Duale Hochschule Baden-Württemberg

Logik und Algebra

6. Übungsblatt

1. Aufgabe:

   (a) Schreiben Sie tabellarisch den zyklischen Binärcode mit $N = 7$ Bit Codebitlänge und $n = 4$ Bit Datenbits zum Generatorpolynom $p(x) = x^3 + x^2 + 1$ für alle möglichen 16 Datenbit-Kombinationen auf.

   (b) Sortieren Sie die Codewörter aus der gerade bestimmten Tabelle so um, dass die ersten vier Bits gerade mit den Datenbits übereinstimmen, und somit einen systematischen Code darstellen.

2. Aufgabe: Bei einer Übertragung von drei Ascii-Zeichen, aufgeteilt in jeweils zweimal 4 Bits, wurde der in Abbildung 3.3.1 dargestellte $(7, 4)$-Hammingcode zum Generatorpolynom $p(x) = x^3 + x + 1$ verwendet. Bei der Übertragung kann pro Codewort maximal ein Bit gestört sein. Bestimmen Sie die korrigierten Codewörter und bestimmen Sie die Nachricht.

$$(0,0,0,1,1,0,1) \quad (0,0,0,1,1,1,0)$$
$$(0,0,1,1,1,1,0) \quad (1,1,0,1,1,1,1)$$
$$(1,0,1,0,1,1,0) \quad (1,0,1,1,0,1,1)$$

3. Aufgabe: Alice und Bob möchten mit dem Diffie-Hellman Protokoll auf $\mathbb{Z}_{17}$ und Basis $\alpha = 3$ einen geheimen Sitzungsschlüssel berechnen. Alice hat das Geheimnis $a = 3$ und Bob hat das Geheimnis $b = 4$. Welche Nachrichten senden Alice und Bob sich gegenseitig? Und welchen gemeinsamen Sitzungsschlüssel berechnen sie beide jeweils daraus?

4. Aufgabe:

   (a) Führen Sie zu den Werten 9 und 88 den erweiterten euklidischen Algorithmus durch.

   (b) Zeigen Sie, dass in $\mathbb{Z}_{115}$ das Tupel $(9, 115)$ ein korrekter öffentlicher RSA-Schlüssel ist und berechnen Sie den zugehörigen privaten Schlüssel.

   (c) Verschlüsseln Sie die Nachricht $m = 2$ mit dem öffentlichen RSA-Schlüssel $(9, 115)$.

5. Aufgabe:

   (a) Führen Sie zu den Werten 17 und 220 den erweiterten euklidischen Algorithmus durch.

   (b) Zeigen Sie, dass $(17, 253)$ ein korrekter öffentlicher RSA-Schlüssel in $\mathbb{Z}_{253}$ ist, und berechnen Sie den zugehörigen privaten Schlüssel.

   (c) Als Urheber eines Dokuments mit Inhalt $m = 2$ (ein sehr kurzes Dokument), wollen Sie dieses unterschreiben, und verschlüsseln dieses mit Ihrem privaten Schlüssel als Signatur. Wie lautet diese Signatur, und wie überprüfen nun andere, die nur Ihren öffentlichen Schlüssel kennen und das Dokument m samt Signatur erhalten, dass das Dokument von Ihnen ist?

Lösung 5. Übungsblatt

Lösung 1: Die Umkehrabbildungen lauten:

$$f_1^{-1}(x) = x = f_1(x),\ f_2^{-1}(x) = 1 - x = f_2(x),\ f_3^{-1}(x) = \frac{1}{x} = f_3(x),$$

$$f_4^{-1}(x) = \frac{x-1}{x} = f_6(x),\ f_5^{-1}(x) = \frac{x}{x-1} = f_5(x),\ f_6^{-1}(x) = \frac{1}{1-x} = f_4(x)$$

Die Verknüpfungstabelle ist:

