


Die in dieser Übung geforderten Implementationen sollen Ideen aus der Vorlesung verwenden und effizienter als bloßes Durchprobieren aller Möglichkeiten sein.

6. Implementieren Sie eine Funktion, die zu einem Element  $a \in \mathbb{F}_q$  und einer natürlichen Zahl  $m$  die  $p^m$ -te Wurzel von  $a$  berechnet. (Hier ist  $p$  eine Primzahl und  $\mathbb{F}_q$  ein endlicher Körper der Charakteristik  $p$ .)
7. Implementieren Sie eine Funktion, die ein gegebenes Polynom  $f \in \mathbb{F}_q[X]$  in quadratfreie Faktoren zerlegt.
8. Implementieren Sie eine Funktion, die testet, ob ein gegebenes Polynom  $f \in \mathbb{F}_q[X]$  irreduzibel ist.
9. Implementieren Sie eine Funktion, die zu einem gegebenen quadratfreien reduziblen Polynom  $f \in \mathbb{F}_q[X]$  ein  $f$ -reduzierendes Polynom berechnet.
10. Implementieren Sie den Berlekamp-Algorithmus zur Faktorisierung quadratfreier Polynome über endlichen Körpern.
11.  Implementieren Sie eine Funktion, die mittels Berlekamp-Algorithmus beliebige Polynome über endlichen Körpern faktorisiert.