum_{k=0}^{n} k^2}_{\frac{n(n+1)(2n+1)}{6} \text{ nach I.V.}} + (n+1)^2 = \frac{n(n+1)(2n+1)}{6} + (n+1)^2 =$$

$$= \frac{n(n+1)(2n+1) + 6(n+1)^2}{6} = \frac{(n+1)\cdot[n(2n+1) + 6(n+1)]}{6} =$$

$$= \frac{(n+1)\cdot(2n^2+7n+6)}{6} \overset{*)}{=} \frac{(n+1)\cdot(n+2)\cdot(2n+3)}{6}$$

$$= \frac{(n+1)\cdot[(n+1)+1]\cdot[2(n+1)+1]}{6}$$

*) $2n^2+7n+6$ faktorisieren

$2x^2+7x+6 = 0$

$\Rightarrow x_{1/2} = \frac{-7 \pm \sqrt{49 - 4\cdot 2\cdot 6}}{4} = \frac{-7 \pm 1}{4}$

$x_1 = -2$, $x_2 = -\frac{3}{2}$

$\Rightarrow 2x^2+7x+6 = 2(x+2)(x+\frac{3}{2}) = (x+2)(2x+3)$

$\Rightarrow 2n^2+7n+6 = (n+2)(2n+3)$

A34

e) z.z. $\sum_{k=0}^{n} k^3 = \frac{n^2(n+1)^2}{4}$

Ind. anfang: $n=0$

l.S. $\sum_{k=0}^{0} k^3 = 0$

r.S. $\frac{0^2(0+1)^2}{4} = 0$

Induktionsschritt: $n \to n+1$

$$\sum_{k=0}^{n+1} k^3 = \underbrace{\sum_{k=0}^{n} k^3}_{\frac{n^2(n+1)^2}{4} \text{ nach I.V.}} + (n+1)^3 = \frac{n^2(n+1)^2}{4} + (n+1)^3 =$$

$$= \frac{n^2(n+1)^2 + 4(n+1)^3}{4} = \frac{(n+1)^2 \cdot [n^2 + 4(n+1)]}{4} =$$

$$= \frac{(n+1)^2 \cdot [n^2+4n+4]}{4} = \frac{(n+1)^2 \cdot (n+2)^2}{4} = \frac{(n+1)^2 \cdot [(n+1)+1]^2}{4}$$

f) z.z. $\sum_{k=0}^{n} q^k = \frac{1-q^{n+1}}{1-q}$ $(q \neq 1)$

Ind. anfang: $n=0$

l.S. $\sum_{k=0}^{0} q^k = q^0 = 1$

r.S. $\frac{1-q^1}{1-q} = 1$

Induktionsschritt: $n \to n+1$

$$\sum_{k=0}^{n+1} q^k = \underbrace{\sum_{k=0}^{n} q^k}_{\frac{1-q^{n+1}}{1-q} \text{ nach I.V.}} + q^{n+1} = \frac{1-q^{n+1}}{1-q} + q^{n+1} =$$

$$= \frac{1-q^{n+1} + (1-q)q^{n+1}}{1-q} = \frac{1-q^{n+1}+q^{n+1}-q^{n+2}}{1-q} =$$

$$= \frac{1-q^{n+2}}{1-q} = \frac{1-q^{(n+1)+1}}{1-q}$$

A34 g) z.z. $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$

Ind. anfang: $n=0$

l.S. $(a+b)^0 = 1$

r.S. $\sum_{k=0}^{0} \binom{0}{k} a^{0-k} b^k = \binom{0}{0} = 1$

Induktionsschritt: $n \to n+1$

$$\sum_{k=0}^{n+1} \binom{n+1}{k} a^{n+1-k} b^k = \sum_{k=0}^{n} \binom{n+1}{k} a^{n+1-k} b^k + \underbrace{\binom{n+1}{n+1}}_{1} a^0 b^{n+1} =$$

$$= \sum_{k=0}^{n} \binom{n+1}{k} a \cdot a^{n-k} b^k + b^{n+1} = a \cdot \sum_{k=0}^{n} \binom{n+1}{k} a^{n-k} \cdot b^k + b^{n+1} \overset{(*)}{=}$$

Um auf die Summe die I.V. anwenden zu können, muss noch der Binomialkoeffizient $\binom{n+1}{k}$ geeignet umgeformt werden. Dazu verwenden wir die Formel $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$ für $1 \le k \le n$. Da die Formel für $k \ge 1$ gilt, müssen wir in obiger Summen den Summanden für $k=0$ separat schreiben.

