Spezielle Aspekte: Kryptographie *SoSe 2011*
PD Dr. Barbara Baumeister
Tutoren: Patrick Wegener, Philipp Neumann, Patrick Odenbach

12. Übungsblatt

Abgabe: Mittwoch, 29.6.11

Aufgabe 1 *Verwenden Sie den Babystep-Giantstep-Algorithmus um den diskreten Logarithmus von* 15 *zur Basis* 2 mod 73 *zu berechnen.*

Aufgabe 2 *Lösen Sie* $3^x \equiv 22 \bmod 109$ *mit dem Babystep-Giantstep-Algorithmus.*

Aufgabe 3 *Es ist* $\langle 2 \rangle = \mathbb{Z}_{1117}^*$ *(*1117 *ist eine Primzahl). Lösen Sie* $2^x \equiv 507 \bmod 1117$ *mit dem Pohlig-Hellman-Algorithmus.*

Aufgabe 4
(a) Sei G eine Gruppe und $g \in G$ ein Element der Ordnung n. Sei d eine natürliche Zahl mit $d \leq n$. Bestimmen Sie die Ordnung von g^d.
(b) Sei $G = \mathbb{Z}_{17}^*$ und $g = 3$. Bestimmen Sie die Ordnungen von g, g^5 und g^2.