Kryptographie *WS 2015/16*
Barbara Baumeister
Tutoren: Apolonia Gottwald, Soeren Senkovic

5. Übungsblatt

Abgabe: Donnerstag, 26.11.2015

Aufgabe 1 (a) Sei G eine Gruppe und $g \in G$ ein Element der Ordnung n. Sei d eine natürliche Zahl. Bestimmen Sie die Ordnung von g^d.

(b) Sei $G = \mathbb{Z}_{55}^*$ und $g = 2$. Bestimmen Sie die Ordnungen von g, g^2 und g^7. Hinweis: Benutzen Sie den Chinesischen Restsatz.

Aufgabe 2 Sei $m \in \mathbb{N}$ so, dass $p_1 = 6m+1, p_2 = 12m+1$ und $p_3 = 18m+1$ Primzahlen sind. Zeigen Sie, dass $C = p_1p_2p_3$ eine Carmichael-Zahl ist (Verfahren von Chernick).

Aufgabe 3 Beweisen Sie

(a) mit dem Fermat-Test, dass die fünfte Fermat-Zahl $2^{2^5} + 1$ keine Primzahl ist.

(b) dass jede Fermat-Zahl Primzahl oder Pseudoprimzahl zu der Basis 2 ist.

(c) mit dem Miller-Rabin-Test, dass $2^{2^5} + 1$ keine Primzahl ist.

Aufgabe 4 Schreiben Sie ein Programm, welches den Miller-Rabin-Test durchführt und bestimmen Sie damit eine 512-Bit-Zahl, die zu mindestens 80% eine Primzahl ist.

Zusatzaufgabe Sei p eine Primzahl. Zeigen Sie, dass $\mathbb{Z}_p^*$ zyklisch ist.