$$\overset{(*)}{=} a \cdot \left[ \underbrace{\binom{n+1}{0}}_{1} a^n + \sum_{k=1}^{n} \underbrace{\binom{n+1}{k}}_{\binom{n}{k}+\binom{n}{k-1}} a^{n-k} b^k \right] + b^{n+1} =$$

$$= a \cdot \Big[ \underbrace{a^n + \sum_{k=1}^{n} \binom{n}{k} a^{n-k} b^k}_{\sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k} + \sum_{k=1}^{n} \binom{n}{k-1} a^{n-k} b^k \Big] + b^{n+1} =$$

Indexverschiebung $k \to k-1$

$$= a \cdot \Big[ \underbrace{\sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k}_{(a+b)^n \text{ nach I.V.}} + \sum_{k=0}^{n-1} \binom{n}{k} a^{n-(k+1)} b^{k+1} \Big] + b^{n+1}$$

$$= a \cdot \Big[ (a+b)^n + a^{-1} b \sum_{k=0}^{n-1} \binom{n}{k} a^{n-k} b^k \Big] + b^{n+1} =$$

$$= a \cdot (a+b)^n + b \sum_{k=0}^{n-1} \binom{n}{k} a^{n-k} b^k + b \cdot b^n =$$

$$= a \cdot (a+b)^n + b \cdot \Big[ \underbrace{\sum_{k=0}^{n-1} \binom{n}{k} a^{n-k} \cdot b^k + b^n}_{\sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k = (a+b)^n \text{ nach I.V.}} \Big] = a \cdot (a+b)^n + b(a+b)^n =$$

$$= (a+b)^n \cdot (a+b) = (a+b)^{n+1}$$

(A34) h) z.z. $\binom{n}{k}$ = Anzahl aller $k$-el. Teilmengen einer $n$-el. Menge $M$ (TM = Teilmenge)

Ind. anfang: $n=0$

Dann ist nur $k=0$ möglich. Die $0$-el. Menge $M$ ist die leere Menge um besitzt nur die leere Menge als $0$-el. Teilmenge, d.h. die Anzahl aller $0$-el. TM ist gleich $1$; andererseits ist $\binom{0}{0}=1$.

Induktionsschritt: $n \to n+1$

Sei $M$ eine $(n+1)$-el. Menge. Wir betrachten in $M$ ein fest, aber bel. gewähltes Element $*$ ($*$ bel. Bezeichnung) und teilen die $k$-el. Teilmengen von $M$ wie folgt auf (für $1 \leq k \leq n$)

$K_* = \{$alle $k$-el. TM von $M$ die $*$ enthalten$\}$

$\overline{K_*} = \{$alle $k$-el TM von $M$, die $*$ <u>nicht</u> enthalten$\}$.

Für die Menge $P_k(M)$ aller $k$-el. Teilmengen von $M$ gilt dann

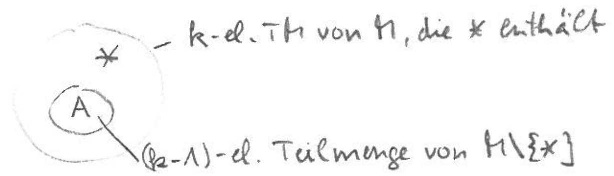
$$P_k(M) = K_* \cup \overline{K_*},$$

wobei zudem $K_* \cap \overline{K_*} = \emptyset$ gilt. Daher folgt die Mächtigkeiten (= Anzahl von Elementen):

$$|P_k(M)| = |K_*| + |\overline{K_*}|$$

Wir wollen nun die Mächtigkeiten $|K_*|$ und $|\overline{K_*}|$ bestimmen:

Jedes Menge aus $K_*$ besteht aus $*$ und $k-1$ Elementen aus $M\setminus\{*\}$




Da $|M\setminus\{*\}|=n$ gilt, gibt es nach I.V. genau $\binom{n}{k-1}$ $(k-1)$-el. TM von $M\setminus\{*\}$. und da es genauso viele $k$-el. TM von $M$ gibt, die $*$ enthalten, folgt

$$|K_*| = \binom{n}{k-1}$$

Da jede Menge aus $\overline{K}_*$ eine $k$-el. TM von $M\setminus\{x\}$ ist und $|M\setminus\{x\}| = n$ ist, folgt (wiederum) aus der I.V.

$$|\overline{K}_*| = \binom{n}{k}$$

Somit folgt insgesamt:

$$|P_k(M)| = |K_*| + |\overline{K}_*| = \binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$$

Da wir für obige Überlegungen $1 \leq k \leq n$ vorausgesetzt haben, müssen jetzt noch die verbleibenden Fälle $k = 0$ und $k = n+1$ betrachtet werden.

