# Seite 6, Lösung der Übungen

Übung 1: Gesucht ist der ggT(217, 63)

$$217 = 3 \cdot 63 + 28$$
$$63 = 2 \cdot 28 + (7)$$
$$28 = 4 \cdot 7$$

↑ Der letzte nicht verschwindende Rest ist der ggT(217, 63).

Stelle den ggT(217, 63) als Vielfachensumme der Zahlen 217 und 63 dar:

$$7 = 63 - 2 \cdot 28$$
$$= 63 - 2 \cdot (217 - 3 \cdot 63)$$
$$= 63 - 2 \cdot 217 + 6 \cdot 63$$
$$= (-2) \cdot 217 + 7 \cdot 63 \quad \text{(1. Darstellung)}$$

$$+ \left\{ \begin{array}{l} 0 = 63 \cdot 217 - 217 \cdot 63 \end{array} \right.$$

$$7 = 61 \cdot 217 - 210 \cdot 63 \quad \text{(2. Darstellung)}$$

Übung 2: Gesucht ist der

ggT(672, 105)

$672 = 6 \cdot 105 + 42$

$105 = 2 \cdot 42 + 21$

$42 = 2 \cdot 21$

Der letzte nicht verschwindende Rest ist der ggT(672, 105).

Stelle den ggT(672, 105) = 21 als Vielfachsumme von 672 und 105 dar:

$21 = 105 - 2 \cdot 42$

$= 105 - 2 \cdot (672 - 6 \cdot 105)$

$= (-2) \cdot 672 + 13 \cdot 105$ (1. Darstellung)

$+ \{ 0 = 105 \cdot 672 - 672 \cdot 105$

$21 = 103 \cdot 672 - 659 \cdot 105$ (2. Darstellung)

Ergänzung zu Übung 1/2 auf Seite 6

Alternative Möglichkeit, ohne ggT mehrfach Vielfache zu subtrahieren:

Übung 1: Schritte

$\begin{pmatrix} 217 \\ 1 \\ 0 \end{pmatrix}$ ($217 = 1 \cdot 217 + 0 \cdot 63$)

$\begin{pmatrix} 63 \\ 0 \\ 1 \end{pmatrix}$ ($63 = 0 \cdot 217 + 1 \cdot 63$)

Bilde nun sukzessive

$$\begin{pmatrix} 217 \\ 1 \\ 0 \end{pmatrix} - 3 \cdot \begin{pmatrix} 63 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 28 \\ 1 \\ -3 \end{pmatrix} \quad (28 = 1 \cdot 217 - 3 \cdot 63)$$

$$\begin{pmatrix} 63 \\ 0 \\ 1 \end{pmatrix} - 2 \cdot \begin{pmatrix} 28 \\ 1 \\ -3 \end{pmatrix} = \begin{pmatrix} 7 \\ -2 \\ 7 \end{pmatrix} \quad (7 = (-2) \cdot 217 + 7 \cdot 63)$$

$$\begin{pmatrix} 28 \\ 1 \\ -3 \end{pmatrix} - 4 \cdot \begin{pmatrix} 7 \\ -2 \\ 7 \end{pmatrix} = \begin{pmatrix} 0 \\ 9 \\ -31 \end{pmatrix}$$

Vektor

Das ist der letzte Vektor mit 1. Komponente $\neq 0$.

Von diesem Vektor die 1. Komponente ist der ggT(217, 63).
Die Vielfache seiner Komponenten wurde mitgeliefert.

Übung 2:

$$\begin{pmatrix} 672 \\ 1 \\ 0 \end{pmatrix} - 6 \cdot \begin{pmatrix} 105 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 42 \\ 1 \\ -6 \end{pmatrix}$$

$$\begin{pmatrix} 105 \\ 0 \\ 1 \end{pmatrix} - 2 \cdot \begin{pmatrix} 42 \\ 1 \\ -6 \end{pmatrix} = \begin{pmatrix} 21 \\ -2 \\ 13 \end{pmatrix}$$

$$\begin{pmatrix} 42 \\ 1 \\ -6 \end{pmatrix} - 2 \cdot \begin{pmatrix} 21 \\ -2 \\ 13 \end{pmatrix} = \begin{pmatrix} 0 \\ 5 \\ -32 \end{pmatrix}$$

Das ist der entscheidende Vektor.

$$ggT(672, 105) = 21$$

Vielfache Summe darstellen:

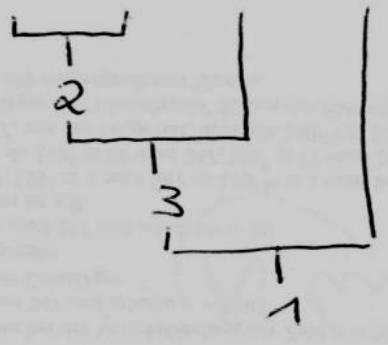
$$21 = -2 \cdot 672 + 13 \cdot 105$$

Das alternative Verfahren zum Bestimmen des ggT und der Vielfachensumme darstellen ist effektiv und sehr einfach in einem Programm umsetzbar.

