

Codierungstheorie Übungsblatt 7

Aufgabe 1

a) Wir zeigen $\text{ggf}(m+n, m) = \text{ggf}(m, n)$ mithilfe des euklid. Algorithmus und einer Fallunterscheidung.

1. Fall: $m \geq n$

Wir nutzen die ersten Schritte im euklid. Algorithmus und erhalten für $\text{ggf}(m+n, m)$:

$$m+n = \cancel{a_1} \cdot m + n \Rightarrow m = a_1 \cdot n + \cancel{m \bmod n}$$

Für $\text{ggf}(m, n)$ erhalten wir, da $m \geq n$:

$$m = a_2 \cdot n + \cancel{n \bmod m} \bmod n$$

Es ist offensichtlich, dass $a_1 = a_2$ gilt, und somit haben wir gezeigt, dass der euklidische Algorithmus in beiden Fällen auf die selben Schritte kommt. Damit kommt der Algorithmus auch in beiden Fällen auf die selbe Antwort und $\text{ggf}(m+n, m) = \text{ggf}(m, n)$ gilt.

2. Fall: $n \geq m$

Wir nutzen wieder den euklid. Algorithmus ~~für $m+n, m$~~ für $\text{ggf}(m+n, m)$:

$$m+n = a_1 \cdot m + \cancel{m \bmod (m+n)} \bmod m$$

Wir setzen $r := m \bmod (m+n)$. Dann gilt:

$$m+n = a_1 \cdot m + r \quad | -m$$

$$n = (a_1 - 1)m + r$$

$$n = (a_1 - 1)m + \cancel{m \bmod n} \bmod m$$

Wir nutzen nun ebenfalls wieder den euklid. Algorithmus für $\text{ggf}(m, n) = \text{ggf}(n, m)$:

$$n = a_2 \cdot m + \cancel{m \bmod n} \bmod m$$

Es ist offensichtlich, dass $a_2 = (a_1 - 1)$ gilt. In beiden Fällen erhalten wir deshalb im 2. Schritt des euklid. Algorithmus:

$$m = a_3 \cdot (m \bmod n) + \cancel{m \bmod (m \bmod n)} \bmod m$$

Da beide auf den selben Schritt im euklid. Algorithmus kommen, gilt auch in diesem Fall: $\text{ggf}(m+n, m) = \text{ggf}(m, n)$.

Da $m \geq n \vee m \leq n$, gilt $\text{ggf}(m+n, m) = \text{ggf}(m, n)$ für alle m und n in den natürlichen Zahlen.

Aufgabe 2

Wir berechnen die Inversen von Elementen in Primkörpern mithilfe des erweiterten euklidischen Algorithmus:

$$467 = 3 \cdot 144 + 29 \Rightarrow 29 = 467 - 3 \cdot 144$$

$$144 = 4 \cdot 29 + 28 \Rightarrow 28 = 144 - 4 \cdot 29$$

$$29 = 7 \cdot 28 + 1 \Rightarrow 1 = 29 - 7 \cdot 28$$

$$28 = 28 \cdot 1 + 0$$

$$1 = 29 - 7 \cdot 28 = 29 - 1 \cdot (144 - 4 \cdot 29)$$

$$= 5 \cdot 29 - 1 \cdot 144$$

$$= 5 \cdot (467 - 3 \cdot 144) - 1 \cdot 144$$

$$= 5 \cdot 467 - 16 \cdot 144$$

$$\Rightarrow 1 \equiv -16 \cdot 144 \pmod{467}$$

$$\Rightarrow \frac{1}{144} \equiv -16 \equiv \frac{445}{728} \pmod{467}$$

$$\Rightarrow a = \frac{1}{144} = \frac{445}{\cancel{88} \cancel{-728}}$$

$$\text{ges.: } b = \frac{77}{365}$$

$$\begin{aligned} 467 &= 7 \cdot 365 + 96 \Rightarrow 96 = 467 - 7 \cdot 365 \\ 365 &= 3 \cdot 96 + 77 \Rightarrow 77 = 365 - 3 \cdot 96 \\ 96 &= 7 \cdot 77 + 19 \Rightarrow 19 = 96 - 77 \\ 77 &= 4 \cdot 19 + 7 \Rightarrow 7 = 77 - 4 \cdot 19 \\ 19 &= 19 \cdot 1 + 0 \end{aligned}$$

$$\begin{aligned} 7 &= 77 - 4 \cdot 19 \\ &= 77 - 4 \cdot (96 - 77) \\ &= 5 \cdot 77 - 4 \cdot 96 \\ &= 5 \cdot (365 - 3 \cdot 96) - 4 \cdot 96 \\ &= 5 \cdot 365 - 79 \cdot 96 \\ &= 5 \cdot 365 - 19 \cdot (467 - 365) \\ &= 24 \cdot 365 - 79 \cdot 467 \end{aligned}$$

$$\Rightarrow 7 \equiv 24 \cdot 365 \pmod{467}$$

$$\Rightarrow \frac{7}{365} = 24 \Rightarrow \frac{77}{365} = 77 \cdot 24 = \underline{\underline{408}} = b$$

$$\text{ges.: } c = \frac{60}{420}$$

$$\begin{aligned} 467 &= 7 \cdot 420 + 47 \\ 420 &= 10 \cdot 47 + 70 \\ 47 &= 4 \cdot 70 + 7 \\ 70 &= 10 \cdot 7 + 0 \end{aligned}$$