$\boxed{k=0}$: $M$ enthält nur 1 0-el. TM, und zwar die leere Menge $\emptyset$; andererseits ist $\binom{n+1}{0} = 1$

$\boxed{k=n+1}$: $M$ enthält nur 1 $(n+1)$-el. TM, und zwar die Menge $M$ selbst; andererseits ist $\binom{n+1}{n+1} = 1$.

A35 a) $\left.\begin{array}{l}56 = 2^3 \cdot 7 \\ 49 = 2^0 \cdot 7^2\end{array}\right\} \Rightarrow \begin{array}{l} ggT(56,49) = 2^0 \cdot 7 = 7 \\ kgV(56,49) = 2^3 \cdot 7^2 = 392\end{array}$

b) $\left.\begin{array}{l}128 = 2^7 \cdot 3^0 \\ 96 = 2^5 \cdot 3^1\end{array}\right\} \Rightarrow \begin{array}{l} ggT(128,96) = 2^5 \cdot 3^0 = 32 \\ kgV(128,96) = 2^7 \cdot 3 = 384\end{array}$

c) $\left.\begin{array}{l}500 = 2^2 \cdot 3^0 \cdot 5^3 \cdot 7^0 \\ 525 = 2^0 \cdot 3^1 \cdot 5^2 \cdot 7^1\end{array}\right\} \Rightarrow \begin{array}{l} ggT(500,525) = 2^0 \cdot 3^0 \cdot 5^2 \cdot 7^0 = 25 \\ kgV(500,525) = 2^2 \cdot 3^1 \cdot 5^3 \cdot 7^1 = 10500\end{array}$

d) $\left.\begin{array}{l}2205 = 3^2 \cdot 5 \cdot 7^2 \cdot 11^0 \\ 22275 = 3^4 \cdot 5^2 \cdot 7^0 \cdot 11^1\end{array}\right\} \Rightarrow \begin{array}{l} ggT(2205,22275) = 3^2 \cdot 5 \cdot 7^0 \cdot 11^0 = 45 \\ kgV(2205,22275) = 3^4 \cdot 5^2 \cdot 7^2 \cdot 11 = 1091475\end{array}$

e) $\left.\begin{array}{l}68600 = 2^3 \cdot 5^2 \cdot 7^3 \cdot 11^0 \\ 67375 = 2^0 \cdot 5^3 \cdot 7^2 \cdot 11 \\ 11011 = 2^0 \cdot 5^0 \cdot 7^1 \cdot 11^2 \cdot 13\end{array}\right\} \Rightarrow \begin{array}{l} ggT(68600,67375,11011) = 2^0 \cdot 5^0 \cdot 7 \cdot 11^0 = 7 \\ kgV(68600,67375,11011) = 2^3 \cdot 5^3 \cdot 7^3 \cdot 11^2 \cdot 13 = \\ = 539539000\end{array}$

A36 a) $ggT(48,162)$

$162 = 3 \cdot 48 + 18 \Rightarrow 6 = -1 \cdot 48 + 3 \cdot (162 - 3 \cdot 48) = 3 \cdot 162 - 10 \cdot 48$

$48 = 2 \cdot 18 + 12 \Rightarrow 6 = 18 - 1 \cdot (48 - 2 \cdot 18) = -1 \cdot 48 + 3 \cdot 18$

$18 = 1 \cdot 12 + 6 \Rightarrow 6 = 18 - 1 \cdot 12$

$12 = 2 \cdot 6 + 0$

$\Rightarrow ggT(48,162) = 6 = 3 \cdot 162 - 10 \cdot 48$

b) $ggT(1323,3087)$

$3087 = 2 \cdot 1323 + 441 \Rightarrow 441 = 3087 - 2 \cdot 1323$

$1323 = 3 \cdot 441 + 0$

$\Rightarrow ggT(1323,3087) = 441 = 3087 - 2 \cdot 1323$

c) $ggT(13475,2541)$

$13475 = 5 \cdot 2541 + 770 \Rightarrow 77 = -3 \cdot 2541 + 10 \cdot (13475 - 5 \cdot 2541) = 10 \cdot 13475 - 53 \cdot 2541$

$2541 = 3 \cdot 770 + 231 \Rightarrow 77 = 770 - 3 \cdot (2541 - 3 \cdot 770) = -3 \cdot 2541 + 10 \cdot 770$

