WOLFGANG K. SEILER
Tel. 2515

A5, C201

1. März 2018

3. Übungsblatt Zahlentheorie

Aufgabe 1: *(6 Punkte)*

a) Zeigen Sie: Für jedes $a \in (\mathbb{Z}/m)^\times$ definiert die Multiplikation mit a eine bijektive Abbildung von $(\mathbb{Z}/m)^\times$ nach $(\mathbb{Z}/m)^\times$.

b) Folgern Sie, daß $\prod_{x\in(\mathbb{Z}/m)^\times} x = \prod_{x\in(\mathbb{Z}/m)^\times}(ax)$ und daß für alle zu m teilerfremden $a \in \mathbb{Z}$ gilt $a^{\varphi(m)} \equiv 1 \bmod m$.

c) Zeigen Sie, daß für eine Primzahl p und beliebige $a, b \in \mathbb{Z}$ gilt $(a+b)^p \equiv a^p + b^p \bmod p$. *Hinweis: Verwenden Sie den binomischen Lehrsatz!*

d) Leiten Sie daraus einen neuen Beweis des kleinen Satzes von FERMAT ab!

Aufgabe 2: *(4 Punkte)*

a) Beweisen Sie die WILSONsche Kongruenz: Für jede Primzahl p ist $(p-1)! \equiv -1 \bmod p$. *Hinweis:* Betrachten Sie die Faktoren in $(p-1)!$ als Elemente des Körpers $\mathbb{F}_p$, und beachten Sie, daß mit jedem Element i auch dessen (nicht notwendigerweise von i verschiedenes) Inverses vorkommt.

b) Zeigen Sie auch die Umkehrung: Gilt für $p \in \mathbb{N} \smallsetminus \{1\}$ die Kongruenz $(p-1)! \equiv -1 \bmod p$, so ist p eine Primzahl.

Aufgabe 3: *(5 Punkte)*

a) Berechnen Sie im Körper $\mathbb{F}_{17}$ die folgenden Elemente:

$$x_1 = 3 - 14, \qquad x_2 = 12 \cdot 13, \qquad x_3 = 10/11, \qquad x_4 = 2^{100}$$

b) Finden Sie eine primitive Wurzel von $\mathbb{F}_{17}$!

Aufgabe 4: *(5 Punkte)*

a) p sei eine Primzahl, und zu $a \in \mathbb{F}_p^\times$ gebe es ein $x \in \mathbb{F}_p$ mit $x^2 = a$. Zeigen Sie: Dann ist $x^{p+1} = a$.

b) Nun sei $p \equiv 3 \bmod 4$. Zeigen Sie: Wenn es in $\mathbb{F}_p$ eine Lösung x der Gleichung $x^2 = a$ gibt, so ist auch $y = a^{(p+1)/4}$ eine Lösung.

c) Bestimmen Sie im Körper $\mathbb{F}_{127}$ die Lösungsmenge der Gleichung $x^2 = 3$!

d) *Ditto* für $x^2 = 11$!

e) *Ditto* für $x^2 + 2x = 10$!

Aufgabe 5: *(4 Punkte)*

a) Zeigen Sie: Für jede Primzahl p ist $(\mathbb{Z}/2p)^\times$ zyklisch!

b) Sind p und q zwei verschiedene ungerade Primzahlen, so ist $(\mathbb{Z}/pq)^\times$ nicht zyklisch.

c) Für welche $m \leq 15$ ist die prime Restklassengruppe $(\mathbb{Z}/m)^\times$ zyklisch?

Abgabe bis zum Donnerstag, dem 8. März 2018, um 10.10 Uhr