~~$$\begin{aligned} 7 &= 47 - 4 \cdot 10 \\ &= 47 - 4 \cdot (420 - 10 \cdot 47) \\ &= 47 - 47 - 4 \cdot 420 \\ &= 40 \cdot (467 - 420) - 4 \cdot 420 \\ &= 40 \cdot 467 - 44 \cdot 420 \\ &= 40 \cdot 467 - 44 \cdot 420 \end{aligned}$$~~

~~$$\Rightarrow 7 \equiv -764 \cdot 420 \pmod{467} \equiv 297 \cdot 420$$~~

~~$$\Rightarrow \frac{7}{420} = 297 \Rightarrow \frac{60}{420} = 60 \cdot 297 \equiv 302 \pmod{467}$$~~

~~$$\Rightarrow c = \frac{60}{420} = 302$$~~

$$\begin{aligned} 7 &= 47 - 4 \cdot 10 & \Rightarrow 7 \equiv -45 \cdot 420 \pmod{467} \\ &= 47 - 4(420 - 10 \cdot 47) & \equiv 476 \cdot 420 \pmod{467} \\ &= 47 \cdot 47 - 4 \cdot 420 & \\ &= 47(467 - 420) - 4 \cdot 420 & \Rightarrow \frac{7}{420} = 476 \\ &= 47 \cdot 467 - 45 \cdot 420 & \\ & & \Rightarrow \frac{60}{420} = 60 \cdot 476 \stackrel{467}{\equiv} \underline{\underline{66}} = c \end{aligned}$$

Aufgabe 3

$$\left(\begin{array}{cccc|c} 1 & 1 & 1 & 1 & 0 \\ 1 & 2 & 3 & 4 & 0 \\ 1 & 4 & 9 & 13 & 0 \end{array} \right) \xrightarrow{\text{I}-\text{II}} \left(\begin{array}{cccc|c} 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 2 & 3 & 0 \\ 0 & 3 & 8 & 2 & 0 \end{array} \right) \xrightarrow{\text{II}-\text{III}} \left(\begin{array}{cccc|c} 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 2 & 3 & 0 \\ 0 & 0 & 6 & 0 & 0 \end{array} \right)$$

$$\begin{aligned} x_4 &= 0; \quad x_3 = -\frac{x_2}{2}; \quad x_2 = -2x_3; \quad x_1 = -x_2 - x_3 = 2x_3 - x_3 = x_3 \\ \Rightarrow (x_1, x_2, x_3, x_4) &= \{(1, 1, 1, 0), (2, 9, 2, 0), (3, 7, 3, 0), (4, 5, 4, 0), (5, 3, 5, 0), \\ &\quad (6, 7, 6, 0), (7, 12, 7, 0), (8, 10, 8, 0), (9, 8, 9, 0), (10, 6, 10, 0), \\ &\quad (11, 4, 11, 0), (12, 2, 12, 0), (0, 0, 0, 0)\} \end{aligned}$$

$$\Rightarrow \text{Basis: } v = (1, -2, 1, 0) = (1, 1, 1, 0)$$

Aufgabe 4

F_4 mit $\alpha^2 = \alpha + 1$

$$\left(\begin{array}{cccc|c} 1 & 1 & 1 & 1 & 0 \\ 1 & \alpha & 1 & \alpha & 0 \\ \alpha & 1 & \alpha+1 & \alpha & 0 \end{array} \right) \xrightarrow{\text{II} + \text{I}} \left(\begin{array}{cccc|c} 1 & 1 & 1 & 1 & 0 \\ 0 & \alpha+1 & 0 & \alpha+1 & 0 \\ 1 & \alpha & 0 & 1 & 0 \end{array} \right) \xrightarrow{\text{III} \cdot \alpha^2} \left(\begin{array}{cccc|c} 1 & 1 & 1 & 1 & 0 \\ 0 & \alpha+1 & 0 & \alpha+1 & 0 \\ 0 & \alpha+1 & 1 & \alpha & 0 \end{array} \right)$$

x_2 frei \rightarrow Wir setzen $x_2 := ?$

$$\Rightarrow x_3 = ? = x_2 \quad x_1 + ? + ? + ? = 0 \Rightarrow x_1 = ?$$

$$\Rightarrow x_4 = ? = x_2$$

$$\Rightarrow v = (1, 1, 1, 1)$$

Allg. Lsg.:

$$\underline{a \cdot v = (a, a, a, a)}$$

Aufgabe 7 b)

Beh.: $\text{ggT}(f_n, f_{n+1}) = 1$ für alle $n \geq 1$

Bew. via Induktion:

l. A.: $n=1$: $\text{ggT}(f_1, f_2) = \text{ggT}(1, 1) = 1,$

l. S.: $n \mapsto n+1$:

$$\text{ggT}(f_{n+1}, f_{n+2}) = \text{ggT}(f_{n+1}, f_{n+1} + f_n)$$

Per Induktionsbehauptung wissen wir, dass $\text{ggT}(f_{n+1}, f_n) = 1$.

Per Aufgabe 7 a) wissen wir, dass

$$\text{ggT}(f_{n+1}, f_{n+1} + f_n) = \text{ggT}(f_{n+1}, f_n).$$

Damit gilt $\text{ggT}(f_{n+1}, f_{n+2}) = 1$ \square