GRUPPEN UND SYMMETRIEN
5. ÜBUNGSBLATT

JULIA SAUTER

Abgabe bis Do, 14.11.19, 12:00h in den Postfächern Ihrer Tutoren im Kopierraum.

Aufgabe 5.1 (Potenzieren von Restklassen)

(a) Berechnen Sie jeweils $r \in \{0, 1, \ldots, n-1\}$, so dass die Potenz gleich $\overline{r} \in \mathbb{Z}/n\mathbb{Z}$ ist.
   1. $\overline{3}^{1003}$ in $\mathbb{Z}/10\mathbb{Z}$,
   2. $\overline{7}^{115}$ in $\mathbb{Z}/22\mathbb{Z}$.

(b) Die multiplikative Gruppe $(\mathbb{Z}/11\mathbb{Z})^\times = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{(-5)}, \overline{(-4)}, \overline{(-3)}, \overline{(-2)}, \overline{(-1)}\}$ ist zyklisch und hat vier Erzeuger. Berechnen Sie die Ordnungen aller Elemente in dieser Gruppe und finden Sie dadurch die vier Erzeuger.

Aufgabe 5.2 (Aufgabe zu Fermatzahlen) Eine *Fermatzahl* ist eine Zahl der Form $2^{2^n} + 1$ mit $n \geq 0$. Die ersten fünf Fermatzahlen sind $3, 5, 17, 257$ und 65537. Fermat vermutete, dass alle solchen Zahlen Primzahlen sind. Euler widerlegte die Vermutung, indem er zeigte, dass $2^{32} + 1$ durch 641 teilbar ist. In dieser Aufgabe möchten wir Eulers Gegenbeispiel gruppentheoretisch nachvollziehen.

(a) Berechne iterativ $\overline{2}^1, \overline{2}^2, \overline{2}^4, \overline{2}^8, \overline{2}^{16}$ und $\overline{2}^{32} \in (\mathbb{Z}/641\mathbb{Z})^\times$ durch Quadrieren des vorangegangenen Ergebnisses. Gib alle Ergebnisse in der Form $\overline{r}$ mit $0 \leq r \leq 640$ an.

(b) Folgere, dass $641 | 2^{32} + 1$ gilt.

(c) Bestimme die Ordnung von $\overline{2}$ in $(\mathbb{Z}/641\mathbb{Z})^\times$.

Aufgabe 5.3 (RSA) Es wird der öffentliche Schlüssel $N = 22$ und $e = 7$ vorgegeben. Die verschüsselte Nachricht lautet

$$1\ \ 12\ \ 3\ \ 1 \qquad 15\ \ 1\ \ 9\ \ 4\ \ 1 \qquad 3\ \ 13\ \ 4$$

Um die entschlüsselte Nachricht zu verstehen, identifiziert man die ersten 21 Buchstaben des Alphabets $A, B, C, \ldots, U$ entsprechend mit $1, 2, 3, \ldots, 21$. Entschlüsseln Sie die Nachricht.

Aufgabe 5.4

(a) Berechnen Sie $\varphi(15), \varphi(5), \varphi(3)$ und finden Sie alle Elemente in $(\mathbb{Z}/15\mathbb{Z})^\times$, $(\mathbb{Z}/5\mathbb{Z})^\times$ und $(\mathbb{Z}/3\mathbb{Z})^\times$.

(b) Schreiben Sie die Bilder der Elemente unter dem Isomorphismus des chinesischen Restsatzes in einer Tabelle auf:

$$(\mathbb{Z}/15\mathbb{Z})^\times \to (\mathbb{Z}/5\mathbb{Z})^\times \times (\mathbb{Z}/3\mathbb{Z})^\times$$
$$k + 15\mathbb{Z} \mapsto (k + 5\mathbb{Z}, k + 3\mathbb{Z})$$

(c) Zeigen Sie, dass $(\mathbb{Z}/5\mathbb{Z})^\times$ und $(\mathbb{Z}/3\mathbb{Z})^\times$ zyklische Gruppen sind.

(d) Folgern Sie, dass $(\mathbb{Z}/15\mathbb{Z})^\times$ isomorph zu $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ist und zeigen Sie, dass die Gruppe nicht zyklisch ist.