

- ① a) Ist $\mathbb{Z}_{5891}$ ein Körper? (Begründung!)
 b) Welches ist die kleinste Primzahl, die größer ist als 5891?

- ② Berechnen Sie das multiplikative Inverse von 19 in $\mathbb{Z}_{71}$, und zwar von Hand nach dem erweiterten euklid. Algorithmus.

- ③ Die folgende Botschaft c wurde gemäß unserer Konvention in $\mathbb{Z}_{31}$ mit der Verschlüsselungsmatrix m gewonnen:

$$m = \begin{pmatrix} 1 & 29 & 4 \\ 4 & 22 & 3 \\ 24 & 27 & 6 \end{pmatrix} \quad c = \begin{pmatrix} 20 & 12 & 30 & 28 & 6 & 27 & 8 \\ 12 & 23 & 26 & 13 & 11 & 2 & 17 \\ 7 & 12 & 21 & 19 & 19 & 28 & 24 \end{pmatrix}$$

Sie lautet das Wort nach dem letzten Leerzeichen der Originalbotschaft b ?

- ④ $\mathbb{Z}_{10}^*$ sei die Teilmenge derjenigen Elemente von $\mathbb{Z}_{10}$, die ein multiplikatives Inverses haben.

- a) Welche Elemente enthält $\mathbb{Z}_{10}^*$?
 b) Bilden die Elemente von $\mathbb{Z}_{10}^*$ eine multiplikative Gruppe? Versuchen Sie, die Gruppentafel aufzustellen.
 c) Nennen Sie eine 'Standardgruppe', welche isomorph ist zu $\mathbb{Z}_{10}^*$.

⑤

				
2x3	1x3	3x1	3x3	3x2
A	B	C	D	E

Welche der Notizen A, ..., E lässt sich mit welcher multiplizieren (Reihenfolge der Faktoren ist wichtig!), und von welchem Typ ist das Ergebnis der Multiplikation?

Beispiel: $D \cdot C$ heißt 3x1

$A \cdot A$ / (nicht definiert)

⑥

Gegeben seien die drei Matrizen

$$A = \begin{pmatrix} 5 & 3 & 7 \\ 3 & -6 & -8 \\ 4 & 5 & -3 \end{pmatrix}, \quad b = \begin{pmatrix} x \\ y \\ z \end{pmatrix}, \quad c = \begin{pmatrix} 1 \\ 6 \\ 37 \end{pmatrix}$$

Alle Zahlen sollen aus $\mathbb{Q}$ stammen.

- Welches System von linearen Gleichungen wird beschrieben durch $A \cdot b = c$?
- Welcher Befehl meines TR führt mit der übergebenen Matrix den Gauß'sche Algorithmus durch?
- Welche Matrix müssen Sie die dem Befehl übergeben, damit Sie anschließend A^{-1} und die Werte x, y und z der Lösung ablesen können?
- Welches sind die Lösungen x, y und z , und wie sieht die Matrix A^{-1} schon geschrieben aus?



① a) $5891 = 43 \cdot 137$!! nicht prim, $\mathbb{Z}_{5891}$ ist kein Körper.
Lösung ab. mit $\text{factor}(5891)$ oder $\text{isPrime}(5891)$... 4

8/8 b) $\text{nextPrime}(5892)$ liefert 5897 ! 4

②

$$\begin{aligned} 71 &= 3 \cdot 19 + 14 \\ 19 &= 1 \cdot 14 + 5 \\ 14 &= 2 \cdot 5 + 4 \\ 5 &= 1 \cdot 4 + 1 \end{aligned}$$

6

$$\begin{aligned} 1 &= 5 - 1 \cdot 4 = 5 - (14 - 2 \cdot 5) = 3 \cdot 5 - 14 \\ &= 3 \cdot (19 - 14) - 14 = 3 \cdot 19 - 4 \cdot 14 = \\ &= 3 \cdot 19 - 4 \cdot (71 - 3 \cdot 19) = \underline{15 \cdot 19 - 4 \cdot 71} = 1 \end{aligned}$$

