Mitschrift
Diskrete Mathematik, SS 2015
Prof. Dr. Josef Hörwick

M. Zell

19. November 2015

Inhaltsverzeichnis

1 Hinweise **8**

2 Mengen **9**
2.1 Mengengleichheit . . . 9
2.2 Leere Menge . . . 9
2.3 Unendliche Mengen . . . 9
2.4 Definitionen . . . 9
2.4.1 Teilmenge . . . 9
2.4.2 Durchschnitt . . . 10
2.4.3 Vereinigung . . . 10
2.4.4 Differenz . . . 11
2.4.5 Grundmenge Ω . . . 11
2.5 Potenzmenge . . . 11
2.5.1 Mächtigkeit von Mengen . . . 12

3 Relationen **12**
3.1 Das Direkte Produkt von zwei Mengen . . . 12
3.2 Relation . . . 12
3.3 Äquivalenzrelation . . . 12
3.4 Grundmenge $\mathbb{Z}$ . . . 13
3.5 Funktionen . . . 14
3.5.1 Umkehrabbildung . . . 15
3.5.2 Komposition . . . 15

4 Fehlererkennung **16**
4.1 Fehlererkennender Code . . . 16
4.2 Codes über Gruppen . . . 17
4.3 Permutationen . . . 20

5 Graphentheorie **22**
5.1 Königsberger Brückenproblem . . . 22
5.2 Haus vom Nikolaus . . . 23
5.3 Hamiltonkreise . . . 24
5.4 Chinesisches Postboten-Problem . . . 26
5.5 Das Problem des Handlungsreisenden . . . 27

6 Symmetrien des gleichseitigen Dreiecks (Wiederholung) **28**

7 Kryptographie **29**
7.1 Symmetrische Verfahren . . . 29
7.1.1 Stromchiffren . . . 29
7.2 Blockverschlüsselung . . . 32
7.2.1 EBC-Mode . . . 32
7.2.2 CBC-Mode . . . 33
7.2.3 CFB-Mode . . . 33

8 Graphentheorie 35
8.1 G heißt bipartit, ... 35
8.2 Kantenzug: 35
8.3 Definition zusammenhängender Graph: 36
8.4 Kantenzüge 36
8.4.1 Länge eines Kantenzugs 36
8.4.2 geschlossene Kantenzüge 36
8.4.3 Weg 36
8.4.4 Kreis 37
8.4.5 Grad einer Ecke 37
8.5 Das Königsberger Brückenproblem 37
8.5.1 vollständiger Graph mit 5 Ecken 38
8.6 Das Haus vom Nikolaus 40

9 Lösung zur Prüfung SS 2011 41
9.1 Aufgabe 1 41
9.1.1 1a 41
9.1.2 1b 41
9.2 Aufgabe 2 41
9.2.1 2a 41
9.2.2 2b 41
9.3 Aufgabe 3 41
9.4 Aufgabe 4 42
9.4.1 Direktlösung 42
9.4.2 Lösung mit chinesischem Restsatz 42

10 Lösung zur Prüfung SS 2010 44
10.1 Aufgabe 1 44
10.1.1 a 44
10.1.2 b 44
10.1.3 c 44
10.2 Aufgabe 2 44
10.3 Aufgabe 3 44
10.3.1 a 44
10.3.2 b 45
10.4 Aufgabe 4 45
10.5 Aufgabe 5 45
10.5.1 a 45
10.5.2 b 45
10.5.3 c 46
10.6 Aufgabe 6 46

11 Lösung zur Prüfung SS 2012 47
11.1 Aufgabe 1 47
11.1.1 a 47
11.1.2 b 47
11.2 Aufgabe 2 47
11.2.1 a 47
11.2.2 b 47
11.3 Aufgabe 3 47

11.3.1 a . . . 47
11.3.2 b . . . 48
11.4 Aufgabe 4 . . . 48
11.4.1 a . . . 48
11.4.2 b . . . 48
11.4.3 c . . . 48
11.5 Aufgabe 5 . . . 48

12 Lösung zur Prüfung SS 2012 49
12.1 Aufgabe 1 . . . 49
12.2 Aufgabe 2 . . . 49
12.2.1 a . . . 49
12.2.2 b . . . 49
12.3 Aufgabe 3 . . . 49
12.3.1 a . . . 49
12.3.2 b . . . 49
12.4 Aufgabe 4 . . . 50
12.5 Aufgabe 5 . . . 50
12.5.1 a . . . 50
12.5.2 b . . . 50
12.6 Aufgabe 6 . . . 50
12.7 Aufgabe 7 . . . 50

13 Einzelne Aufgaben 51
13.1 Dominosteine in 3xn-Feld unterbringen . . . 51
13.2 Rechnen im $\mathbb{Z}_{11}$ . . . 52
13.2.1 Lineares Gleichungssystem . . . 52
13.2.2 Quadratische Gleichung . . . 52
13.3 Kombinatorikaufgabe . . . 52
13.4 Einheitengruppe . . . 53
13.5 Verschlüsseln und Entschlüsseln mit Permutationen . . . 53
13.6 Graphentheorie . . . 53
13.6.1 eulersche Linie . . . 53
13.6.2 eulerscher Kreis . . . 54

14 Lösung zur Prüfung SS 2008 55
14.1 Aufgabe 1 . . . 55
14.2 Aufgabe 2 . . . 55
14.3 Aufgabe 3 . . . 55
14.3.1 a . . . 55
14.3.2 b . . . 55
14.3.3 c . . . 56
14.4 Aufgabe 4 . . . 56
14.4.1 a . . . 56
14.4.2 b . . . 56
14.5 Aufgabe 5 . . . 56
14.5.1 a . . . 56
14.5.2 b . . . 56
14.5.3 c . . . 56

15 Einzelne Aufgaben **57**
15.1 Siebformel . . . 57
15.1.1 Beispiel . . . 57
15.1.2 Berechnung . . . 57
15.2 Symmetriegruppe eines Rechtecks . . . 57
15.3 RSA-Algorithmus . . . 58

16 Prüfungsstoff **58**

17 Hilfsmittel für die Prüfung **59**
17.1 Eulerkreis und Eulertour . . . 59
17.2 Chinesischer Restsatz . . . 59
17.3 Permutationen . . . 59
17.3.1 Anzahl Permutationen ohne Fixpunkte . . . 59
17.4 ggT . . . 59
17.4.1 euklidischer Algorithmus . . . 60
17.4.2 Erweiterter euklidischer Algorithmus . . . 60
17.5 schnelle Exponentation . . . 60
17.6 $\mathbb{Z}_n^*$ . . . 60
17.6.1 $\mathbb{Z}_4^*$ . . . 61
17.6.2 $\mathbb{Z}_5^*$ . . . 61
17.6.3 $\mathbb{Z}_6^*$ . . . 61
17.6.4 $\mathbb{Z}_7^*$ . . . 61
17.6.5 $\mathbb{Z}_8^*$ . . . 61
17.6.6 $\mathbb{Z}_9^*$ . . . 61
17.6.7 $\mathbb{Z}_{10}^*$ . . . 62
17.6.8 $\mathbb{Z}_{11}^*$ . . . 62
17.6.9 $\mathbb{Z}_{12}^*$ . . . 62
17.6.10 $\mathbb{Z}_{13}^*$ . . . 62
17.6.11 $\mathbb{Z}_{14}^*$ . . . 63
17.6.12 $\mathbb{Z}_{15}^*$ . . . 63
17.6.13 $\mathbb{Z}_{16}^*$ . . . 63
17.6.14 $\mathbb{Z}_{17}^*$ . . . 64
17.6.15 $\mathbb{Z}_{18}^*$ . . . 64
17.6.16 $\mathbb{Z}_{19}^*$ . . . 65
17.6.17 $\mathbb{Z}_{20}^*$ . . . 65
17.6.18 $\mathbb{Z}_{21}^*$ . . . 65
17.6.19 $\mathbb{Z}_{22}^*$ . . . 66
17.6.20 $\mathbb{Z}_{24}^*$ . . . 66

Abbildungsverzeichnis

1 A ist eine (echte) Teilmenge von B 9
2 Schnittmenge von A und B 10
3 Vereinigungsmenge von A und B 10
4 B ohne A 11
5 Menge von acht Buchexemplaren mit eingezeichneter Äquivalenzrelation „x und y besitzen dieselbe ISBN“ als Pfeildiagramm und den Äquivalenzklassen (Quelle: Wikipedia). 13
6 Das sind alle Kongruenzen 19
7 Spiegelungen an h,g, Drehungen um Z um 180° und id 19
8 Fünfeck: 5 Spiegelungen, 4 Drehungen, id (10) 20
9 Gleichseitiges Dreieck 21
10 7 Brücken 22
11 Abstraktion 7 Brücken 22
12 Eulertour 23
13 Ein zusammenhängender Graph 23
14 Mehrere zusammenhängende Kantenfolgen 24
15 Das ist das Haus 24
16 Offene Eulertour 24
17 Wo ist der Hamiltonkreis? 25
18 Ist der graph hamiltonsch? 25
19 Ist der graph hamiltonsch? 26
20 Tiefensuche 27
21 Das Haus vom Nikolaus 27
22 Spiegelungen an w1, w2, w3, Drehungen 120, 240, id 28
23 Verschlüsselung und Entschlüsselung (f, g sind öffentlich und k, $\tilde{k}$ geheim) 29
24 Funktionsweise symmetrische Verschlüsselung. Die Rote + Operation ist eigentlich eine - Operation. Bei Bits, also mod 2, kann aber Plus durch Minus ersetzt werden. 30
25 Beispiel 31
26 Blockverschlüsselung 32
27 vollständige Graphen 35
28 bipartite Graphen 35
29 Ein Kantenzug 36
30 Ein zusammenhängender Graph und ein Graph mit zwei Zusammenhangskomponenten 36
31 Königsberger Brückenproblem 37
32 Königsberger Brückenproblem als Graph 37
33 eulerscher Kreis mit 10 Kanten 38
34 Kreise finden in Graphen 38
35 Ein eulerscher Grad 39
36 Richtig für $m = 2, m = 3$ 39
37 Kreis C und Zusammenhangskomponente Z 39
38 offene eulersche Linie 40
39 Eulersche Linie 40
40 Der Induktionsanfang für $n = 1, n = 2$ 42
41 Mögliche Anfänge bei den Dominosteinen 42
42 Die Rosinen werden verteilt 50

43 Wie kann man die 1x2 Steine im Feld unterbringen? 51
44 Eulersche Linie und eulerscher Kreis 54
45 Auf diese Menge wenden wir die Siebformel an 57
46 Spiegelungen an s und t, Drehung d um 180, Drehung id um 360 58

1 Hinweise

Diese Mitschrift basiert auf der Vorlesung „Diskrete Mathematik“ von Prof. Dr. Josef Hörwick im SS 2015. Du kannst sie gerne benutzen, kopieren und an andere weitergeben. Auch in der Prüfung - soweit zugelassen [1] - kannst du sie gerne als Hilfsmittel verwenden, wenn das meine Nutzung als Prüfungshilfsmittel nicht in irgendeiner Weise beeinträchtigt.

Natürlich besteht kein Anspruch auf Aktualität, Richtigkeit, Fortsetzung meines Angebots oder dergleichen. Sollten dir Fehler auffallen oder solltest du Verbesserungsvorschläge haben, würde ich mich über eine E-Mail (zell@hm.edu) freuen. Wenn du mir als kleines Dankeschön z.B. ein Club-Mate[2] ausgeben möchtest, findest du mich meistens hier: `http://fi.cs.hm.edu/fi/rest/public/timetable/group/if3b`. Wenn nicht, ist es auch ok ;-)

Nach der Prüfung werde ich den LaTeX-Quelltext veröffentlichen, damit die Mitschrift weitergeführt, korrigiert und ergänzt werden kann.

Viele Grüße
M. Zell

[1] `http://www.cs.hm.edu/meinstudium/studierenden_services/fi_pruefungskatalog.de.html`
[2] `http://www.clubmate.de/ueber-club-mate.html`

2 Mengen

Mengen sind **ungeordnet** und enthalten **verschiedene Elemente**: $M = \{4, 3, 5\} = \{5, 4, 3\} = \{3, 3, 4, 5\}$.

2.1 Mengengleichheit

Zwei Mengen A und B sind **gleich**, wenn sie dieselben Elemente enthalten: $x \in A \Leftrightarrow x \in B$.

2.2 Leere Menge

Man bezeichnet damit die Menge, die keinerlei Elemente enthält. Die Zeichen für die leere Menge sind $\emptyset$ oder $\{\}$. Die leere Menge ist Teilmenge jeder Menge ($\emptyset \subseteq A$).

2.3 Unendliche Mengen

Ein Beispiel für unendliche Mengen ist die Menge der natürlichen Zahlen ($\mathbb{N} = \{1, 2, 3, 4, ...\}$). Aber auch $M = \{n \in \mathbb{N} : 7 \text{ teilt } n\} = \{7, 14, 21, 28, ...\} = 7 \cdot \mathbb{N}$

2.4 Definitionen

2.4.1 Teilmenge

Eine Menge A heißt Teilmenge einer Menge B, wenn jedes Element von A auch Element von B ist. Formal: $A \subset B \ :\Longleftrightarrow \forall x \, (x \in A \ \rightarrow x \in B)$.
Beispiel: $B = \{2, 3, 4, 5\}, A = \{3, 4\}, A \subset B, \emptyset \in B$

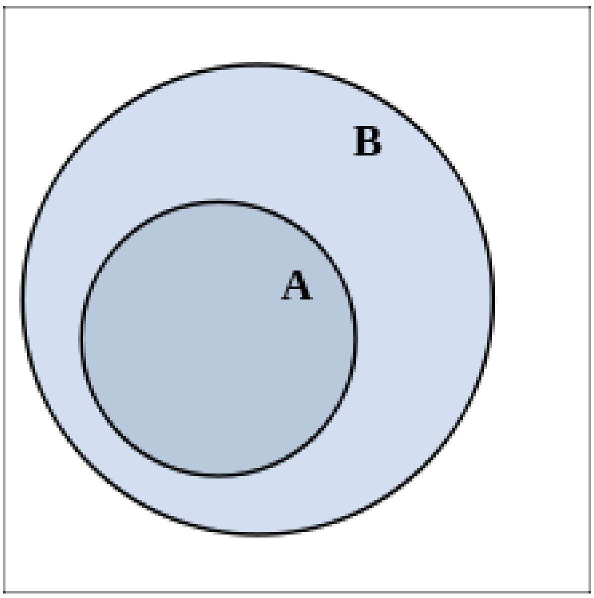


Abbildung 1: A ist eine (echte) Teilmenge von B

2.4.2 Durchschnitt

$A \cap B : \{x : x \in A \wedge x \in B\}$
Beispiel: $A = \{3,5,6\}, B = \{3,\{5,6\},6,7\}, A \nsubseteq B \Rightarrow A \cap B = \{3,6\}$. Bei mehreren Mengen: $\bigcap_{i \in \mathbb{N}} A_i = A_1 \cap A_2 \cap A_3 \cap ... = \{x : \forall i \in \mathbb{N} : x \in A_i\}$

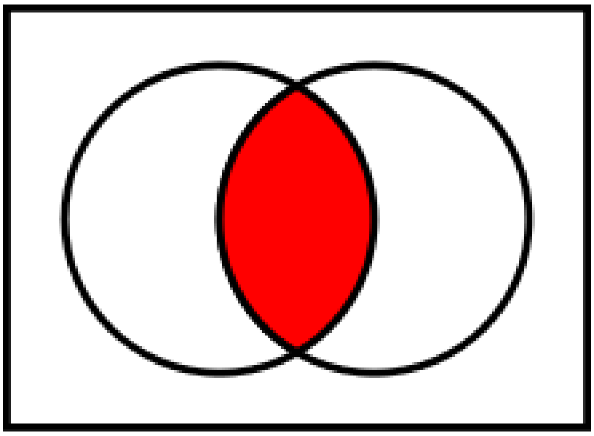


Abbildung 2: Schnittmenge von A und B

2.4.3 Vereinigung

$A \cup B : \{x : x \in A \vee x \in B\}$
Beispiel: $A = \{3,5,6\}, B = \{3,\{5,6\},6,7\}, A \nsubseteq B \Rightarrow A \cup B = \{3,5,6,7,\{5,6\}\}$. Bei mehreren Mengen: $\bigcup_{i \in \mathbb{N}} A_i = A_1 \cup A_2 \cup A_3 \cup ... = \{x : \exists i : x \in A_i\}$, auch: $\bigcup_{i=1}^{3} A_i = A_1 \cup A_2 \cup A_3$

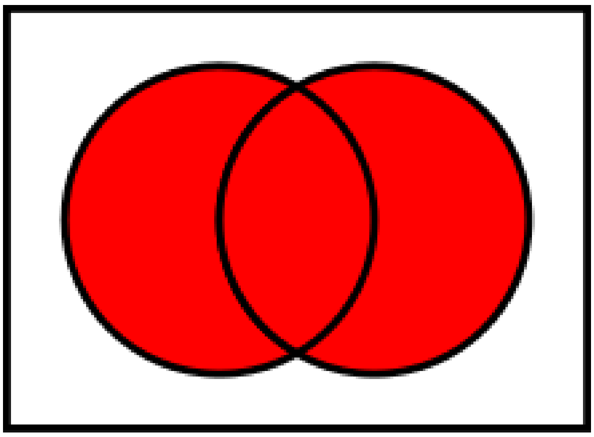


Abbildung 3: Vereinigungsmenge von A und B

2.4.4 Differenz

$A \setminus B := \{x \mid (x \in A) \wedge (x \notin B)\}$
Beispiel: $B \setminus A = \{\{5, 6\}, 7\}$

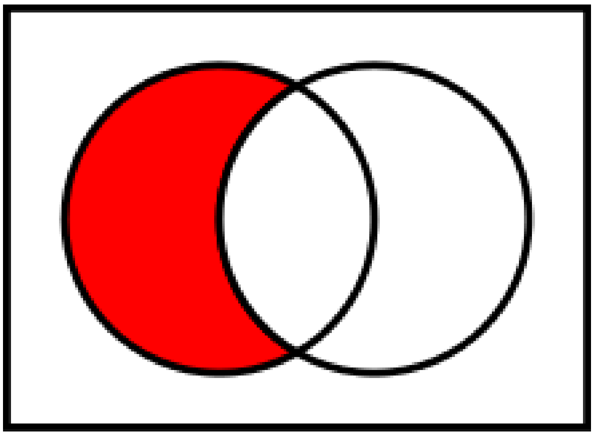


Abbildung 4: B ohne A

2.4.5 Grundmenge Ω

$A \subset \Omega \rightarrow \bar{A} = \Omega \setminus A$, auch: $\bar{A} = \{x \in \Omega : x \notin A\}$

Satz 2.1. $A = B \Leftrightarrow A \subset B \wedge B \subset A$

Satz 2.2. *Es gilt:*

- $\overline{\bigcup_{i\in\mathbb{N}} A_i} = \bigcap_{i\in\mathbb{N}} \overline{A_i}$
- $\overline{\bigcap_{i\in\mathbb{N}} A_i} = \bigcup_{i\in\mathbb{N}} \overline{A_i}$

Beweis. Sei

- $x \in \overline{\bigcup_{i\in\mathbb{N}} A_i} \Leftrightarrow x \notin \bigcup_{i\in\mathbb{N}} A_i \Leftrightarrow x \notin A_i \forall i \in \mathbb{N} \Leftrightarrow x \in \overline{A_i} \forall i \in \mathbb{N} \Leftrightarrow x \in \bigcap_{i\in\mathbb{N}} \overline{A_i}$
- $x \in \overline{\bigcap_{i\in\mathbb{N}} A_i} \Leftrightarrow x \notin \bigcap_{i\in\mathbb{N}} A_i \Leftrightarrow \exists i \in \mathbb{N}$ mit $x \notin A_i \Leftrightarrow \exists i \in \mathbb{N}$ mit $x \in \overline{A_i} \Leftrightarrow x \in \bigcup_{i\in\mathbb{N}} \overline{A_i}$

□

2.5 Potenzmenge

Die Potenzmenge P(M) ist die Menge aller Teilmengen von M. Beispiel: $M = \{1, 2, 3\} \Rightarrow P(M) = \{\{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}, \{\}\}$. Es fällt auf, dass P(M) 8 Elemente also die Mächtigkeit $|P(M)| = 8 = 2^3$ hat.

