Kryptologie, SS03 Aufgabenblatt 1

Aufgabe 1

Die Menge $G = \{1,2,3,4,6,8,9,11,12,13,16,17,18,19,22,23,24,26,27,29,31,32,33,34\}$ besitzt 24 Elemente. Es gilt
$G = \{n \in \mathbb{N} | 1 \leq n < 35$ und n ist weder durch durch 5 noch durch 7 teilbar$\}$.
Auf G wird eine Gruppenoperation definiert, indem man die Elemente zunächst als natürliche Zahlen multipliziert und dann den Rest nimmt, der bei Division durch 35 bleibt, also z.B. $9 \cdot 11 = 29$.

a) Finden Sie zu jedem Element von G das Inverse!

b) Wenn man ein Element $a \in G$ nimmt und dann alle Produkte $a, a \cdot a, a \cdot a \cdot a$, etc. bildet, bis 1 herauskommt, bilden die so gewonnenen Elemente eine Untergruppe von G.

Finden Sie durch Wahl geeigneter Ausgangselemente Untergruppen mit 1,2,3,4,6,8 und 12 Elementen.

Aufgabe 2

Sei $(G, \cdot)$ eine Gruppe und $H \subset G$ eine Untergruppe.

a) Für $a \in G$ definieren wir die Linksnebenklasse $\overline{a} := aH := \{ah | h \in H\}$.
Man zeige: $\overline{x} = \overline{y} \Leftrightarrow x^{-1}y \in H$

b) Zeigen Sie: durch $a \sim b \quad :\Leftrightarrow \quad a^{-1} \cdot b \in H$ wird auf G eine Äquivalenzrelation erklärt, d.h es gilt: $\forall a \in G : a \sim a, \quad \forall a, b \in G : a \sim b \Leftrightarrow b \sim a, \; \forall a, b, c \in G : a \sim b$ und $b \sim c \Rightarrow a \sim c$

Die Äquivalenzklasse eines Elements $a \in G$, also die Menge $\{b \in G | \; b \sim a\}$ ist offenbar gleich der Linksnebenklasse $\overline{a} := aH := \{ah | h \in H\}$

c) Zeigen Sie: Die Abbildung $H \to aH, \; h \to ah$ ist bijektiv

c) Man zeige: $\overline{x} \neq \overline{y} \Leftrightarrow \overline{x} \cap \overline{y} = \emptyset$

d) Zeigen Sie: Wenn $\overline{x} = \overline{y}$ und $\overline{z} = \overline{w}$ dann $\overline{xz} = \overline{yw}$

d) Im Beispiel von Aufgabe 3 wählen Sie die Untergruppe $H := \{1,4,9,11,16,29\}$. Es gibt insgesamt 4 Äquivalenzklassen, von denen H eine ist. Bestimmen Sie auch die anderen!

Aufgabe 3

Sei $p \in \mathbb{N}$ eine Primzahl, $\mathbb{Z}^*_p := \{1, 2, \ldots, p-1\}$. Auf $\mathbb{Z}^*_p$ betrachten wir die Multiplikation „modulo *p*", d.h. wir multiplizieren 2 Elemente zunächst als natürliche Zahlen und nehmen dann den Rest, der bei Division dieses Ergebnisses durch *p* bleibt.

a) Man zeige:
Ist $x \in \mathbb{Z}^*_p$, so ist die durch die Multiplikation mit *x* gegebene Abbildung $\mathbb{Z}^*_p \to \mathbb{Z}^*_p$, $a \to xa$ bijektiv.

b) Wieso sind 1 und *p*-1 die einzigen Elemente von $\mathbb{Z}^*_p$, für die gilt: $x^2 = 1$?

c) Wieso gilt daher in $\mathbb{Z}^*_p$ $\quad 1 \cdot 2 \cdot \ldots \cdot (p-2) = 1$? (*p*>3 vorausgesetzt)