TH Brandenburg
Online Studiengang IT Sicherheit
Fachbereich Informatik und Medien
Algorithmen und Datenstrukturen
Prof. Dr. rer. nat. Ulrich Baum

Einsendeaufgabe 6

Sommersemester 2022
Abgabetermin 21. Mai 2022

Mara Schulke
Matrikel-Nr. 20215853

Einsendeaufgabe 6

6.1 Zyklische Gruppen

(a)

$$O = \{1, 2, 3, 4, 6, 12\}$$

$$\forall o \in O : o \,|\, 12$$

(b)

$$a^4 \neq a^6 \neq 1 \Rightarrow a \text{ ist ein Generator für } Z_{13}^*, \text{ da gilt :}$$

$$\forall o_n \in O : \exists n \in Z_{13}^* \wedge |<n>| = o_n : \forall o_m \in \{o_m \in O : o_n \,|\, o_m\} : n^{o_m} = 1$$

Anders ausgedrückt gilt für alle Elemente der Ordnung n (also $a^n = 1$) dass bei einem Vielfachen der Ordnung nk mit $k \in \mathbb{N} : a^{nk} = 1$. Somit lässt sich aus dem Fakt das $a^{nk} = 1$ ist nicht ableiten ob a die Ordnung n oder nk (mit $k \neq 1$) hat.

Ist allerdings $a^{nk} \neq 1$ schließt man somit alle Teiler von nk aus. Also konkreter: Gilt $a^4 \neq 1$ kann a nicht die Ordnung 1, 2 oder 4 haben. Wenn nun zusätzlich $a^6 \neq 1$ gilt kann a auch nicht die Ordnung 1, 2, 3 oder 6 haben. Da jedes Element eine Ordnung haben muss bleibt nun nurnoch die Ordnung 12 über und wir sind sicher dass a ein Generator für Z_{13}^* ist.

(c)

$$g = xy$$