Wolfgang K. Seiler A5, C201
Tel. 2515

25. Februar 2014

3. Übungsblatt Zahlentheorie

Aufgabe 1: *(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 $p \in \mathbb{N} \setminus \{1\}$ die Kongruenz $(p-1)! \equiv -1 \bmod p$, so ist p eine Primzahl.

Aufgabe 2: *(5 Punkte)*

a) Berechnen Sie im Körper $\mathbb{F}_{257}$ die folgenden Elemente:

$$x_1 = 3 - 100, \qquad x_2 = 100 \cdot 100, \qquad x_3 = 11/19, \qquad x_4 = 2^{4100}$$

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

Aufgabe 3: *(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 4: *(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 $m \le 15$ ist die prime Restklassengruppe $(\mathbb{Z}/m)^\times$ zyklisch?

Aufgabe 5: *(2 Punkte)*

a) Wie viele Elemente hat die Gruppe $(\mathbb{Z}/2014)^\times$?
Hinweis: Die Primfaktorzerlegung von 2014 ist $2^2 \cdot 19 \cdot 53$.

b) Ist diese Gruppe zyklisch?

Abgabe bis zum Dienstag, dem 4. März 2014, um 11.55 Uhr