**Seite 12 – Beispiele :**

Beispiel 1 :

$$5 + 3 + 1 + 4 = 1$$

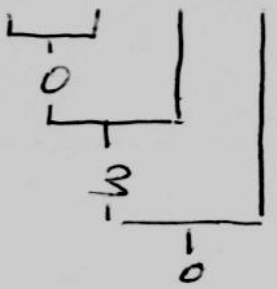



Beispiel 2 : Was bedeutet $4 \cdot 3$ ?

$$4 \cdot 3 = \underbrace{3 + 3 + 3 + 3}_{\text{4 x aufaddiert}}$$

Somit gilt in $\mathbb{Z}_6$ :

$$4 \cdot 3 = 3 + 3 + 3 + 3 = 0$$




Frage 1: $-3$ ist die Zahl, die zu $+3$ addiert $0$ ergibt.
$-10.5$ ist die Zahl, die zu $+10.5$ addiert $0$ ergibt

Beispiel 3 : $-3$ in $\mathbb{Z}_5$ ist die Zahl, die zu 3 addiert $0$ ergibt, also $2 \Rightarrow -3 = 2$ in $\mathbb{Z}_5$.
$-5$ in $\mathbb{Z}_6$ ist die Zahl, die zu 5 addiert $0$ ergibt, also $1 \Rightarrow -5 = 1$ in $\mathbb{Z}_6$.

Beispiel 4: $4 - 3 \cdot 2 + 1 =$

$4 - (2+2+2) + 1 = 4 + (-(2+2+2)) + 1 =$

$4 + (-1) + 1 = 4 + 4 + 1$

$= 3 + 1 = 4$

Frage 2: $\frac{1}{2}$ ist die rationale Zahl, die mit 2 multipliziert 1 ergibt. Analog sind $\frac{1}{38}$ und $\frac{1}{265}$ definiert.

Beispiel 5: $\frac{1}{3}$ in $\mathbb{Z}_5$ ist die Zahl, die mit 3 multipliziert 1 ergibt. Laut Multiplikationstabelle $\mathbb{Z}_5$ ist $\frac{1}{3} = 2$.

$\frac{1}{4}$ in $\mathbb{Z}_5$ ist die Zahl, die mit 4 multipliziert 1 ergibt also 4.

Beispiel 6: $\frac{1}{3} - \frac{1}{2} + 4 = 2 + (-3) + 4$

$= 2 + 2 + 4$

$= 3$

$\frac{2}{3} - \frac{3}{4} + 2 = 2 \cdot \frac{1}{3} + \left(-3 \cdot \frac{1}{4}\right) + 2 =$

$2 \cdot 2 + (-3 \cdot 4) + 2 = 2 \cdot 2 + (-2) + 2 =$

$4 + 3 + 2 = 2 + 2 = 4$

**Beispiel 7 :**

Wir wollen wissen, was $38^{67}$ mod 3 ist. $38^{67}$ mod 3 ist in Elmt der Menge $\mathbb{Z}_3 = \{0,1,2\}$. Wir gehen zur Beantwortung der Frage in 3 Schritten vor

1. Schritt: 38 läßt beim Teilen durch 3 den Rest 2. Damit ist $38 \in [2]$ = äquivalenz bzgl. der Teilung durch 3 zum Rest 2.

2. Schritt: Statt $38^{67}$ muß also "nur" $2^{67}$ betrachtet werden und zwar in der Menge $\mathbb{Z}_3$. Anhäufung multiplikationstabelle $\mathbb{Z}_3$ liefert sich

$2^1 = 2 \quad 2^3 = 2 \quad 2^5 = 2 \ldots\ldots$

$2^2 = 1 \quad 2^4 = 1 \quad 2^6 = 1 \ldots\ldots$

3. Schritt: Ersetzen die Exponenten möglichst

$2^{\text{ungerade Zahl}} = 2$ in $\mathbb{Z}_3$

$2^{\text{gerade Zahl}} = 1$ in $\mathbb{Z}_3$,

also

$2^{67} = 2$ mod 3 damit

$2^{67}$ mod 3 = $38^{67}$ mod 3

liefert.

