Diskrete Strukturen

Sommer 2019

Prof. Stefan Lucks, Jannis Bossert
<firstname>.<lastname>(at)uni-weimar.de

Bauhaus-Universität Weimar

December 10, 2019

Aufgabe 1: Generatoren

Geben Sie alle Generatoren (erzeugende Elemente) an von:

a) $(\mathbb{Z}_{11}^*, \cdot)$

Aufgabe 1: Generatoren

Geben Sie alle Generatoren (erzeugende Elemente) an von:

a) $(\mathbb{Z}_{11}^*, \cdot)$

$\mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

Aufgabe 1: Generatoren

Geben Sie alle Generatoren (erzeugende Elemente) an von:

a) $(\mathbb{Z}_{11}^*, \cdot)$

$\mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

$1 : \{1\}$ Nein

Aufgabe 1: Generatoren

Geben Sie alle Generatoren (erzeugende Elemente) an von:

a) $(\mathbb{Z}_{11}^*, \cdot)$

$\mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

$1 : \{1\}$ Nein

$2 : \{2, 4, 8, 5, 10, 9, 7, 3, 6, 1\}$ Ja

Aufgabe 1: Generatoren

Geben Sie alle Generatoren (erzeugende Elemente) an von:

a) $(\mathbb{Z}_{11}^*, \cdot)$

$\mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
$1 : \{1\}$ Nein
$2 : \{2, 4, 8, 5, 10, 9, 7, 3, 6, 1\}$ Ja
$3 : \{3, 9, 5, 4, 1\}$ Nein

Aufgabe 1: Generatoren

Geben Sie alle Generatoren (erzeugende Elemente) an von:

a) $(\mathbb{Z}_{11}^*, \cdot)$

$\mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
$1 : \{1\}$ Nein
$2 : \{2, 4, 8, 5, 10, 9, 7, 3, 6, 1\}$ Ja
$3 : \{3, 9, 5, 4, 1\}$ Nein
$4 : \{4, 5, 9, 3, 1\}$ Nein

Aufgabe 1: Generatoren

Geben Sie alle Generatoren (erzeugende Elemente) an von:

a) $(\mathbb{Z}_{11}^*, \cdot)$

$\mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
$1 : \{1\}$ Nein
$2 : \{2, 4, 8, 5, 10, 9, 7, 3, 6, 1\}$ Ja
$3 : \{3, 9, 5, 4, 1\}$ Nein
$4 : \{4, 5, 9, 3, 1\}$ Nein
$5 : \{5, 3, 4, 9, 1\}$ Nein

Aufgabe 1: Generatoren

Geben Sie alle Generatoren (erzeugende Elemente) an von:

a) $(\mathbb{Z}_{11}^*, \cdot)$

$\mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
$1 : \{1\}$ Nein
$2 : \{2, 4, 8, 5, 10, 9, 7, 3, 6, 1\}$ Ja
$3 : \{3, 9, 5, 4, 1\}$ Nein
$4 : \{4, 5, 9, 3, 1\}$ Nein
$5 : \{5, 3, 4, 9, 1\}$ Nein
$6 : \{6, 3, 7, 9, 10, 5, 8, 4, 2, 1\}$ Ja

Aufgabe 1: Generatoren

Geben Sie alle Generatoren (erzeugende Elemente) an von:

a) $(\mathbb{Z}_{11}^*, \cdot)$

$\mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
$1 : \{1\}$ Nein
$2 : \{2, 4, 8, 5, 10, 9, 7, 3, 6, 1\}$ Ja
$3 : \{3, 9, 5, 4, 1\}$ Nein
$4 : \{4, 5, 9, 3, 1\}$ Nein
$5 : \{5, 3, 4, 9, 1\}$ Nein
$6 : \{6, 3, 7, 9, 10, 5, 8, 4, 2, 1\}$ Ja
$7 : \{7, 5, 2, 3, 10, 4, 6, 9, 8, 1\}$ Ja