2.5.1 Mächtigkeit von Mengen

Die Mächtigkeit von Mengen heißt auch Kardinalität.

Satz 2.3. *Sei M endlich:* $|P(M)| = 2^{|M|}$

Beweis. Jede Abbildung $f : M \longmapsto 0,1$ entspricht einer Teilmenge A von M. $x \in A \Leftrightarrow f(x) = 1$. Wir zählen die Abbildungen $f : M \longmapsto 0,1$:

$$M = \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 0 & 1 & 1 & 0 & 1 \end{array} \Rightarrow 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^5 \text{ Möglichkeiten für f.}$$ □

3 Relationen

3.1 Das Direkte Produkt von zwei Mengen

$A \times B = \{(a, b) : a \in A, b \in B\}$
Es gilt: $(a, b) = (c, d) \Leftrightarrow a = c$ und $b = d$

Beispiel: $A = \{1, 2, 3\}, B = a, b \Rightarrow A \times B = \{(1, a), (2, a), (3, a), (1, b), (2, b), (3, b)\}$

3.2 Relation

Eine Relation R auf A,B ist eine Teilmenge von $A \times B$, z.B.: $A = \{1, 2, 3\}, B = \{a, b\}, R = \{(1, a), (2, b), (3, b)\}$. Für $(1.a) \in \mathbb{R}$ schreibt man auch 1 R a oder 1 $\sim$ a. Die beiden Mengen A,B können gleich sein. Relationen auf A,A oder kurz: Relation auf A: $A = \{1, 2, 3\}, R = \{(1, 2), (1, 3), (2, 3)\}$ oder

Für Relationen kann man beliebige Zeichen verwenden, hier eben $\sim$.

Beispiel: Relation auf $\mathbb{N}$: $A = \mathbb{N}$
$\leq$: $\{(a, b) \in \mathbb{N}^2 : a \leq b\}$
$=$: $\{(a, b) \in \mathbb{N}^2 : a = b\} = \{(a, a) : a \in \mathbb{N}\}$

3.3 Äquivalenzrelation

Sei v eine Relation auf M mit folgenden Eigenschaften:

1. $a \sim a, \forall a \in M$ (reflexiv)
2. $a \sim b \Rightarrow b \sim a$ (symmetrisch)
3. $a \sim b \wedge b \sim c \Rightarrow a \sim c$ (transitiv)

Beispiel: M =ist die Menge von Kugeln mit den Farben rot, blau, weiß. Kugel a $\sim$ Kugel b $\Leftrightarrow a, b$ haben dieselbe Farbe:

- $\sim$ ist reflexiv ✓
- $\sim$ ist symmetrisch ✓
- $\sim$ ist transitiv ✓

$\Rightarrow \sim$ ist Äquivalenzrelation.

3.4 Grundmenge $\mathbb{Z}$

$x \sim y \Leftrightarrow x - y \in 5 \cdot \mathbb{Z} = \{5z : z \in \mathbb{Z}\} = \{-10, -5, 0, 5, 10, ...\}$
$x \sim y \Leftrightarrow x$ und y unterscheiden sich durch ein Vielfaches von 5, z.B.: $3 \sim 8, -7 \sim 3, -8 \sim -23$.

- $\sim$ ist reflexiv ✓
- $\sim$ ist symmetrisch ✓
- $\sim$ ist transitiv ✓

$\Rightarrow \sim$ ist Äquivalenzrelation.

Definition 3.1 (Äquivalenzklassen)**.** *$\sim$ sei eine Äquivalenzrelation auf M, dann gilt:*
$[x] = \{y \in M : x \sim y\}$ heißt Äquivalenzklasse von x. Natürlich gilt auch: $x \in [x]$.

Satz 3.1. *Die Äquivalenzklassen bilden eine Zerlegung von M.*

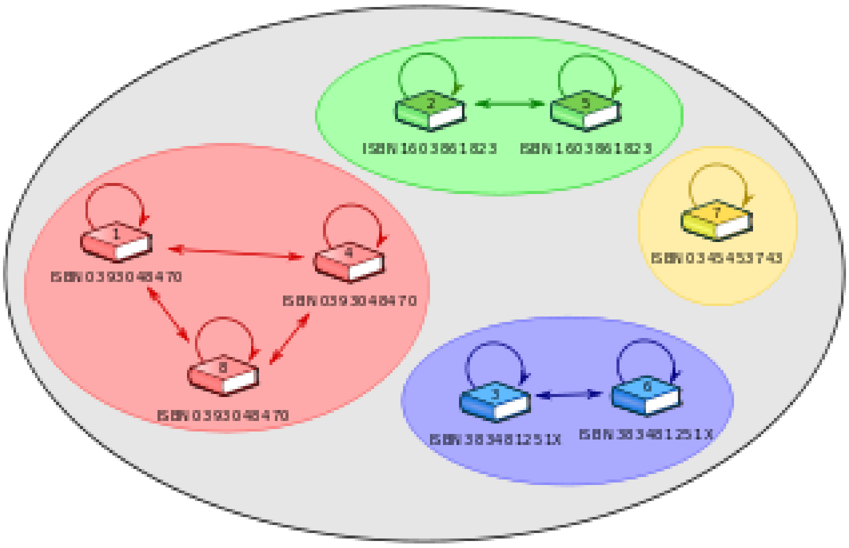


Abbildung 5: Menge von acht Buchexemplaren mit eingezeichneter Äquivalenzrelation „x und y besitzen dieselbe ISBN“ als Pfeildiagramm und den Äquivalenzklassen (Quelle: Wikipedia).

Beweis. Falls $y \in [x]$, so ist $[y] = [y]$

$$\left.\begin{array}{l} \text{Sei } a \in [x] \Rightarrow a \sim x \Rightarrow a \sim y \Rightarrow a \in [y] \Rightarrow [x] \subset [y] \\ \text{Sei } a \in [y] \Rightarrow a \sim y \Rightarrow a \sim x \Rightarrow a \in [x] \Rightarrow [y] \subset [x] \end{array}\right\} [x] = [y]$$

Falls $[x] \cap [y] \neq \emptyset$, z.B.: $a \in [x]$ und $a \in [y] \Rightarrow [a] = [x] = [y]$, also $[x] = [y] \Rightarrow$ Zerlegung von M. $\square$

Beispiel: Die Zerlegung durch die Äquivalenzklassen kann man anhand des Beispiels $x \sim y \Leftrightarrow x - y \in 5 \cdot \mathbb{Z}$ gut auf einem Zahlenstrahl zeigen (Abb. **??**).

blau: $\overbrace{[0]}^{\text{Klassen}} = \overbrace{\{..., -10, -5, 0, 5, 10, ...\}}^{\text{Jeder Wert kann Representant der Klasse sein}} = [15] = [-5]$
rot: $[1] = \{..., -9, -4, 1, 6, ...\} = [6] = [-4]$
grün: $[2] = \{..., -8, -3, 2, 7, ...\} = [-8] = [7]$

Die Zerlegung einer Menge M in Klassen entsprechn den Äquivalenzrelationen auf M.

3.5 Funktionen

Definition 3.2 (Funktion)**.** *Eine Relation R auf den Mengen A,B heißt Funktion von A nach B, wenn gilt: Zu jedem $a \in A$ gibt es genau ein $b \in B$ mit $(a, b) \in R$.*

Schreibweise: $f : \begin{cases} A \to B \\ a \to f(a) \end{cases}$
mit A Definitionsbereich, B Zielbereich, R Graph von A ($R = \{(a, f(a)) : a \in A\}$) und W Wertebereich ($\{f(a) : a \in A\}$).

Definition 3.3 (Bild von D)**.** *Sei $D \subset A : f(D) = \{f(x) : x \in D\}$ (auch: Zielmenge, Wertemenge, Wertebereich)*

Definition 3.4 (Urbild von E)**.** *Sei $E \subset B : f^{-1}(E) = \{x \in A : f(x) \in E\}$. Das Urbild einer Teilmenge der Zielmenge von f ist eine Teilmenge der Definitionsmenge.*

Definition 3.5 (injektiv, auch: linkseindeutig)**.** *Sei $f : A \to B$. f ist injektiv, falls $x, y \in A$ und $x \neq y \Rightarrow f(x) \neq f(y)$*

Elemente aus A bilden nicht auf dasselbe Element in B ab. Wie kann man zeigen, dass eine Funktion injektiv ist? Zeige: $f(x) = f(y) \Rightarrow x = y$.

Definition 3.6 (surjektiv, auch: rechtstotal)**.** *Sei $f : A \to B$. f ist surjektiv, falls $f(a) = B$*

Auf jedes Element der Wertemenge B wird abgebildet.

Definition 3.7 (bijektiv)**.** *Sei $f : A \to B$. f ist bijektiv, wenn injektiv und surjektiv.*

f bijektiv, dann immer umkehrbar. Man kann die Umkehrfunktion definieren: $f^{-1} : B \to A, b \to a$ mit $f(a) = b$

Beweis. Sei $f : A \to B$
f surjektiv $\Rightarrow \exists a$ mit $f(a) = b$
f injektiv $\Rightarrow$ Es gibt höchstens ein a mit f(a)=b. □

3.5.1 Umkehrabbildung

$$f: \begin{array}{ccc} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 5 & 0 & 3 \end{array}$$

$$f^{-1}: \begin{array}{ccc} 0 & 3 & 5 \\ \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 \end{array}$$

Die Umkehrfunktion von f^{-1} ist f.

3.5.2 Komposition

Definition 3.8 (Komposition)**.** *Für* $A \xrightarrow{f} B \xrightarrow{g} C$ *schreibt man auch* $g \circ f$ *(Komposition):* $g \circ f : A \to C, a \to g(f(a))$
Es seien f und g ein Paar von Funktion und Umkehrfunktion.
$(g \circ f)(x) = x, g \circ f = id$
$(f \circ g)(x) = x, f \circ g = id$
$id(x) = x$

Satz 3.2. $f : A \to B$ *ist injektiv* $\Rightarrow \exists g : B \to A$ *mit* $g \circ f = id$*.*

4 Fehlererkennung

4.1 Fehlererkennender Code

Teilmenge C von V. Sender schickt $c \in C$. Empfänger empfängt c' aus V. Ist c' in C akzeptiert er, sonst lehnt er ab.

Beispiel (Übermitteln einer Vierstellige Zahl): Man fügt eine fünfte Zahl (Kontrollzahl) hinzu, sodass die $Quersumme = 0$ mod 10 ist.
$V = \{(a_1, ..., a_5) : a_i = 0, 1, ..., 9\}$
$C = \{(a_1, ..., a_5) \in V : a_1 + a_2 + a_3 + a_4 + a_5 = 0 \text{ mod } 10\}$
Code n zur Basis q: $C = \{(a_1, ..., a_5) : 0 \leq a_i \leq q - 1\}$
Paritätscode: Code der Länge n zur Basis q und

Es soll ein Vielfaches von 10 rauskommen

$$C \equiv \{(a_1, ..., a_5) : 0 \leq a_1 \leq q - 1 \text{ und } a_1 + ... + a_n = 0 \equiv q\}$$

Beispiel: $n = 5, q = 11$. Ist der Code $(3, 0, 10, 4, 5) \in C$?
$3 + 0 + 10 + 4 + 5 = 22$

Satz Jeder Paritätscode erkennt Einzelfehler (eine Stelle ändern).

Beweis Das Codewort ist $a_1, ..., a_i, ..., a_n$ Codewort
Es kommt zu einem Fehler $a_1, ..., \underbrace{a_i'}_{Fehler}, ..., a_n$

$$a_1 + a_i' + ... + a_n - \underbrace{(a_1 + ... + a_i + ... + a_n)}_{0} = a_i' - a_i \neq 0 \text{ mod } q$$

Vertauschungsfehler: a_i und a_j werden vertauscht. Ein Paritätscode erkennt keinen Vertauschungsfehler!

Idee: Gewichte! Basis q, n Stellen, Gewichte g_i mit $1 \leq g_i \leq q - 1$
$g_1a_1 + ... + g_na_n \equiv 0 \text{ mod } q$

Satz: Ist g_n teilerfremd zu q, so kann man immer die Kontrollziffer a_n ausrechnen.

Beweis $g_1a_1 + ... + g_na_n = 0$ mod q !
$g_na_n = -g_1a_1 - ... - g_{n-1}a_{n-1}$

$$a_n = \underbrace{g_n^{-1}}_{\text{existiert, da } g_n \text{ teilerfremd zu } q.} (-g_1a_1 - ... - g_{n-1}a_{n-1})$$

Satz: Ein Paritätscode mit Gewichten erkennt jeden Einzelfehler der Stelle a_i, wenn g_i und q teilerfremd sind.

Beweis: $a_1 \to a_1'(falsch)$
$g_1a_1' + ... + g_na_n =$
$g_1a_1' + ... + g_na_n - (g_1a_1 + ... + g_na_n) =$
$g_1a_1' - g_1a_1 = \underbrace{\underbrace{g_1}_{\neq 0}\underbrace{(a_1' - a_1)}_{\neq 0}}_{\text{Einheit } (g_1 \text{ teilerfremd zu } q). \text{ Kein Nullteiler.}} \neq 0$

Folgerung: Damit man alle Einzelfehler erkennen kann, müssen g_i teilerfremd zu q sein.

Satz: Ein Paritätscode mit Gewichten erkennt den Vertauschungsfehler $a_i \leftrightarrow a_j$, wenn $g_i - g_j$ teilerfremd zu q ist.

Beweis: Vertauschungsfehler, z.B.: $a_1 \leftrightarrow a_2$
$g_1a_2 + g_2a_1 + g_3a_3 + ... + g_na_n =$
$g_1a_2 + g_2a_1 + ... + g_na_n - (g_1a_1 + ... + g_na_n) =$
$g_1a_2 + g_2a_1 - g_1a_1 - g_2a_2 =$
$g_1(a_2 - a_1) + g_2(a_1 - a_2) =$
$g_1(a_2 - a_1) - g_2(a_2 - a_1) =$
$\underbrace{\underbrace{(g_1 - g_2)}_{\neq 0}\underbrace{(a_2 - a_1)}_{\neq 0}}_{Einheit, kein Nullteiler} \neq 0$ mod q

Beispiel: Ein Paritätscode der Länge 10 zur Basis $q = 11$.

	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}
g_i	10	9	8	7	6	5	4	3	2	1

Erkennt jeden Einzelfehler und jeden Vertauschungsfehler! Das ist der ISBN-Code bei den Büchern (10=X).

Beispiel (ISBN-Code): "Die letzte Stelle **2** kann nicht einfach gewählt werden, sondern muss stimmen! "

	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}
	3	1	5	7	2	2	1	8	9	**2**
g_i	10	9	8	7	6	5	4	3	2	1
Produkt 30	9	40	49	12	10	4	24	18		
mod 11	8	9	7	5	1	10	4	2	7	**2**

$\sum = 8 + 9 + 7 + 5 + 1 + 10 + 4 + 2 + 7 = 53 = 9$

4.2 Codes über Gruppen

Wiederholung: $(G, \cdot)$ ist eine Gruppe, wenn:

- $\cdot$ ist assoziativ
- Es gibt ein neutrales Element e
- Jedes a hat ein Inverses b, d.h. $ab = ba = e$

Das Inverse ist eindeutig und heißt a^{-1}

Satz Gleichungen der Form $ax = b$ sind eindeutig lösbar.

