



Übungsblatt 2

Aufgabe 1 (Modulo Rechnen)

- (a) Sei $1 < n \in \mathbb{N}$. Wir schreiben $a \equiv_n b$ für $a, b \in \mathbb{Z}$, wenn $a \equiv b \pmod{n}$. Zeigen Sie, daß \equiv_n eine Äquivalenzrelation ist.
- (b) Zeigen Sie per Induktion, daß

$$\left(\prod_{i=1}^k (a_i \pmod{n}) \right) \pmod{n} = \left(\prod_{i=1}^k a_i \right) \pmod{n}$$

für alle $n, k \in \mathbb{N}$ und alle $a_1, \dots, a_k \in \mathbb{Z}$.

Aufgabe 2 (Modulo Rechnen)

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

- (a) Zeigen Sie, daß (X, \circ) eine abelsche Gruppe ist.
Hinweis: Wir schreiben $a|b$ (sprich: a teilt b) falls $b \equiv 0 \pmod{a}$. Für eine Primzahl p und $a, b, c \in \mathbb{N}$ gilt: $ab = cp \Rightarrow (p|a \vee p|b)$.
- (b) Finden Sie das kleinste $x \in \mathbb{N}$, so daß $23 \cdot x \equiv 15 \pmod{61}$. Hinweis: $23 \cdot 8 \equiv 1 \pmod{61}$.

Aufgabe 3 (Modulo Rechnen)

Man kann auch mit Polynomen modulo rechnen. Wir betrachten hier Polynome in einer Variablen und ganzzahligen Koeffizienten, d.h. die Menge $\mathbb{Z}[X]$. Seien $a, b, c \in \mathbb{Z}[X]$, dann gilt $a \equiv b \pmod{c}$ genau dann, wenn es ein $k \in \mathbb{Z}[X]$ gibt, so daß $a = b + kc$. Bsp:

$$X^5 \equiv (-X^2 + X + 1) \pmod{(X^3 + X + 1)},$$

da $(-X^2 + X + 1) + (X^3 + X + 1)(X^2 - 1) = X^5$.

- (a) Bestimmen Sie $g \in \mathbb{Z}[X]$ kleinsten Grades, für das $g \equiv (3X^4 + X) \pmod{(X^3 + X + 1)}$ gilt.
- (b) Bestimmen Sie $f \in \mathbb{Z}[X]$ kleinsten Grades, für das $f \equiv X^8 \pmod{(X^5 + X^3 + 1)}$ gilt.

Aufgabe 4 (Stromchiffren)

Mit der Notation aus dem Buch „Einführung in die Kryptographie“. Wir betrachten zwei Stromchiffren mit $n = 4$ und Schlüsseln aus $\{0, 1\}^4$. Wir bezeichnen mit z_i das i -te Bit des Schlüsselstroms und definieren $z_i = k_i$ für $i \leq n$, wobei (k_1, \dots, k_n) der verwendete Schlüssel ist.

- (a) Sei $z_{i+4} = (z_i + z_{i+1} + z_{i+3}) \pmod{2}$. Welche Periodenlänge hat der Schlüsselstrom für die Schlüssel $s_1 = 1000$, $s_2 = 1010$, $s_3 = 1110$ und $s_4 = 1001$?
- (b) Sei $z_{i+4} = (z_i + z_{i+1}) \pmod{2}$. Welche Periodenlänge hat der Schlüsselstrom für die oben genannten Schlüssel in diesem Fall?