TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

Prof. Dr. Ulrich Thiel
Laura Voggesberger, M. Sc.

Mathematik für Informatik: Algebraische Strukturen

Sommersemester 2022 - Übungsblatt 7

Abgabetermin: 17.06.2022, 10:00 Uhr, Briefkästen Gebäude 48 Erdgeschoss oder als eine PDF mit dem Button im OLAT hochladen. Die Programmieraufgaben dürfen als extra Datei (zum Beispiel txt) hochgeladen werden.

Aufgabe 1 (4 Punkte)**.** Sei R ein Ring. Zeigen Sie durch Verwendung der Ringaxiome, dass für alle $x, y \in R$ gilt

$$0 \cdot x = x \cdot 0 = 0, \quad (-x)y = x(-y) = -xy, \quad (-x)(-y) = xy.$$

Aufgabe 2 (4 Punkte)**.** Zeigen Sie: In einem endlichen Ring R mit Einselement ist jedes Element entweder eine Einheit oder ein Nullteiler.
Hinweis: Konstruieren Sie für jedes Element $a \in R$ den Ringhomomorphismus $\rho_a : R \to R$, $r \mapsto ar$. Beweisen Sie, dass ρ_a injektiv ist, wenn a kein Nullteiler ist. Warum ist dann ρ_a auch surjektiv und damit a eine Einheit?

Aufgabe 3 (4 Punkte)**.** Gegeben sind folgende Paare von öffentlichen Schlüsseln eines RSA-Kryptosystems und eine damit verschlüsselte Nachricht. Geben Sie die Originalnachrichten an (mit Herleitung).

(a) $(n, e) = (493, 45)$ und $c = 56$.

(b) $(n, e) = (10201, 137)$ und $c = 5203$.
Hinweis: Sei p eine Primzahl. Dann gilt $\varphi(p^2) = p^2 - p$.

Aufgabe 4 (4 Punkte)**.** Benutzen Sie den kleinen Satz von Fermat zur Lösung folgender Aufgaben:

(a) Berechnen Sie ohne Computer 6^{52} mod 11 und 6^{100003} mod 101.

(b) Zeigen Sie, dass 17 ein Teiler von $11^{104} + 1$ ist.

Zusatzaufgabe 5 (4 Punkte)**.** Verwenden Sie ein Computeralgebrasystem Ihrer Wahl.

(a) Implementieren Sie das Faktorisierungsverfahren von Pollard.

(b) Testen Sie Ihre Implementierung an Beispielen.