Aufgabe 1: Generatoren

Geben Sie alle Generatoren (erzeugende Elemente) an von:

a) $(\mathbb{Z}_{11}^*, \cdot)$

$\mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
$1 : \{1\}$ Nein
$2 : \{2, 4, 8, 5, 10, 9, 7, 3, 6, 1\}$ Ja
$3 : \{3, 9, 5, 4, 1\}$ Nein
$4 : \{4, 5, 9, 3, 1\}$ Nein
$5 : \{5, 3, 4, 9, 1\}$ Nein
$6 : \{6, 3, 7, 9, 10, 5, 8, 4, 2, 1\}$ Ja
$7 : \{7, 5, 2, 3, 10, 4, 6, 9, 8, 1\}$ Ja
$8 : \{8, 9, 6, 4, 10, 3, 2, 5, 7, 1\}$ Ja

Aufgabe 1: Generatoren

Geben Sie alle Generatoren (erzeugende Elemente) an von:

a) $(\mathbb{Z}_{11}^*, \cdot)$

$\mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

$1 : \{1\}$ Nein

$2 : \{2, 4, 8, 5, 10, 9, 7, 3, 6, 1\}$ Ja

$3 : \{3, 9, 5, 4, 1\}$ Nein

$4 : \{4, 5, 9, 3, 1\}$ Nein

$5 : \{5, 3, 4, 9, 1\}$ Nein

$6 : \{6, 3, 7, 9, 10, 5, 8, 4, 2, 1\}$ Ja

$7 : \{7, 5, 2, 3, 10, 4, 6, 9, 8, 1\}$ Ja

$8 : \{8, 9, 6, 4, 10, 3, 2, 5, 7, 1\}$ Ja

$9 : \{9, 4, 3, 5, 1\}$ Nein

Aufgabe 1: Generatoren

Geben Sie alle Generatoren (erzeugende Elemente) an von:

a) $(\mathbb{Z}_{11}^*, \cdot)$

$\mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
$1 : \{1\}$ Nein
$2 : \{2, 4, 8, 5, 10, 9, 7, 3, 6, 1\}$ Ja
$3 : \{3, 9, 5, 4, 1\}$ Nein
$4 : \{4, 5, 9, 3, 1\}$ Nein
$5 : \{5, 3, 4, 9, 1\}$ Nein
$6 : \{6, 3, 7, 9, 10, 5, 8, 4, 2, 1\}$ Ja
$7 : \{7, 5, 2, 3, 10, 4, 6, 9, 8, 1\}$ Ja
$8 : \{8, 9, 6, 4, 10, 3, 2, 5, 7, 1\}$ Ja
$9 : \{9, 4, 3, 5, 1\}$ Nein
$10 : \{10, 1\}$ Nein

Aufgabe 1: Generatoren

Geben Sie alle Generatoren (erzeugende Elemente) an von:

a) $(\mathbb{Z}_{11}^*, \cdot)$

$\mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
$1 : \{1\}$ Nein
$2 : \{2, 4, 8, 5, 10, 9, 7, 3, 6, 1\}$ Ja
$3 : \{3, 9, 5, 4, 1\}$ Nein
$4 : \{4, 5, 9, 3, 1\}$ Nein
$5 : \{5, 3, 4, 9, 1\}$ Nein
$6 : \{6, 3, 7, 9, 10, 5, 8, 4, 2, 1\}$ Ja
$7 : \{7, 5, 2, 3, 10, 4, 6, 9, 8, 1\}$ Ja
$8 : \{8, 9, 6, 4, 10, 3, 2, 5, 7, 1\}$ Ja
$9 : \{9, 4, 3, 5, 1\}$ Nein
$10 : \{10, 1\}$ Nein
Wir haben also folgende Generatoren: $\{2, 6, 7, 8\}$

