Übungen zur Elementaren Zahlentheorie **Sommersemester 2018**

Prof. Dr. Rainer Weissauer Blatt 5

Abgabe bis 25. Mai

Für eine Primzahl p ist $\mathbb{F}_p = \mathbb{Z}/(p)$ der endliche Körper mit p Elementen.

1. Aufgabe: Konstruieren Sie ein primitives Element von $\mathbb{F}_{37}^{\times}$. Sie sollen dabei auch zeigen, dass das gefundene Element tatsächlich primitiv ist.

2. Aufgabe: Zeigen Sie: Es gilt $X(X-1)(X-2)\cdot\cdots\cdot(X-p+1) = X^p - X$ in $\mathbb{F}_p[X]$.

3. Aufgabe: Zeigen Sie für die Eulersche phi-Funktion:

(a) $\phi(m) \leq m-1$ für ganze $m \geq 2$, wobei $\phi(m) = m-1$ genau dann wenn m prim,

(b) $\phi(mn) = \phi(m)\phi(n)$ für teilerfremde ganze Zahlen $m, n \geq 1$.

4. Aufgabe: Für $p \neq 2$ sei $d \in \mathbb{F}_p^{\times} \setminus (\mathbb{F}_p^{\times})^2$ beliebig.
Zeigen Sie: Die Gleichung $x^2 - dy^2 = 1$ hat genau $p+1$ Lösungen $(x,y) \in \mathbb{F}_p \oplus \mathbb{F}_p$.
Hinweis: Verwenden Sie Aufgabe 4 von Blatt 4.