Beweis:

- Sei x eine Lösung $\Rightarrow ax = b \Rightarrow x = a^{-1}b$
- Setze $x = a^{-1}b \Rightarrow aa^{-1}b = b$

□

Satz: Die Abbildung

$$a_l : \quad \begin{cases} G \to G \\ x \to ax \end{cases}$$

ist bijektiv.

Beweis:

- injektiv: Sei $ax = ay \Rightarrow x = y$
- surjektiv: Falls $|G|$ endlich (klar!), $ax = b; x = a^{-1}b$

□

Beispiel 1: $(\mathbb{Z}, +), (\mathbb{Z}_n, +)$, $(\mathbb{Z}_n^*, \cdot), (\mathbb{R}, +), (\mathbb{R}^*, \cdot)$ Gruppen

Beispiel 2: Menge M: $G = \{f : M \to M, \text{mit f bijektiv}\}$
Komposition: (Hintereinanderausführung) $(G, \cdot)$ Gruppe. $e = id\ id(x) = x$. Das Inverse von f ist die Umkehrabbildung f^{-1}

Beispiel 3: Eine bijektive Abbildung der Ebene in sich heißt Kongruenz, wenn sie die Abstände erhält: $d(x, y) = d(\varphi(x), \varphi(y)) \Rightarrow$ Winkel bleiben erhalten.
Die Kongruenzen (vgl. Abb. 6) bilden bezüglich $\circ$ eine Gruppe.

- Verschiebungen
- Spiegelungen
- Drehungen
- Gleitspiegelungen

Beispiel 4 (Symmetrie einer ebenen Figur): Alle Kongruenzen, welche die Figur auf sich abbilden, bilden eine Gruppe (vgl. Abb. 7).
Gruppentafel

$\circ$	id	dr	h	g
id	id	dr	h	g
dr	dr	id	**g**	h
h	h	g	id	dr
g	g	h	dr	id

g: wegen $dr \circ h = g$ (erst h, dann dr)
$1 \to 4$
$2 \to 3$
$3 \to 2$
$4 \to 1$

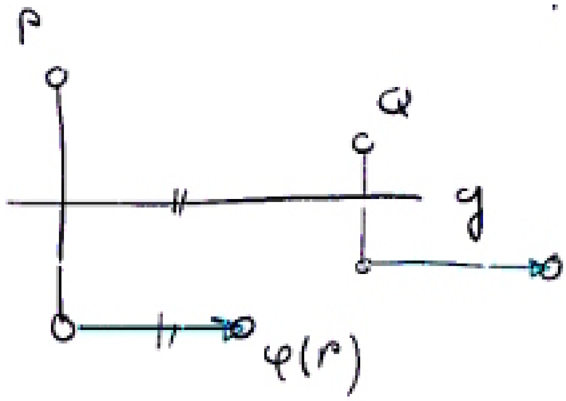


Abbildung 6: Das sind alle Kongruenzen

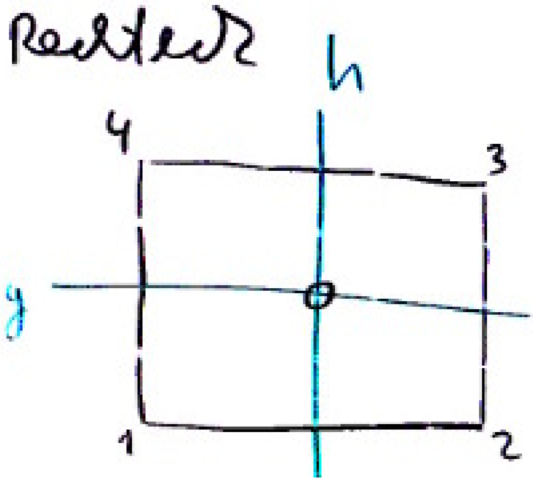


Abbildung 7: Spiegelungen an h,g, Drehungen um Z um 180° und id

Definition: Code über Gruppe $(G, \cdot)$ der Länge n und Kontrollsymbol $c \in G$: $\{(a_1, ..., a_n) \colon a_i \in G \text{ und } a_1 a_2 ... a_n = c\}$

Satz: Ein Gruppencode erkennt Einzelfehler.

Beweis:

$$(1)\ a_1(a_2...a_n) = c$$
$$(2)\ a'_1(a_2...a_n) = c$$
$$\Rightarrow a_1 = a'_1 \square$$

Ein Gruppencode kann einen Vertauschungsfehler erkennen oder nicht. Ist G kommutativ, so werden Vertauschungsfehler **nicht** erkannt.

$a_1 a_2 (a_3 ... a_n) = c$
$a_2 a_1 (a_3 ... a_n) = c$
$\Rightarrow a_1 a_2 = a_2 a_1$

Eine Gruppe eignet sich umso besser, je weniger sie kommutativ ist.

4.3 Permutationen

Eine Permutation ist eine bijektive Abbildung einer endlichen Menge auf sich.

$$\pi_1: \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 & 5 & 4 \end{array}$$

$$\pi_2: \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 5 & 1 & 2 & 4 & 3 \end{array}$$

$$\pi_1 \circ \pi_2 \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 2 & 5 & 3 & 4 \end{array}$$

$$\pi_2^{-1} \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 3 & 5 & 4 & 1 \end{array}$$

Gruppencode mit Permutationen: Länge n, Gruppe G, Permutationen der Gruppe: $\pi_1, \pi_2, ..., \pi_n$, Kontrollsymbol $c \subset G$.
$C = \{(a_1, ..., a_n) \colon a_i \in$ G und $\pi_1(a_1)\pi_2(a_2)....\pi_n(a_n) = c\}$

Satz: Ein Gruppencode mit Permutationen erkennt Einzelfehler.

Beweis: $\pi_1(a_1)....\pi_n(a_n) = c$
$\pi_1(a_1')\pi_2(a_2)....\pi_n(a_n) = c$
$\Rightarrow \pi_1(a_1) = \pi_1(a_1') \Rightarrow a_1 = a_1'$
$\square$

Satz: Ein Gruppencode mit Permutationen erkennt den Vertauschungsfehler der Stellen $i, i+1$, wenn Folgendes gilt:

- $\pi_i(g) \cdot \pi_{i+1}(h) \neq \pi_i(h) \cdot \pi_{i+1}(g)\ \forall g \neq h$

"klar" $\square$

Beispiel (Code der deutschen Geldscheine): Gruppe: *Diedergruppe* Ordnung 10. Das sind die Symmetrien des regelmäßigen 5-Ecks:

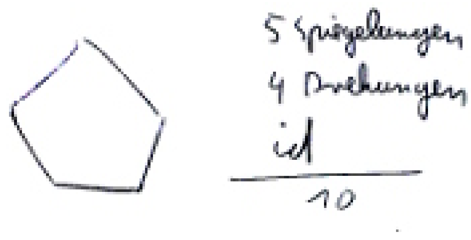


Abbildung 8: Fünfeck: 5 Spiegelungen, 4 Drehungen, id (10)

Bilden Gruppe (10 Elemente). Wir bezeichnen die Symmetrien mit $0, 1, ..., 9$ ($0 \widehat{=} id$). Der Code soll die Länge n = 11 haben. Das Kontrollsymbol c sei 0. Wir benötigen 11 Permutationen.

$$\pi_1 : \begin{array}{cccccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 5 & 7 & 6 & 2 & 8 & 3 & 0 & 9 & 4 \end{array}$$

$\pi_2 = \pi_1 \circ \pi_1 = \pi_1^2$
$\pi_3 = \pi_1 \circ \pi_1 \circ \pi_1 = \pi_1^3$
$\vdots$
$\pi_{11} = \pi_1^{11}$
$Code = \{(a_1, a_2, ..., a_{11}) \colon 0 \leq a_i \leq 9 \text{ und } \pi_1(a_1)\pi_2(a_2)...\pi_{11}(a_{11}) = 0\}$
Wie berechnet man die "Kontrollziffer" a_{11}? $c = 0$
$\pi_1(a_1)...\pi_{11}(a_{11}) = c$
$\pi_{11}(a_{11}) = [\pi_1(a_1)...\pi_{10}(a_{10})]^{-1} \cdot c$
$a_{11} = \pi_{11}^{-1}[(\pi_1(a_1...\pi_{10}(a_{10}))^{-1} \cdot c]$

Beispiel (Symmetrie eines gleichseitigen Dreiecks) Spiegelungen w1, w2, w3, Drehungen um Z 120, 240 und id (vgl. Abb. 9)

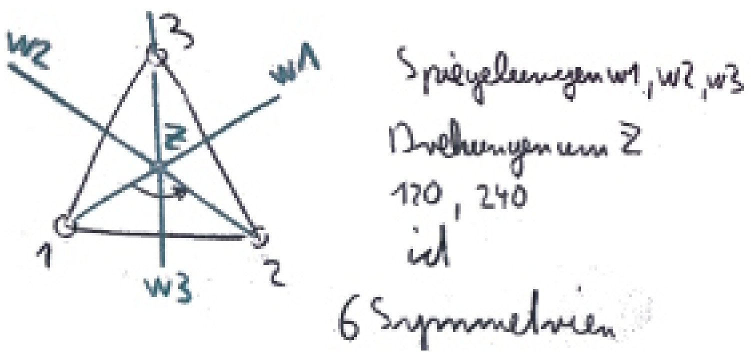


Abbildung 9: Gleichseitiges Dreieck

Gruppentafel

$\circ$	id	w1	w2	w3	120	240
id	id	w1	w2	w3	120	240
w1	w1	id	120	240	w2	w3
w2	w2	240	id	120	w3	w1
w3	w3	120	240	id	w1	w2
120	120	w3	w1	w2	240	id
240	240	w2	w3	w1	id	120

5 Graphentheorie

5.1 Königsberger Brückenproblem

Ziel: Eine Tour über die Brücken. Jede Brücke soll nur einmal benutzt werden. Start- und Endpunkt sollen gleich sein. Lösung: Das Problem wird mit Hilfe der Graphentheorie modelliert.

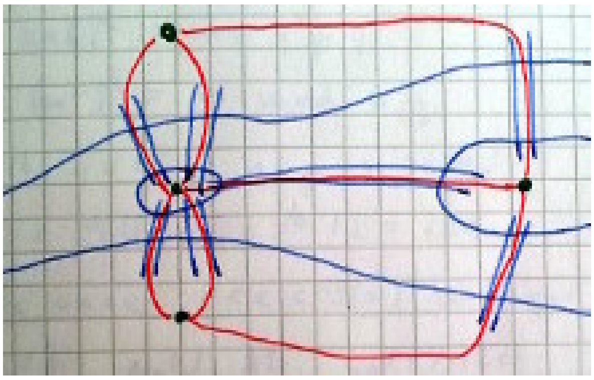


Abbildung 10: 7 Brücken

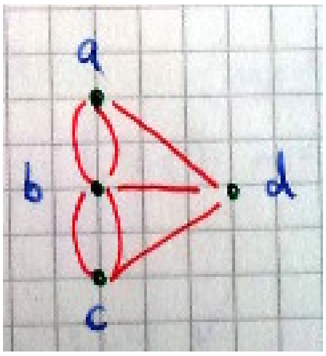


Abbildung 11: Abstraktion 7 Brücken

ein Graph $G = (V, E)$
V: Knotenmenge (endlich)
E: Kantenmenge $E \subseteq \binom{v}{2}$
$V = \{a, b, c, d\}$
$E = \{\{a, b\}, \{a, b\}, \{b, c\}, \{b, c\}, \{a, d\}, \{b, d\}, \{c, d\}\}$
Knotengrad (Grad): $deg(v)$ = Anzahl von Kanten mit v inzident

Eulertour ist eine Tour, die jede Kante genau einmal benutzt. Anfangspunkt und Endpunkt sind identisch.

Beispiel Gegeben ist der Graph G (vgl. Abb. 12). Gesucht ist eine Eulertour ($\Rightarrow G$ eulersch). Eine mögliche Eulertour ist $ae_qbe_3de_5ce_{12}be_2ee_7de_6fe_8ee_{11}ge_{10}fe_9ce_4a$

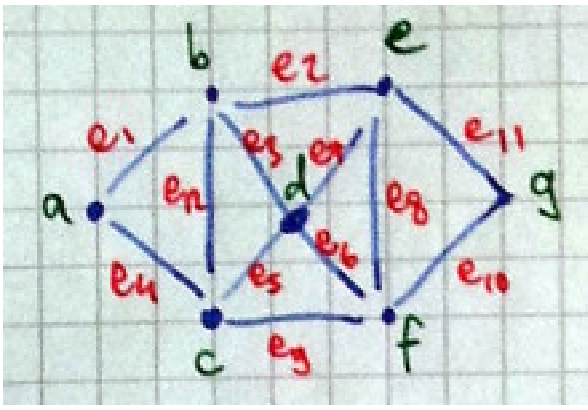


Abbildung 12: Eulertour

Definition G ist eulersch, wenn

- G zusammenhängend
- deg(v) gerade $\forall v \in V$

Das sind zwei notwendige Bedingungen für die Eigenschaft *eulersch*. Sind sie auch hinreichend? G ist zusammenhängend, da es für je zwei Knoten u,v eine Kantenfolge gibt (ein Weg, vgl. Abb. 13).

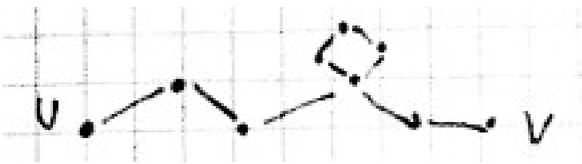


Abbildung 13: Ein zusammenhängender Graph

Satz: Ein zusammenhängender Graph G besitzt genau dann eine Eulertour, wenn alle Knoten einen geraden Grad haben.

Beweis: Im Beispiel findet man auf Anhieb eine geschlossene Kantenfolge (auch: Kreis, z.B. $\{a, b, c, d\}$ orange) finden. Eine weitere ist $\{b, e, f, c\}$ (rot). Beide lassen sich zu einer Kantenfolge zusammenfassen (grün) und solange erweitern, bis alle Kanten bedeckt sind (blau). $\square$

5.2 Haus vom Nikolaus

15 $deg(d), deg(e)$ ungerade. Wir suchen eine offene Eulertour (Kantenfolge, diesmal aber Anfangspunkt $\neq$ Endpunkt).

Bemerkung: In jedem Graphen ist die Anzahl von Knoten ungeraden Grades gerade: $\sum_{v \in V} deg(v) = 2m$ mit m Anzahl Kanten.

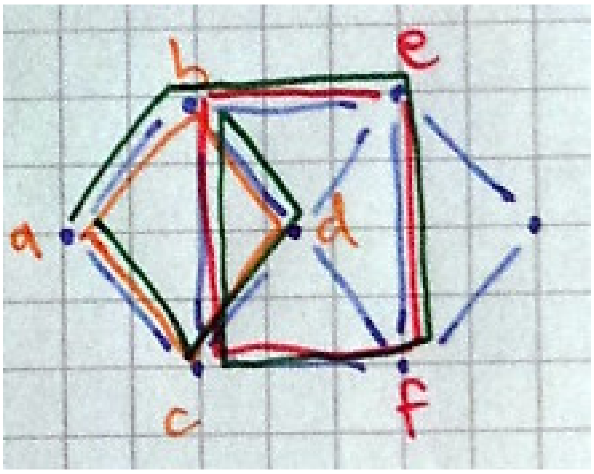


Abbildung 14: Mehrere zusammenhängende Kantenfolgen

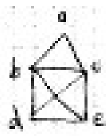


Abbildung 15: Das ist das Haus ...

Satz: Ein zusammenhängender Graph G besitzt genau dann eine **offene** Eulertour, wenn alle Knoten **bis auf zwei** einen geraden Grad haben.

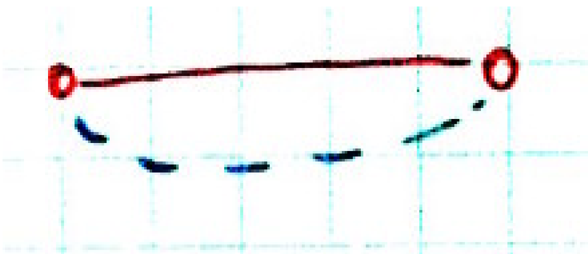


Abbildung 16: Offene Eulertour

5.3 Hamiltonkreise

Hamiltonkreise sind Kreise, die jeden Knoten genau einmal besuchen. Im Graph 17 wird ein Hamiltonkreis gesucht.

Beispiel: Ist G (Abb. 18) hamiltonsch? Der Graph hat 10 Knoten. Es gibt einen Kreis, der aber nur maximal 9 Knoten hat. Daher ist G nicht hamiltonsch. Er heißt **Peterson-Graph**.

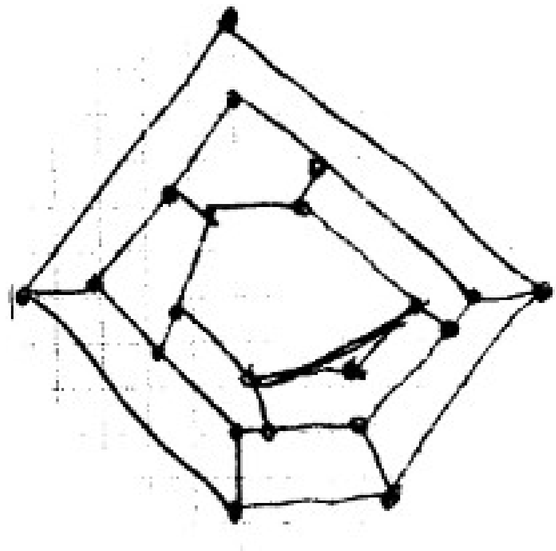


Abbildung 17: Wo ist der Hamiltonkreis?

