Codierung, 19.10.2022

Mittwoch, 19. Oktober 2022 12:55

Bsp. $\mathbb{Z}/20\mathbb{Z}$

$5+8 = 13$ $\quad 2\cdot 6 = 12$

$15+18 = 13$ $\quad 12\cdot 6 = 12$

$15+5 = 0$ $\quad 10\cdot 17 = 1$

dh.: $-15 = 5$ $\quad$ dh.: $\frac{1}{13} = 17$

$5\cdot 12 = 0$

$10^2 = 0$

Beispiel: $m = 19$, $n = 11$

$r_0 = 19$, $r_1 = 11$

$i=0$: $19 = 1\cdot 11 + 8 \Rightarrow 8 = 19 - 1\cdot 11$, $r_2 = 8$

$i=1$: $11 = 1\cdot 8 + 3 \Rightarrow 3 = 11 - 1\cdot 8$, $r_3 = 3$

$i=2$: $8 = 2\cdot 3 + 2 \Rightarrow 2 = 8 - 2\cdot 3$, $r_4 = 2$

$i=3$: $3 = 1\cdot 2 + 1 \Rightarrow 1 = 3 - 1\cdot 2$, $r_5 = 1$

$i=4$: $2 = 2\cdot 1 + 0$

STOPP $\quad ggT(19,11) = 1$

$1 = 3 - 1\cdot 2 = 3 - 1\cdot(8 - 2\cdot 3)$

$= 3\cdot 3 - 1\cdot 8 = 3\cdot(11-8) - 1\cdot 8$

$= 3\cdot 11 - 4\cdot 8 = 3\cdot 11 - 4(19-11)$

$= 7\cdot 11 - 4\cdot 19$

$a = -4$, $b = 7$

$1 = 7\cdot 11 - 4\cdot 19$

$\Rightarrow 1 = 7\cdot 11 \bmod 19$

$\Rightarrow \frac{1}{11} = 7$ im $\mathbb{F}_{19}$

Bsp.: $m = 101$, $n = 13$

$i=0$: $101 = 7\cdot 13 + 10 \Rightarrow 10 = 101 - 7\cdot 13$

$i=1$: $13 = 1\cdot 10 + 3 \Rightarrow 3 = 13 - 1\cdot 10$

$i=2$: $10 = 3\cdot 3 + 1 \Rightarrow 1 = 10 - 3\cdot 3$

$i=3$: $3 = 3\cdot 1 + 0$

STOPP $\quad ggT(101,13) = 1$

$1 = 10 - 3\cdot 3 = 10 - 3(13 - 10)$

$= 4\cdot 10 - 3\cdot 13 = 4\cdot(101 - 7\cdot 13) - 3\cdot 13$

$= 4\cdot 101 - 31\cdot 13$

$a = 4$, $b = -31$

$1 = 4\cdot 101 - 31\cdot 13$

$\Rightarrow 1 = (-31)\cdot 13 \bmod 101 = 70\cdot 13 \bmod 101$

$\Rightarrow \frac{1}{13} = 70$ im $\mathbb{F}_{101}$

Übung $\quad m = 239$, $n = 144$

$1 = 46 - 15\cdot 3 = 46 - 15\cdot(49 - 46)$

Übung $m = 239$, $n = 144$

$i=0$: $239 = 1 \cdot 144 + 95 \Rightarrow 95 = 239 - 144$

$i=1$: $144 = 1 \cdot 95 + 49 \Rightarrow 49 = 144 - 95$

$i=2$: $95 = 1 \cdot 49 + 46 \Rightarrow 46 = 95 - 49$

$i=3$: $49 = 1 \cdot 46 + 3 \Rightarrow 3 = 49 - 46$

$i=4$: $46 = 15 \cdot 3 + 1 \Rightarrow 1 = 46 - 15 \cdot 3$

$i=5$: $3 = 3 \cdot 1 + 0$

STOPP $\quad ggT(239, 144) = 1$

$1 = 46 - 15 \cdot 3 = 46 - 15 \cdot (49 - 46)$

$= 16 \cdot 46 - 15 \cdot 49 = 16 (95 - 49) - 15 \cdot 49$

$= 16 \cdot 95 - 31 \cdot 49 = 16 \cdot 95 - 31 (144 - 95)$

$= 47 \cdot 95 - 31 \cdot 144 = 47 (239 - 144) - 31 \cdot 144$

$= 47 \cdot 239 - 78 \cdot 144$

$a = 47$, $b = -78$

$1 = 47 \cdot 239 - 78 \cdot 144$

$1 = (-78) \cdot 144 \mod 239 = 161 \cdot 144 \mod 239$

$\Rightarrow \frac{1}{144} = 161$ in $\mathbb{F}_{239}$

Übung: $\frac{1}{82}$, $\frac{127}{90}$ in $\mathbb{F}_{179}$

$\frac{1}{82}$:

$179 = 2 \cdot 87 + 5$

$87 = 17 \cdot 5 + 2$

$5 = 2 \cdot 2 + 1$

$2 = 2 \cdot 1 + 0$

STOPP

$1 = 5 - 2 \cdot 2 = 5 - 2 \cdot (87 - 17 \cdot 5)$

$= 35 \cdot 5 - 2 \cdot 87 = 35 \cdot (179 - 2 \cdot 87) - 2 \cdot 87$

$= 35 \cdot 179 - 72 \cdot 87$

$\mod 179$: $1 = (-72) \cdot 87 = 107 \cdot 82$

$\Rightarrow \frac{1}{87} = 107$

$\frac{1}{90}$:

$179 = 1 \cdot 90 + 89$

$90 = 1 \cdot 89 + 1$

$89 = 89 \cdot 1 + 0$

STOPP

$1 = 90 - 1 \cdot 89$

$= 90 - 1 (179 - 90)$

$= 2 \cdot 90 - 1 \cdot 179$

$\mod 179$: $1 = 2 \cdot 90$

$\Rightarrow \frac{1}{90} = 2$ in $\mathbb{F}_{179}$

$\Rightarrow \frac{127}{90} = 127 \cdot \frac{1}{90} = 127 \cdot 2 = 75$ in $\mathbb{F}_{179}$

Beispiel: LGS über $\mathbb{F}_7$:

$2x + 3y + 4z = 5$

$$\begin{aligned} 2x + 3y + 4z &= 5 \\ 3x + 4y + 5z &= 4 \\ 2x + 6y + z &= 1 \end{aligned}$$

$$\left(\begin{array}{ccc|c} 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 4 \\ 2 & 6 & 1 & 1 \end{array}\right) \xrightarrow[\text{III}\cdot 4]{\text{I}\cdot 4,\ \text{II}\cdot 5} \left(\begin{array}{ccc|c} 1 & 5 & 2 & 6 \\ 1 & 6 & 4 & 6 \\ 1 & 3 & 4 & 4 \end{array}\right)$$

$$\xrightarrow[\text{III}-\text{I}]{\text{II}-\text{I}} \left(\begin{array}{ccc|c} 1 & 5 & 2 & 6 \\ 0 & 1 & 2 & 0 \\ 0 & 5 & 2 & 5 \end{array}\right) \xrightarrow{\text{III}-5\,\text{II}} \left(\begin{array}{ccc|c} 1 & 5 & 2 & 6 \\ 0 & 1 & 2 & 0 \\ 0 & 0 & 6 & 5 \end{array}\right)$$

$$\xrightarrow{\text{III}\cdot 6} \left(\begin{array}{ccc|c} 1 & 5 & 2 & 6 \\ 0 & 1 & 2 & 0 \\ 0 & 0 & 1 & 2 \end{array}\right) \xrightarrow[\text{I}-2\,\text{II}]{\text{II}-2\,\text{III}} \left(\begin{array}{ccc|c} 1 & 5 & 0 & 2 \\ 0 & 1 & 0 & 3 \\ 0 & 0 & 1 & 2 \end{array}\right)$$

$$\xrightarrow{\text{I}-5\,\text{II}} \left(\begin{array}{ccc|c} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 3 \\ 0 & 0 & 1 & 2 \end{array}\right) \qquad \begin{aligned} x &= 1 \\ y &= 3 \\ z &= 2 \end{aligned}$$

Übung: über $\mathbb{F}_3$

$$\begin{aligned} x + 2y + z &= 0 \\ 2x + 2y + z &= 0 \end{aligned}$$

$$\left(\begin{array}{ccc|c} 1 & 2 & 1 & 0 \\ 2 & 2 & 1 & 0 \end{array}\right) \xrightarrow{\text{II}-2\,\text{I}} \left(\begin{array}{ccc|c} 1 & 2 & 1 & 0 \\ 0 & 1 & 2 & 0 \end{array}\right)$$

z

frei

$$\begin{aligned} x + 2y + z &= 0 \\ y + 2z &= 0 \end{aligned}$$

$z = a \in \mathbb{F}_3$ beliebig $\Rightarrow y = a$, $x = 0$

Lösungen $\mathbb{L} = \{(0,0,0), (0,1,1), (0,2,2)\}$

Lösungen $\mathbb{L} = \{(0,0,0), (0,1,1), (0,2,2)\}$

Basis: $v = (0,1,1)$

Bsp.: $M = \{0, 1, \alpha, \alpha+1\}$

+	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	α	1	0

kommutative Gruppe

$\Rightarrow$ Körper

·	1	α	$\alpha+1$
1	1	α	$\alpha+1$
α	α	$\alpha+1$	1
$\alpha+1$	$\alpha+1$	1	α

kommutative Gruppe

$\mathbb{F}_4$

K endlicher Körper, $1 \in K$

$n = n \cdot 1 = \underbrace{1 + 1 + \dots + 1}_{n\text{-mal}}$

$\underbrace{1 + 1 + \dots + 1}_{n\text{-mal}} = \underbrace{1 + 1 + \dots + 1}_{m\text{-mal}}$

(da K endlich ist)

$0 = \underbrace{1 + \dots + 1}_{(m-n)\text{-mal}}$

also: es gibt immer ein n mit $n \cdot 1 = 0$ in K

Bsp.: $\mathbb{F}_4$ $1, \alpha$ $\alpha^2 = \alpha + 1$

$(\alpha+1)\alpha = \alpha^2 + \alpha = \alpha + \alpha + 1 = 1$

$(\alpha+1)\alpha = \alpha^2+\alpha = \alpha+\alpha+1 = 1$

Bsp.: $\mathbb{F}_8$: $1, \alpha, \alpha^2$ $\qquad \alpha^3 = \alpha+1$

$(1+\alpha)+(\alpha+\alpha^2) = 1+2\cdot\alpha+\alpha^2 = 1+\alpha^2$

$(\alpha+1)\alpha = \alpha^2+\alpha$

$(\alpha+1)\alpha^2 = \alpha^3+\alpha^2 = \alpha+1+\alpha^2 = \alpha^2+\alpha+1$

$(\alpha^2+1)\alpha^2 = \alpha^4+\alpha^2 = \alpha\cdot\alpha^3+\alpha^2 = \alpha(\alpha+1)+\alpha^2$

$= \alpha^2+\alpha+\alpha^2 = 2\alpha^2+\alpha = \alpha$