**Beispiel 8 : Die Frage lautet $57^{183}$ mod 5 = ?**

1. Schritt: 57 entspricht der 2 in $\mathbb{Z}_5$.

2. Schritt: Bilde $2^{183}$ in $\mathbb{Z}_5$

$2^1 = 2$ $2^5 = 2$ ……

$2^2 = 4$ $2^6 = 4$ ……

$2^3 = 3$ $2^7 = 3$ ……

$2^4 = 1$ $2^8 = 1$ ……

3. Schritt: In welcher der 4 Reihen wird $2^{183}$ erscheinen?

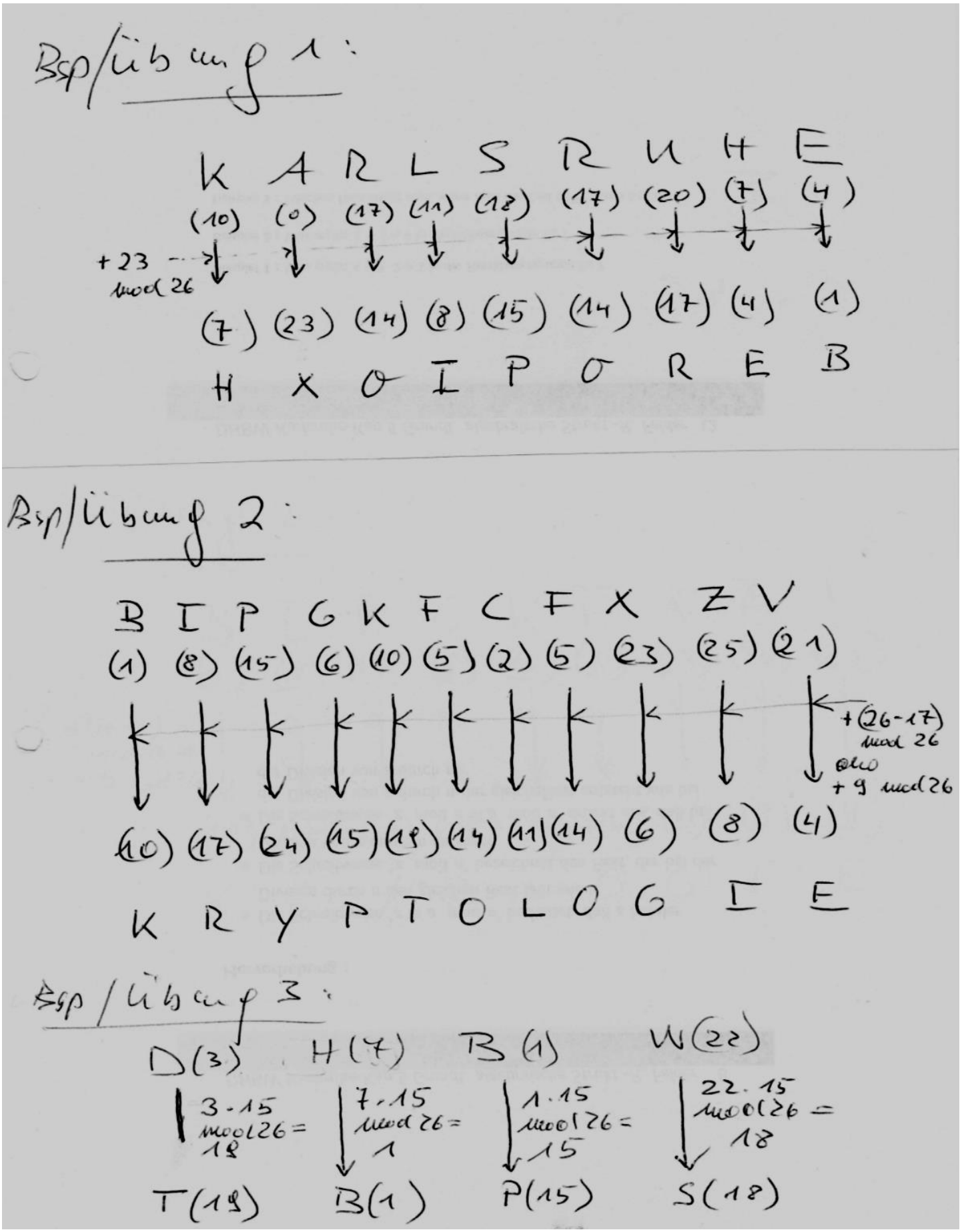
Erkenne

- in der 1. Reihe kommen alle Exponenten vor, die durch 4 geteilt den Rest 1 ergeben
- in der 2. Reihe kommen alle Exponenten vor, die durch 4 geteilt den Rest 2 ergeben
- In der 3. Reihe kommen alle Exponenten vor, die durch 4 geteilt den Rest 3 ergeben
- In der 4. Reihe kommen alle durch 4 teilbaren Exponenten vor