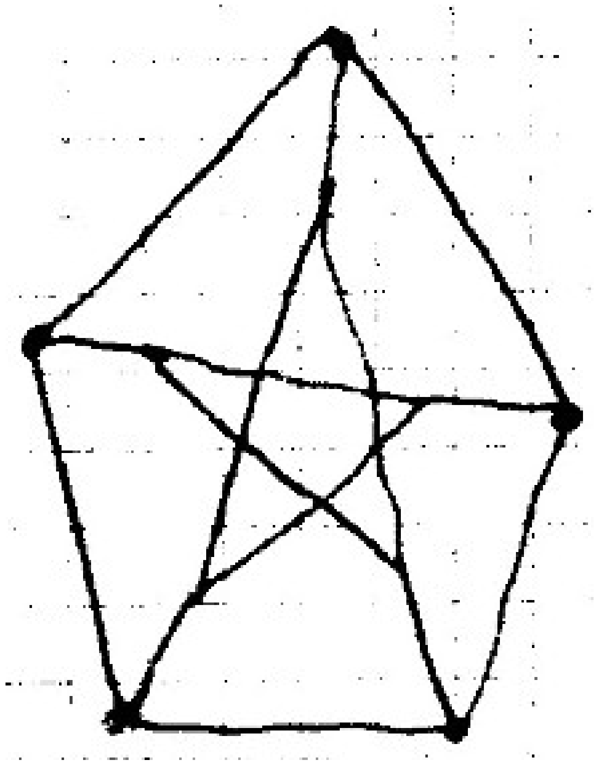


Abbildung 18: Ist der graph hamiltonsch?

Satz: Ist $deg(u) = deg(v) \geq n$, mit n Anzahl Knoten und u,v nicht benachbart $\Rrightarrow$ G ist hamiltonsch (nicht umgekehrt!).

Beispiel: $V = \{u, v\}, n = 6$
$deg(a) + deg(b) = 6 \geq 6 \Rightarrow OK$
$def(u) + deg(v) = 4 < 6 \Rightarrow nichtOK$
$def(u) + deg(c) = 5 < 6 \Rightarrow nichtOK$

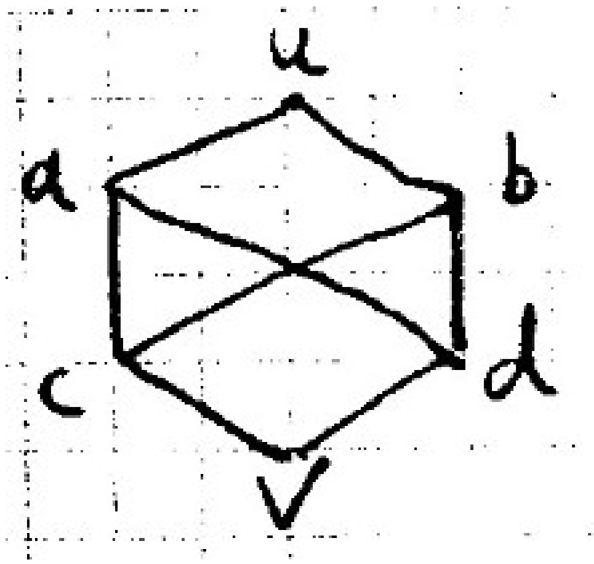


Abbildung 19: Ist der graph hamiltonsch?

Idee Hülle (Hamilton Abschluss): $n - 1 = deg_G(u) + deg_G < n$
$deg_{G'}(u) + deg_{G'}(a) = n$
G nicht hamiltonsch und $deg_G(u) + deg_G(v) \geq n \Rightarrow G' = G + uv$ nicht hamiltonsch.

Bemerkung G ist hamiltonsch $\Rrightarrow G' = G + uv$ hamiltonsch.

Beweis: ausgelassen.

Obere Schranke für die Anzahl der Knoten: $deg(u) \leq n - 1 < n$

Beispiel (Tiefensuche): Man kann Hamiltonkreise mithilfe der Tiefenbaumsuche finden. Interessant dabei ist, wie lange die Suche dauert.
Grad: höchstens n (vgl. obere Schranke)
Tiefe: $n - 1 < n$
$\Rightarrow n^n \approx e^n \approx 2^n = 1024$

5.4 Chinesisches Postboten-Problem

Jetzt werden dem bekannten Graphen G Längen zugeordnet, d.h. der Graph wird **gewichtet**. Gesucht wird die kürzeste Tour durch alle Punkte.

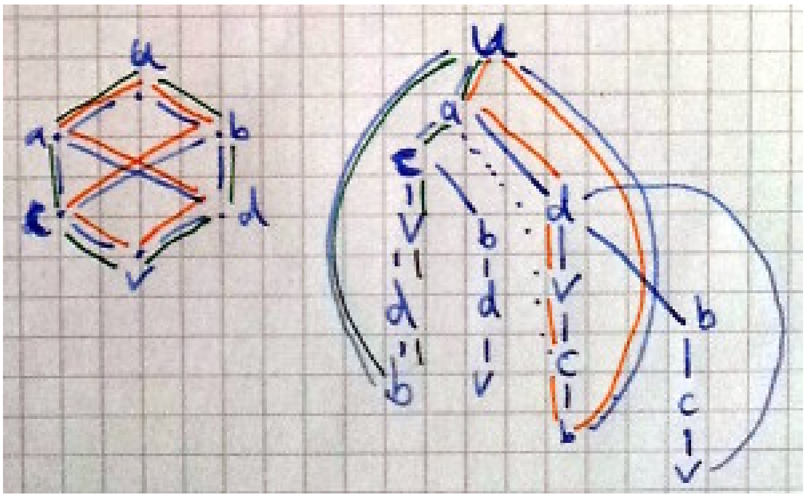


Abbildung 20: Tiefensuche

Falls G eulersch ist, dann ist die Lösung die Eulertour. Was gilt, wenn G nicht eulersch ist?

Beispiel (Haus vom Nikolaus): Gesucht wird der kürzeste Weg zwischen zwei Punkten. Dabei betrachten wir die Länge der offenen Eulertour. Die Länge entspricht der Summe der gewichteten Kanten.
In diesem Fall: Länge = 29.
$+uv = 39$
$+uav = 32$
$+ubv = 36$
Dabei ist uav die kürzeste Strecke unter allen Kantenfolgen.

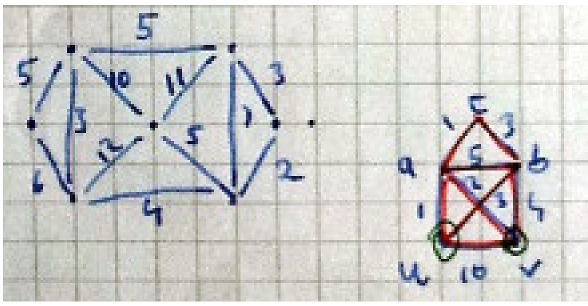


Abbildung 21: Das Haus vom Nikolaus

5.5 Das Problem des Handlungsreisenden

Wir suchen den kürzesten Hamiltonkreis. Eine Möglichkeit der Lösung ist die Tiefensuche.

6 Symmetrien des gleichseitigen Dreiecks (Wiederholung)

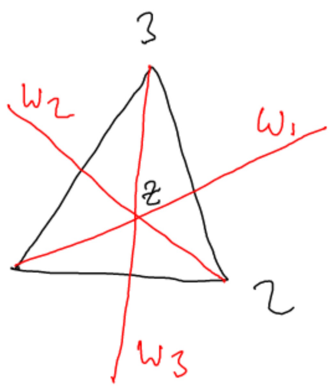


Abbildung 22: Spiegelungen an w1, w2, w3, Drehungen 120, 240, id

∘	id	w1	w2	w3	120	240
id	id	w1	w2	w3	120	240
w1	w1	id	120	240	w2	w3
w2	w2	240	id	120	X	w1
w3	w3	120	240	id	w1	w2
120	120	w3	w1	w2	240	id
240	240	w2	w3	w1	id	120

X machen wir ausführlich: $w2 \circ 120$, $1 \rightarrow 2$, $2 \rightarrow 1$, $3 \rightarrow 3$, $\Rightarrow X = w3$

Gruppencode (ohne Permutationen) der Länge $n = 7$ mit Kontrollsymbol $c = id$: $w1, 120, w1, w3, 120, w3, x$, berechne x passend.

$w1 \circ 120 \circ w1 \circ w3 \circ 120 \circ w3 \circ x = id$

$(w1 \circ 120) \circ (w1 \circ w3) \circ (120 \circ w3) \circ x = id$

$(w2 \circ 240) \circ w2 \circ x = id$

Klammerung wegen Assoziativität beliebig!

$(w1 \circ w2) \circ x = id$

$120 \circ x = id$

$\Rightarrow x = 240$

Gruppencode (mit Permutationen) der Länge $n = 4$ mit Permutationen, Kontrollsymbol $c = id$

$$\begin{array}{lcccccc} & id & w1 & w2 & w3 & 120 & 240 \\ \pi_1: & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & w1 & 120 & id & 240 & w2 & w3 \end{array}$$

$$\begin{array}{lcccccc} & id & w1 & w2 & w3 & 120 & 240 \\ \pi_2: & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 120 & id & 240 & w1 & w2 & w3 \end{array}$$

$$\begin{array}{lcccccc} & id & w1 & w2 & w3 & 120 & 240 \\ \pi_3: & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & w3 & 120 & w1 & 240 & w2 & id \end{array}$$

$$\pi_4: \begin{array}{cccccc} id & w1 & w2 & w3 & 120 & 240 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 240 & w3 & w1 & w2 & id & 120 \end{array}$$

$w1, 240, w3, x$ berechne x passend:
$\pi_1(w1) \circ \pi_2(240) \circ \pi_3(w3) \circ \pi_4(x) = id$
$(120 \circ w3) \circ 240 \circ \pi_4(x) = id$
$w1 \circ \pi_4(x) = id$
$\Rightarrow \pi_4(x) = w1$
$\Rightarrow x = w2$

Beispiel ISBN-Code: Paritätscode mit Gewichten der Länge $n = 10$ mit Basis $q = 11$. Zeichen: $0, 1, 2, ..., 9, 10 = x$

	$a1$	$a2$	$a3$	$a4$	$a5$	$a6$	$a7$	$a8$	$a9$	$a10$
Gew	10	9	8	7	6	5	4	3	2	1

Ergänze zu einem Code-Wort: 3-528-06783-a:
$3 \cdot 10 + 5 \cdot 9 + 2 \cdot 8 + 8 \cdot 7 + 0 \cdot 6 + 6 \cdot 5 + 7 \cdot 4 + 8 \cdot 3 + 3 \cdot 2 + a \cdot 1 = 0$ mod 11
$30 + 45 + 16 + 56 + 30 + 28 + 24 + 6 + a = 0$
$8 + 1 + 5 + 1 + 8 + 6 + 2 + 6 + a = 0$
$37 + a = 0$
$4 + a = 0 \Rightarrow a = 7$

7 Kryptographie

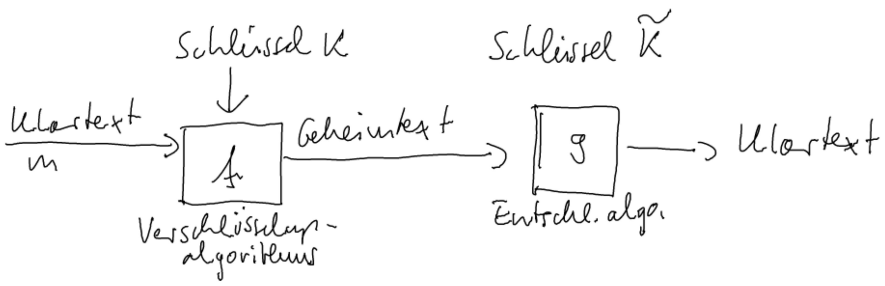


Abbildung 23: Verschlüsselung und Entschlüsselung (f, g sind öffentlich und k, $\tilde{k}$ geheim)

symmetrisch $k = \tilde{k}$ oder $\tilde{k} = k$ kann aus k leicht berechnet werden.

asymmetrisch $k \neq \tilde{k}, \tilde{k}$ kann nicht oder nur sehr schwer berechnet werden.

7.1 Symmetrische Verfahren

7.1.1 Stromchiffren

Als Klartext nehmen wir eine Bitfolge. Der geheime Schlüssel auch.

Nachteil des Verfahrens: langer Schlüssel

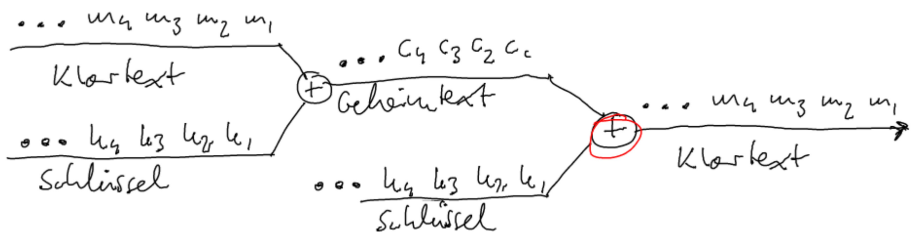
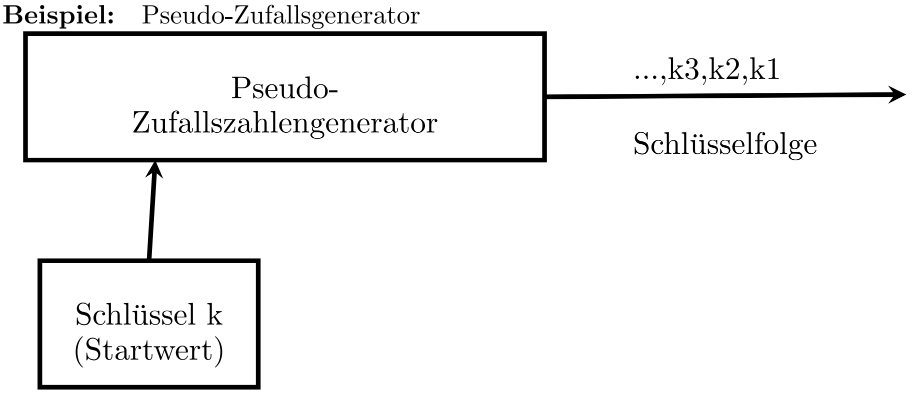


Abbildung 24: Funktionsweise symmetrische Verschlüsselung. Die Rote + Operation ist eigentlich eine - Operation. Bei Bits, also mod 2, kann aber Plus durch Minus ersetzt werden.

Beispiel: Pseudo-Zufallsgenerator



binäres Schieberegister Wir rechnen mod 2

- Berechne $w = c_1 s_1 + c_2 s_2 + ... + c_n s_n$
- s1 ausgeben
- Alle s_i um eins nach rechts schieben
- $s_n := w$

Der Schlüssel ist die erste Belegung von $s_1, ..., s_n$

Beispiel Zellen gleiche Belegung: Dann geht es von vorne los → Der Schlüsselstrom ist periodisch.

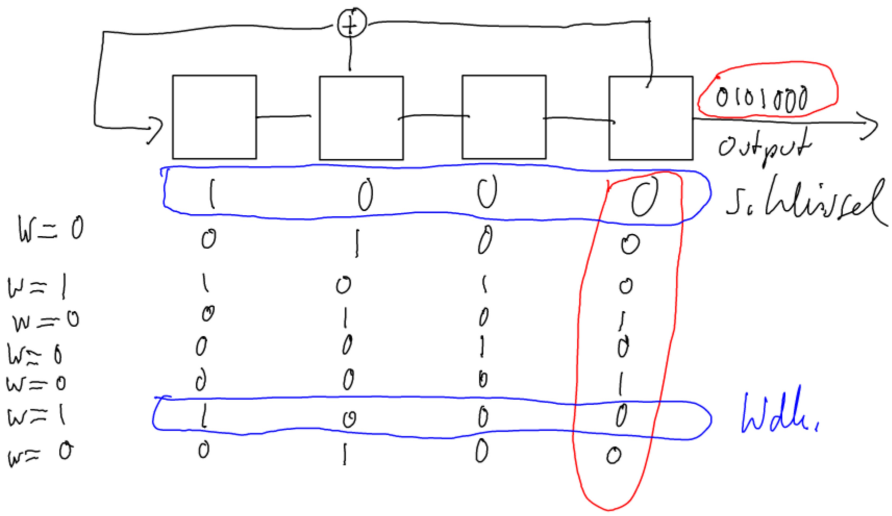


Abbildung 25: Beispiel

7.2 Blockverschlüsselung

Es werden nun Blöcke fester Länge verschlüsselt. Es gibt verschiedene Modi.

7.2.1 EBC-Mode

Jeder Block wird unabhängig von den anderen Blöcken verschlüsselt.

