AUSGEWÄHLTE KAPITEL DER ZAHLENTHEORIE
9. ÜBUNGSBLATT

PROF. DR. HENNING KRAUSE
DR. JULIA SAUTER

Aufgabe 1. Berechne $[5]_m^{100}$ für $m = 2, 3, 4, 5, 6, 7, 8, 9, 10$.
Hinweis: Denke an einen Satz von Euler.

Aufgabe 2.

(1) Zeige, dass für alle $x \in \mathbb{Z}$ gilt: $[x]_8^{24} \in \{[0]_8, [1]_8\}$ und $[x]_9^{24} \in \{[0]_9, [1]_9\}$ und folgere $72|x^{24}(x^{24} - 1)$.
(2) Zeige, dass für alle $x \in \mathbb{Z}$ gilt: $[x]_{72}^{24} \in \{[0]_{72}, [1]_{72}, [9]_{72}, [-8]_{72}\}$.
(3) Finde alle $x \in \mathbb{Z}$, die die folgende Kongruenz erfüllen $x^{24} + 8 \equiv 0 \pmod{72}$.

Aufgabe 3.

(1) Finde die Ordnungen von $1, 2, 3, 4, 5, 6$ modulo 7.
(2) Finde die Primitivwurzeln modulo 7.
Finde eine Primitivwurzeln g modulo 11 und zeigen Sie, dass alle Primitivwurzel modulo 11 gegeben sind durch
$$\{[g]_{11}, [g]_{11}^3, [g]_{11}^7, [g]_{11}^9\}.$$

Aufgabe 4. (zum RSA-Algorithmus) Sei $m = pq \in \mathbb{N}$ mit $p \neq q$ Primzahlen und $d \in \mathbb{N}$ teilerfremd zu $\varphi(m)$, das heißt es gibt ein $e \in \mathbb{N}$ mit $[d]_{\varphi(m)}[e]_{\varphi(m)} = [1]_{\varphi(m)}$. Die Verschlüsselung ist die Zuordnung $[x]_m \mapsto [x]_m^d$ auf den Restklassen modulo m und die Entschlüsselung ist die Zuordnung $[y]_m \mapsto [y]_m^e$. Wenn d, m gegeben sind, aber p, q unbekannt sind, so kann man $\varphi(m)$ nicht effizient berechnen, damit auch nicht e, und somit kann man auch nicht entschlüsseln.
Es sei $m = 33$ und $d = 3$. Wir ordnen den Buchstaben $A, B, \ldots, Z$ die Restklassen $0, 1, \ldots, 25$ modulo 33 zu.

(a) Verschlüssele *Hello* mit m und d.
(b) Finde e wie oben beschrieben und entschlüssele $29, 24, 0$.

Abgabe: Freitag, 17. Juni 2016, bis 10.15 Uhr in der Vorlesung. Für jede Aufgabe gibt es 4 Punkte.