$770 = 3 \cdot 231 + 77 \Rightarrow 77 = 770 - 3 \cdot 231$

$231 = 3 \cdot 77 + 0$

$\Rightarrow ggT(13475,2541) = 77 = 10 \cdot 13475 - 53 \cdot 2541$

A36 d) $ggT(24310, 31395)$

$$31395 = 1\cdot 24310 + 7085 \Rightarrow 65 = -51\cdot 24310 + 175(31395 - 1\cdot 24310) = 175\cdot 31395 - 226\cdot 24310$$

$$24310 = 3\cdot 7085 + 3055 \Rightarrow 65 = 22\cdot 7085 - 51\cdot(24310 - 3\cdot 7085) = -51\cdot 24310 + 175\cdot 7085$$

$$7085 = 2\cdot 3055 + 975 \Rightarrow 65 = -7\cdot 3055 + 22\cdot(7085 - 2\cdot 3055) = 22\cdot 7085 - 51\cdot 3055$$

$$3055 = 3\cdot 975 + 130 \Rightarrow 65 = 975 - 7\cdot(3055 - 3\cdot 975) = -7\cdot 3055 + 22\cdot 975$$

$$975 = 7\cdot 130 + 65 \Rightarrow 65 = 975 - 7\cdot 130$$

$$130 = 2\cdot 65 + 0$$

$$\Rightarrow ggT(24310, 31395) = 65 = 175\cdot 31395 - 226\cdot 24310$$

e) $ggT(242000, 4695327)$

$$4695327 = 19\cdot 242000 + 97327 \Rightarrow 1 = 22014\cdot 242000 - 54737\cdot(4695327 - 19\cdot 242000)$$

$$242000 = 2\cdot 97327 + 47346 \Rightarrow 1 = -10709\cdot 97327 + 22014(242000 - 2\cdot 97327) = 22014\cdot 242000 - 54737\cdot 97327$$

$$97327 = 2\cdot 47346 + 2635 \Rightarrow 1 = 596\cdot 47346 - 10709\cdot(97327 - 2\cdot 47346) = -10709\cdot 97327 + 22014\cdot 47346$$

$$47346 = 17\cdot 2635 + 2551 \Rightarrow 1 = -577\cdot 2635 + 596\cdot(47346 - 17\cdot 2635) = 596\cdot 47346 - 10709\cdot 2635$$

$$2635 = 1\cdot 2551 + 84 \Rightarrow 1 = 19\cdot 2551 - 577(2635 - 1\cdot 2551) = -577\cdot 2635 + 596\cdot 2551$$

$$2551 = 30\cdot 84 + 31 \Rightarrow 1 = -7\cdot 84 + 19(2551 - 30\cdot 84) = 19\cdot 2551 - 577\cdot 84$$

$$84 = 2\cdot 31 + 22 \Rightarrow 1 = 5\cdot 31 - 7\cdot(84 - 2\cdot 31) = -7\cdot 84 + 19\cdot 31$$

$$31 = 1\cdot 22 + 9 \Rightarrow 1 = -2\cdot 22 + 5\cdot(31 - 1\cdot 22) = 5\cdot 31 - 7\cdot 22$$

$$22 = 2\cdot 9 + 4 \Rightarrow 1 = 9 - 2\cdot(22 - 2\cdot 9) = -2\cdot 22 + 5\cdot 9$$

$$9 = 2\cdot 4 + 1 \Rightarrow 1 = 9 - 2\cdot 4$$

$$4 = 4\cdot 1 + 0$$

$$\Rightarrow ggT(242000, 4695327) = -54737\cdot 4695327 + 1062017\cdot 242000$$

**A37** a) in $\mathbb{Z}/4\mathbb{Z}$

$$\bar{3}^2\cdot(\bar{7}-\bar{8})^3 = \bar{9}\cdot(-\bar{1})^3 = -\bar{9} = \underline{\underline{\bar{3}}}$$

b) in $\mathbb{Z}/13\mathbb{Z}$

$$(\bar{8}-\bar{3})^4 - (\bar{4}-\overline{10})^{-1} = \bar{5}^4 - (-\bar{6})^{-1} = \overline{625} - \bar{7}^{-1} =$$

$$= \bar{1} - \bar{2} = -\bar{1} = \underline{\underline{\overline{12}}};$$

Bestimmung von $\bar{7}^{-1}$: $\bar{7}\cdot\bar{7} = \overline{14} = \bar{1}$

bzw. $13 = 1\cdot 7 + 6 \Rightarrow 1 = 7 - 1\cdot(13 - 1\cdot 7) = -1\cdot 13 + 2\cdot 7$