Aufgabe 1: Generatoren

Geben Sie alle Generatoren (erzeugende Elemente) an von:

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

Aufgabe 1: Generatoren

Geben Sie alle Generatoren (erzeugende Elemente) an von:

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

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

Aufgabe 1: Generatoren

Geben Sie alle Generatoren (erzeugende Elemente) an von:

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

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

$1 : \{1\}$ Nein

Aufgabe 1: Generatoren

Geben Sie alle Generatoren (erzeugende Elemente) an von:

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

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

Aufgabe 1: Generatoren

Geben Sie alle Generatoren (erzeugende Elemente) an von:

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

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

Aufgabe 1: Generatoren

Geben Sie alle Generatoren (erzeugende Elemente) an von:

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

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

Aufgabe 1: Generatoren

Geben Sie alle Generatoren (erzeugende Elemente) an von:

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

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

Aufgabe 1: Generatoren

Geben Sie alle Generatoren (erzeugende Elemente) an von:

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

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

Aufgabe 1: Generatoren

Geben Sie alle Generatoren (erzeugende Elemente) an von:

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

$\mathbb{Z}_{14}^* = \{1, 3, 5, 9, 11, 13\}$
$1 : \{1\}$ Nein
$3 : \{3, 9, 13, 11, 5, 1\}$ Ja
$5 : \{5, 11, 13, 9, 3, 1\}$ Ja
$9 : \{9, 11, 1\}$ Nein
$11 : \{11, 9, 1\}$ Nein
$13 : \{13, 1\}$ Nein
Wir haben also folgende Generatoren: $\{3, 5\}$

Aufgabe 2: Ordnung

Erklären Sie zunächst in eigenen Worten, was die Ordnung einer Gruppe und was die Ordnung eines Elementes einer Gruppe ist. Erläutern Sie außerdem, was die eulersche φ-Funktion $\varphi(n)$ berechnet.
Bestimmen Sie andschließend die Ordnung von

a) $(\mathbb{Z}_{12}^*, \cdot)$

b) 5 in $(\mathbb{Z}_{14}^*, \cdot)$

c) $\varphi(1999)$

Aufgabe 2: Ordnung

Die **Ordnung einer Gruppe** ist die Anzahl der Elemente in G.

Die **Ordnung eines Elementes einer Gruppe** gibt an, wie oft man das Element mit sich selbst verknüpfen muss, damit das neutrale Element der Gruppe entsteht.

$\varphi(n)$ ist die Ordnung von $\mathbb{Z}_n^*$

Aufgabe 2: Ordnung

$(\mathbb{Z}_{12}^*, \cdot)$

Aufgabe 2: Ordnung

$(\mathbb{Z}_{12}^*, \cdot) = \{1, 5, 7, 11\}$, Ordnung also $= 4$

Aufgabe 2: Ordnung

$(\mathbb{Z}_{12}^*, \cdot) = \{1, 5, 7, 11\}$, Ordnung also $= 4$

5 in $(\mathbb{Z}_{14}^*, \cdot)$:

Aufgabe 2: Ordnung

$(\mathbb{Z}_{12}^*, \cdot) = \{1, 5, 7, 11\}$, Ordnung also $= 4$

5 in $(\mathbb{Z}_{14}^*, \cdot)$:
$5^1 \bmod 14 = 5$

Aufgabe 2: Ordnung

$(\mathbb{Z}_{12}^*, \cdot) = \{1, 5, 7, 11\}$, Ordnung also $= 4$

5 in $(\mathbb{Z}_{14}^*, \cdot)$:
$5^1 \bmod 14 = 5$
$5^2 \bmod 14 = 11$

Aufgabe 2: Ordnung

$(\mathbb{Z}_{12}^*, \cdot) = \{1, 5, 7, 11\}$, Ordnung also $= 4$

5 in $(\mathbb{Z}_{14}^*, \cdot)$:
$5^1 \bmod 14 = 5$
$5^2 \bmod 14 = 11$
$5^3 \bmod 14 = 13$

