TECHNISCHE UNIVERSITÄT DRESDEN

Fachrichtung Mathematik · **Institut für Algebra** · Modul Math Ma ANGALG WiSe 2016/17

Dr. Jens Zumbrägel 03. Nov. 2016

2. Übungsblatt zur Angewandten Algebra

modulare Arithmetik, endliche Körper

1. Sei $a \in \mathbb{N}$ mit $0 \leq a < 1000$ und die drei letzten Dezimalstellen von $17a$ seien 001. Was ist a? Wie lautet die Antwort, wenn die letzten Ziffern 209 sind?

2. Zeige, dass $f = X^3 + X + 1 \in \mathbb{F}_2[X]$ irreduzibel ist und betrachte $\mathbb{F}_8 = \mathbb{F}_2[X]/\langle f \rangle$.

   (a) Berechne die Inversen aller Elemente in $\mathbb{F}_8^*$ unter Verwendung des erweiterten Euklidischen Algorithmus.

   (b) Warum erzeugt $x := [X] \in \mathbb{F}_8^*$ die multiplikative Gruppe? Berechne x^k für $k \leq 7$ und verifiziere die Ergebnisse in (a).

3. Schreibe Sage-Code, der den endlichen Körper $\mathbb{F}_8 = \mathbb{F}_2[X]/\langle X^3+X+1 \rangle$ definiert. Berechne dann mit Sage für alle $\alpha \in \mathbb{F}_8^*$ die Inversen α^{-1}.

4. Betrachte den Unterring $R \subseteq \mathbb{C}$ mit

$$R := \mathbb{Z} + \mathbb{Z}\sqrt{5}i = \{a + b\sqrt{5}i \mid a, b \in \mathbb{Z}\} .$$

   Zeige, dass die *Normabbildung* $N : R \to \mathbb{N}$, $(a + b\sqrt{5}i) \mapsto a^2 + 5b^2$ multiplikativ ist. Bestimme die Einheitengruppe R^* und zeige, dass die Elemente 2, 3, $1+\sqrt{5}i$ in R irreduzibel, jedoch nicht alle prim sind.

5. Sei K ein Körper und $f \in K[X]$. Zeige:

   (a) Ist $\deg f \in \{2, 3\}$, dann ist f genau dann irreduzibel, wenn f keine Nullstelle in K hat;

   (b) diese Aussage ist für $\deg f = 4$ im Allgemeinen falsch.

6. Zeige, dass $X^2 + 1$ und $X^2 + X + 4$ irreduzibel über $\mathbb{F}_{11}$ sind. Finde einen Isomorphismus

$$\mathbb{F}_{11}[X]/\langle X^2 + 1 \rangle \longrightarrow \mathbb{F}_{11}[X]/\langle X^2 + X + 4 \rangle .$$