UNIVERSITÄT DES SAARLANDES

Fachrichtung Mathematik
Prof. Dr. Simon Brandhorst
Dr. Tobias Columbus

Elementare Zahlentheorie

Übungsblatt 11

Aufgabe 1 (4 Punkte)
Bestimmen Sie die Ordnungen von 7 und 13 in $(\mathbb{Z}/23\mathbb{Z})^\times$.

Aufgabe 2 (4 Punkte)
Finden Sie das kleinste $x \in \mathbb{N}$ welches das System

$$x \equiv 2 \mod 6 \qquad x \equiv 5 \mod 7 \qquad x \equiv 4 \mod 5$$

simultaner Kongruenzen löst.

Aufgabe 3 (4 Punkte)

(a) Folgern sie aus dem chinesischen Restsatz, dass $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$ für teilerfremde natürliche Zahlen $m, n \in \mathbb{N}$.

(b) Zeigen Sie, dass für $n = p_1^{e_1} \cdot \dots \cdot p_r^{e_r}$ mit paarweise verschiedenen Primzahlen $p_1, \dots, p_r$ die Gleichung

$$\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_r}\right)$$

gilt.

Aufgabe 4 (4 Punkte)
Für eine Zahl $N \in \mathbb{Z}$ heißt $a \in (\mathbb{Z}/N\mathbb{Z})^\times$ ein *quadratischer Rest mod* N, wenn es ein $x \in (\mathbb{Z}/N\mathbb{Z})^\times$ gibt, so dass $x^2 = a$. In dieser Aufgabe untersuchen wir quadratische Reste mod p für eine ungerade Primzahl p. Zeigen Sie:

(a) Die quadratischen Reste sind eine Untergruppe von $(\mathbb{Z}/p\mathbb{Z})^\times$.

(b) Für einen quadratischen Rest $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ gibt es maximal zwei $x \in (\mathbb{Z}/N\mathbb{Z})^\times$ mit $x^2 = a$ und somit gibt es mindestens $\frac{p-1}{2}$ quadratische Reste mod p.

(c) Für $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ ist

$$a^{\frac{p-1}{2}} = \begin{cases} 1 & \text{falls } a \text{ ein quadratischer Rest mod } p \text{ ist,} \\ -1 & \text{sonst.} \end{cases}$$

und es gibt genau $\frac{p-1}{2}$ quadratische Reste mod p.

Hinweis: Ein Polynom f hat maximal $\deg(f)$ Nullstellen in $\mathbb{Z}/p\mathbb{Z}$.

Abgabe bis spätestens Montag, den 24. 06. 2019, um 12:00 Uhr. Werfen Sie Ihre Lösungsvorschläge in die dafür vorgesehenen Einwurfkästen vor dem Zeichensaal in Gebäude E 2 5. Abgabe zu zweit ist möglich. Bitte geben Sie Ihren Namen, Ihre Matrikelnummer und Ihre Übungsgruppe and!