Aufgabe 2: Ordnung

$(\mathbb{Z}_{12}^*, \cdot) = \{1, 5, 7, 11\}$, Ordnung also $= 4$

5 in $(\mathbb{Z}_{14}^*, \cdot)$:
$5^1 \bmod 14 = 5$
$5^2 \bmod 14 = 11$
$5^3 \bmod 14 = 13$
$5^4 \bmod 14 = 9$

Aufgabe 2: Ordnung

$(\mathbb{Z}_{12}^*, \cdot) = \{1, 5, 7, 11\}$, Ordnung also $= 4$

5 in $(\mathbb{Z}_{14}^*, \cdot)$:
$5^1 \bmod 14 = 5$
$5^2 \bmod 14 = 11$
$5^3 \bmod 14 = 13$
$5^4 \bmod 14 = 9$
$5^5 \bmod 14 = 1$

Aufgabe 2: Ordnung

$(\mathbb{Z}_{12}^*, \cdot) = \{1, 5, 7, 11\}$, Ordnung also $= 4$

5 in $(\mathbb{Z}_{14}^*, \cdot)$:
$5^1 \bmod 14 = 5$
$5^2 \bmod 14 = 11$
$5^3 \bmod 14 = 13$
$5^4 \bmod 14 = 9$
$5^5 \bmod 14 = 1$

$\varphi(1999)$

Aufgabe 2: Ordnung

$(\mathbb{Z}_{12}^*, \cdot) = \{1, 5, 7, 11\}$, Ordnung also $= 4$

5 in $(\mathbb{Z}_{14}^*, \cdot)$:
$5^1 \bmod 14 = 5$
$5^2 \bmod 14 = 11$
$5^3 \bmod 14 = 13$
$5^4 \bmod 14 = 9$
$5^5 \bmod 14 = 1$

$\varphi(1999) = 1998$

Aufgabe 3: Gruppeneigenschaften

a) Untersuchen Sie die folgende potentielle Gruppe $(\{0,1\}^n, \oplus)$ auf Ihre Gruppeneigenschaften. $\{0,1\}^n$ meint dabei n-bit Werte und $\oplus$ XOR.

Aufgabe 3: Gruppeneigenschaften

a) Untersuchen Sie die folgende potentielle Gruppe $(\{0,1\}^n, \oplus)$ auf Ihre Gruppeneigenschaften. $\{0,1\}^n$ meint dabei n-bit Werte und $\oplus$ XOR.

- Kommutativität: gilt.

Aufgabe 3: Gruppeneigenschaften

a) Untersuchen Sie die folgende potentielle Gruppe $(\{0,1\}^n, \oplus)$ auf Ihre Gruppeneigenschaften. $\{0,1\}^n$ meint dabei n-bit Werte und $\oplus$ XOR.

- Kommutativität: gilt.
- Abgeschlossenheit: gilt.

Aufgabe 3: Gruppeneigenschaften

a) Untersuchen Sie die folgende potentielle Gruppe $(\{0,1\}^n, \oplus)$ auf Ihre Gruppeneigenschaften. $\{0,1\}^n$ meint dabei n-bit Werte und $\oplus$ XOR.

- Kommutativität: gilt.
- Abgeschlossenheit: gilt.
- Assoziativität:

$$a \oplus (b \oplus c) = (a \oplus b) \oplus c.$$

Gilt. Damit ist $(\{0,1\}^n, \oplus)$ eine **Halbgruppe**.

Aufgabe 3: Gruppeneigenschaften

a) Untersuchen Sie die folgende potentielle Gruppe $(\{0,1\}^n, \oplus)$ auf Ihre Gruppeneigenschaften. $\{0,1\}^n$ meint dabei n-bit Werte und $\oplus$ XOR.