Also ist $15 = 19^{-1} \pmod{71}$. 8

③

$$m^{-1} = \begin{pmatrix} 30 & 25 & 14 \\ 10 & 20 & 4 \\ 21 & 27 & 14 \end{pmatrix} \quad c = \begin{pmatrix} 20 & 12 & 30 & 28 & 6 & 27 & 8 \\ 12 & 23 & 26 & 13 & 11 & 2 & 17 \\ 7 & 12 & 21 & 19 & 19 & 28 & 24 \end{pmatrix}$$

8

$$b = m^{-1} \cdot c = \begin{pmatrix} 6 & 18 & 15 & 5 & 8 & 12 & 9 \\ 3 & 8 & 5 & 27 & 15 & 19 & 20 \\ 5 & 18 & 14 & 27 & 7 & 21 & 2 \end{pmatrix}$$

GUB 8

((FROEHLI; CHE_OST; ERN_GUB))

④ a) $\mathbb{Z}_{10}^* = \{1, 3, 7, 9\}$ 4 (alle mit $\text{ggT}(x, 10) = 1$)

b)

	1	3	9	7
1	1	3	9	7
3	3	9	7	1
9	9	7	1	3
7	7	1	3	9

c) wie C_4 ! 4

$d_{0^\circ}, d_{90^\circ}, d_{180^\circ}, d_{270^\circ}$

$\downarrow$
 d

$1, d, d^2, d^3$

$1, 3, 3^2, 3^3$!!

12/12

5

$$A \cdot A \quad /$$

$$A \cdot B \quad /$$

$$A \cdot C \rightarrow 2 \times 1$$

$$A \cdot D \rightarrow 2 \times 3$$

$$A \cdot E \rightarrow 2 \times 2$$

$$C \cdot A \quad /$$

$$C \cdot B \rightarrow 3 \times 3 \quad !$$

$$C \cdot C \quad /$$

$$C \cdot D \quad /$$

$$C \cdot E \quad /$$

$$E \cdot A \rightarrow 3 \times 3$$

$$E \cdot B \quad /$$

$$E \cdot C \quad /$$

$$E \cdot D \quad /$$

$$E \cdot E \quad /$$

$$B \cdot A \quad /$$

$$B \cdot B \quad /$$

$$B \cdot C \rightarrow 1 \times 1 \quad (!)$$

$$B \cdot D \rightarrow 1 \times 3$$

$$B \cdot E \rightarrow 1 \times 2$$

$$D \cdot A \quad /$$

$$D \cdot B \quad /$$

$$D \cdot C \rightarrow 3 \times 1$$

$$D \cdot D \rightarrow 3 \times 3$$

$$D \cdot E \rightarrow \underline{3 \times 2}$$

je 2

mit Abgang für Punkte!

22/22

6

$$\begin{array}{rcl} a) & 5x + 3y + 7z & = 1 \\ & 3x - 6y - 8z & = 6 \\ & 4x + 5y - 3z & = 37 \end{array}$$

4

$$b) \quad \text{rref}(\dots) \quad !$$

4

$$c) \quad \begin{pmatrix} 5 & 3 & 7 & 1 & 0 & 0 & 1 \\ 3 & -6 & -8 & 0 & 1 & 0 & 6 \\ 4 & 5 & -3 & 0 & 0 & 1 & 37 \end{pmatrix}$$

4

20/20

$$d) \quad b = \begin{pmatrix} 2 \\ 4 \\ -3 \end{pmatrix}, \quad \text{also} \quad x=2, \quad y=4 \quad \text{und} \quad z=-3$$

3

$$A^{-1} = \frac{1}{494} \cdot \begin{pmatrix} 58 & 44 & 18 \\ -23 & -43 & 61 \\ 39 & -13 & -39 \end{pmatrix} = \begin{pmatrix} \frac{29}{247} & \frac{22}{247} & \frac{9}{247} \\ -\frac{23}{494} & -\frac{43}{494} & \frac{61}{494} \\ \frac{3}{38} & -\frac{1}{38} & -\frac{3}{38} \end{pmatrix}$$

5

Darstellung:

8/8

→ total

100P.

100

95

90

85

80

75

70

65

60

55

50

45

40

35

6.0

5.0

4.0

3.0

Schritt der ♀ : $5.9\overline{333}$!Kleinstschritt $\approx \cancel{5.206} 5.206 > 5.2$

Schritt der ♂ : 4.686

Note: $4.0 + (58 - P) / 18$