Universität Bielefeld
Lehrender: Prof. Dr. William Crawley-Boevey
Tutorien: Dr. Julia Sauter und Vincent Klinksiek
WS 2021/2022
Abgabe: Montag 15.11.2021 12:00

AUSGEWÄHLTE KAPITEL: ELEMENTARE ZAHLENTHEORIE
BLATT 5

Aufgabe 1. $(1+2+1)$ Es sei $m = a_n a_{n-1} \dots a_0$ eine Zahl im 10-er System, das heißt

$$m = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \cdots + a_n \cdot 10^n.$$

Zeige das Folgende:

(1) m ist durch 3 teilbar genau dann, wenn $\sum_{i=0}^{n} a_i$ durch 3 teilbar ist.
(2) m ist durch 4 teilbar genau dann, wenn $2a_1 + a_0$ durch 4 teilbar ist.
m ist durch 8 teilbar genau dann, wenn $4a_2 + 2a_1 + a_0$ durch 8 teilbar ist.
(3) Benutze die Teilbarkeitsregeln von oben sowie aus der Vorlesung, um zu zeigen, dass

$$8|27720 \qquad 9|27720 \qquad 11|27720$$

und, dass 17050 nicht durch 66 teilbar ist.

Aufgabe 2. $(1+1+1+1)$ Finde alle Restklassen, die Lösungen der folgenden Kongruenzen sind.

(1) $42x \equiv 21 \pmod{91}$
(2) $(-42)x \equiv 21 \pmod{91}$
(3) $41x \equiv 21 \pmod{91}$
(4) $41x \equiv 20 \pmod{91}$

Aufgabe 3. (4) Die sechste Legion schrieb um 50 vor Christus an Caesar (in deutsch):

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

Entschlüssele die Nachricht. 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.

Aufgabe 4. $(1+1+1+1)$ Bearbeite die folgenden Punkte:

(1) Schreibe eine Liste der Werte $[x]_5^2$ für $x \in \{0,1,2,3,4\}$.
(2) Folgere, dass es kein $[x]_5$ mit $x \in \{0,1,2,3,4\}$ gibt, so dass $[x]_5^2 + [3]_5 = [0]_5$ gilt.
(3) Folgere nun ohne Primfaktorzerlegung, dass es kein $x \in \mathbb{Z}$ gibt mit $x^2 + 3 = 0$.
(4) Benutze $[25]_5 = [0]_5$ und (3), um zu zeigen, dass es kein $x \in \mathbb{Z}$ gibt mit

$$x^2 + 25x + 3 = 0.$$