- Kommutativität: gilt.
- Abgeschlossenheit: gilt.
- Assoziativität:

$$a \oplus (b \oplus c) = (a \oplus b) \oplus c.$$

  Gilt. Damit ist $(\{0,1\}^n, \oplus)$ eine **Halbgruppe**.
- Neutrales Element e:

$$a \oplus 0 = 0 \oplus a = a.$$

  Damit ist $(\{0,1\}^n, \oplus)$ ein **Monoid**.

Aufgabe 3: Gruppeneigenschaften

a) Untersuchen Sie die folgende potentielle Gruppe $(\{0,1\}^n, \oplus)$ auf Ihre Gruppeneigenschaften. $\{0,1\}^n$ meint dabei n-bit Werte und $\oplus$ XOR.

- Kommutativität: gilt.
- Abgeschlossenheit: gilt.
- Assoziativität:

$$a \oplus (b \oplus c) = (a \oplus b) \oplus c.$$

  Gilt. Damit ist $(\{0,1\}^n, \oplus)$ eine **Halbgruppe**.
- Neutrales Element e:

$$a \oplus 0 = 0 \oplus a = a.$$

  Damit ist $(\{0,1\}^n, \oplus)$ ein **Monoid**.
- Inverses Element a^{-1}:

$$a \oplus a = a \oplus a = e.$$

  Damit ist $(\{0,1\}^n, \oplus)$ eine **Gruppe**.

Aufgabe 3: Gruppeneigenschaften

b) Untersuchen Sie die folgende potentielle Gruppe auf ihre Gruppeneigenschaften:
$(\mathbb{Z}_{13}, \circ)$ mit $a, b \in \mathbb{Z}_{13}$ und $a \circ b := (2 \cdot a + 2 \cdot b) \bmod 13$.

Aufgabe 3: Gruppeneigenschaften

b) Untersuchen Sie die folgende potentielle Gruppe auf ihre Gruppeneigenschaften:
$(\mathbb{Z}_{13}, \circ)$ mit $a, b \in \mathbb{Z}_{13}$ und $a \circ b := (2 \cdot a + 2 \cdot b) \bmod 13$.

- Kommutativität (abelsche Gruppe): Gilt aufgrund der Kommutativität der Addition ganzer Zahlen.

Aufgabe 3: Gruppeneigenschaften

b) Untersuchen Sie die folgende potentielle Gruppe auf ihre Gruppeneigenschaften:
$(\mathbb{Z}_{13}, \circ)$ mit $a, b \in \mathbb{Z}_{13}$ und $a \circ b := (2 \cdot a + 2 \cdot b) \bmod 13$.

- Kommutativität (abelsche Gruppe):
- Gruppoid (Abgeschlossenheit): Gilt

$$a, b \in \mathbb{Z}_{13} \Longrightarrow (a \circ b) \in \mathbb{Z}_{13}$$

Es gilt: $\mathbb{Z}_{13} := \{0, \ldots, 12\}$ und $a \circ b = (2a + 2b) \bmod 13$. Damit liefert die Operation $\circ$ immer einen Werte im Bereich $\{0, \ldots, 12\}$.
$(\mathbb{Z}_n \setminus \{0\}, \cdot)$ ist ein **Gruppoid**.

Aufgabe 3: Gruppeneigenschaften

b) Untersuchen Sie die folgende potentielle Gruppe auf ihre Gruppeneigenschaften:
$(\mathbb{Z}_{13}, \circ)$ mit $a, b \in \mathbb{Z}_{13}$ und $a \circ b := (2 \cdot a + 2 \cdot b) \bmod 13$.

