Übungen zur Elementaren Zahlentheorie **Sommersemester 2018**

Prof. Dr. Rainer Weissauer Blatt 7

Abgabe bis 8. Juni

Beantworten Sie jeweils knapp die folgenden Fragen.

(a) In einem Hauptidealring R seien $a, b \in R$ Teiler von $n \in R$ mit $\mathrm{ggT}(a, b) = 1$. Warum ist ab ein Teiler von n?

(b) Wie definiert man den größten gemeinsamen Teiler zweier Elemente in einem Hauptidealring?

(c) Sei $\mathbb{F}_q$ ein endlicher Körper mit q Elementen. Wie kann man die additive Gruppe $(\mathbb{F}_q, +)$ beschreiben?

(d) Sei $n \geq 1$ eine natürliche Zahl und K ein Körper. Warum kann man das Polynom $X^n - Y^n \in K[X, Y]$ durch das Polynom $X - Y$ teilen? Wie kann man den Quotienten als Polynom beschreiben?

(e) Sei $\phi : G \to H$ ein Gruppenhomomorphismus zwischen endlichen Gruppen. Warum gilt $\#G = \#\ker(\phi) \cdot \#\mathrm{Bild}(\phi)$?

(f) Für einen Körper K sei $f \in K[X]$ ein Polynom vom Grad r. Unter welcher Bedingung an f ist $K[X]/(f)$ nullteilerfrei? Warum ist $(1, X, X^2, \ldots, X^{r-1})$ eine Vektorraumbasis von $K[X]/(f)$?

(g) Sei $f : A \to B$ eine Abbildung zwischen endlichen Mengen. Warum ist f injektiv genau dann wenn f surjektiv ist?

(h) Sei $\mathbb{F}_q$ ein endlicher Körper mit q Elementen und l ein Teiler von q. Warum bildet die Teilmenge $\{x \in \mathbb{F}_q \mid x = x^l\}$ einen Unterkörper von $\mathbb{F}_q$? Wieviele Elemente hat dieser Unterkörper?

(i) Beim RSA-Verfahren verwendet man ein Produkt zweier Primzahlen. Warum sollten diese Primzahlen möglichst groß sein? Woraus bestehen jeweils Schlüssel und Gegenschlüssel?

(j) Warum ist der Gaußsche Zahlenring ein euklidischer Ring?

(k) Für reelles $x \geq 1$ sei $\pi(x) = \#\{p \in \mathbb{N} \text{ prim } \mid p \leq x\}$ die Primzahlfunktion. Wie kann man das Wachstum von $\pi(x)$ für große x beschreiben?