ETH Zürich, D-INFK
HS 2016, 14. November 2016

Prof. Ueli Maurer
Daniel Tschudi

Diskrete Mathematik
Übung 9

9.1 Gruppenhomomorphismen ($\star\,\star$)

Ziel dieser Aufgabe ist es, Lemma 5.5 (i) zu beweisen. Seien dazu $\langle G; *, \tilde{}, e_G\rangle$ und $\langle H; \circ, \hat{}, e_H\rangle$ zwei Gruppen und sei weiter $\psi : G \to H$ ein Gruppenhomomorphismus. Zeigen Sie $\psi(e_G) = e_H$.

9.2 Ordnung und Untergruppen

a) ($\star$) Geben Sie die Ordnung aller Elemente in $\langle \mathbb{Z}_6; \oplus\rangle$ an.

b) ($\star\,\star$) Es seien H_1 und H_2 Untergruppen von G. Zeigen Sie: $H_1 \cup H_2$ ist genau dann eine Untergruppe von G wenn $H_1 \subseteq H_2$ oder $H_2 \subseteq H_1$ ist.

9.3 Die Gruppe $\mathbb{Z}_m^*$

a) ($\star$) Bestimmen Sie die Ordnung und die Elemente der Gruppe $\langle \mathbb{Z}_{36}^*; \odot\rangle$.

b) ($\star\,\star$) Bestimmen Sie alle Generatoren der Gruppe $\langle \mathbb{Z}_{11}^*; \odot\rangle$.

c) ($\star\,\star\,\star$) Geben Sie einen Isomorphismus von $\langle \mathbb{Z}_{15}^*; \odot\rangle$ nach $\langle \mathbb{Z}_{20}^*; \odot\rangle$ an.

9.4 Diffie-Hellman Revisited

a) ($\star\,\star$) Weil Alice schneller addieren als multiplizieren kann, schlägt sie vor, den Diffie-Hellman-Schlüsselaustausch in der Gruppe $\langle \mathbb{Z}_n; \oplus\rangle$ durchzuführen. Beschreiben Sie, welche Nachrichten in diesem Fall Alice und Bob austauschen. Zeigen Sie, warum dies unsicher ist, das heisst, zeigen Sie, wie Eve, die diese Nachrichten mitliest, den gemeinsamen Schlüssel von Alice und Bob effizient berechnen kann.

b) ($\star\,\star\,\star$) Da nach Aufgabenteil a) das Diffie-Hellman-Schlüsselaustauschprotokoll in der Gruppe $\langle \mathbb{Z}_n; \oplus\rangle$ unsicher ist und nach Theorem 5.7 jede zyklische Gruppe von Ordnung n zu $\langle \mathbb{Z}_n; \oplus\rangle$ isomorph ist, folgert Bob, dass das Protokoll für alle zyklischen Gruppen unsicher ist. Hat er recht?

9.5 RSA-Attacke ($\star\,\star\,\star$)

Ein Text m wurde mit RSA verschlüsselt an drei Personen gesendet, die als öffentliche Schlüssel $(n_1, 3)$, $(n_2, 3)$ beziehungsweise $(n_3, 3)$ verwenden, die paarweise verschieden sind. Sie haben die drei Chiffrate c_1, c_2 und c_3 abgefangen. Wie können Sie daraus und aus den öffentlichen Schlüsseln m effizient berechnen?

9.6 Elementare Eigenschaften von Ringen ($\star\,\star$) *(7 Punkte)*

Ziel dieser Aufgabe ist es, Lemma 5.17 (ii) – (iv) zu beweisen. Dazu dürfen Sie Lemma 5.17 (i) ohne Beweis verwenden.

Sei $\langle R; +, -, 0, \cdot, 1\rangle$ ein Ring und $a, b \in R$. Zeigen Sie:

a) $(-a)b = -(ab)$ *(2 Punkte)*

b) $(-a)(-b) = ab$ *(3 Punkte)*

c) Wenn R mindestens zwei Elemente enthält, gilt $1 \neq 0$. *(2 Punkte)*

Abgabe am 21./22. November 2016
Korrigiert wird Aufgabe 9.6