$7 = 1\cdot 6 + 1 \Rightarrow 1 = 7 - 1\cdot 6$

$6 = 6\cdot 1 + 0$

$\Rightarrow 1 = -1\cdot 13 + 2\cdot 7 \Rightarrow \bar{1} = \underbrace{-\bar{1}\cdot\overline{13}}_{0} + \bar{2}\cdot\bar{7} = \bar{2}\cdot\bar{7} \Rightarrow \bar{2} = \bar{7}^{-1}$

c) in $\mathbb{Z}/23\mathbb{Z}$

$$-\frac{8}{9} + \left(\frac{2}{3} - \frac{8}{5}\right)^2 - \left(1 - \frac{1}{18}\right) = -\frac{8}{9} + \left(\frac{10-24}{15}\right)^2 - \frac{17}{18}$$

$$= -\frac{8}{9} + \left(\frac{-14}{15}\right)^2 - \frac{17}{18} = -\frac{8}{9} + \frac{196}{225} - \frac{17}{18} = -\frac{8}{9} + \frac{12}{18} - \frac{17}{18} =$$

$$= \frac{-16+12-17}{18} = -\frac{21}{18} = \frac{2}{18} = 2\cdot\frac{1}{18} = 2\cdot 9 = \underline{\underline{18}},$$

$\hookrightarrow \frac{1}{9} = \underline{\underline{18}}$

Bestimmung von $\frac{1}{18}$:

$23 = 1\cdot 18 + 5 \Rightarrow 1 = 2\cdot 18 - 7\cdot(23 - 1\cdot 18) = -7\cdot 23 + 9\cdot 18$

$18 = 3\cdot 5 + 3 \Rightarrow 1 = -1\cdot 5 + 2\cdot(18 - 3\cdot 5) = 2\cdot 18 - 7\cdot 5$

$5 = 1\cdot 3 + 2 \Rightarrow 1 = 3 - 1\cdot(5 - 1\cdot 3) = -1\cdot 5 + 2\cdot 3$

$3 = 1\cdot 2 + 1 \Rightarrow 1 = 3 - 1\cdot 2$

$2 = 2\cdot 1 + 0$

$\Rightarrow \frac{1}{18} = 9$ (in $\mathbb{Z}/23\mathbb{Z}$) $\left(\Rightarrow \frac{1}{9} = 18\right)$

d, in $\mathbb{Z}/7\mathbb{Z}$

$$\left[(-3)^2\right]^{-3} - \left(-\frac{2}{5}\right)^4 + \frac{1}{6} = 9^{-3} - \frac{16}{625} + \frac{1}{6} =$$

$$= \frac{1}{2^3} - \frac{2}{2} + \frac{1}{6} = \frac{1}{8} - 1 + \frac{1}{6} = \frac{1}{1} - 1 + \frac{1}{6} = \frac{1}{6} = \underline{\underline{6}}$$

Bestimmung von $\frac{1}{6}$:

$7 = 1 \cdot 6 + 1 \implies 1 = 7 - 1 \cdot 6 \implies \frac{1}{6} = -1 = 6$

---

allg.: $(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{k} \mid 1 \le k \le n-1,\ ggT(k,n) = 1\}$ Einheiten

A38 a)

i) $(\mathbb{Z}/4\mathbb{Z})^\times = \{\bar{1}, \bar{3}\}$ ; $\bar{1}^{-1} = \bar{1}$, $\bar{3}^{-1} = \bar{3}$, da $\bar{3} \cdot \bar{3} = \bar{9} = \bar{1}$.

ii) $(\mathbb{Z}/6\mathbb{Z})^\times = \{\bar{1}, \bar{5}\}$ ; $\bar{1}^{-1} = \bar{1}$, $\bar{5}^{-1} = \bar{5}$, da $\bar{5} \cdot \bar{5} = \overline{25} = \bar{1}$

iii) $(\mathbb{Z}/7\mathbb{Z})^\times = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$ ; $\bar{1}^{-1} = \bar{1}$, $\bar{2}^{-1} = \bar{4}$ da $\bar{2} \cdot \bar{4} = \bar{8} = \bar{1}$

$\bar{3}^{-1} = \bar{5}$, da $\bar{3} \cdot \bar{5} = \overline{15} = \bar{1}$

$\bar{4}^{-1} = \bar{2}$, $\bar{5}^{-1} = \bar{3}$.

iv) $(\mathbb{Z}/8\mathbb{Z})^\times = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$ ; $\bar{1}^{-1} = \bar{1}$, $\bar{3}^{-1} = \bar{3}$ da $\bar{3} \cdot \bar{3} = \bar{9} = \bar{1}$

$\bar{5}^{-1} = \bar{5}$, da $\bar{5} \cdot \bar{5} = \overline{25} = \bar{1}$

$\bar{7}^{-1} = \bar{7}$ da $\bar{7} \cdot \bar{7} = \bar{1}$

v) $(\mathbb{Z}/9\mathbb{Z})^\times = \{\bar{1}, \bar{2}, \bar{4}, \bar{5}, \bar{7}, \bar{8}\}$, $\bar{1}^{-1} = \bar{1}$, $\bar{2}^{-1} = \bar{5}$ da $\bar{2} \cdot \bar{5} = \overline{10} = \bar{1}$

