Universität Bielefeld
Lehrender: Prof. Dr. William Crawley-Boevey
Tutorien: Dr. Julia Sauter und Vincent Klinksiek
WS 2021/2022
Abgabe: Montag 20.12.2021 12:00

AUSGEWÄHLTE KAPITEL: ELEMENTARE ZAHLENTHEORIE
BLATT 10

Aufgabe 1. **(**$2+2$**)** Sei n eine positive natürliche Zahl.

(1) Zeige, dass
$$\varphi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_m}\right),$$
wobei m eine positive natürliche Zahl ist und $p_1,\dots,p_m$ die paarweise verschiedenen Primfaktoren von n sind.
(2) Beschreibe alle Zahlen n, welche $\varphi(n) = \frac{2n}{5}$ erfüllen.

Hinweis:
(i) Wenn $n = 100 = 2^2\cdot 5^2$, dann sind die paarweise verschiedenen Primfaktoren von n die Primzahlen 2 und 5.
(ii) Die Aussage (1) steht ohne Begründung bereits in der Vorlesung. Zur Begründung kann die folgende Aussage aus der Vorlesung ohne Beweis benutzt werden: Sind a und b teilerfremde positive natürliche Zahlen, so gilt $\varphi(a\cdot b) = \varphi(a)\cdot\varphi(b)$.

Hinweis / Wiederholung: Sei m eine positive natürliche Zahl. Eine Primitivwurzel modulo m ist ein primer Rest modulo m der Ordung $\varphi(m)$.

Aufgabe 2. **(**$2+2$**)** Bearbeite die folgenden Punkte.

(1) Zeige, dass es keine Primitivwurzel modulo 12 gibt.
(2) Es sei p eine Primzahl und g eine Primitivwurzel modulo p. Zeige, dass
$$[g]_p, [g]_p^2, \dots, [g]_p^{p-1}$$
paarweise verschieden sind. Folgere, dass dies alle primen Reste modulo p sind.

Aufgabe 3. **(**$1+1+2$**)** Bearbeite die folgenden Punkte.

(1) Finde die Ordnungen von $1,2,3,4,5,6$ modulo 7.
(2) Finde die Primitivwurzeln modulo 7.
(3) 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 befindet sich auf Seite 2.

Aufgabe 4. (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 $\underline{Hello}$ mit m und d.
(b) Finde e wie oben beschrieben und entschlüssele $29, 24, 0$.