

8. Übungsblatt**für die Woche 09.12. - 15.12.2019***Gruppen, Untergruppen, Euler-Fermat, Verschlüsselung*

Ü43 Es wird die Menge U aller Lösungen der Gleichung $z^4 = 1$ in $\mathbb{C}$ betrachtet.

- (a) Zeigen Sie, dass U bzgl. der üblichen Multiplikation in den komplexen Zahlen eine Untergruppe von $(\mathbb{C} \setminus \{0\}; \cdot)$ bildet. Stellen Sie dazu die Verknüpfungstafel auf.
- (b) Geben Sie für das Element $1+i$ die Linksnebenklasse von U in $(\mathbb{C} \setminus \{0\}; \cdot)$ an, und skizzieren Sie diese Menge in der Gaußschen Zahlenebene.
- (c) Finden Sie alle Untergruppen von $(U; \cdot)$. Welche Ordnungen haben die Elemente?
- (d) Ist $(U; \cdot)$ zu $(\mathbb{Z}_4; +)$ isomorph?

Ü44 Verwenden Sie bei den folgenden Aufgaben den Satz von Euler-Fermat:

- (a) Finden Sie alle $x \in \mathbb{Z}_{40}$, die die Gleichung $123^{321} \cdot x \equiv 4 \pmod{40}$ erfüllen.
- (b) Zeigen Sie für alle $m \in \mathbb{N}$, dass m^{13} und m im Dezimalsystem die gleiche Endziffer haben.

Ü45 Das RSA-Verfahren soll mit kleinen Zahlen getestet werden. Man nehme $p=7$ und $q=11$.

- (a) Der öffentliche Schlüssel sei $e=23$. Berechnen Sie den privaten Schlüssel d .
- (b) Verschlüsseln Sie mit dem öffentlichen Schlüssel aus (a) die Zahl $m=12$.
(Überprüfen Sie das Ergebnis durch Entschlüsselung mit dem privaten Schlüssel.)

H46 A Person A und Person B wollen abhörsicher miteinander kommunizieren und dazu einen gemeinsamen geheimen Schlüssel verwenden. Die Erzeugung des Schlüssels mit dem Diffie-Hellman-Merkle-Verfahren soll anhand kleiner Zahlen ausgetestet werden. Die beiden einigen sich auf die Primzahl $p := 41$ und die Primitivwurzel $g := 2$ in $\mathbb{Z}_p^*$.

- (a) Person A wählt eine persönliche Geheimzahl a in $\mathbb{Z}_p$ so aus, dass $g^a \equiv 5 \pmod{41}$ gilt. Bestimmen Sie ein solches a .
- (b) Person B wählt als persönliche Geheimzahl $b = 309$. Berechnen Sie den gemeinsamen geheimen Schlüssel c .

H47 Es seien $(G; \circ)$ eine Gruppe und $a, b \in G$ beliebige Elemente. Beweisen Sie, dass für die Linksnebenklassen einer beliebigen Untergruppe U von G folgende Aussagen äquivalent sind (d.h. für jedes Paar aus den drei Aussagen gilt die eine genau dann, wenn die andere gilt):

- (a) $a \circ U = b \circ U$,
- (b) $b \in a \circ U$,
- (c) $a^{-1} \circ b \in U$.

Hinweis: Beweisen Sie dazu folgende Kette von Implikationen: $(a) \Rightarrow (b) \Rightarrow (c) \Rightarrow (a)$.

H48 Verwenden Sie bei den folgenden Aufgaben den Satz von Euler-Fermat:

- (a) Berechnen Sie die letzten zwei Ziffern der Zahl 211^{1043} .
- (b) Zeigen Sie, dass für zwei beliebige Primzahlen p und q mit $p \neq q$ und jede Zahl $a \in \mathbb{Z}$, die nicht durch p oder q teilbar ist, gilt:

$$a^{(p-1)(q-1)} \equiv 1 \pmod{p \cdot q}.$$

- (c) Zeigen Sie für alle $m \in \mathbb{N}$, dass $\frac{1}{5}m^5 + \frac{1}{3}m^3 + \frac{7}{15}m$ eine natürliche Zahl ist.

