Übungen zur Vorlesung Elementare Zahlentheorie (SS 18)

PD Dr. Jürgen Müller, Dr. Martin Bender

(10.1) Aufgabe: Polynomringe.
Es sei R ein Integritätsbereich. Man zeige:

a) Der Polynomring $R[X]$ ist ebenfalls ein Integritätsbereich.

b) Es seien $0 \neq g \in R[X]$ normiert und $f \in R[X]$. Man zeige: Es gibt eindeutig bestimmte $q, r \in R[X]$ mit $f = qg + r$, wobei $r = 0$ oder $\text{Grad}(r) < \text{Grad}(g)$.

c) Man zeige: Der Ring $R[X]$ ist genau dann Euklidisch, wenn R ein Körper ist. Welche Gradfunktion kann man in diesem Fall wählen?

(10.2) Aufgabe: Lagrange-Interpolation.
Es seien K ein Körper, $k \in \mathbb{N}$, und $a_1, \ldots, a_k \in K$ paarweise verschieden.

a) Man zeige: Die Ideale $\langle X - a_i \rangle \trianglelefteq K[X]$, für $i \in \{1, \ldots, k\}$, sind paarweise teilerfremd; siehe Aufgabe **(9.4)**.

b) Aus **(a)** folgere man: Sind $b_1, \ldots, b_k \in K$, so gibt es genau ein **Lagrange-Interpolationspolynom** $f \in K[X]$ mit $f = 0$ oder $\text{Grad}(f) < k$, und $f(a_i) = b_i$, für alle $i \in \{1, \ldots, k\}$. (Die a_i heißen auch die zugehörigen **Stützstellen**.)

(10.3) Aufgabe: Simultane Kongruenzen.
Man untersuche die folgenden Systeme linearer Kongruenzen auf Lösbarkeit in $\mathbb{Z}$, und bestimme gegebenenfalls alle Lösungen:

i) $5X \equiv 3 \pmod 7, \quad 2X \equiv 4 \pmod 8, \quad 3X \equiv 1 \pmod 5.$

ii) $3X \equiv 9 \pmod{27}, \quad X \equiv 57 \pmod{99}, \quad 22X \equiv -55 \pmod{121}.$

(10.4) Aufgabe: Hensel-Lemma.
a) Man untersuche die polynomielle Kongruenz $X^4 \equiv 1 \pmod{5^k}$ auf Lösbarkeit in $\mathbb{Z}/5^k\mathbb{Z}$, und bestimme gegebenenfalls alle Lösungen, für $k \in \{1, \ldots, 8\}$.

b) Wie kann man daraus die Faktorisierung des Polynoms $X^4 - 1 \in \mathbb{Z}[X]$ berechnen? (Zur Erinnerung: Der Ring $\mathbb{Z}[X]$ ist faktoriell.)