$\bar{4}^{-1} = \bar{7}$, da $\bar{4} \cdot \bar{7} = \overline{28} = \bar{1}$

$\bar{5}^{-1} = \bar{2}$, $\bar{7}^{-1} = \bar{4}$, $\bar{8}^{-1} = \bar{8}$ da $\bar{8} \cdot \bar{8} = \overline{64} = \bar{1}$

vi) $(\mathbb{Z}/12\mathbb{Z})^\times = \{\bar{1}, \bar{5}, \bar{7}, \overline{11}\}$ ; $\bar{1}^{-1} = \bar{1}$, $\bar{5}^{-1} = \bar{5}$ da $\bar{5} \cdot \bar{5} = \overline{25} = \bar{1}$

$\bar{7}^{-1} = \bar{7}$ da $\bar{7} \cdot \bar{7} = \overline{49} = \bar{1}$,

$\overline{11}^{-1} = \overline{11}$, da $\overline{11} \cdot \overline{11} = \overline{121} = \bar{1}$

A38 a) vii) $(\mathbb{Z}/15\mathbb{Z})^{\times} = \{\bar{1}, \bar{2}, \bar{4}, \bar{7}, \bar{8}, \overline{11}, \overline{13}, \overline{14}\}$

$\bar{1}^{-1} = \bar{1}$, $\bar{2}^{-1} = \bar{8}$, da $\bar{2}\cdot\bar{8} = \overline{16} = \bar{1}$, $\bar{4}^{-1} = \bar{4}$ da $\bar{4}\cdot\bar{4} = \overline{16} = \bar{1}$

$\bar{7}^{-1} = \overline{13}$ da $\bar{7}\cdot\overline{13} = \overline{91} = \bar{1}$, $\bar{8}^{-1} = \bar{2}$, $\overline{11}^{-1} = \overline{11}$ da $\overline{11}\cdot\overline{11} = \overline{121} = \bar{1}$

$\overline{13}^{-1} = \bar{7}$, $\overline{14}^{-1} = \overline{14}$ da $\overline{14}\cdot\overline{14} = \overline{196} = \bar{1}$

viii) $(\mathbb{Z}/30\mathbb{Z})^{\times} = \{\bar{1}, \bar{7}, \overline{11}, \overline{13}, \overline{17}, \overline{19}, \overline{23}, \overline{29}\}$

$\bar{1}^{-1} = \bar{1}$, $\bar{7}^{-1} = \overline{13}$ da $\bar{7}\cdot\overline{13} = \overline{91} = \bar{1}$, $\overline{11}^{-1} = \overline{11}$ da $\overline{11}\cdot\overline{11} = \overline{121} = \bar{1}$

$\overline{13}^{-1} = \bar{7}$, $\overline{17}^{-1} = \overline{23}$ da $\overline{17}\cdot\overline{23} = \overline{391} = \bar{1}$, $\overline{19}^{-1} = \overline{19}$ da $\overline{19}\cdot\overline{19} = \overline{361} = \bar{1}$

$\overline{29}^{-1} = \overline{29}$ da $\overline{29}\cdot\overline{29} = \overline{841} = \bar{1}$

b) Bestimme $\overline{13}^{-1}$ in $\mathbb{Z}/9757\mathbb{Z}$

$= 5\cdot 9757 - 3768\cdot 13$

$$9757 = 753\cdot 13 + 8 \Rightarrow 1 = -3\cdot 13 + 5\cdot(9757 - 753\cdot 13) =$$
$$13 = 1\cdot 8 + 5 \Rightarrow 1 = 2\cdot 8 - 3(13 - 1\cdot 8) = -3\cdot 13 + 5\cdot 8$$
$$8 = 1\cdot 5 + 3 \Rightarrow 1 = -1\cdot 5 + 2\cdot(8 - 1\cdot 5) = 2\cdot 8 - 3\cdot 5$$
$$5 = 1\cdot 3 + 2 \Rightarrow 1 = 3 - 1\cdot(5 - 1\cdot 3) = -1\cdot 5 + 2\cdot 3$$
$$3 = 1\cdot 2 + 1 \Rightarrow 1 = 3 - 1\cdot 2$$
$$2 = 2\cdot 1 + 0$$

$$\Rightarrow 1 = 5\cdot 9757 - 3768\cdot 13$$

$$\Rightarrow \bar{1} = \underbrace{\overline{5\cdot 9757}}_{\bar{0}} - \overline{3768\cdot 13}$$

$$\Rightarrow \overline{13}^{-1} = \overline{-3768} = \overline{-3768 + 9757} = \overline{6029};$$