- Kommutativität (abelsche Gruppe):
- Gruppoid (Abgeschlossenheit): Gilt
- Assoziativität:

$$a \circ (b \circ c) = (a \circ b) \circ c$$
$$(a \circ (2b + 2c)) \bmod 13 = ((2a + 2b) \circ c) \bmod 13$$
$$(2a + 2 \cdot (2b + 2c)) \bmod 13 = (2 \cdot (2a + 2b) + 2c) \bmod 13.$$

Gegenbeispiel für $a = 1, b = c = 2$:

$$(2 + 2 \cdot (4 + 4)) \bmod 13 = (2 \cdot (2 + 4) + 4) \bmod 13$$
$$(2 + 2 \cdot 8) \bmod 13 = (2 \cdot 6 + 4) \bmod 13$$
$$18 \bmod 13 = 16 \bmod 13$$
$$5 \neq 3$$

$(\mathbb{Z}_n \setminus \{0\}, \cdot)$ ist keine **Halbgruppe**; und damit auch weder Monoid noch Gruppe.

Aufgabe 3: Gruppeneigenschaften

c) Sei $\mathsf{DLog}_{2,11}(a)$ der diskrete Logarithmus zur Basis 2 in $\mathbb{Z}_{11}$. Es gilt für alle $a \in \mathbb{Z}_{10}$: $\mathsf{DLog}_{2,11}(2^{a \bmod 10} \bmod 11) = a$. Zum Beispiel ist $\mathsf{DLog}_{2,11}(5) = 4$, denn $2^4 \bmod 11 \equiv 5$. Untersuchen Sie die folgende potentielle Gruppe auf ihre Gruppeneigenschaften:
$(\mathbb{Z}_{10}, \circ)$ mit $a, b \in \mathbb{Z}_{10}$ und $a \circ b := \mathsf{DLog}_{2,11}(2^a \cdot 2^b \bmod 11)$.

Aufgabe 3: Gruppeneigenschaften

c) Sei $\mathrm{DLog}_{2,11}(a)$ der diskrete Logarithmus zur Basis 2 in $\mathbb{Z}_{11}$. Es gilt für alle $a \in \mathbb{Z}_{10}$: $\mathrm{DLog}_{2,11}(2^{a \bmod 10} \bmod 11) = a$. Zum Beispiel ist $\mathrm{DLog}_{2,11}(5) = 4$, denn $2^4 \bmod 11 \equiv 5$. Untersuchen Sie die folgende potentielle Gruppe auf ihre Gruppeneigenschaften:
$(\mathbb{Z}_{10}, \circ)$ mit $a, b \in \mathbb{Z}_{10}$ und $a \circ b := \mathrm{DLog}_{2,11}(2^a \cdot 2^b \bmod 11)$.

- Kommutativität (abelsche Gruppe): Gilt aufgrund der Kommutativität der Addition ganzer Zahlen, da $a \circ b = b \circ a = 2^{a+b} \bmod 1$

Aufgabe 3: Gruppeneigenschaften

c) Sei $\text{DLog}_{2,11}(a)$ der diskrete Logarithmus zur Basis 2 in $\mathbb{Z}_{11}$. Es gilt für alle $a \in \mathbb{Z}_{10}$: $\text{DLog}_{2,11}(2^{a \bmod 10} \bmod 11) = a$. Zum Beispiel ist $\text{DLog}_{2,11}(5) = 4$, denn $2^4 \bmod 11 \equiv 5$. Untersuchen Sie die folgende potentielle Gruppe auf ihre Gruppeneigenschaften:
$(\mathbb{Z}_{10}, \circ)$ mit $a, b \in \mathbb{Z}_{10}$ und $a \circ b := \text{DLog}_{2,11}(2^a \cdot 2^b \bmod 11)$.

