Kryptographie *WS 2012/13*
Barbara Baumeister

6. Übungsblatt

Abgabe: Donnerstag, 22.11.2012

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 $G = \mathbb{Z}_{45}^*$ und $g = 2$. Bestimmen Sie die Ordnungen von g, g^2 und g^5. Hinweis: Benutzen Sie den Chinesischen Restsatz.

Aufgabe 2 Beweisen Sie

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

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

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

Aufgabe 3 Sei $m \in \mathbb{N}$ so, dass $p_1 = 6m + 1, p_2 = 12m + 1$ und $p_3 = 18m + 1$ Primzahlen sind.

(a) Zeigen Sie, dass $C = p_1 p_2 p_3$ eine Carmichael-Zahl ist (Verfahren von Chernick).

(Zusatzaufgabe) Ist c noch eine Carmichael-Zahl, wenn p_1, p_2 und p_3 drei paarweise verschiedene Primzahlen von der Form $p_1 = 6u_1 + 1, p_2 = 12u_2 + 1$ und $p_3 = 18u_3 + 1$ mit $u_1, u_2, u_3 \in \mathbb{N}$ sind?

Aufgabe 4 Schreiben Sie ein Programm, welches des Miller-Rabin-Test durchführt und bestimmen Sie damit eine 512-Bit-Primzahl.