$a \circ b$	$b = f_1$	$b = f_2$	$b = f_3$	$b = f_4$	$b = f_5$	$b = f_6$
$a = f_1$	f_1	f_2	f_3	f_4	f_5	f_6
$a = f_2$	f_2	f_1	f_6	f_5	f_4	f_3
$a = f_3$	f_3	f_4	f_1	f_2	f_6	f_5
$a = f_4$	f_4	f_3	f_5	f_6	f_2	f_1
$a = f_5$	f_5	f_6	f_4	f_3	f_1	f_2
$a = f_6$	f_6	f_5	f_2	f_1	f_3	f_4

Nachprüfung der Gruppeneigenschaften:

- $\circ$ ist Verknüpfung auf der Menge $M = \{f_1, f_2, f_3, f_4, f_5, f_6\}$.
- Die Verknüpfung $\circ$ ist assoziativ.
- Die Funktion f_1 ist das neutrale Element der Gruppe.
- Zu jeder Funktion gibt es ein inverses Element in der Menge, es ist jeweils die Umkehrabbildung.

Damit ist $(M, \circ)$ eine Gruppe. Da $f_2 \circ f_3 = f_6 \neq f_4 = f_3 \circ f_2$ ist, ist sie nicht kommutativ.

Lösung 2: Sei $(G, \cdot)$ eine Gruppe mit $|G| = n$ Elementen mit neutralem Element $1 \in G$ und $x \in G$.

(a) Zu zeigen ist: Es gibt ein kleinstes $k \in \mathbb{N}$ mit $x^k = 1$:

Angenommen für alle $k \in \mathbb{N}$ gelte $x^k \neq 1$. Sei $M = \{x, x^2, x^3, \ldots, x^n\} \subseteq G$, so kann nach Annahme $1 \notin M$ sein, und $|M| < n$. Also gibt gibt es $u < v$ mit $x^u = x^v$, da es ja n Einträge in der Definition von M waren, aber nur höchstens $n - 1$ Elemente in M sind. Also ist

$$x^v = \underbrace{x \cdot \ldots \cdot x}_{v \text{ Faktoren}} = \underbrace{x \cdot \ldots \cdot x}_{v-u \text{ Faktoren}} \cdot \underbrace{x \cdot \ldots \cdot x}_{u \text{ Faktoren}} = x^{v-u} \cdot x^u \stackrel{!}{=} x^u$$

und damit ist $x^{v-u} = 1$, da G Gruppe und die Identität eindeutig bestimmt ist. Das ist im Widerspruch zur Annahme, dass es kein $x^k = 1$ gebe. Sei nun $K = \{k \in \mathbb{N} :\ x^k = 1\}$ die Menge alle Potenzen, für die $x^k = 1$ ist. Da $\leq$ Vollordnung ist und K nach unten beschränkt ist, hat K ein kleinstes Element, und das ist das gesuchte k.

(b) Zu zeigen ist: $U \neq \emptyset$ und für $a, b \in U$ ist $a \cdot b^{-1} \in U$ und $a \cdot b = b \cdot a$.

- Da $x^k \in U$ ist $U \neq \emptyset$.
- Sei $a, b \in U$, mit $a = x^u$ und $b = x^v$. Dann ist $b^{-1} = x^{k-v}$, denn $x^{k-v} \circ x^v = x^k = 1$. Und $a \circ b^{-1} = x^u \circ x^{k-v} = x^{u+k-v}$. ist $u + k - v \leq k$, so ist $a \circ b^{-1} \in U$. Ist aber $u + k - v > k$, so ist $u - v > 0$ und $u - v \leq k$ und

  $$x^{u+k-v} = x^k \cdot x^{u-v} = 1 \cdot x^{u-v}$$

  und damit auch in diesem Fall $a \circ b^{-1} \in U$. Damit ist U Untergruppe von G.
- Sei $a, b \in U$, mit $a = x^u$ und $b = x^v$, so ist

  $$a \cdot b = \underbrace{x \cdot \ldots \cdot x}_{u \text{ Faktoren}} \cdot \underbrace{x \cdot \ldots \cdot x}_{v \text{ Faktoren}} = \underbrace{x \cdot \ldots \cdot x}_{u+v=v+u \text{ Faktoren}} = \underbrace{x \cdot \ldots \cdot x}_{v \text{ Faktoren}} \cdot \underbrace{x \cdot \ldots \cdot x}_{u \text{ Faktoren}} = b \cdot a$$

  und damit ist U kommutativ.

