Kryptosysteme, Keymanagment (KSK3) für CMS
1. Übungsblatt für den 10. Oktober 2006

1. Welche der folgenden Strukturen sind Gruppen, welche sind keine Gruppen? (Bitte begründen Sie Ihre Antwort).

   (a) $(\mathbb{Z}, +, -, 0)$,

   (b) $(\mathbb{N}, +, -, 0)$,

   (c) $(\mathbb{Z} \setminus \{0\}, \cdot, ^{-1}, 1)$,

   (d) $(\mathbb{Z}_3 \setminus \{[0]_3\}, \cdot, ^{-1}, [1]_3)$,

   (e) $(\mathbb{Z}_4 \setminus \{[0]_4\}, \cdot, ^{-1}, [1]_4)$.

2. Bestimmen Sie jeweils die Ordnung aller Elemente der Gruppe

   (a) $(\mathbb{Z}_5, +, -, [0]_5)$,

   (b) $(\mathbb{Z}_6, +, -, [0]_6)$,

   (c) $(\mathbb{Z}_{11} \setminus \{[0]_{11}\}, \cdot, ^{-1}, [1]_{11})$.

3. (*Internet/Literatur-Recherche*) Finden Sie eine nicht-abelsche Gruppe der Ordnung 6 und machen Sie sich mit deren Rechenoperationen vertraut. Berechnen Sie die Ordnungen aller Elemente.

4. (*Mathematica darf verwendet werden*) Alice und Bob führen einen Diffie-Hellman-Schlüsselaustausch (Algorithmus 1.11) mit $p = 41$ durch. Sie einigen sich auf die Primitivwurzel $g = [11]_{41}$ in $\mathbb{Z}_{41}^*$. Alice wählt $a = [27]_{41}$ und Bob wählt $b = [12]_{41}$. Berechnen Sie $A := g^a \mod p$ und $B := g^b \mod p$ und bestätigen Sie dann, dass $B^a \mod p = A^b \mod p$.

5. Schreiben Sie eine *Mathematica*-Funktion `PrimitiveRoots` mit einem Argument, sodass `PrimitiveRoots[`p`]` eine Liste aller Primitivwurzeln modulo p zurückgibt wobei p eine Primzahl ist. (Eine Primitivwurzel modulo p ist ein Element der Gruppe $(\mathbb{Z}_p \setminus \{[0]_p\}, \cdot, ^{-1}, [1]_p)$ mit Ordnung $p - 1$).