D-MATH Grundstrukturen FS 2023
Prof. Richard Pink

Serie 11

Modul-Arithmetik

1. (a) Finde das multiplikative Inverse von $\overline{a}$ in $\mathbb{Z}/n\mathbb{Z}$ für $(a,n) = (2,5)$, $(4,25)$, $(17,49)$.
   (b) Bestimme alle Quadrate in $\mathbb{Z}/n\mathbb{Z}$ für $n = 4, 7, 17$.
   (c) Zeige, dass eine Summe zweier Quadrate in $\mathbb{Z}$ nicht kongruent zu 3 modulo (4) ist.

2. Gegeben sei ein endlicher Körper k der Ordnung 25 mit der Basis $1, a$ als Vektorraum über $\mathbb{F}_5$ und $a^2 = \overline{3}$. Setze $b := a + \overline{1}$.
   (a) Bestimme $a^4, a^6, b^2, b^3, b^4, b^5$ als $\mathbb{F}_5$-Linearkombinationen von $\overline{1}, a$.
   (b) Bestimme b^{-1} als $\mathbb{F}_5$-Linearkombination von $\overline{1}, a$.
   (c) Folgere, dass jedes Element von $k^\times$ eine Potenz von b ist.

3. Mit dem *Euklidischen Algorithmus* kann man den grössten gemeinsamen Teiler zweier natürlicher Zahlen a_0 und a_1 bestimmen und diesen als $\mathbb{Z}$-Linearkombination von a_0 und a_1 ausdrücken. Dafür nehmen wir $a_0 > 0$ an und konstruieren iterativ $a_0, a_1, \ldots$ wie folgt. Zeige:
   (a) Sind a_{k-1} und a_k bereits konstruiert mit $a_k > 0$, so existieren eindeutige $q_k, a_{k+1} \in \mathbb{Z}$ mit $a_{k-1} = q_k a_k + a_{k+1}$ und $0 \leqslant a_{k+1} < a_k$. *(Division mit Rest)*
   (b) Setze $(u_0, v_0, u_1, v_1) := (1, 0, 0, 1)$ und in (a) ausserdem $u_{k+1} := u_{k-1} - q_k u_k$ und $v_{k+1} := v_{k-1} - q_k v_k$ für alle $k \geqslant 1$. Dann gilt $a_k = u_k a_0 + v_k a_1$ für alle k.
   (c) Sind a_{k-1} und a_k konstruiert, so gilt $\mathrm{ggT}(a_0, a_1) = \mathrm{ggT}(a_{k-1}, a_k)$.
   (d) Es existiert ein k mit $a_k = 0$, und für dieses gilt
   $$\mathrm{ggT}(a_0, a_1) \;=\; a_{k-1} \;=\; u_{k-1}a_0 + v_{k-1}a_1.$$
   (e) Bestimme $\mathrm{ggT}(25, 12)$ und $\mathrm{ggT}(497, 284)$ und $\mathrm{ggT}(864, 124)$ als Linearkombination der Ausgangszahlen.
   (f) Sei p eine Primzahl und $a \in \mathbb{Z}$ kein Vielfaches von p. Bestimme mit dem Euklidischen Algorithmus für $a_0 := p$ und $a_1 := a$ das multiplikative Inverse von $\overline{a}$ in $\mathbb{F}_p$.
   (g) Berechne das multiplikative Inverse von $\overline{33}$ in $\mathbb{F}_{71}$ und von $\overline{845}$ in $\mathbb{F}_{997}$.

*4. Zeige, dass der Euklidische Algorithmus in $O(\log(a_1 + 1)))$ Schritten terminiert.