- Kommutativität (abelsche Gruppe): Gilt
- Gruppoid (Abgeschlossenheit): Gilt
  Da $\varphi(11) = 10$ gilt: $2^a \cdot 2^b \bmod 11 = 2^{a+b \bmod 10} \bmod 11$
  Somit gilt:

$$\underset{2,11}{\text{DLog}}(2^a \bmod 11) \in \mathbb{Z}_{10}, \text{ für alle } a \in \mathbb{Z}_{10}.$$

Aufgabe 3: Gruppeneigenschaften

c) Sei $\mathsf{DLog}_{2,11}(a)$ der diskrete Logarithmus zur Basis 2 in $\mathbb{Z}_{11}$. Es gilt für alle $a \in \mathbb{Z}_{10}$: $\mathsf{DLog}_{2,11}(2^{a \bmod 10} \bmod 11) = a$. Zum Beispiel ist $\mathsf{DLog}_{2,11}(5) = 4$, denn $2^4 \bmod 11 \equiv 5$. Untersuchen Sie die folgende potentielle Gruppe auf ihre Gruppeneigenschaften:
$(\mathbb{Z}_{10}, \circ)$ mit $a, b \in \mathbb{Z}_{10}$ und $a \circ b := \mathsf{DLog}_{2,11}(2^a \cdot 2^b \bmod 11)$.

- Kommutativität (abelsche Gruppe): Gilt
- Gruppoid (Abgeschlossenheit): Gilt
- Assoziativität: Gilt

$$a \circ (b \circ c) = (a \circ b) \circ c$$

$$\mathsf{DLog}_{2,11}(2^{a+\mathsf{DLog}_{2,11}(2^{b+c} \bmod 11)} \bmod 11) = \mathsf{DLog}_{2,11}(2^{\mathsf{DLog}_{2,11}(2^{a+b} \bmod 11)+c} \bmod 11)$$

$$\mathsf{DLog}_{2,11}(2^a \cdot 2^{b+c} \bmod 11) = \mathsf{DLog}_{2,11}(2^{a+b} \cdot 2^c \bmod 11)$$

$$a + b + c \bmod 10 = a + b + c \bmod 10.$$

Es ist eine **Halbgruppe**.

Aufgabe 3: Gruppeneigenschaften

c) Sei $\text{DLog}_{2,11}(a)$ der diskrete Logarithmus zur Basis 2 in $\mathbb{Z}_{11}$. Es gilt für alle $a \in \mathbb{Z}_{10}$: $\text{DLog}_{2,11}(2^{a \bmod 10} \bmod 11) = a$. Zum Beispiel ist $\text{DLog}_{2,11}(5) = 4$, denn $2^4 \bmod 11 \equiv 5$. Untersuchen Sie die folgende potentielle Gruppe auf ihre Gruppeneigenschaften:
$(\mathbb{Z}_{10}, \circ)$ mit $a, b \in \mathbb{Z}_{10}$ und $a \circ b := \text{DLog}_{2,11}(2^a \cdot 2^b \bmod 11)$.

- Kommutativität (abelsche Gruppe): Gilt
- Gruppoid (Abgeschlossenheit): Gilt
- Assoziativität: Gilt
- Neutrales Element e: Gilt

$$a \circ e = e \circ a = a$$

$$\underset{2,11}{\text{DLog}}(2^{a+e} \bmod 11) = \underset{2,11}{\text{DLog}}(2^{e+a} \bmod 11)$$

$$\underset{2,11}{\text{DLog}}(2^{a+0} \bmod 11) = \underset{2,11}{\text{DLog}}(2^{e+0} \bmod 11) = a.$$

Das neutrale Element ist 0. Es ist ein **Monoid** mit $e = 0$.

Aufgabe 3: Gruppeneigenschaften

c) Sei $\text{DLog}_{2,11}(a)$ der diskrete Logarithmus zur Basis 2 in $\mathbb{Z}_{11}$. Es gilt für alle $a \in \mathbb{Z}_{10}$: $\text{DLog}_{2,11}(2^{a \bmod 10} \bmod 11) = a$. Zum Beispiel ist $\text{DLog}_{2,11}(5) = 4$, denn $2^4 \bmod 11 \equiv 5$. Untersuchen Sie die folgende potentielle Gruppe auf ihre Gruppeneigenschaften:
$(\mathbb{Z}_{10}, \circ)$ mit $a, b \in \mathbb{Z}_{10}$ und $a \circ b := \text{DLog}_{2,11}(2^a \cdot 2^b \bmod 11)$.

