Übungen zu Elementare Zahlentheorie

Blatt 10

Aufgabe 1.

a) Es seien a, b und k ganze Zahlen. Zeigen Sie, dass die folgenden Aussagen äquivalent sind:

- (i) Die diophantische Gleichung $ax + by = k$ ist lösbar.
- (ii) Es ist $\text{ggT}(a, b)$ ein Teiler von k .

Falls $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$ eine spezielle Lösung von $ax + by = k$ ist, so ist die Menge aller Lösungen von $ax + by = k$ gerade die Menge

$$\left\{ \left(x_0 + t \cdot \frac{b}{\text{ggT}(a, b)}, y_0 - t \cdot \frac{a}{\text{ggT}(a, b)} \right) \mid t \in \mathbb{Z} \right\} .$$

b) Bestimmen Sie jeweils die Lösungsmenge der folgenden drei diophantischen Gleichungen:

- (1) $2013x + 171y = 3$
- (2) $2013x + 171y = 10$
- (3) $2013x + 171y = 30$

Aufgabe 2.

a) Es seien p eine Primzahl und $1 \leq \beta \leq \alpha$ natürliche Zahlen und $s \in \mathbb{Z}$ mit $p \nmid s$. Zeigen Sie, dass die folgenden Aussagen äquivalent sind:

- (i) Die quadratische Kongruenz $x^2 \equiv p^\beta \cdot s \pmod{p^\alpha}$ ist lösbar.
- (ii) Es gilt $2 \mid \beta$ und die quadratische Kongruenz $x^2 \equiv s \pmod{p^{\alpha-\beta}}$ ist lösbar.

b) Bestimmen Sie jeweils die Lösungsmenge der folgenden drei quadratischen Kongruenzen:

- (1) $x^2 \equiv 5 \cdot 5 \cdot 5 \cdot 5 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \pmod{5 \cdot 5 \cdot 5 \cdot 5 \cdot 5}$
- (2) $x^2 \equiv 7 \cdot 7 \cdot 7 \cdot 5 \cdot 2 \cdot 2 \pmod{7 \cdot 7 \cdot 7 \cdot 7 \cdot 7}$
- (3) $x^2 \equiv 7 \cdot 7 \cdot 7 \cdot 7 \cdot 7 \cdot 5 \cdot 2 \cdot 2 \pmod{7 \cdot 7 \cdot 7 \cdot 7 \cdot 7}$

Aufgabe 3.

a) Es sei m eine ungerade natürliche Zahl und es seien $a, b, c \in \mathbb{Z}$. Zudem sei $[a]_m$ in $\mathbb{Z}/m\mathbb{Z}$ invertierbar. Zeigen Sie, dass die Lösungsmenge der Gleichung

$$(*) \quad [a]_m x^2 + [b]_m x + [c]_m = [0]_m$$

in dem Ring $\mathbb{Z}/m\mathbb{Z}$ übereinstimmt mit der Lösungsmenge der Gleichung

$$([2]_m [a]_m x + [b]_m)^2 = [b]_m^2 - [4]_m [a]_m [c]_m \quad .$$

Zeigen Sie anschließend, dass die folgenden Aussagen äquivalent sind:

(i) Die Gleichung (*) ist lösbar in $\mathbb{Z}/m\mathbb{Z}$.

(ii) Es ist $[b]_m^2 - [4]_m[a]_m[c]_m$ eine quadratische Restklasse in $\mathbb{Z}/m\mathbb{Z}$.

b) Zeigen Sie, dass für jede Primzahl p die Gleichung

$$[6]_m x^2 + [7]_m x + [2]_m = [0]_m$$

eine Lösung hat, jedoch die Lösungsmenge der Gleichung

$$6x^2 + 7x + 2 = 0$$

über dem Ring $\mathbb{Z}$ leer ist.

Aufgabe 4.

a) Bestimmen Sie jeweils die Lösungsmenge der folgenden drei quadratischen Kongruenzen:

(1) $x^2 \equiv 1 \pmod{70}$

(2) $x^2 + 2x + 2 \equiv 0 \pmod{210}$

(3) $x^2 + 2x + 2 \equiv 0 \pmod{455}$

b) Berechnen Sie die folgenden Legendre-Symbole:

$$\left(\frac{3}{19}\right), \quad \left(\frac{5}{19}\right), \quad \left(\frac{6}{19}\right), \quad \left(\frac{18}{19}\right)$$