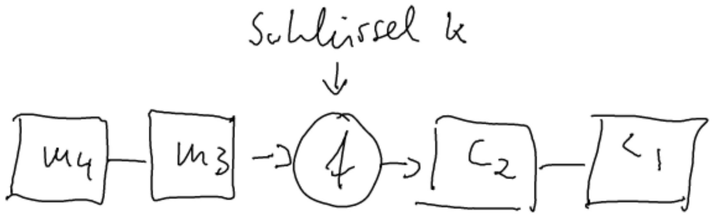


Abbildung 26: Blockverschlüsselung

Beispiel: Alphabet: $\{0, 1, 2, ..., 9\}$ mit der Blocklänge 5. Verschlüsselung mittels Permutationen (geheim)
$c(i) := m(\pi(i))$:
π:

$$\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 4 & 1 & 5 & 3 \end{array}$$

Verschlüsseln:
π^{-1}:

$$\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 1 & 5 & 2 & 4 \end{array}$$

Entschlüsseln: $c(\pi^{-1}(i)) = m(\pi(\pi^{-1}(i))) = m(i)$
$m(i) = c(\pi^{-1}(i))$

Beispiel: Klartext $m = (3, 2, 1, 0, 1)$ mit $m(3) = 1, m(5) = 1$
Verschlüsseln:
$c(1) = m(\pi(1)) = m(2) = 2$
$c(2) = m(\pi(2)) = m(4) = 0$
$c(3) = 3$
$c(4) = 1$
$c(5) = 1$
$c = (2, 0, 3, 1, 1)$
Entschlüsseln:
$m(1) = c(\pi^{-1}(1)) = c(3) = 3$
$m(2) = c(\pi^{-1}(2)) = c(1) = 2$
$m(3) = c(5) = 1$
$m(4) = c(2) = 0$
$m(5) = c(4) = 1$

$m = (3, 2, 1, 0, 1)$

7.2.2 CBC-Mode

Startwert: c_0 öffentlich
Alphabet: $(\mathbb{Z}_n, +)$
Verschlüsseln: $c_i := f(c_{i-1} \oplus m_i)$
Entschlüsseln: $m_i := f^{-1}(c_i) \ominus c_{i-1}$
Verschlüsselung von m hängt ab, wo m steht (Anfang, Mitte oder Ende). Bei mod 2 ist $\oplus$ und $\ominus$ das gleiche.

Beispiel: Alphabet: $(\mathbb{Z}_2, +)$, mod 2
Blocklänge: $n = 5$
Verschlüsselung f: Permutationen
Startwert (öffentlich): $c_0 = (1, 1, 1, 0, 0)$
π:
$$\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 3 & 5 & 1 & 4 \end{array}$$
π^{-1}:
$$\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 4 & 1 & 2 & 5 & 3 \end{array}$$
$m1 = (1, 0, 1, 0, 1), m2 = (0, 0, 1, 1, 0)$

Verschlüsseln: $c_1 = f(c_0 \oplus m_1) = f[(1, 1, 1, 0, 0) \oplus (1, 0, 1, 0, 1)] = f(0, 1, 0, 0, 1) = (1, 0, 1, 0, 0) = c_1$
$c_2 = f(c_1 \oplus m_2) = f[(1, 0, 1, 0, 0) \oplus (0, 0, 1, 1, 0)] = f(1, 0, 0, 1, 0) = (0, 0, 0, 1, 1) = c_2$

Entschlüsseln: $m_1 := f^{-1}(c_1) \ominus c_0 \to m_1 := f^{-1}(c_1) \oplus c_0$ (wegen mod 2)
$= f^{-1}(1, 0, 1, 0, 0) \oplus (1, 1, 1, 0, 0) = (0, 1, 0, 0, 1) \oplus (1, 1, 1, 0, 0) = (1, 0, 1, 0, 1)$

$m_2 = f^{-1}(c_2) \oplus c_1 = f^{-1}(0, 0, 0, 1, 1) \oplus (1, 0, 1, 0, 0) = (1, 0, 0, 1, 0) \oplus (1, 0, 1, 0, 0) = (0, 0, 1, 1, 0)$

7.2.3 CFB-Mode

Alphabet: $(\mathbb{Z}_m, +)$
Blockchiffre der Länge n: E_k
Der Klartext wird in Blöcke der Länge $r < n$ eingeteilt. Außerdem benötigen wir einen Startvektor/Initialisierungsvektor (IV) der Länge n.

Verschlüsseln: $I_1 = IV$

1. $O_j := E_k(I_j)$
2. $t_j :=$ Die ersten r Zeichen von O_j

3. $c_j := m_j \oplus t_j$
4. $I_{j+1} :=$ Die ersten r Zeichen von I_j löschen und c_j hinten anhängen.

Entschlüsseln: $I_1 = IV$

1. $O_j := E_k(I_j)$
2. $t_j :=$ Die ersten r Zeichen von O_j
3. $m_j := c_j \ominus t_j$
4. $I_{j+1} :=$ Die ersten r Zeichen von I_j löschen und c_j hinten anhängen.

Beispiel: Alphabet: $(\mathbb{Z}_1 0, +)$
Blockchiffre der Länge $n = 6$

$$\text{Permutation } \pi\text{:} \quad \begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 6 & 1 & 5 & 2 & 4 \end{array}$$

$IV = (2, 0, 8, 3, 3, 1)$
Klartext, Schlüsseltext: Blocklänge $r = 4$ $m_1 = (2, 0, 5, 1), m_2 = (9, 7, 1, 2)$

Verschlüsseln: $I_1 = (2, 0, 8, 3, 3, 1)$
1. Schritt:

1. $O_1 = E(I_1) = (8, 1, 2, 3, 0, 3)$
2. $t_1 = (8, 1, 2, 3)$
3. $c_1 = m_1 \oplus t_1 = (2, 0, 5, 1) \oplus (8, 1, 2, 3) = (0, 1, 7, 4)$
4. $I_2 = (3, 1, 0, 1, 7, 4)$

2. Schritt:

1. $O_2 = E(I_2) = (0, 4, 3, 7, 1, 1)$
2. $t_2 = (0, 4, 3, 7)$
3. $c_2 = m_2 \oplus t_2 = (9, 7, 1, 2) \oplus (0, 4, 3, 7) = (9, 1, 4, 9)$
4. $I_3 = (7, 4, 9, 1, 4, 9)$

Entschlüsseln: $IV = (2, 0, 8, 3, 3, 1)$
1. Schritt

1. $O_1 = E(I_1) = (8, 1, 2, 3, 0, 3)$
2. $t_1 = (8, 1, 2, 3)$
3. $m_1 = c_1 \ominus t_1 = (0, 1, 7, 4) \ominus (8, 1, 2, 3) = (2, 0, 5, 1)$✓
4. $I_2 = (3, 1, 0, 1, 7, 4)$

2. Schritt

1. $O_2 = E(I_2) = (0, 4, 3, 7, 1, 1)$
2. $t_2 = (0, 4, 3, 7)$
3. $m_2 = c_2 \ominus t_2 = (9, 1, 4, 9) \ominus (0, 4, 3, 7) = (9, 7, 1, 2)$✓
4. $I_3 = (7, 4, 9, 1, 4, 9)$

8 Graphentheorie

Graph: Ein Graph besteht aus Ecken und Kanten. Jede Kante verbindet zwei verschiedene Ecken.

vollständig Jede Ecke wird mit jeder anderen Ecke durch genau eine Kante verbunden. G vollständig mit n Ecken $\Rightarrow Kantenzahl = \binom{n}{2} = \frac{n(n-1)}{1 \cdot 2}$

Abbildung 27: vollständige Graphen

8.1 G heißt bipartit,

wenn man seine Ecken in 2 Klassen einteilen kann, so dass jede Kante die zwei Klassen verbindet.

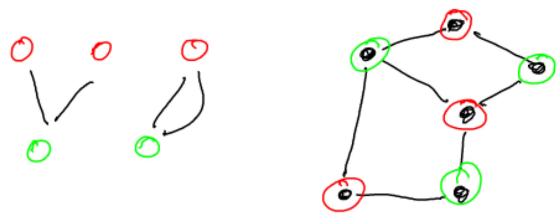


Abbildung 28: bipartite Graphen

8.2 Kantenzug:

$e_0 k_1 e_1 k_2 e_2 k_3 e_3 k_4 e_4$
e_i: Ecken
k_i: Kanten (k_i verbindet e_{i-1} und e_i)
Der Kantenzug verbindet Anfangs- und End-Ecke. Anfangs- und End-Ecke können identisch sein.

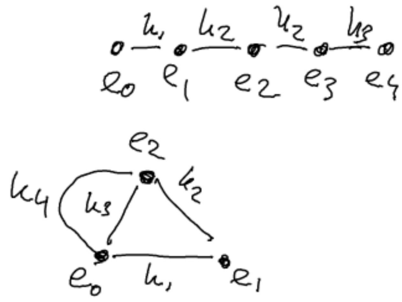


Abbildung 29: Ein Kantenzug

8.3 Definition zusammenhängender Graph:

Ein Graph heißt zusammenhängend, wenn je zwei Ecken durch einen Kantenzug verbunden werden können.

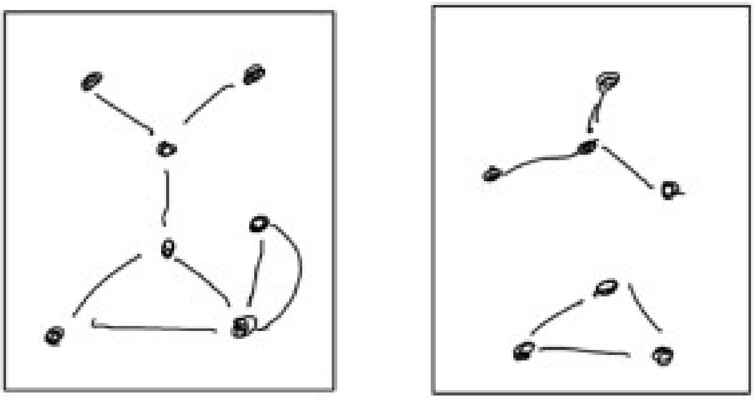


Abbildung 30: Ein zusammenhängender Graph und ein Graph mit zwei Zusammenhangskomponenten

8.4 Kantenzüge

8.4.1 Länge eines Kantenzugs

Die Anzahl der durchlaufenen Kanten.

8.4.2 geschlossene Kantenzüge

Ein Kantenzug heißt geschlossen, wenn die Anfangsecke gleich Endecke ist.

8.4.3 Weg

Ein Kantenzug heißt Weg, wenn alle seine Kanten verschieden sind.

8.4.4 Kreis

Ein Weg heißt Kreis, wenn Anfangsecke gleich Endecke ist.

8.4.5 Grad einer Ecke

Anzahl der Kanten die die Ecke verlassen.

8.5 Das Königsberger Brückenproblem

Es gibt einen Fluss mit zwei Inseln und 7 Brücken. Gibt es einen Spaziergang (Kreis), so dass man über jede Brücke genau einmal geht und am Ende wieder am Anfangspunkt ist?

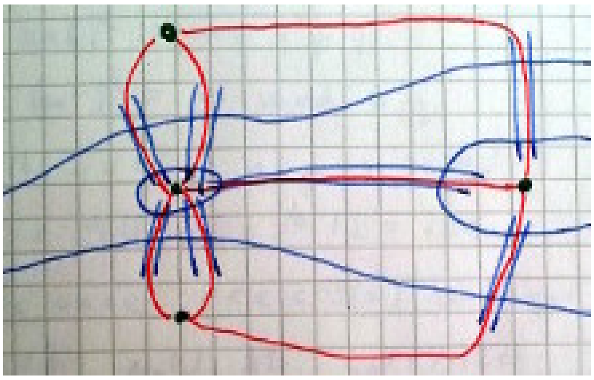


Abbildung 31: Königsberger Brückenproblem

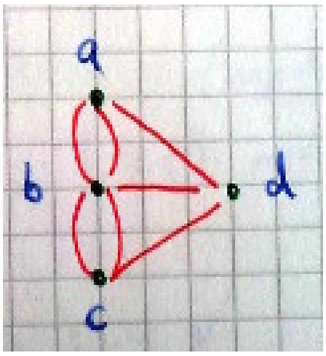


Abbildung 32: Königsberger Brückenproblem als Graph

eulersch Ein Kreis eines Graphen heißt eulersch, wenn in ihm jede Kante genau einmal vorkommt und die Anfangsecke gleich der Endecke ist. Das Brückenproblem kann umformuliert werden: Hat der Graph einen eulerschen Kreis?

8.5.1 vollständiger Graph mit 5 Ecken

Das Brückenproblem kann umformuliert werden: Hat der Graph einen eulerschen Kreis? Als erstes sehen wir uns ein Beispiel (Abb. 33) an.

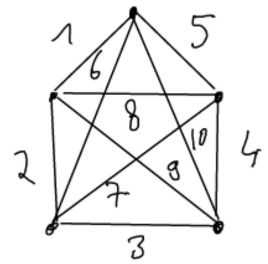


Abbildung 33: eulerscher Kreis mit 10 Kanten

Satz: Sei G ein zusammenhängender Graph und jede Ecke habe einen Grad ≥ 2. Dann gibt es einen Kreis in G.

Beweis: mittels Beispiel (Abb. 34). Man fängt irgendwo an und findet in A1B2C3D4E5B den einen Kreis B2C3D4E5B. □

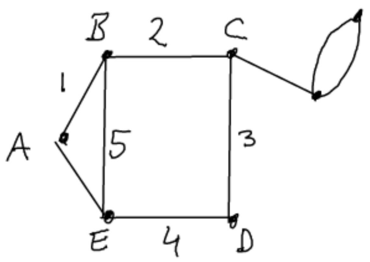


Abbildung 34: Kreise finden in Graphen

Satz (Euler 1736): Wenn G einen eulerschen Kreis hat, dann hat jede Ecke von G geraden Grad.

Beweis: Wir durchlaufen den eulerschen Kreis und malen dabei die Kanten rot an (Abb. 35). Einmal durchlaufen → Grad 2, zweimal durchlaufen → Grad 4. Grad Anfang und Ende: 1 (Start) + 2 (je Durchlauf) + 1 (Ziel) → gerader Grad.

Das Brückenproblem ist demnach **nicht** eulersch.

Satz: Wenn in einem zusammenhängenden Graphen jede Ecke geraden Grad hat, dann ist der Graph eulersch.

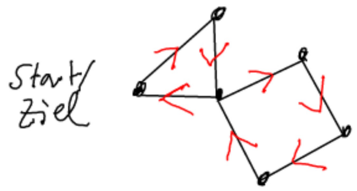


Abbildung 35: Ein eulerscher Grad

Beweis: Induktionsbeweis nach Anzahl m der Kanten (Abb. 36).

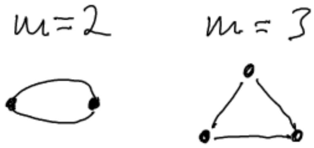


Abbildung 36: Richtig für $m = 2, m = 3$

Angenommen richtig für $Kantenzahl < m$.
Zeige: Dann richtig für m Kanten.
Sei also G ein zusammenhängender Graph mit m Kanten und jede Ecke hat geraden Grad. Dann gibt es einen Kreis in G (siehe oben). Wir betrachten einen Kreis C in G, der maximale Länge hat. Dann ist C ein eulerscher Kreis (Behauptung), wegen:

Widerspruchsbeweis: Angenommen C ist **nicht** eulersch. Wir entfernen die Kanten von C aus G. Vom Restgraphen betrachten wir eine Zusammenhangskomponente Z. Jede Ecke von Z hat geraden Grad (da die Kanten von einem Kreis entfernt wurden). $\underbrace{\Rightarrow}_{I.V.}$ Z hat eulerschen Kreis.
Eine Ecke von Z wird von C getroffen (Abb. 37). Dann kann der Kreis C vergrößert werden. **Widerspruch, da C maximale Länge hatte!** $\Rightarrow$ C ist eulerscher Kreis $\square$

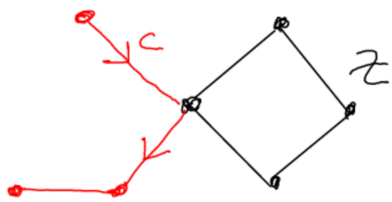


Abbildung 37: Kreis C und Zusammenhangskomponente Z

Folgerung: Der vollständige Graph mit n Ecken ist eulersch, wenn n ungerade ist.

Definition: Ein Weg, der kein Kreis ist, heißt offene eulersche Linie, wenn jede Kante darin vorkommt ($\Rightarrow genaueinmalvorkommt$).

Satz: Wenn G eine offene eulersche Linie hat, dann hat G **genau zwei** Ecken mit ungeradem Grad.

Beweis: Die rote Linie verbindet A und B (Abb. 38). Dann ist das ein eulerscher Kreis. □

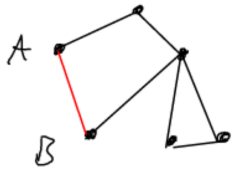


Abbildung 38: offene eulersche Linie

Satz: Für jeden zusammenhängenden Graphen gilt: Wenn es genau zwei Ecken mit ungeradem Grad gibt, dann hat G eine offene eulersche Linie.

Beweis: Gegeben ist die offene eulersche Linie (schwarz). Verbinde A und B durch eine Kante (rot). Jetzt hat jede Ecke geraden Grad $\Rightarrow$ Es gibt einen eulerschen Kreis. Dieser kann z.B. so aussehen: $e_0k_1e_1k_2e_2k_3e_3k_4e_4k_5e_5$ Rote Kante könnte z.B. k_4 sein $\Rightarrow$ offene eulersche Linie: $e_4k_5e_0k_1e_1k_2e_2k_3e_3$. Verbindet e4 und e3. Start- und Endpunkt haben ungeraden Grad. □

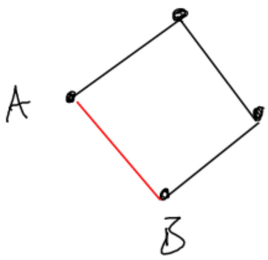
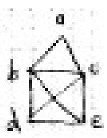


Abbildung 39: Eulersche Linie

8.6 Das Haus vom Nikolaus

Genau zwei Ecken mit ungeradem Grad (links- und rechtsunten, also A und B) $\Rightarrow$ offene eulersche Linie mit Start/Ende: A, B. Man muss bei A oder B anfangen! 