$2^{183}$ wird in der 3. Reihe erscheinen

$\Rightarrow 2^{183} \bmod 5 = 57^{183} \bmod 5 = 3$

# Seite 17 : Lösungen zu den Übungen



# Seite 31 : Ausführung der Beispiele zur Polynomdivision

(1) $(x^3+2x) : (x+1) = x^2 - x + 3$

$-x^3 \pm x^2$

$-x^2+2x$

$\mp x^2 \mp x$

$3x$

$-3x \pm 3$

$-3$ $\Longrightarrow$

$x^3+2x = (x^2-x+3)\cdot(x+1) + (-3)$

$= p(x)$ $= s(x)$ $= q(x)$ $= r(x)$

(2) $(x^3+1) : (x+1) = x^2 - x + 1$

$-x^3 \pm x^2$

$-x^2+1$

$\mp x^2 \mp x$

$x+1$

$x+1$

$0$ $\Longrightarrow$

$x^3+1 = (x^2-x+1)\cdot(x+1) + 0$

$= p(x)$ $= s(x)$ $= q(x)$ $= r(x)$

(3) $(x^3+1):(x+1) = x^2+x+1$

$-x^3 \pm x^2$

$-x^2+1$

$\hookrightarrow x^2+1$

$-x^2 \pm x$

$-x+1$

$\hookrightarrow x+1$

$-x \pm 1$

$0$ $\Longrightarrow$

$$\underbrace{x^3+1}_{=P(x)} = \underbrace{(x^2+x+1)}_{=S(x)} \cdot \underbrace{(x+1)}_{=q(x)} + \underbrace{0}_{=r(x)}$$

(4) $(x^3+2x+2):(x+4) = x^2+x+3$

$-x^3 \pm 4x^2$

$-4x^2+2x+2$

$\hookrightarrow x^2+2x+2$

$-x^2 \pm 4x$

$-2x+2$

$\hookrightarrow 3x+2$

$-3x \pm 2$

$0$ $\longrightarrow$

$$\underbrace{x^3+2x+2}_{P(x)} = \underbrace{(x^2+x+3)}_{S(x)} \cdot \underbrace{(x+4)}_{q(x)} + \underbrace{0}_{r(x)}$$

(5) $(x^3+2x+2) : (x+4) = x^2+3x+4$

$-x^3 \pm 4x^2$

$(-4x^2+2x+2)$

$3x^2+2x+2$

$-3x^2 \pm 12x$

$(-10x+2)$

$4x+2$

$-4x \pm 16$

$(-14)$

$\circ$

Probe: $(x^2+3x+4)\cdot(x+4) =$

$x^3+7x^2+16x+16 =$

$x^3+2x+2$

(6) $(x^3+2x+2) : (x+4) = x^2+7x+7$

$-x^3 \pm 4x^2$

$(-4x^2+2x+2)$

$7x^2+2x+2$

$-7x^2 \pm 28x$

$(-26x+2)$

$7x+2$

$-7x \pm 28$

$(-26)$

$\rightarrow$

$7$

$\underbrace{x^3+2x+2}_{P(x)} = \underbrace{(x^2+7x+7)}_{S(x)} \cdot \underbrace{(x+4)}_{q(x)} + \underbrace{7}_{r(x)}$

# Seite 31 : Ausführung der Beispiele zur ggT-Bestimmung

(1) $(x^3+3x^2-28x-60) : (x^3+7x^2+4x-12) = 1$

$-x^3 \pm 7x^2 \pm 4x \mp 12$

$-4x^2-32x-48$

$(x^3+7x^2+4x-12) : (-4x^2-32x-48) = -\frac{1}{4}x$

$-x^3 \pm 8x^2 \pm 12x$

$-x^2-8x-12$

$(-4x^2-32x-48) : (-x^2-8x-12) = 4$

$\mp 4x^2 \mp 32x \mp 48$

$0$

$\Rightarrow$ Der letzte nicht verschwindende Rest ist das Polynom

$-x^2-8x-12$

$\Rightarrow ggT(\ldots,\ldots) = x^2+8x+12$

Zur Beachtung: Der ggT zweier Polynome ist normiert, d.h. der Koeffizient der höchsten x-Potenz ist 1.

(2) $(x^3+x^2+x+1) : (x^3+x+1) = 1$

$-x^3+x+1$

$x^2$

$(x^3+x+1) : x^2 = x$

$-x^3$

$x+1$

$x^2 : (x+1) = x$

$-x^2+x$

$x$

$(x+1) : x = 1$

$-x$

$1$

$x : 1 = x$

$-x$

$0$

$\Rightarrow$ Der letzte nicht verschwindende Rest ist 1 $\Rightarrow$

$ggT(\dots,\dots) = 1$