Zahlentheorie

Übung, LVA 405.031
C. Fuchs, I. Vukusic

8. Übungsblatt, SS 2022

13.05.2022

1. Sei $n > 1$ und $a, x, y \in \mathbb{Z}$ mit $a \neq 0$. Zeige, dass $ax \equiv ay \bmod n \Leftrightarrow x \equiv y \bmod n/\mathrm{ggT}(a, n)$ gilt.

2. Berechne: a) $98^5 + 345 \cdot 567 - 56^3 + 922^5 - 20225 \bmod 2$, b) $57^{68} - 18^3 - 3991201134 \bmod 2$, c) $96^3 \bmod 36$, d) $75^3 + 2 \cdot 75^2 - 75 \bmod 45$, e) $20^{12} - 3 \cdot 19^{12} \bmod 5$, f) $18^{123456789} \bmod 9$. Versuche dabei, immer mit möglichst wenig Aufwand zu rechnen.

3. Zeige, dass die Restklassen $[-a]$ und $[a]$ im Restklassenring $\mathbb{Z}/n\mathbb{Z}$ im Allgemeinen nicht gleich sind, sondern nur für besondere Paare $a \in \mathbb{Z}$ und $n \in \mathbb{N}$. Gib drei verschiedene (besondere) Paare an, für die in $\mathbb{Z}/n\mathbb{Z}$ die Gleichung $[-a] = [a]$ gilt.

4. Bestimme für die folgenden Restklassengleichungen jeweils die Lösung $x \in \mathbb{Z}_n$: a) $9 + x = 4$ in $\mathbb{Z}_{12}$, b) $12 + x = 29$ in $\mathbb{Z}_{37}$, c) $71 + x = 12$ in $\mathbb{Z}_{98}$. Rechne dabei jeweils im Restklassenring!

5. Beim sogenannten Caesar-Verschlüsselungsverfahren werden die Buchstaben eines zu verschlüsselnden Wortes zunächst gemäß $0 = 0, 1 = 1, \ldots,$ A $= 10,$ B $= 11, \ldots,$ Z $= 35,$ Ä $= 36,$ Ö $= 37,$ Ü $= 38,$. $= 39,$ _ $= 40$ durch Zahlen, dann jede der so erhaltenene Zahlen x durch $x + e \bmod 41$ mit einem festen geheimen Schlüssel e ersetzt und anschließend die entstehende Zahl wieder als Buchstabe des verschlüsselten Wortes interpretiert. Verschlüssele mit diesem Verfahren und der Wahl $e = 3$ die Nachricht ZAHLENTHEORIE_IST_SCHOEN. Wie wird entschlüsselt? Entschlüssele die Geheimnachricht JDOOLD2HVW2RPQLV2GLYLVD2LQ2SDUWHV2WUHV. Erkläre, warum dieses Verfahren unsicher ist.