RUHR UNIVERSITÄT BOCHUM

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Gottfried Herold

Präsenzübungen zur Vorlesung

Zahlentheorie

SS 2013

Blatt 6 / 13.–15. Mai 2013

AUFGABE 1:
Sei G eine zyklische Gruppe. Wie viele verschiedene Erzeuger g mit $G = \langle g \rangle$ gibt es, falls

(a) G unendlich ist.

(b) $|G| = n \in \mathbb{N}$.

AUFGABE 2:
Sei G eine endliche abelsche Gruppe mit p Elementen, wobei p prim. Zeigen Sie, dass G zyklisch ist.

Hinweis/Bemerkung: Verwenden Sie den Satz von Lagrange. Da der Satz von Lagrange auch für nicht-abelsche Gruppen (mit anderem Beweis als in der Vorlesung) gilt, muss man in dieser Aufgabe eigentlich nicht fordern, dass G abelsch ist.

AUFGABE 3:
Sei $I = (4 + i) \subset \mathbb{Z}[i]$ das von $4 + i$ *erzeugte Ideal*.
Geben Sie eine endliche Menge $b_1, b_2, \ldots, b_k \in I$ an, so dass $I = \langle b_1, \ldots, b_k \rangle$ von den b_i als *abelsche Gruppe erzeugt* wird.

Bemerkung zur Notation: Wir benutzen hier zur Unterscheidung runde Klammern für das erzeugte Ideal und spitze Klammern für die erzeugte abelsche Gruppe.

AUFGABE 4:
Wie viele Untergruppen mit genau p Elementen hat $\mathbb{Z}/(p) \times \mathbb{Z}/(p)$?

AUFGABE 5:
Geben Sie einen Erzeuger der multiplikativen Gruppe von $\mathbb{F}_{13}^*$ an.