ELEMENTARE ZAHLENTHEORIE
5. Übungsblatt

Julia Sauter, Andrew Hubery

Aufgabe 1.

Lösen Sie die folgende lineare Kongruenzen.

(a) $2x \equiv 7 \pmod{13}$.

(b) $12x \equiv 29 \pmod{71}$.

(c) $3x \equiv 6 \pmod{18}$.

(d) $14x \equiv 21 \pmod{49}$.

(1+1+2+2 Punkte)

Aufgabe 2.

Finden Sie alle $x \in \mathbb{Z}$, die die folgenden simultanen Kongruenzen lösen.

(a) $x \equiv 2 \pmod{6}$, $x \equiv 2 \pmod{5}$, $x \equiv 5 \pmod{9}$.

(b) $x \equiv 7 \pmod{3}$, $x \equiv 8 \pmod{4}$, $x \equiv 9 \pmod{5}$, $x \equiv 10 \pmod{7}$.

(je 2 Punkte)

Aufgabe 3.

Die sechste Legion schrieb um 50 vor Christus an Caesar (in deutsch):

NSP ZQOA UCJJAOBP KOFOBRCJJOP, OAPOB UBSEE KPL LAIG, OAPOB GJOAP MAH XKPL

Es wurden den Buchstaben A bis Z die Zahlen 0 bis 25 zugeordnet und die Caesar Verschlüsselung mit der Vorschrift $y \equiv 3x + 2 \pmod{26}$ zur Verschlüsselung benutzt.

Entschlüsseln Sie die Nachricht.

(3 Punkte)

Abgabe: Dienstag 21. Mai, bis 12 Uhr in die Postfächer der Tutoren im V3–126

Aufgabe 4.

Wir wissen schon, dass Kongruenz modulo m eine Äquivalenzrelation ist (Eigenschaften 36 aus der Vorlesung). Für $x \in \mathbb{Z}$ schreiben wir $[a]_m$ für die Äquivalenzklasse von x, also $[a]_m \coloneqq \{b \in \mathbb{Z} \mid b \equiv a \pmod{m}\}$. (Wenn m fest ist, schreibt man auch $\bar{a}$ statt $[a]_m$.)

(a) Seien $m, n \geq 1$ teilerfremd. Zeigen Sie, mit Hilfe des chinesischen Restsatzes, dass die folgende Abbildung eine Bijektion ist.

$$\mathbb{Z}/mn\mathbb{Z} \to (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}), \quad [a]_{mn} \mapsto \big([a]_m, [a]_n\big).$$

(b) Für $\underline{a} = (a_1, \ldots, a_r) \in \mathbb{Z}^r$ schreiben wir nun $[\underline{a}]_m \coloneqq ([a_1]_m, \ldots, [a_r]_m) \in (\mathbb{Z}/m\mathbb{Z})^r$. Zeigen Sie jetzt, dass die folgende Abbildung auch eine Bijection ist.

$$(\mathbb{Z}/mn\mathbb{Z})^r \to (\mathbb{Z}/m\mathbb{Z})^r \times (\mathbb{Z}/n\mathbb{Z})^r, \quad [\underline{a}]_{mn} \mapsto \big([\underline{a}]_m, [\underline{a}]_n\big), \quad m, n \text{ teilerfremd.}$$

(c) Sei jetzt $f \in \mathbb{Z}[x_1, \ldots, x_r]$ ein Polynom. Begründen Sie, warum für $\underline{a}, \underline{b} \in \mathbb{Z}^r$ mit $[\underline{a}]_m = [\underline{b}]_m$ gilt $f(\underline{a}) \equiv f(\underline{b}) \pmod{m}$.

(d) Setzen Sie nun

$$\mathcal{S}_f(m) \coloneqq \{[\underline{a}]_m \in (\mathbb{Z}/m\mathbb{Z})^r \mid f(\underline{a}) \equiv 0 \pmod{m}\}.$$

Beweisen Sie, mit Hilfe des Teils (c), dass die Abbildung aus (b) induziert eine Bijektion

$$\mathcal{S}_f(mn) \to \mathcal{S}_f(m) \times \mathcal{S}_f(n), \quad [\underline{a}]_{mn} \mapsto \big([\underline{a}]_m, [\underline{a}]_n\big).$$

Schließen Sie daraus, dass die Funktion

$$S_f \colon \mathbb{N} \to \mathbb{C}, \quad m \mapsto |\mathcal{S}_f(m)|$$

multiplikativ ist.

(2+1+2+2 Punkte)