(A39) $N = p \cdot q = 13 \cdot 17 = 221$ ; $e = 35$

$\varphi(N) = (p-1)(q-1) = 12 \cdot 16 = 192$

a) z.z. $\overline{e}$ ist eine Einheit in $\mathbb{Z}/\varphi(N)\mathbb{Z}$

$$\left.\begin{aligned} e &= 35 = 5 \cdot 7 \\ 192 &= 2^6 \cdot 3 \end{aligned}\right\}$$ 35 und 192 sind teilerfremd $\Rightarrow$ e ist ein öffentliche Schlüssel

d ist geheimer Schlüssel, wenn $\overline{d} = \overline{e}^{-1}$ in $\mathbb{Z}/\varphi(N)\mathbb{Z}$ gilt.

Bestimme d mit Hilfe des erweiterten Euklidischen Algorithmus:

$192 = 5 \cdot 35 + 17 \quad \Rightarrow 1 = 35 - 2 \cdot (192 - 5 \cdot 35) = -2 \cdot 192 + 11 \cdot 35$

$35 = 2 \cdot 17 + 1 \quad \Rightarrow 1 = 35 - 2 \cdot 17$

aus $1 = -2 \cdot 192 + 11 \cdot 35$ folgt: $\overline{11} = \overline{35}^{-1}$ in $\mathbb{Z}/192\mathbb{Z}$.

$\Rightarrow$ geheime Schlüssel $d = 11$.

b)

| ASCII-Code | Zeichen |
|---|---|
| 65 | A |
| 66 | B |
| ⋮ | ⋮ |
| 82 | R |
| 83 | S |

Verschlüsseln:

$R \mathrel{\hat{=}} 82 \qquad 82^{35} \bmod 221 = 82^{2 \cdot 17 + 1} \bmod 221 =$

$= (82^2)^{17} \cdot 82 \bmod 221 = 94^{17} \cdot 82 \bmod 221$

$= 94^{2 \cdot 8 + 1} \cdot 82 \bmod 221 = (94^2)^8 \cdot 94 \cdot 82 \bmod 221$

$= 217^8 \cdot 194 \bmod 221 = (217^2)^4 \cdot 194 \bmod 221$

$= 16^4 \cdot 194 \bmod 221 = 120 \cdot 194 \bmod 221 = 75 \bmod 221$

$75 \mathrel{\hat{=}} K$

zu A25 b,

$S \mathrel{\hat{=}} 83 \qquad 83^{35} \bmod 221 = 83^{2\cdot 17+1} \bmod 221 = (83^2)^{17}\cdot 83 \bmod 221$

$= 38^{17}\cdot 83 \bmod 221 = 38^{2\cdot 8+1}\cdot 83 \bmod 221 = (38^2)^8\cdot 38\cdot 83 \bmod 221$

$= 118^8\cdot 38\cdot 83 \bmod 221 = (118^2)^4\cdot 60 \bmod 221 =$

$= 1^4\cdot 60 \bmod 221 = 60 \bmod 221$

$60 \mathrel{\hat{=}} <$

$A \mathrel{\hat{=}} 65 \qquad 65^{35} \bmod 221 = 65^{2\cdot 17+1} \bmod 221 = (65^2)^{17}\cdot 65 \bmod 221 =$

$= 26^{17}\cdot 65 \bmod 221 = 26^{2\cdot 8+1}\cdot 65 \bmod 221 = (26^2)^8\cdot 26\cdot 65 \bmod 221$

$= 13^8\cdot 143 \bmod 221 = (13^2)^4\, 143 \bmod 221 = 169^4\cdot 143 \bmod 221$

$= 52\cdot 143 \bmod 221 = 143 \bmod 221$

$143 \mathrel{\hat{=}} \AA$

$RSA \longrightarrow K < \AA$ (verschlüsseln)

Entschlüsseln

$K \mathrel{\hat{=}} 75 \qquad 75^{11} \bmod 221 = 75^{2\cdot 5+1} \bmod 221 =$

$= (75^2)^5\cdot 75 \bmod 221 = 100^5\cdot 75 \bmod 221 =$

$= 100^{2\cdot 2+1}\cdot 75 \bmod 221 = (100^2)^2\cdot 100\cdot 75 \bmod 221$

$= 55^2\cdot 207 \bmod 221 = 152\cdot 207 \bmod 221 = 82 \bmod 221$

$82 \mathrel{\hat{=}} R$

$< \mathrel{\hat{=}} 60 \qquad 60^{11} \bmod 221 = 60^{2\cdot 5+1} \bmod 221 = (60^2)^5\cdot (60) \bmod 221$