9 Lösung zur Prüfung SS 2011

9.1 Aufgabe 1

9.1.1 1a

$\overbrace{x^2}^{a^2} + \overbrace{10x}^{2b} + 1 = 11$
$x^2 + 2 \cdot 5x + 5^2 = 11 - 1 + 5^2$
$(x+5)^2 = 10 + 25 = 35 = 9$
$x + 5 = \pm 3$
$x_1 + 5 = 3, x_1 = -2 = 11$
$x_2 + 5 = -3, x_2 = -8 = 5$

$(a+b)^2 = a^2 + 2ab + b^2$

9.1.2 1b

$I : x + 2y = 12$
$II : 3x + y = 11 \Rightarrow y - 6y = 11 - 36 = -25$
$-5y = -25 \Rightarrow y = 5$
in I einsetzen: $x + 2 \cdot 5 = 12 \Rightarrow x = 2$

9.2 Aufgabe 2

9.2.1 2a

$\mathbb{Z}_{14}^* = \{1, 3, 5, 9, 11, 13\}$

$\cdot$	1	3	5	9	11	13
1	1	3	5	9	11	13
3	3	9	1	13	5	11
5	5	1	11	3	13	9
9	9	13	3	11	1	5
11	11	5	13	1	9	3
13	13	11	9	5	3	1

Hinweis: In jeder Zeile/Spalte kommt jede Zahl **genau einmal** vor!

9.2.2 2b

$\pi_1(a) \cdot \pi_2(b) \cdot \pi_3(c) = 1$
$\pi_1(3) \cdot \pi_2(11) \cdot \pi_3(x) = 1 \; 11 \cdot 3 \cdot \pi_3(x) = 1$
$5 \cdot \pi_3(x) = 1$
$\pi_3(x) = 3 \Rightarrow x = 9$

(3,11,·)

Löse: 5 mal was ist 1?

9.3 Aufgabe 3

$1, 2, 3, 5, 8, 13, ...$
$fib(n) = fib(n-1) + fib(n-2)$
Anzahl der Möglichkeiten: $g(n)$

Induktionsanfang: $n = 1$
$g(1) = 1, fib(1) = 1$

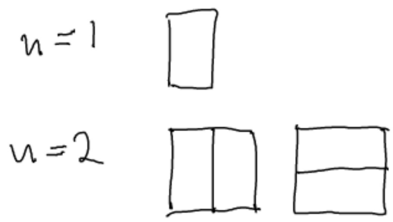


Abbildung 40: Der Induktionsanfang für $n = 1, n = 2$

$n = 2$
$g(2) = 2, fib(2) = 2$

Induktionsschritt: Anfänge (Abb. 41):

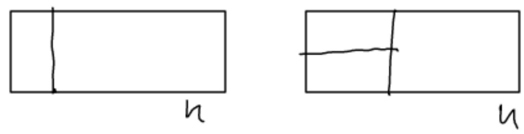


Abbildung 41: Mögliche Anfänge bei den Dominosteinen

$g(n) = g(n-1) + g(n-2) = fib(n-1) + fib(n-2) = fib(n)$

9.4 Aufgabe 4

9.4.1 Direktlösung

A hat 33 Zähne (0 bis 32), B hat 14 Lücken (0 bis 13).

Wann greift Zahl 6 von A in die Lücke 10 von B? x ist die Anzahl der Zähne.
$z + k \cdot 33 = 9 + t \cdot 14 = x$
$x \equiv 2 \bmod 33$ (chin. Restsatz)
$x \equiv 9 \bmod 14$

(mod 14!)

In welche Lücken greift der Zahn 6 von A? $3, 3 - 33 = -30 = 12, 12 - 33 = -21 = 7, 7 - 33 = -26 = 2, 2 - 33 = -31 = 11, 11 - 33 = -22 = 6, 6 - 33 = -27 = 1, 1 - 33 = -32 = \underline{\mathbf{10}}$
$x = 2 + 7 \cdot 33 = \underline{\mathbf{233}} = 9 + t \cdot 14$
$t = \frac{233-9}{14} = 16$

9.4.2 Lösung mit chinesischem Restsatz

$x \equiv a_1(= 2) \bmod m_1(= 33)$
$x \equiv a_2(= 9) \bmod m_2(= 14)$
$m_1 \cdot m_2 = 462$

$M_1 = 14, M_2 = 33$
$y_i \cdot M_i \equiv 1 \text{ mod } m_i$ $i = \frac{1}{2}$
$y_1 \cdot 14 \equiv 1 \text{ mod } 33$

euklidischer Algorithmus $ggT(33, 14)$
$33 = 2 \cdot 14 + 5$
$14 = 2 \cdot 5 + 4$
$5 = 1 \cdot 4 + 1$

Erweiterter euklidischer Algorithmus Die bisherigen Werte kannten wir schon, daher brauchen wir den erweiterten euklidischen Algorithmus.
$1 = 5 - 4 = 5 - (14 - 25) = 3 \cdot 5 - 14 = 3(33 - 2 \cdot 14) - 14 = 3 \cdot 33 - 7 \cdot 14 = 1 \Rightarrow (-7) \cdot 14 \equiv 1 \text{ mod } 33$
$y_1 = -7 = 26 = y_1$
$y_2 \cdot M_2 \equiv 1 \text{ mod } m_2$
$y_2 \cdot 33 \equiv 1 \text{ mod } 14$
$3 \cdot 33 \equiv 1 \text{ mod } 14$
$y_2 = 3$
$x = \sum_{i=1}^{2} a_i y_i M_i = 2 \cdot 26 \cdot 14 + 9 \cdot 3 \cdot 33 = 1619$ x ist eindeutig modulo $m_1 \cdot m_2 = 462$
Gesucht ist das **erste Greifen** des Zahnes: $1619 \pm k \cdot 462, x = 233 \pmod{462}$

10 Lösung zur Prüfung SS 2010

10.1 Aufgabe 1

10.1.1 a

S_{10} hat 10! Elemente. S_{10} hat zwei Fixpunkte: 6 und 9.
$\pi 10! = id$. Die zwei Fixpunkte bleiben gleich. Deshalb lassen wir sie weg. $\Rightarrow$ $\pi 8! = id$.

10.1.2 b

$$\pi^2 : \begin{array}{cccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 5 & 4 & 8 & 10 & 3 & 6 & 1 & 7 & 9 & 2 \end{array}$$

$$\pi^{-1} \begin{array}{cccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 4 & 7 & 10 & 8 & 6 & 5 & 1 & 9 & 2 \end{array}$$

10.1.3 c

Haben wir nicht gemacht. Wir machen das jetzt trotzdem:
Zykel: $\underbrace{(1,8,5,7,3)}_{Zykel} \circ \underbrace{(2,10,4)}_{Zykel}$. Die Fixpunkte lässt man weg.

10.2 Aufgabe 2

Beweis. Zeige: $91|(n^{13} - n)$
$n^{13} - n \equiv 0 \bmod 91$
$n^{13} = n$ mit mod 91, 91 zerlegen wir in die Primzahlen: $91 = 7 \cdot 13$
$\mathbb{Z}_{91} \to \mathbb{Z}_7 \times \mathbb{Z}_{13}$ (Isomorphismus)
$\underbrace{x}_{\text{mod } 91} \to (\underbrace{x}_{\text{mod } 7}, \underbrace{x}_{\text{mod } 13})$
Zeige: $(\underbrace{n^{13}}_{\text{mod } 7}, \underbrace{n^{13}}_{\text{mod } 13}) = (n, n)$
I $\underbrace{n^6}_{\text{n kein Vielfaches von 7}} = 1 \; n^6 n^6 n = n$
II $\underbrace{n^{12}}_{\text{n kein Vielfaches von 13}} = 1 \; n^{12} n = n$

$\square$

10.3 Aufgabe 3

10.3.1 a

Rechne in $(\mathbb{Z}_{10}, +, \cdot)$, **kein** Körper.
I: $x + 5y = 0$
II: $4x + 2y = 6$
II - 4I: $2y - 20y = 6 \Leftrightarrow -18y = 6 \Leftrightarrow 2y = 6 \Rightarrow y_1 = 3, y_2 = 8$
I: $x_1 + 5 \cdot 3 = 0$
$x_1 = -15 = 5$

II: $x_2 + 5 \cdot 8 = 0$
$x_2 = -40 = 0$
Zwei Lösungen: (5,3) und (0,8)

10.3.2 b

$\mathbb{Z}_{10}^*$ teilerfremd zu 10: $\{1, 3, 7, 9\}$

$\cdot$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

ord 3: 3,9,7,1 $\Rightarrow$ 4
ord 7: 7,9,3,1 $\Rightarrow$ 4
ord 9: 9,1 $\Rightarrow$ 2

10.4 Aufgabe 4

Zeige: $\sum_{k=1}^{n} k^3 = \frac{n^2(n+1)^2}{4}$

Beweis. **n=1:**
linke Seite: 1
rechte Seite: $\frac{1(1+1)^2}{4} = 1\checkmark$
Induktionsschritt von $n \to (n+1)$
Zeige: $\sum_{k=1}^{n+1} k^3 = \frac{(n+1)^2(n+2)^2}{4} \overset{\longleftrightarrow}{Ind.V.} \frac{n^2(n+1)^2}{4} + (n+1)^3 = \frac{(n+1)^2(n+2)^2}{4} \Leftrightarrow$
$n^2(n+1)^2 + 4(n+1)^3 = (n+1)^2(n+2)^2 \mid : (n+1)^2$
$\Leftrightarrow n^2 + 4(n+1) = (n+2)^2 \Leftrightarrow n^2 + 4n + 4 = n^2 + 4n + 4\checkmark$ $\square$

10.5 Aufgabe 5

10.5.1 a

Es gibt $3! = 6$ Permutationen. Der Code hat $6 \cdot 6 = 36$ Elemente.
$\underbrace{\pi_1}_{6} \circ \underbrace{\pi_2}_{6} \circ \pi_3 = id$

10.5.2 b

$(\pi_1, \pi_2, \cdot)$ ergänze.

$$\pi_1 : \begin{array}{ccc} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 1 & 3 & 2 \end{array}$$

$$\pi_2 : \begin{array}{ccc} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 3 & 2 & 1 \end{array}$$

$\pi_1 \circ \pi_2 = id$

$$\pi_1 \circ \pi_2 : \begin{array}{ccc} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 \end{array}$$

π Inverses von $\pi_1 \circ \pi_2$

$$\pi : \begin{array}{ccc} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 3 & 1 & 2 \end{array}$$

10.5.3 c

G ist nicht kommutativ. Vertauschungsfehler werden zum Teil erkannt.

10.6 Aufgabe 6

$ggT(450, 588):$
$588 = 1 \cdot 450 + 138$
$450 = 3 \cdot 138 + 36$
$138 = 3 \cdot 36 + 30$
$36 = 1 \cdot 30 + 6$
$30 = 5 \cdot 6 + 0$
$ggT = 6$

Kombination von 6:
$6 = 36 - 30 = 36 - (138 - 3 \cdot 36) = 4 \cdot 36 - 138 = 4(450 - 3 \cdot 138) - 138 = 4 \cdot 450 - 13 \cdot 138 = 4 \cdot 450 - 13(588 - 450) = 17 \cdot 450 - 13 \cdot 588 = 6$
Kombination von 42:
$42 = 7 \cdot 6 - 7(17 \cdot 450 - 13 \cdot 588) = 119 \cdot 450 - 91 \cdot 588 = 42$

11 Lösung zur Prüfung SS 2012

11.1 Aufgabe 1

11.1.1 a

sparen wir uns

11.1.2 b

sparen wir uns

11.2 Aufgabe 2

$(\mathbb{Z}_{13}, +, \cdot)$ Körper

11.2.1 a

$x + 7y = 5$
$5x + y = 8$
II-5 * I: $y - 35y = 8 - 25$
$-34y = -17$
$8y = 4$
$4 \cdot 2y = 4$
$2y = 1$
$y = 7$
in I: $x + 7 \cdot 7 = 5$
$x = -44 = 8$

11.2.2 b

$\underbrace{x^2}_{a^2} + \underbrace{3x}_{2b} = 2$ mit $(a+b)^2 = a^2 + 2ab + b^2; 2b = 3 \Rightarrow 2 \cdot 8 = 16 = 3 \Rightarrow b = 8$
$x^2 + 2 \cdot 8x + 8^2 = 2 + 8^2$
$(x+8)^2 = 2 + 64 = 66$
$(x+8)^2 = 1$
$x_1 + 8 = 1 \Rightarrow x_1 = -7 = 6$
$x_2 + 8 = -1 \Rightarrow x_2 = -9 = 4$ **Test:** $x = 4 : 16 + 12 = 2\checkmark$
$x = 6 : 36 + 18 = 2\checkmark$

11.3 Aufgabe 3

11.3.1 a

$\mathbb{Z}_{10}^* = \{1, 3, 7, 9\}$:

$\cdot$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

11.3.2 b

$c = \{(a, b, c) : a, b, c \in \mathbb{Z}_{10}^* \text{ und } \pi_1(a) \cdot \pi_2(b) \cdot \pi_3(c) = 1\}$
Ergänze: $(3, 9, x)$
$\pi_1(3) \cdot \pi_2(9) \cdot \pi_3(x) = 1$
$7 \cdot 7 \cdot \pi_3(x) = 1$
$9 \cdot \pi_3(x) = 1$
$\pi_3(x) = 9 \Rightarrow x = 3$

11.4 Aufgabe 4

11.4.1 a

Die Gesamtzahl entspricht der Anzahl der Permutationen mit $n = 20$, also 20! Möglichkeiten.

11.4.2 b

Richtig ankommen sind die Fixpunkte, d.h. Anzahl der Permutationen ohne Fixpunkt (keiner kommt richtig an).
$a(n) = n! \underbrace{(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + ... + (-1)^n \frac{1}{n!})}_{\approx e^{-1}} \approx n! e^{-1} = \frac{20!}{e}$

11.4.3 c

$P = \frac{\text{günstige Fälle}}{\text{alle Fälle}} = \frac{20! - \frac{20!}{e}}{20!} = 1 - \frac{1}{e} = 0,63$

11.5 Aufgabe 5

Zahn 10 von A in Lücke 8 von B?
A: $41 + t \cdot 45 = x \Rightarrow x \equiv 41 \mod 45$
B: $33 + s \cdot 38 = x \Rightarrow x \equiv 33 \mod 38$
45 $(3 \cdot 3 \cdot 5)$ und 38 $(2 \cdot 19)$ sind teilerfremd.

simultane Kongruenz chin. Restsatz

chinesischer Restsatz
$x \equiv a_1 \mod m_1$ mit $a_1 = 41, m_1 = 45$
$x \equiv a_2 \mod m_2$ mit $a_2 = 33, m_2 = 38$
$\Rightarrow m = m_1 \cdot m_2 = 1710$
$M_1 = m_2 = 38, M_2 = 45$
$y_1 \cdot M_1 \equiv 1 \mod m_1 \Leftrightarrow y_1 \cdot 38 \equiv 1 \mod 45$
$y_2 \cdot M_2 \equiv 1 \mod m_2 \Leftrightarrow y_2 \cdot 45 \equiv 1 \mod 38$
Zwischenrechnung: mit euklidischem Algorithmus $ggT(45, 38) : 45 = 1 \cdot 38 + 7 \Rightarrow 38 = 5 \cdot 7 + 3 \Rightarrow 7 = 2 \cdot 3 + 1$
$1 = 7 - 2 \cdot 3 = 7 - 2(38 - 5 \cdot 7) = 11 \cdot 7 - 2 \cdot 38 = 11(45 - 38) - 2 \cdot 38 = 11 \cdot 45 - 13 \cdot 38 = 1$
Fortsetzung $(-13) \cdot 38 \equiv 1 \mod 45 \Rightarrow y_1 = -13 = 32$
$11 \cdot 45 \equiv 1 \mod 38 \Rightarrow y_2 = 11$
x ausrechnen $x = a_1 \cdot y_1 \cdot M_1 + a_2 \cdot y_2 \cdot M_2 = 41 \cdot 32 \cdot 38 + 33 \cdot 11 \cdot 45 = 66191$.
Diese Lösung ist eindeutig mod $m = 1710$. Das erste mal trifft der Zahn 10 also in die Lücke 8 (x so klein wie möglich):
$x = 1211$

12 Lösung zur Prüfung SS 2012

12.1 Aufgabe 1

$ggT(91, 55) \Rightarrow 91 = 1 \cdot 55 + 36 \Rightarrow 55 = 1 \cdot 36 + 19 \Rightarrow 36 = 1 \cdot 19 + 17 \Rightarrow 19 = 1 \cdot 17 + 2 \Rightarrow 17 = 8 \cdot 2 + 1$
$1 = 17 - 8 \cdot 2 = 17 - 8(19 - 17) = 9 \cdot 17 - 8 \cdot 19 = 9(36 - 19) - 8 \cdot 19 = 9 \cdot 36 - 17 \cdot 19 = 9 \cdot 36 - 17(55 - 36) = 26 \cdot 36 - 17 \cdot 55 = 26(91 - 55) - 17 \cdot 55 = 26 \cdot 91 - 43 \cdot 55 = 1$

12.2 Aufgabe 2

12.2.1 a

$(\mathbb{Z}_{11}, +, \cdot)$
I: $2x + y = 0$
II: $x - 3y = 10$
I-2 * II: $y + 6y = -20 \Leftrightarrow 7y = 2(= 13 = 24 = 35) \Rightarrow y = 5$
in II: $x - 3 \cdot 5 = 10 \Rightarrow x = 25 = 3$

12.2.2 b

$x = log(a) \Leftrightarrow 2^x = a$
$log(5) =?$ (einfach ausprobieren)
$2, 2^2 = 4, 2^3 = 8, 2^4 = 16 = 5 \Leftrightarrow 2^4 = 5 \Rightarrow log(5) = 4$
Kann man von jeder Zahl $\neq 0$ den Logarithmus bilden? Wir bilden dazu die Zweierpotenzen: $2, 2^2 = 4, 2^3 = 8, 2^4 = 16 = 5, 2^5 = 10, 2^6 = 9, 2^7 = 7, 2^8 = 3, 2^9 = 6, 2^{10} = 1$. Das sind alle. Also kann man mit jeder Zahl den Logarithmus bilden.

