Aufgaben

Blatt 3 : Der Satz von Euler-Fermat, zyklische Gruppen

Aufgabe 1. Bestimmen Sie die Lösungen $x \in \mathbb{Z}$ von :

a. $x^{1477} \equiv 54 \pmod{97}$,

b. $x^{39} \equiv 3 \pmod{13}$.

Aufgabe 2.

a. Seien $n \in \mathbb{N}$ und $R = \mathbb{Z}/n\mathbb{Z}$. Zeigen Sie :

$$n \text{ ist eine Primzahl} \Leftrightarrow \forall a \in R \setminus \{0\} : \; a^{n-1} \equiv 1 \pmod{n}.$$

b. Gilt die Äquivalenz :

$$n \text{ ist eine Primzahl} \Leftrightarrow \forall a \in R^{\times} : \; a^{n-1} \equiv 1 \pmod{n}?$$

Hinweis : $n = 561$.

Aufgabe 3. Seien $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$ und $g = \operatorname{ggT}(a, n)$. Zeigen sie, dass unter Annahme von $g|b$ die Gleichung

$$ax \equiv b \pmod{n} \tag{1}$$

genau g Lösungen in $\mathbb{Z}/n\mathbb{Z}$ hat :

$$x + n\mathbb{Z}, \; x + n/g + n\mathbb{Z}, \ldots, \; x + (g-1)n/g + n\mathbb{Z},$$

wobei x eine beliebige Lösung von (1) ist.

Aufgabe 4. Es sei $m \in \mathbb{N}$ und $\varphi : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ ein Automorphismus von $\mathbb{Z}/m\mathbb{Z}$, d.h. φ ist ein bijekiver Gruppenhomomorphismus. Zeigen Sie :

a. Das Element $\bar{k}$ in $\mathbb{Z}/m\mathbb{Z}$ $(m \neq 0)$ hat Ordnung $m/\operatorname{ggT}(m, k)$,

b. $\varphi(\bar{1})$ hat Ordnung m,

c. $G = \operatorname{Aut}(G)$, die Menge der Automorphismen von G, ist eine Gruppe bezüglich „$\circ$“ (der Komposition von Abbildungen),

d. Die Gruppe G ist isomorph zu $(\mathbb{Z}/m\mathbb{Z})^{\times}$.

`Die Blätter sollen bis Donnerstag, den 06.11. um 14.15 Uhr in die dafür vorgesehenen Einwurfkästen im Foyer des Mathematischen Instituts abgegeben werden.`