**Kryptosysteme, Keymanagment (KSK3) für CMS**
**2. Übungsblatt für den 17. Oktober 2006**

1. (*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.

2. (*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 $a = 27$ und Bob wählt $b = 12$. Berechnen Sie $A := g^a \mod p$ und $B := g^b \mod p$ und bestätigen Sie dann, dass $B^a \mod p = A^b \mod p$.

3. 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 $p - 1$).

4. Geben Sie eine Gruppe an, die genau eine Untergruppe besitzt.

5. Sei $\mathbf{G} := (G, \circ, ^{inv}, e)$ eine Gruppe der Ordnung $p$, wobei $p$ prim ist. Zeigen Sie, dass $\mathbf{G}$ genau zwei Untergruppen besitzt. Welche zwei?

6. Sei $\mathbf{G} := (G, \circ, ^{inv}, e)$ eine Gruppe. Zeigen Sie:

$$g^m \circ g^n = g^{m+n},$$

   für alle $g \in G$ und alle $m, n \in \mathbb{Z}$. (*Hinweis:* $g^0 = e$; Fallunterscheidung $n > 0$ und $m > 0$, usw.)

7. Gegeben sei eine natürliche Zahl $n$. Für einen positiven Teiler $t$ von $n$ bezeichne $U_t$ die Menge aller Vielfachen von $[t]_n$:

$$U_t := \{[k \cdot t]_n \mid k \in \mathbb{Z}\} = \{[0]_n, [t]_n, [2t]_n, \ldots, [n - t]_n\}.$$

   Zeigen Sie, dass $(U_t, +, -, [0]_n)$ eine Untergruppe von $(\mathbb{Z}_n, +, -, [0]_n)$ ist (für jeden positiven Teiler $t$ von $n$). Können Sie auch zeigen, dass dies schon alle Untergruppen von $(\mathbb{Z}_n, +, -, [0]_n)$ sind?

8. Bestimmen Sie alle Untergruppen von $(\mathbb{Z}_{30}, +, -, [0]_{30})$. Wieviele sind es? Versuchen Sie die Teilmengenbeziehungen zwischen den Untergruppen graphisch darzustellen. (*Hinweis:* Sie können das vorhergehende Beispiel verwenden.)