



Lösungsblatt 2

Aufgabe 1 (Modulo Rechnen)

- (a) Um zu sehen, daß \equiv_n eine Äquivalenzrelation ist, müssen wir die Transitivität, Reflexivität und Symmetrie zeigen. Symmetrie und Reflexivität sind trivial. Für die Transitivität betrachten wir $a \equiv_n b$ und $b \equiv_n c$. Wir haben somit:

$$\begin{aligned} a &= b + k_a n \quad \wedge \quad b = c + k_b n \\ \Rightarrow a &= c + k_b n + k_a n \end{aligned}$$

woraus $a \equiv_n c$ folgt.

- (b) Wie wir schon gesehen haben, gilt $(ab) \equiv ((a \bmod n)(b \bmod n)) \bmod n$. Es bleibt also nur noch zu zeigen, daß die Aussage für k gilt, wenn sie für $k - 1$ gilt. Dies ist leicht zu sehen:

$$\begin{aligned} & \left(\prod_{i=1}^k a_i \right) \bmod n \\ \equiv & \left(\left(\prod_{i=1}^{k-1} a_i \right) \bmod n \right) (a_k \bmod n) \\ \equiv & \left(\left(\prod_{i=1}^{k-1} (a_i \bmod n) \right) \bmod n \right) (a_k \bmod n) \\ \equiv & \left(\prod_{i=1}^{k-1} (a_i \bmod n) \right) (a_k \bmod n) \\ \equiv & \prod_{i=1}^k (a_i \bmod n) \end{aligned}$$

Aufgabe 2 (Modulo Rechnen)

Sei p eine beliebige Primzahl. Wir betrachten die Menge $X = \{1, 2, \dots, p-1\}$ mit der Operation $\circ : X^2 \rightarrow X, (x, y) \mapsto xy \bmod p$.

- (a) Wir stellen eine Möglichkeit für den Beweis vor: Die 1 ist das neutrale Element, die Kommutativität ergibt sich aus der Kommutativität der Multiplikation der ganzen Zahlen. Um die Abgeschlossenheit und die Existenz eines inversen Elements zu sehen, müssen wir ein wenig mehr Aufwand treiben. Dazu definieren wir für alle $a \in X$ die Funktion

$$\circ_a : X \rightarrow X, x \mapsto ax \bmod p.$$

Seien $b \neq c$ Elemente von X . Angenommen, $\circ_a(b) = 0$, dann gilt $ab = kp$ für ein $k \in \mathbb{Z}$. Da p eine Primzahl ist, müsste also nach dem Hinweis gelten, daß $p|a$ oder $p|b$. Dies kann nicht sein, da a und b kleiner als p sind. Dies zeigt die Abgeschlossenheit von X unter der Operation \circ .

Wir wollen nun zeigen, daß die Multiplikation mit einem Element eine Permutation ist. Angenommen, $\circ_a(b) = \circ_a(c)$, dann gilt $ab = ac + kp$ für ein $k \in \mathbb{Z}$. Wir nehmen oBdA an, daß $b > c$. Wir erhalten $a(b-c) = kp$. Nach dem Hinweis kann dies nicht sein, da sowohl a , als auch $(b-c)$ kleiner als p sind. Also ist \circ_a für alle $a \in X$ eine Permutation. Damit gibt es für alle \circ_a ein eindeutiges Urbild der 1, welches das Inverse von a ist. Die Assoziativität der Operation \circ ergibt sich z.B. direkt aus der Aufgabe 1 (b).

- (b) $8 \cdot 23 \cdot x \equiv 1 \cdot x \bmod 61$, weiterhin $8 \cdot 23 \cdot x \equiv 8 \cdot 15 \bmod 61$ und damit $x \equiv 59 \bmod 61$.

Aufgabe 3 (Modulo Rechnen)

- (a) $g \equiv 3X^3X + X \equiv 3X(-X-1) + X \equiv -3X^2 - 2X \bmod (X^3 + X + 1)$
 (b) $f \equiv X^3X^5 \equiv X^3(-X^3-1) \equiv -X^6 - X^3 \equiv X(X^3+1) - X^3 \equiv X^4 - X^3 + X \bmod (X^5 + X^3 + 1)$

Aufgabe 4 (Stromchiffren)

(a)

i	Schlüsselstrom	Periodenlänge
1	1000111000...	6
2	101010...	2
3	111000...	6
4	1001001...	3

(b)

i	Schlüsselstrom	Periodenlänge
1	100010011010111100...	15

Da s_2, \dots, s_4 in dem Schlüsselstrom von s_1 auftauchen, ist die Periodenlänge des Schlüsselstroms jeweils 15.