Übungen zur Elementaren Zahlentheorie **Sommersemester 2018**

Prof. Dr. Rainer Weissauer Blatt 6

Abgabe bis 1. Juni

---

1. Aufgabe: Fixieren Sie die Primzahlen $p = 5$ und $q = 7$.

(a) Berechnen Sie für $n = pq$ die Eulersche phi-Funktion $m = \varphi(n)$.

(b) Bestimmen Sie zu $f = 5$ ein multiplikatives Inverses e modulo m.

(c) Sei x die Anzahl der Buchstaben Ihres Namens.[1] Verschlüsseln Sie x nach dem RSA-Verfahren mit dem Schlüssel (n, f), indem Sie $y = x^f \pmod n$ berechnen.

(d) Prüfen Sie nach ob $x = y^e \pmod n$.

2. Aufgabe: Sei R ein kommutativer nullteilerfreier Ring mit endlich vielen Elementen. Zeigen Sie: R ist ein Körper.

3. Aufgabe: Seien p und l Primzahlen, sodass l ein Teiler von $p-1$ ist. Sei $d \in \mathbb{F}_p^\times \setminus (\mathbb{F}_p^\times)^l$. Zeigen Sie: Das Polynom $f(X) = X^l - d$ ist irreduzibel in $\mathbb{F}_p[X]$.
Hinweis: Für einen Erzeuger a von $\mathbb{F}_p^\times$ sei $\zeta = a^{(p-1)/l}$, dann gilt $f(X) = f(\zeta X)$.

4. Aufgabe: Zeigen Sie: Für jede natürliche Zahl $n \geq 1$ gibt es eine Primzahl p mit

$$n \leq p \leq 100 \cdot n \ .$$

Hinweis: Verwenden Sie die Abschätzung von Tchebychev für die Primzahlfunktion.

[1] Bei Gruppenabgabe wählen Sie einen der Namen.