- Kommutativität (abelsche Gruppe): Gilt
- Gruppoid (Abgeschlossenheit): Gilt
- Assoziativität: Gilt
- Neutrales Element e: Gilt
- Inverses Element a^{-1}:

$$\underset{2,11}{\text{DLog}}(2^{a+a^{-1}} \bmod 11) \equiv \underset{2,11}{\text{DLog}}(2^{a^{-1}+a} \bmod 11) \equiv e$$

$$\underset{2,11}{\text{DLog}}(2^{a+a^{-1}} \bmod 11) \equiv \underset{2,11}{\text{DLog}}(2^{a^{-1}+a} \bmod 11) \equiv \underset{2,11}{\text{DLog}}(2^0).$$

Somit muss $a^{-1} + a \equiv 0 \bmod \varphi(11)$ sein. Das gilt wenn $a^{-1} = 10 - a \bmod 10$ ist, für alle $a \in \mathbb{Z}_{10}$. Es ist demnach eine **Gruppe**.

Aufgabe 4: Eindeutigkeit

Satz 52 (Eindeutigkeit des neutralen Elements)
In einer Halbgruppe gibt es höchstens ein neutrales Element.

Aufgabe 4: Eindeutigkeit

Satz 52 (Eindeutigkeit des neutralen Elements)
In einer Halbgruppe gibt es höchstens ein neutrales Element.

Annahme: Es existieren zwei neutrale Elemente e_1, e_2. Dann muss gelten: $e_1 \circ e_2 = e_1$ und $e_1 \circ e_2 = e_2$. Damit gilt: $e_1 = e_1 \circ e_2 = e_2$.

Aufgabe 4: Eindeutigkeit

Satz 53 (Eindeutigkeit des Inversen)
In einem Monoid gibt es zu jedem Element höchstens ein Inverses. Hat x ein Inverses x^{-1}, dann ist x selbst das Inverse von x^{-1}.

Aufgabe 4: Eindeutigkeit

Satz 53 (Eindeutigkeit des Inversen)
In einem Monoid gibt es zu jedem Element höchstens ein Inverses. Hat x ein Inverses x^{-1}, dann ist x selbst das Inverse von x^{-1}.

Annahme: Es gibt zwei Inverse $\overline{x}, x^{-1}$ für ein Element $x \in (M, \circ)$. Dann gilt:

$$
\begin{aligned}
& x^{-1} \circ \underbrace{(x \circ \overline{x})}_{e} = x^{-1} \\
\overset{\text{Assoziativität}}{\Longleftrightarrow} \; & \underbrace{(x^{-1} \circ x)}_{e} \circ \overline{x} = x^{-1} \\
\Longleftrightarrow \; & e \circ \overline{x} = x^{-1} \\
\overset{\text{Neutrales Element}}{\Longleftrightarrow} \; & \overline{x} = x^{-1}.
\end{aligned}
$$

Aufgabe 4: Eindeutigkeit

Satz 53 (Eindeutigkeit des Inversen)
In einem Monoid gibt es zu jedem Element höchstens ein Inverses. Hat x ein Inverses x^{-1}, dann ist x selbst das Inverse von x^{-1}.

Damit ist gezeigt, dass das Inverse in einem Monoid eindeutig ist. Nun zeigen wir noch, dass x das Inverse von x^{-1} ist.

$$x \circ x^{-1} = e \qquad \mid \circ x^{-1^{-1}}$$
$$x \circ x^{-1} \circ x^{-1^{-1}} = x \circ e = e \circ x^{-1^{-1}}$$
$$x = x^{-1^{-1}}$$

Aufgabe 5: Fermat-Test + RSA

Implementieren Sie den Fermat-Test und den RSA-Algortithmus in Python.

Fragen?