Elementare Zahlentheorie *SoSe 2018*
Barbara Baumeister

10. Übungsblatt

Abgabe: Freitag, 22. Juni 2018, bis 10.00

Aufgabe 1 Berechnen Sie
(a) $\mathrm{ord}_{\mathbb{Z}_{18}}(\overline{5})$, $\mathrm{ord}_{\mathbb{Z}_{18}}(\overline{5}^8)$ und $\mathrm{ord}_{\mathbb{Z}_{18}}(\overline{5}^{19})$.
(b) $\mathrm{ord}_{\mathbb{Z}_{18}^*}(\overline{5})$, $\mathrm{ord}_{\mathbb{Z}_{18}^*}(\overline{5}^8)$ und $\mathrm{ord}_{\mathbb{Z}_{18}^*}(\overline{5}^{19})$.

Aufgabe 2 Berechnen Sie die inversen Elemente zu
(a) $\overline{5}, \overline{8}$ und $\overline{11}$ in $(\mathbb{Z}_{23}, +_{23})$;
(b) $\overline{7}, \overline{11}$ und $\overline{13}$ in $(\mathbb{Z}_{24}^*, \cdot_{23})$.

Aufgabe 3 (a) Sei $n \in \mathbb{N}$, $n \geq 2$ und $\overline{j} \in \mathbb{Z}_n^*$. Zeigen Sie:

$$\mathrm{ord}_{\mathbb{Z}_n^*}(\overline{j}) \mid \varphi(n).$$

(b) Benutzen Sie (a) um auszurechnen
(b.a) $\overline{3}^9$ in $\mathbb{Z}_{20}^*$;
(b.b) $\overline{7}^{18}$ in $\mathbb{Z}_{30}^*$.

Aufgabe 4 Es sei $n \in \mathbb{N}, n \geq 2$ und $\overline{a} \in \mathbb{Z}_n^*$
(a) Es sei $m \in \mathbb{N}$ und $m \equiv 1 \pmod{\varphi(n)}$. Zeigen Sie, dass gilt

$$\overline{a}^m = \overline{a}.$$

(b) Seien $e, d \in \mathbb{Z}_{\varphi(n)}^*$ so, dass $d = e^{-1}$ in $\mathbb{Z}_{\varphi(n)}^*$ ist. Zeigen Sie, dass gilt

$$(\overline{a}^e)^d = \overline{a}.$$