12.3 Aufgabe 3

12.3.1 a

$\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$
Wir bilden die Gruppentafel. In jeder Zeile bzw. Spalte darf und muss jede Zahl genau einmal vorkommen.

$\cdot$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

12.3.2 b

$\pi_1(5) \cdot \pi_2(7) \cdot \pi_3(x) = 1$
$7 \cdot 5 \cdot \pi_3(x) = 1$
$11 \cdot \pi_3(x) = 1$
$\Rightarrow \pi_3(x) = 11 \Rightarrow x = 7$

12.4 Aufgabe 4

$$\pi : \begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 7 & 1 & 5 & 2 & 8 & 4 & 6 \end{array}$$

$c(i) := m(\pi(i)), m(i) := c(\pi^{-1}(i))$

$$\pi^{-1} : \begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 5 & 1 & 7 & 4 & 8 & 2 & 6 \end{array}$$

$m = (A, B, A, A, C, D, D, E)$
$c = (A, D, A, C, B, E, A, D)$
$\tilde{c} = (B, C, E, A, A, D, E, E)$
$\tilde{M} = (E, A, B, E, A, E, C, D)$

12.5 Aufgabe 5

12.5.1 a

Es gibt genau zwei Kanten mit ungeradem Grad.

12.5.2 b

Lösung siehe Angabe.

12.6 Aufgabe 6

Lassen wir weg, weil identisch mit anderem Jahrgang.

12.7 Aufgabe 7

Wir verteilen die $k = 20$ Rosinen auf $n = 10$ Fächer. Wir wählen Fach 1 aus:
Alle Fälle: 10^{20}

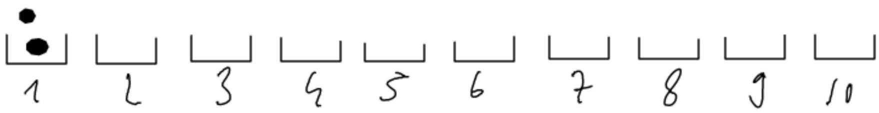


Abbildung 42: Die Rosinen werden verteilt

Günstige Fälle: $\binom{20}{2} \cdot 9^{18}$

$p = \frac{\text{günstige Fälle}}{\text{Nenner}} = \frac{\binom{20}{2} \cdot 9^{18}}{10^{20}} = ... = 0,285$

13 Einzelne Aufgaben

13.1 Dominosteine in 3xn-Feld unterbringen

Wie viele Möglichkeiten a(n) gibt es 1x2-Steine anzuordnen? Wenn n ungerade ist, geht es nicht. Wenn man die Anfänge in Abb. 43 betrachtet kommt man

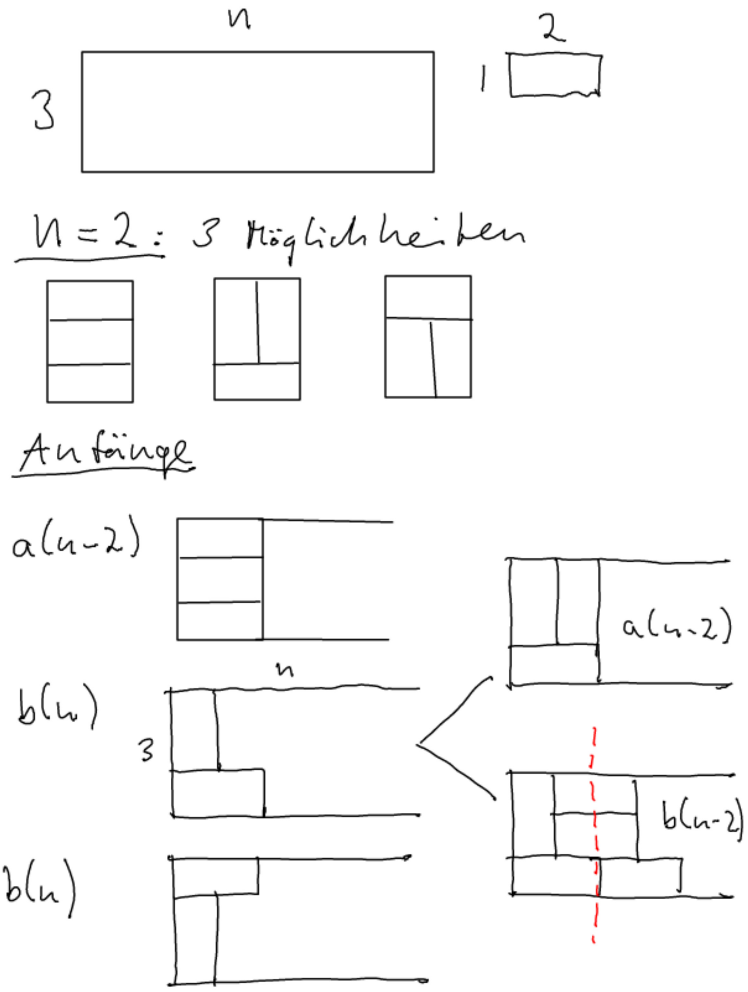


Abbildung 43: Wie kann man die 1x2 Steine im Feld unterbringen?

auf folgende Formeln für die Möglichkeiten:

- $a(n) = a(n-2) + 2b(n)$
- $b(n) = a(n-2) + b(n-2)$

n	2	4	6	8
a(n)	3	$3 + 2 \cdot 4 = 11$	$11 + 2 \cdot 15 = 41$	$41 + 2 \cdot 56 = 153$
b(n)	1	$3 + 1 = 4$	$11 + 4 = 15$	$41 + 15 = 56$

13.2 Rechnen im $\mathbb{Z}_{11}$

Wir rechnen in $(\mathbb{Z}_{11}, +, \cdot)$. 11 ist eine Primzahl also ist das ein Körper.

13.2.1 Lineares Gleichungssystem

I: $x + 3y = 8$
II: $2x + y = 4$

II-2I: $y - 6y = 4 - 16$
$-5y = -12$
$5y = 12 = 23 = 34 = 45$
$\Rightarrow y = 9$

in I: $x + 3 \cdot 9 = 8$
$x = 8 - 27 = -19$
$x = 3$

13.2.2 Quadratische Gleichung

$x^2 + 4x = 10$ mit $(a + b)^2 = a^2 + 2ab + b^2 \Rightarrow b = 2$
$x^2 + 4x + w^2 = 10 + 2^2$
$(x + 2)^2 = 14 = 3$
Die Lösungen finden wir mittels Ausprobieren: $2^2 = 4, 3^2 = 9, 4^2 = 16 = 5$, $5^2 = 25 = 3$
$x + 2 = \pm 5$
$x_1 + 2 = 5 \Rightarrow x_1 = 3$
$x_2 + 2 = -5 \Rightarrow x_2 = -7 = 4$

13.3 Kombinatorikaufgabe

10 Ehepaare sitzen an einem langen Tisch. Auf einer Seite die Männer, auf der anderen die Frauen. Wie groß ist die Wahrscheinlichkeit, dass sich kein Ehepaar gegenüber sitzt?
Das klingt nach Permutationen:

$$\begin{array}{ccccccc} \text{Männer} & 1 & 2 & 3 & 4 & ... & 10 \\ & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ \text{Frauen} & 3 & 4 & 7 & 10 & ... & 5 \end{array}$$

Damit kann man die Aufgabe neu formulieren: Wie groß ist die Wahrscheinlichkeit, dass die Permutationen keinen Fixpunkt hat?
alle Permutationen: n!
Permutationen ohne Fixpunkt: $a(n) = n! \underbrace{(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + ... + (-1)^n \frac{1}{n!})}_{\approx e^{-1}} \approx$

$n!e^{-1} = \frac{10!}{e}$
P(kein Fixpunkt)= $\frac{\text{günstige Fälle}}{\text{alle Fälle}} = \frac{\frac{n!}{e}}{n!} = \frac{1}{e} = 0,367$

13.4 Einheitengruppe

$(\mathbb{Z}_{16}^*, \cdot)$ Einheitengruppe (teilerfremd zu 16): $\mathbb{Z}_{16}^* = \{1, 3, 5, 7, 9, 11, 13, 15\}$
Jetzt machen wir einen Code c über $\mathbb{Z}_{16}^*$.
$c = \{(a, b, c) : abc = 1, a, b, c \in \mathbb{Z}_{16}^*\}$

Ergänze $(5, 11, \cdot)$ zu einem Codewort.
$5 \cdot 11 \cdot x = 1$
$55x = 1$
$7x = 1$
Jetzt probieren wir die Werte aus der o.g. Einheitengruppe aus:
$7 \cdot 3 = 21 = 5$
$7 \cdot 3 = 35 = 3$
$7 \cdot 7 = 49 = 1$
$\Rightarrow x = 7$

Aus wie vielen Elementen besteht der Code? $(a, b, \cdot)$ mit a,b beliebig wählen und $\cdot$ rechnen wir aus. Für a und b gibt es jeweils 8 Möglichkeiten (Anzahl der Elemente der Einheitengruppe), also 64 Elemente. Der Code hat also 64 Codewörter.

13.5 Verschlüsseln und Entschlüsseln mit Permutationen

Wir haben eine gegebene Permutation $\pi : \begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 7 & 1 & 5 & 4 & 2 & 6 \end{array}$

Suche die inverse Permutation $\pi^{-1} : \begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 6 & 1 & 5 & 4 & 7 & 2 \end{array}$

Damit kann man Wörter der Länge 7 verschlüsseln. $c(i) := m(\pi(i))$

Verschlüssle $m = (C, A, B, C, D, E, A) \quad \Rightarrow c = (B, A, C, D, C, A, E)$

Entschlüssle c (mit π^{-1}) $m(i) := c(\pi^{-1}(i))$
$m = (C, A, B, C, D, E, A)\checkmark$

13.6 Graphentheorie

Hat der gegebene Graph (Abb. 44) einen eulerschen Kreis oder eine eulersche Linie?

13.6.1 eulersche Linie

Es gibt genau zwei Knoten (A, E) mit ungeradem Grad $\Rightarrow$ eulersche Linie (rot). Beim Einzeichnen muss man bei einem Knoten mit ungeradem Grad (z.B. A oder E) starten!

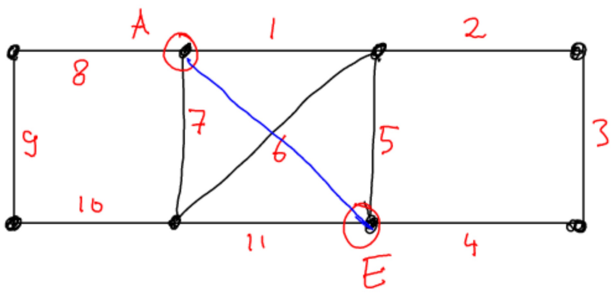


Abbildung 44: Eulersche Linie und eulerscher Kreis

13.6.2 eulerscher Kreis

Füge eine zusätzliche Kante ein, damit ein eulerscher Kreis (nur gerade Grade) entsteht (blau).

14 Lösung zur Prüfung SS 2008

14.1 Aufgabe 1

$n = 1$: linke Seite: 1, rechte Seite 1 ✓
Zeige: $\sum_{k=1}^{n+1} = \frac{(n+1)^2(n+2)^2}{4} \Leftrightarrow \frac{n^2(n+1)^2}{4} + (n+1) = \frac{(n+1)^2(n+2)^2}{4} \Leftrightarrow (n+1)^3 = \frac{(n+1)^2(n+2)^2-n^2(n+1)^2}{4} \Leftrightarrow (n+1) = \frac{(n+2)^2-n^2}{4} = \frac{n^2+4n+4-n^2}{4} \Rightarrow n+1 = n+1$

14.2 Aufgabe 2

ggT(385,595)

a	b	q	r	x	y
595	385	1	210		
385	210	1	175		
210	175	1	35	1	
175	35	5	0	0	1

$\Rightarrow ggT = 35... = 2 \cdot 595 - 3 \cdot 385 \Rightarrow 350 = 10 \cdot 35 = 20 \cdot 595 - 30 \cdot 385$

$y = x_{i+1} - q_i \cdot y_{i+1}$

14.3 Aufgabe 3

14.3.1 a

$(\mathbb{Z}_{15}^*, \cdot) \Rightarrow \{1, 2, 4, 7, 8, 11, 13, 14\}$

$\cdot$	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1

Weil es sich hierbei um eine Gruppe handelt, ist die Tafel symmetrisch zur Diagonalen. Außerdem kommt in jeder Spalte und Zeile jede Zahl nur einmal vor.

14.3.2 b

$11x^2 = 14 \Leftrightarrow x^2 = 11 \cdot 14 = 4 \Rightarrow x = 2, 7, 8, 13$ Gleichung lösen und dann zu x passende Werte aus der Tafel finden.

14.3.3 c

π	1	2	4	7	8	11	13	14
$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
π_1	4	7	11	14	13	8	1	2
π_2	11	14	8	2	1	13	4	7
π_3	8	2	13	7	4	1	11	14
π_4	13	7	1	14	11	4	8	2

$c = \{(a, b, c, d) : \pi_1(a) \cdot \pi_2(b) \cdot \pi_3(c) \cdot \pi_4(d) = 1\}$ d ist frei wählbar. Für a, b, c gibt es jeweils 8 Möglichkeiten $\Rightarrow$ Anzahl der Wörter: $8^3 = 512$

Ergänze $(7, 13, 11, \cdot)$**:** $\pi_1(7) \cdot \pi_2(13) \cdot \pi_3(11) \cdot \pi_4(x) = 1$
$14 \cdot 4 \cdot 1 \cdot \pi_4(x) = 1$
$11 \cdot \pi_4(x) = 1$
$\Rightarrow \pi_4(x) = 11 \Rightarrow x = 8$

14.4 Aufgabe 4

14.4.1 a

$28^{52} = 1$

14.4.2 b

$28^{34} = ?$
$34 = 2^5 + 2^1 \mod 53$
$28^{(2^0)} = 28$
$28^{(2^1)} = 784 = 42$
$28^{(2^2)} = 42^2 = 1764 = 15$
$28^{(2^3)} = 15^2 = 225 = 13$
$28^{(2^4)} = 13^2 = 169 = 10$
$28^{(2^5)} = 10^2 = 100 = 47$
$28^{34} = 28^{2^5+2^1} = 28^{(2^5)} \cdot 28^{(2^1)} = 47 \cdot 42 = 1974 = 13$

14.5 Aufgabe 5

14.5.1 a

7 Personen (Schubfachprinzip)

14.5.2 b

Es gibt 3n gerade, 3n ungerade Elemente. Die ungeraden sollen nun an einer geraden Stelle stehen. Daher gibt es $(3n)!$ Möglichkeiten ungerade Elemente auf geraden Stellen platzieren. Bei den geraden ist es genauso: $(3n)!$. Insgesamt also: $(3n)! \cdot (3n)!$

14.5.3 c

Es gibt 5 unterschiedliche Buchstaben (5 x A , 2 x B, 1 x C, 1 x D, 2 x R) und 11 Stellen. Man kann das mit dem Multinomialkoeffizienten berechnen (allgemein): $\binom{n}{a,b,c} = \frac{n!}{a!b!c!} \Rightarrow \binom{11!}{5,2,1,1,2} = \frac{11!}{5!2!1!1!2!} = \binom{11!}{5!4} = \binom{11\cdot10\cdot9\cdot8\cdot7\cdot6}{4} = 11\cdot10\cdot9\cdot2\cdot7\cdot6 = 83160$

15 Einzelne Aufgaben

15.1 Siebformel

$|A_1 \cup A_2 \cup A_3 \cup A_4| = |A_1| + |A_2| + |A_3| + |A_4| - [|A_1 \cap A_2| + |A_1 \cap A_3| + |A_1 \cap A_4| + |A_2 \cap A_3| + |A_2 \cap A_4| + |A_3 \cap A_4|] + [|A_2 \cap A_3 \cap A_4| + |A_1 \cap A_3 \cap A_4| + |A_1 \cap A_2 \cap A_4| + |A_1 \cap A_2 \cap A_3|] - [|A_1 \cap A_2 \cap A_3 \cap A_4|]$

15.1.1 Beispiel

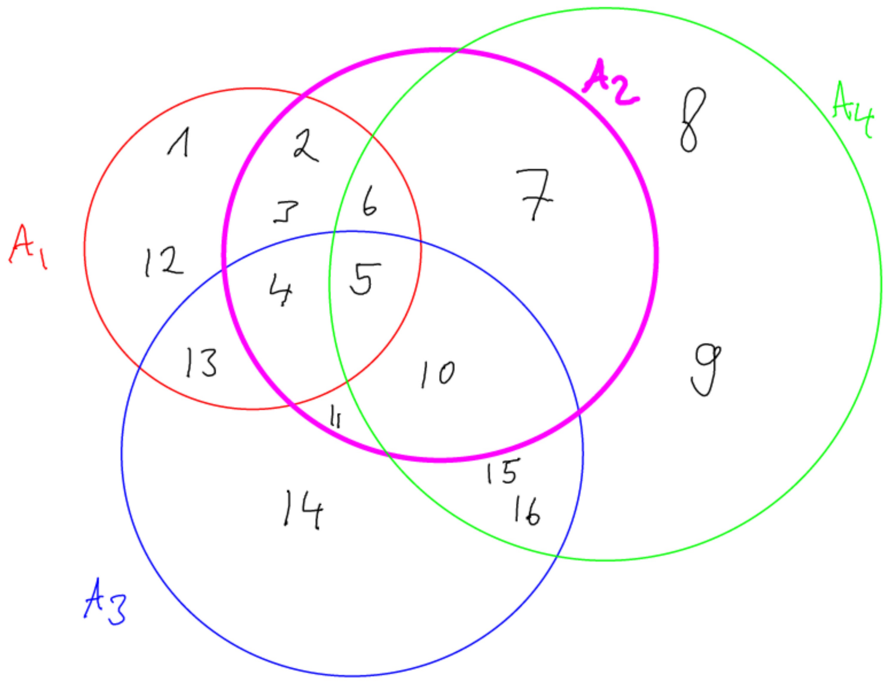


Abbildung 45: Auf diese Menge wenden wir die Siebformel an

15.1.2 Berechnung

$[8+8+8+8] - [5+3+2+4+4+4] + [2+1+2+2] - [1] = 32 - 22 + 7 - 1 = 16$

15.2 Symmetriegruppe eines Rechtecks

Eine Kongruenzabbildung (Drehung, Spiegelung), die das Rechteck auf sich selbst abbildet. Wir bilden die dazugehörige Gruppentafel:

$\circ$	id	d	s	t
id	id	d	s	t
d	d	id	$d \circ s = t$	s
s	s	t	id	d
t	t	s	d	id

Eine Zelle machen wir ausführlich: $d \circ s : A \to D, B \to C, C \to B, D \to A$ Was ist jetzt $d \circ s$? Die Spiegelung an t.