$= 64^5\cdot 60 \bmod 221 = 64\cdot 60 \bmod 221 = 83 \bmod 221$

$83 \mathrel{\hat{=}} S$

$\AA \mathrel{\hat{=}} 143 \qquad 143^{11} \bmod 221 = 143^{2\cdot 5+1} \bmod 221 = (143^2)^5\cdot 143 \bmod 221$

$= 117^5\cdot 143 \bmod 221 = 117^{2\cdot 2+1}\cdot 143 \bmod 221 =$

$= (117^2)^2\cdot 117\cdot 143 \bmod 221 = 208^2\cdot 156 \bmod 221 = 65 \bmod 221$

$65 \mathrel{\hat{=}} A$

A40

a)

$$99 = 33 \cdot 3 + 0$$
$$33 = 11 \cdot 3 + 0$$
$$11 = 3 \cdot 3 + 2$$
$$3 = 1 \cdot 3 + 0$$
$$1 = 0 \cdot 3 + 1$$

$\Rightarrow (99)_3 = 10200$

b)

$$645 = 80 \cdot 8 + 5$$
$$80 = 10 \cdot 8 + 0$$
$$10 = 1 \cdot 8 + 2$$
$$1 = 0 \cdot 8 + 1$$

$\Rightarrow (645)_8 = 1205$

c)

$$2048 = 128 \cdot 16 + 0$$
$$128 = 8 \cdot 16 + 0$$
$$8 = 0 \cdot 16 + 8$$

$\Rightarrow$

$2048 = (800)_{16}$

d)

$$1234 = 617 \cdot 2 + 0$$
$$617 = 308 \cdot 2 + 1$$
$$308 = 154 \cdot 2 + 0$$
$$154 = 77 \cdot 2 + 0$$
$$77 = 38 \cdot 2 + 1$$
$$38 = 19 \cdot 2 + 1$$
$$19 = 9 \cdot 2 + 1$$
$$9 = 4 \cdot 2 + 1$$
$$4 = 2 \cdot 2 + 0$$
$$2 = 1 \cdot 2 + 0$$
$$1 = 0 \cdot 2 + 1$$

$\Rightarrow 1234 =$
$= (10011110010)_2$

e)

$$(756)_8 = 6 + 5 \cdot 8 + 7 \cdot 8^2 = 494$$

$$494 = 98 \cdot 5 + 4$$
$$98 = 19 \cdot 5 + 3$$
$$19 = 3 \cdot 5 + 4$$
$$3 = 0 \cdot 5 + 3$$

$\Rightarrow (756)_8 = (3434)_5$

f)

$$(10AD)_{16} = 13 + 10 \cdot 16 + 1 \cdot 16^3 = 4269$$

$$4269 = 533 \cdot 8 + 5$$
$$533 = 66 \cdot 8 + 5$$
$$66 = 8 \cdot 8 + 2$$
$$8 = 1 \cdot 8 + 0$$
$$1 = 0 \cdot 8 + 1$$

$\Rightarrow (10AD)_{16} = (10255)_8$

g)

$$(121212)_3 = 455$$

$$455 = 227 \cdot 2 + 0$$
$$227 = 113 \cdot 2 + 1$$
$$113 = 56 \cdot 2 + 1$$
$$56 = 28 \cdot 2 + 0$$
$$28 = 14 \cdot 2 + 0$$
$$14 = 7 \cdot 2 + 0$$
$$7 = 3 \cdot 2 + 1$$
$$3 = 1 \cdot 2 + 1$$
$$1 = 0 \cdot 2 + 1$$

$\Rightarrow (121212)_3 = (111000110)_2$

h)

$$(33333)_4 = 1023$$

$$1023 = 63 \cdot 16 + 15$$
$$63 = 3 \cdot 16 + 15$$
$$3 = 0 \cdot 16 + 3$$

$\Rightarrow$

$(33333)_4 = (3FF)_{16}$

A40 k) $(1011011101)_2$

$\rightarrow$ 16-adisch (direkt)

$$\begin{array}{ccc} 3 & 13 & 13 \\ 0011 & 1101 & 1101 \\ 3 & D & D \end{array}$$

$\Rightarrow (1011011101)_2 = (3DD)_{16}$

l) $(AF381ED90D)_{16} \rightarrow$ 2-adisch

$$\begin{array}{cccccccccc} A & F & 3 & 8 & 1 & E & D & 9 & 0 & D \\ 1010 & 1111 & 0011 & 1000 & 0001 & 1110 & 1101 & 1001 & 0000 & 1101 \end{array}$$

$\Rightarrow (AF381ED90D)_{16} =$

$= (1010111100111000000111101101100100001101)_2$