Lösung 3: Sei $\tau = (13)(24)$ und $\sigma = (123)$.

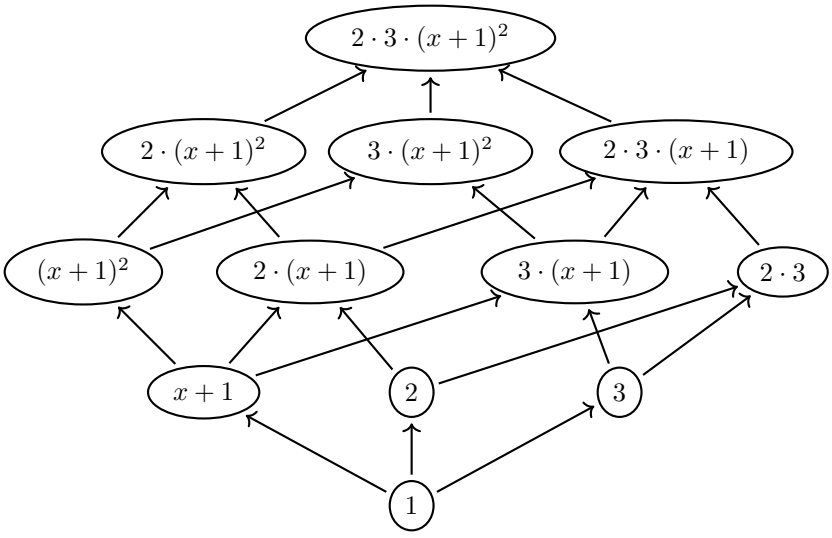
- Es ist $\tau^2 = id$ und $\sigma^2 = (132) = \sigma^{-1}$, $\sigma^3 = id$.
- $\tau \circ \sigma = (142)$, $(\tau \circ \sigma)^2 = (124)$
- $\sigma \circ \tau = (243)$, $(\sigma \circ \tau)^2 = (234)$
- $\tau \circ \sigma^2 = (234) = (\sigma \circ \tau)^2$
- $\sigma^2 \circ \tau = (124) = (\tau \circ \sigma)^2$
- $\tau \circ \sigma \circ \tau = (134)$, $(\tau \circ \sigma \circ \tau)^2 = (143)$
- $\sigma \circ \tau \circ \sigma = (143) = (\tau \circ \sigma \circ \tau)^2$
- $\tau \circ \sigma^2 \circ \tau = (143) = (\tau \circ \sigma \circ \tau)^2$
- $\sigma \circ \tau \circ \sigma^2 = (12)(34)$
- $\sigma^2 \circ \tau \circ \sigma = (14)(23)$
- $\sigma^2 \circ \tau \circ \sigma^2 = (134) = \tau \circ \sigma \circ \tau$

Jedes weitere Verknüpfen von τ oder σ von rechts oder links führt zu $\tau^2 = id$ oder $\sigma^3 = id$ und fällt daher weg. Damit ist das Ergebnis:

$$\langle (13)(24), (123) \rangle = \{id, (123), (124), (132), (134), (142), (143), (234), (243), (12)(34), (13)(24), (14)(23)\}$$

Wegen $\sigma \circ \tau = (243)$ und $\tau \circ \sigma = (142)$ ist die Gruppe nicht kommutativ.

Lösung 4: Es ist $6x^2 + 12x + 6 = 2 \cdot 3 \cdot (x^2 + 2x + 1) = 2 \cdot 3 \cdot (x+1)^2$. Daher ergibt sich:



Lösung 5:

(a)

k	a_k	r_k
0	189	
1	51	$\lfloor \frac{189}{51} \rfloor = 3$
2	$189 - 3 \cdot 51 = 36$	$\lfloor \frac{51}{36} \rfloor = 1$
3	$51 - 1 \cdot 36 = 15$	$\lfloor \frac{36}{15} \rfloor = 2$
4	$36 - 2 \cdot 15 = 6$	$\lfloor \frac{15}{6} \rfloor = 2$
5	$15 - 2 \cdot 6 = 3$	$\lfloor \frac{6}{3} \rfloor = 2$