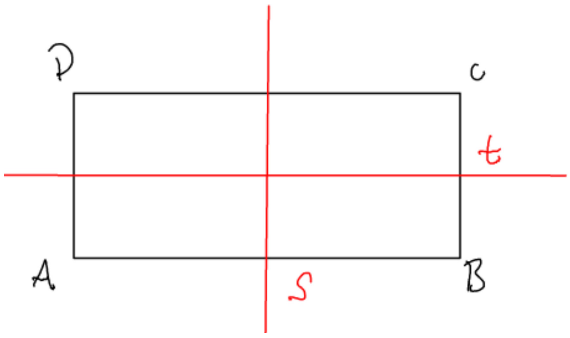


Abbildung 46: Spiegelungen an s und t, Drehung d um 180, Drehung id um 360

15.3 RSA-Algorithmus

Wir brauchen zwei Primzahlen: $p = 5, q = 7$
Dann müssen wir das n ausrechnen: $n = p \cdot q = 35$
Wir brauchen die eulersche Phi-Funktion: $\varphi(n) = \varphi(35) = 4 \cdot 6 = 24$
Jetzt wählen wir ein e: $1 < e < 24$ mit $ggT(e, 24) = 1$. Wir wählen $e = 11$
Berechne d mit $e \cdot d \equiv 1 \bmod \varpi(n)$
$11 \cdot d \equiv 1 \bmod 24$
Mit euklidischem Algorithmus: ggT(11,24)
$24 = 2 \cdot 11 + 2$
$11 = 5 \cdot 2 + 1$
Jetzt Kombination bilden: $1 = 11 - 5 \cdot 2 = 11 - 5(24 - 2 \cdot 11) = 11 \cdot 11 - 5 \cdot 24 = 1$
$\Rightarrow 11 \cdot 11 \equiv 1 \bmod 24$
$11 \cdot d \equiv 1 \bmod 24$
Das Inverse von d ist zufällig auch 11.

Schlüssel öffentlich: n,e
geheim: d
Klartext: $m = 4$
$c = m^e$ mod n
$c = 4^{11} \bmod 35$
$4194304 = 9$

entschlüsseln: $m = c^d$ mod n
$m = 9^{11} \bmod 35$
$m = 9^{11} = 9^5 \cdot 9^6 = 59049 \cdot 531441 = 4 \cdot 1 = 4$

16 Prüfungsstoff

Prüfungen SS2008, SS2010, SS2011, SS2012, WS1415
Außerdem: Aufgaben von heute, Induktionsbeweis Dominosteine, Lineares Gleichungssystem mod x, Quadratische Gleichung mod x, Permutationen (mit und ohne Fixpunkt), Codes (Gruppen mit und ohne Permutationen), Graphen (eulersche Linie, eulerscher Kreis)

17 Hilfsmittel für die Prüfung

17.1 Eulerkreis und Eulertour

Der Eulerkreis enthält alle Kanten des Graphen G **genau einmal**. Der Eulerkreis kann gezeichnet werden ohne abzusetzen. Es gilt:

- G ist eulersch,
- G ist zusammenhängend und jeder Knoten hat geraden Grad.

Eine Eulertour bzw. offene eulersche Linie nennt man einen Weg, der **kein Kreis** ist, wenn jede Kante darin **genau einmal** vorkommt.
G ist **offene eulersche Linie** $\Leftrightarrow$ G hat **genau zwei Knoten** mit **ungeradem Grad**

17.2 Chinesischer Restsatz

Seien $m_1, m_2, ..., m_n$ **teilerfremde** natürliche Zahlen und $a_1, a_2, ..., a_n \in \mathbb{Z}$ beliebig $\exists x \in \mathbb{Z}$ mit:

$$\left.\begin{array}{l} x \equiv a_1 \bmod m_1 \\ x \equiv a_2 \bmod m_2 \\ \quad\quad\vdots \\ x \equiv a_n \bmod m_n \end{array}\right\} \text{simultane Kongruenz}$$

$m = m_1 \cdot m_2 \cdot ... \cdot m_n$
$M_i = \frac{m_1 \cdot m_2 \cdot ... \cdot m_n}{m_i} = \frac{m}{m_i}$

17.3 Permutationen

17.3.1 Anzahl Permutationen ohne Fixpunkte

genaue Berechnung $a(n) = n! \underbrace{(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + ... + (-1)^n \frac{1}{n!})}_{\approx e^{-1}}$

Nährungslösung $a(n) \approx n! e^{-1} = \frac{n!}{e}$

Wahrscheinlichkeit kein Fixpunkt $P = \frac{\text{günstige Fälle}}{\text{alle Fälle}} = \frac{a(n)}{n!}$

17.4 ggT

Seien $a, b \in \mathbb{Z}$ mit $a \neq 0$. Seien q und r Zahlen mit $b = qa + r \Rightarrow ggT(b, a) = ggT(a, r)$.

17.4.1 euklidischer Algorithmus

Der euklidische Algorithmus ist ein Algorithmus aus dem mathematischen Teilgebiet der Zahlentheorie. Mit ihm lässt sich der größte gemeinsame Teiler zweier natürlicher Zahlen a und b berechnen. Als erstes berechnet man a mod b. Dabei erhält man das ganzzahlige Ergebnis der Division und den Rest r. Das macht man so lange, bis man für den Rest 0 erhält. Das aktuelle b ist dann der ggT(a,b). Tabellarisch kann man den Algorithmus wie im folgenden Beispiel durchführen ggT(128,34):

a	b	q	r
128	34	3	26
34	26	1	8
26	8	3	2
8	2	4	0

17.4.2 Erweiterter euklidischer Algorithmus

Der erweiterte euklidische Algorithmus ist ein Algorithmus aus dem mathematischen Teilgebiet der Zahlentheorie. Er berechnet neben dem größten gemeinsamen Teiler ggT(a,b) zweier natürlicher Zahlen a und b noch zwei ganze Zahlen x und y, die die folgende Gleichung erfüllen: $ggT(a, b) = x \cdot a + y \cdot b$.
Den erweiterten euklidischen Algorithmus startet man unten auf der rechten Seite der Tabelle. Das Ergebnis steht dann rechts in der obersten Zeile. Dabei ist $x_i = y_{i+1}$ und $y_i = x_{i+1} - q_i * y_{i+1}$:

a	b	q	r	x	y
128	34	3	26	4	-15
34	26	1	8	-3	4
26	8	3	2	1	-3
8	2	4	0	0	1

17.5 schnelle Exponentation

Im Zahlenkörper $(\mathbb{Z}_{\mathbf{53}}, +, \cdot)$ berechne man: $28^{34} =?$
$34 = 2^5 + 2^1 \bmod \mathbf{53}$
$28^{(2^0)} = 28$
$28^{(2^1)} = 784 = \underline{\mathbf{42}}$
$28^{(2^2)} = \mathbf{42}^2 = 1764 = \mathbf{15}$
$28^{(2^3)} = \mathbf{15}^2 = 225 = \mathbf{13}$
$28^{(2^4)} = \mathbf{13}^2 = 169 = \mathbf{10}$
$28^{(2^5)} = \mathbf{10}^2 = 100 = \underline{\mathbf{47}}$
$28^{34} = 28^{2^5+2^1} = 28^{(2^5)} \cdot 28^{(2^1)} = \underline{\mathbf{47}} \cdot \underline{\mathbf{42}} = 1974 = 13$

17.6 $\mathbb{Z}_n^*$

Wir bezeichnen die Menge derjenigen Restklassen von $\mathbb{Z}_n$, die ein multiplikatives Inverses haben, mit $\mathbb{Z}_n^*$. In $\mathbb{Z}_n^*$ liegen also genau diejenigen Restklassen [a] von $\mathbb{Z}_n$ mit $ggT(a, n) = 1$. Die Restklassen [1] und [n-1] sind stets in $\mathbb{Z}_n^*$ enthalten, denn beide sind teilerfremd zu n.
$\mathbb{Z}_n^*$ ist abgeschlossen bezüglich Multiplikation $\Rightarrow [a] \cdot [b]$ liegt wieder in $\mathbb{Z}_n^*$. $\mathbb{Z}_n^*$ ist eine **Gruppe** $\Rightarrow$ Es gilt das Assoziativgesetz, es gibt ein neutrales Element

und jedes Element hat ein Inverses.

17.6.1 $\mathbb{Z}_4^*$

$\cdot$	1	3
1	1	3
3	3	1

17.6.2 $\mathbb{Z}_5^*$

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

17.6.3 $\mathbb{Z}_6^*$

$\cdot$	1	5
1	1	5
5	5	1

17.6.4 $\mathbb{Z}_7^*$

$\cdot$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

17.6.5 $\mathbb{Z}_8^*$

$\cdot$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

17.6.6 $\mathbb{Z}_9^*$

$\cdot$	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

17.6.7 $\mathbb{Z}_{10}^*$

$\cdot$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

17.6.8 $\mathbb{Z}_{11}^*$

$\cdot$	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2	2	4	6	8	10	1	3	5	7	9
3	3	6	9	1	4	7	10	2	5	8
4	4	8	1	5	9	2	6	10	3	7
5	5	10	4	9	3	8	2	7	1	6
6	6	1	7	2	8	3	9	4	10	5
7	7	3	10	6	2	9	5	1	8	4
8	8	5	2	10	7	4	1	9	6	3
9	9	7	5	3	1	10	8	6	4	2
10	10	9	8	7	6	5	4	3	2	1

17.6.9 $\mathbb{Z}_{12}^*$

$\cdot$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

17.6.10 $\mathbb{Z}_{13}^*$

$\cdot$	1	2	3	4	5	6	7	8	9	10	11	12
1	1	2	3	4	5	6	7	8	9	10	11	12
2	2	4	6	8	10	12	1	3	5	7	9	11
3	3	6	9	12	2	5	8	11	1	4	7	10
4	4	8	12	3	7	11	2	6	10	1	5	9
5	5	10	2	7	12	4	9	1	6	11	3	8
6	6	12	5	11	4	10	3	9	2	8	1	7
7	7	1	8	2	9	3	10	4	11	5	12	6
8	8	3	11	6	1	9	4	12	7	2	10	5
9	9	5	1	10	6	2	11	7	3	12	8	4
10	10	7	4	1	11	8	5	2	12	9	6	3
11	11	9	7	5	3	1	12	10	8	6	4	2
12	12	11	10	9	8	7	6	5	4	3	2	1

17.6.11 $\mathbb{Z}_{14}^*$

$\cdot$	1	3	5	9	11	13
1	1	3	5	9	11	13
3	3	9	1	13	5	11
5	5	1	11	3	13	9
9	9	13	3	11	1	5
11	11	5	13	1	9	3
13	13	11	9	5	3	1

17.6.12 $\mathbb{Z}_{15}^*$

$\cdot$	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1

17.6.13 $\mathbb{Z}_{16}^*$

$\cdot$	1	3	5	7	9	11	13	15
1	1	3	5	7	9	11	13	15
3	3	9	15	5	11	1	7	13
5	5	15	9	3	13	7	1	11
7	7	5	3	1	15	13	11	9
9	9	11	13	15	1	3	5	7
11	11	1	7	13	3	9	15	5
13	13	7	1	11	5	15	9	3
15	15	13	11	9	7	5	3	1

17.6.14 $\mathbb{Z}_{17}^*$

$\cdot$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2	2	4	6	8	10	12	14	16	1	3	5	7	9	11	13	15
3	3	6	9	12	15	1	4	7	10	13	16	2	5	8	11	14
4	4	8	12	16	3	7	11	15	2	6	10	14	1	5	9	13
5	5	10	15	3	8	13	1	6	11	16	4	9	14	2	7	12
6	6	12	1	7	13	2	8	14	3	9	15	4	10	16	5	11
7	7	14	4	11	1	8	15	5	12	2	9	16	6	13	3	10
8	8	16	7	15	6	14	5	13	4	12	3	11	2	10	1	9
9	9	1	10	2	11	3	12	4	13	5	14	6	15	7	16	8
10	10	3	13	6	16	9	2	12	5	15	8	1	11	4	14	7
11	11	5	16	10	4	15	9	3	14	8	2	13	7	1	12	6
12	12	7	2	14	9	4	16	11	6	1	13	8	3	15	10	5
13	13	9	5	1	14	10	6	2	15	11	7	3	16	12	8	4
14	14	11	8	5	2	16	13	10	7	4	1	15	12	9	6	3
15	15	13	11	9	7	5	3	1	16	14	12	10	8	6	4	2
16	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

17.6.15 $\mathbb{Z}_{18}^*$

$\cdot$	1	5	7	11	13	17
1	1	5	7	11	13	17
5	5	7	17	1	11	13
7	7	17	13	5	1	11
11	11	1	5	13	17	7
13	13	11	1	17	7	5
17	17	13	11	7	5	1

17.6.16 $\mathbb{Z}_{19}^*$

·	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
2	2	4	6	8	10	12	14	16	18	1	3	5	7	9	11	13	15	17
3	3	6	9	12	15	18	2	5	8	11	14	17	1	4	7	10	13	16
4	4	8	12	16	1	5	9	13	17	2	6	10	14	18	3	7	11	15
5	5	10	15	1	6	11	16	2	7	12	17	3	8	13	18	4	9	14
6	6	12	18	5	11	17	4	10	16	3	9	15	2	8	14	1	7	13
7	7	14	2	9	16	4	11	18	6	13	1	8	15	3	10	17	5	12
8	8	16	5	13	2	10	18	7	15	4	12	1	9	17	6	14	3	11
9	9	18	8	17	7	16	6	15	5	14	4	13	3	12	2	11	1	10
10	10	1	11	2	12	3	13	4	14	5	15	6	16	7	17	8	18	9
11	11	3	14	6	17	9	1	12	4	15	7	18	10	2	13	5	16	8
12	12	5	17	10	3	15	8	1	13	6	18	11	4	16	9	2	14	7
13	13	7	1	14	8	2	15	9	3	16	10	4	17	11	5	18	12	6
14	14	9	4	18	13	8	3	17	12	7	2	16	11	6	1	15	10	5
15	15	11	7	3	18	14	10	6	2	17	13	9	5	1	16	12	8	4
16	16	13	10	7	4	1	17	14	11	8	5	2	18	15	12	9	6	3
17	17	15	13	11	9	7	5	3	1	18	16	14	12	10	8	6	4	2
18	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

17.6.17 $\mathbb{Z}_{20}^*$

·	1	3	7	9	11	13	17	19
1	1	3	7	9	11	13	17	19
3	3	9	1	7	13	19	11	17
7	7	1	9	3	17	11	19	13
9	9	7	3	1	19	17	13	11
11	11	13	17	19	1	3	7	9
13	13	19	11	17	3	9	1	7
17	17	11	19	13	7	1	9	3
19	19	17	13	11	9	7	3	1

17.6.18 $\mathbb{Z}_{21}^*$

·	1	2	4	5	8	10	11	13	16	17	19	20
1	1	2	4	5	8	10	11	13	16	17	19	20
2	2	4	8	10	16	20	1	5	11	13	17	19
4	4	8	16	20	11	19	2	10	1	5	13	17
5	5	10	20	4	19	8	13	2	17	1	11	16
8	8	16	11	19	1	17	4	20	2	10	5	13
10	10	20	19	8	17	16	5	4	13	2	1	11
11	11	1	2	13	4	5	16	17	8	19	20	10
13	13	5	10	2	20	4	17	1	19	11	16	8
16	16	11	1	17	2	13	8	19	4	20	10	5
17	17	13	5	1	10	2	19	11	20	16	8	4
19	19	17	13	11	5	1	20	16	10	8	4	2
20	20	19	17	16	13	11	10	8	5	4	2	1

17.6.19 $\mathbb{Z}_{22}^*$

·	1	3	5	7	9	13	15	17	19	21
1	1	3	5	7	9	13	15	17	19	21
3	3	9	15	21	5	17	1	7	13	19
5	5	15	3	13	1	21	9	19	7	17
7	7	21	13	5	19	3	17	9	1	15
9	9	5	1	19	15	7	3	21	17	13
13	13	17	21	3	7	15	19	1	5	9
15	15	1	9	17	3	19	5	13	21	7
17	17	7	19	9	21	1	13	3	15	5
19	19	13	7	1	17	5	21	15	9	3
21	21	19	17	15	13	9	7	5	3	1

17.6.20 $\mathbb{Z}_{24}^*$

·	1	5	7	11	13	17	19	23
1	1	5	7	11	13	17	19	23
5	5	1	11	7	17	13	23	19
7	7	11	1	5	19	23	13	17
11	11	7	5	1	23	19	17	13
13	13	17	19	23	1	5	7	11
17	17	13	23	19	5	1	11	7
19	19	23	13	17	7	11	1	5
23	23	19	17	13	11	7	5	1