$\mathrm{ggT}(189, 51) = 3$

k	a_k	r_k
0	189	
1	133	$\lfloor \frac{189}{133} \rfloor = 1$
2	$189 - 133 = 56$	$\lfloor \frac{133}{56} \rfloor = 2$
3	$133 - 2 \cdot 56 = 21$	$\lfloor \frac{56}{21} \rfloor = 2$
4	$56 - 2 \cdot 21 = 14$	$\lfloor \frac{21}{14} \rfloor = 1$
5	$21 - 1 \cdot 14 = 7$	$\lfloor \frac{14}{7} \rfloor = 2$

$\mathrm{ggT}(189, 133) = 7$

(b)

k	a_k	r_k	u_k	v_k
0	196		1	0
1	79	$\lfloor \frac{196}{79} \rfloor = 2$	0	1
2	$196 - 2 \cdot 79 = 38$	$\lfloor \frac{79}{38} \rfloor = 2$	$1 - 2 \cdot 0 = 1$	$0 - 2 \cdot 1 = -2$
3	$79 - 2 \cdot 38 = 3$	$\lfloor \frac{38}{3} \rfloor = 12$	$0 - 2 \cdot 1 = -2$	$1 - 2 \cdot (-2) = 5$
4	$38 - 12 \cdot 3 = 2$	$\lfloor \frac{3}{2} \rfloor = 1$	$1 - 12 \cdot (-2) = 25$	$-2 - 12 \cdot 5 = -62$
5	$3 - 1 \cdot 2 = 1$	$\lfloor \frac{2}{1} \rfloor = 2$	$-2 - 1 \cdot 25 = -27$	$5 - 1 \cdot (-62) = 67$

Damit ist $1 = -27 \cdot 196 + 67 \cdot 79$, also ist 67 die multiplikative Inverse zu 79 in $\mathbb{Z}_{196}$.
Probe: $79 \cdot 67 = 5293 = 1 + 27 \cdot 196$.

k	a_k	r_k	u_k	v_k
0	196		1	0
1	81	$\lfloor \frac{196}{81} \rfloor = 2$	0	1
2	$196 - 2 \cdot 81 = 34$	$\lfloor \frac{81}{34} \rfloor = 2$	$1 - 2 \cdot 0 = 1$	$0 - 2 \cdot 1 = -2$
3	$81 - 2 \cdot 34 = 13$	$\lfloor \frac{34}{13} \rfloor = 2$	$0 - 2 \cdot 1 = -2$	$1 - 2 \cdot (-2) = 5$
4	$34 - 2 \cdot 13 = 8$	$\lfloor \frac{13}{8} \rfloor = 1$	$1 - 2 \cdot (-2) = 5$	$-2 - 2 \cdot 5 = -12$
5	$13 - 1 \cdot 8 = 5$	$\lfloor \frac{8}{5} \rfloor = 1$	$-2 - 1 \cdot 5 = -7$	$5 - 1 \cdot (-12) = 17$
6	$8 - 1 \cdot 5 = 3$	$\lfloor \frac{5}{3} \rfloor = 1$	$5 - 1 \cdot (-7) = 12$	$-12 - 1 \cdot 17 = -29$
7	$5 - 1 \cdot 3 = 2$	$\lfloor \frac{3}{2} \rfloor = 1$	$-7 - 1 \cdot 12 = -19$	$17 - 1 \cdot (-29) = 46$
8	$3 - 1 \cdot 2 = 1$	$\lfloor \frac{2}{1} \rfloor = 2$	$12 - 1 \cdot (-19) = 31$	$-29 - 1 \cdot 46 = -75$

Damit ist $1 = 31 \cdot 196 - 75 \cdot 81$, also ist $196 - 75 = 121$ die multiplikative Inverse zu 81 in $\mathbb{Z}_{196}$.
Probe: $121 \cdot 81 = 9801 = 1 + 50 \cdot 196$.