Aufgabe H01T3A2

(a) Sei G eine endliche abelsche Gruppe und p das Produkt aller Elemente von G. Zeigen Sie: Besitzt G kein oder mehr als ein Element der Ordnung 2, dann gilt $p = e_G$. Existiert dagegen in G genau ein Element a der Ordnung 2, dann ist $p = a$.

(b) Zeigen Sie, dass jede Zahl $n \in \mathbb{N}$, $n \neq 4$ jeweils ein Teiler von $((n-1)!)^2 + (n-1)!$ ist.

Lösung:

zu (a) Besitzt G kein Element der Ordnung 2, dann gilt $g \neq g^{-1}$ für alle $g \neq e_G$. Die Menge $G \setminus \{e_G\}$ besitzt dann eine disjunkte Zerlegung der Form

$$G \setminus \{e_G\} \quad = \quad \bigcup_{i=1}^{r} \{g_i, g_i^{-1}\}$$

mit $r \in \mathbb{N}_0$ und $g_1, ..., g_r \in G$. Wegen $g_i g_i^{-1} = e_G$ für $1 \leq i \leq r$ ist das Produkt über alle Elemente von G ebenfalls gleich Null. Sei nun a das einzige Element der Ordnung 2. Dann gilt $g \neq g^{-1}$ für alle $g \neq e_G, a$. Wir erhalten wiederum eine Zerlegung

$$G \setminus \{a, e_G\} \quad = \quad \bigcup_{i=1}^{r} \{g_i, g_i^{-1}\}$$

Das Produkt über die Elemente auf der rechten Seite ist e_G, also ist das Produkt über alle Elemente von G gleich a. Zum Schluss betrachten wir den Fall, dass G mehr als ein Element der Ordnung 2 besitzt. Weil G abelsch ist, bilden die Elemente der Ordnung ≤ 2 eine endliche Untergruppe U. Alle Elemente in $G \setminus U$ haben Ordnung größer als 2, also gibt es hier eine Zerlegung

$$G \setminus U \quad = \quad \bigcup_{i=1}^{r} \{g_i, g_i^{-1}\}$$

mit $r \in \mathbb{N}_0$ und $g_1, ..., g_r \in G$. Das Produkt über alle Elemente aus $G \setminus U$ ist also wiederum gleich e_G. Laut Vorlesung ist die Untergruppe U als elementar-abelsche Gruppe vom Exponenten 2 isomorph zu $(\mathbb{Z}/2\mathbb{Z})^s$ für ein $s \in \mathbb{N}$ mit $s \geq 2$. Die Summe über die Elemente aus $(\mathbb{Z}/2\mathbb{Z})^s$ ist gleich $0_{(\mathbb{Z}/2\mathbb{Z})^s}$. Denn für jedes $i \in \mathbb{N}$ mit $1 \leq i \leq s$ gibt es in $(\mathbb{Z}/2\mathbb{Z})^s$ jeweils 2^{s-1} Elemente, die an der i-ten Position den Eintrag 1 haben, und ebenso 2^{s-1} Elemente, die dort Eintrag 0 haben. Wegen $s \geq 2$ ergibt die Summe über alle Elemente also an jeder Position den Eintrag $2^{s-1} \cdot \bar{0} + 2^{s-1} \cdot \bar{1} = \bar{0}$. Weil der Isomorphismus $(\mathbb{Z}/2\mathbb{Z})^s \cong U$ das Element $0_{(\mathbb{Z}/2\mathbb{Z})^s}$ auf e_G abbildet, ist das Produkt über alle Elemente aus U gleich e_G.

zu (b) Zunächst betrachten wir den Fall, dass $n = p$ eine ungerade Primzahl ist. Die Gruppe $\mathbb{F}_p^\times$ ist zyklisch, somit ist $-\bar{1}$ das einzige Element der Ordnung 2. Aus Aufgabenteil (a) folgt $\prod_{a=1}^{p-1} \bar{a} = -1$. Dies wiederum bedeutet $(p-1)! \equiv -1 \bmod p$, also $((p-1)!)^2 + (p-1)! \equiv (-1)^2 + 1 \equiv 0 \bmod p$. Im Fall $n = 2$ erhält man die Aussage einfach durch Einsetzen: Es gilt $((2-1)!)^2 + (2-1)! = 1^2 + 1 = 2$, und diese Zahl wird von 2 geteilt.

Setzen wir nun voraus, dass n eine Primzahlpotenz > 4 ist, $n = p^r$ mit einer Primzahl p und $r \geq 2$. Im Fall $r \geq 3$ gilt $p < p^{r-1} \leq n - 1$. Also ist $(n-1)!$ durch $p \cdot p^{r-1} = p^r = n$ teilbar. Im Fall $r = 2$ ist p ungerade, und das Produkt $(p^2 - 1)!$ enthält die Faktoren p und $2p$. Also ist auch in diesem Fall die Zahl $(n-1)!$ durch $p^r = n$ teilbar. In beiden Fällen wird damit auch $((n-1)!)^2 + (n-1)!$ von n geteilt.

Zum Schluss betrachten wir den Fall, dass n keine Primzahlpotenz ist. Sei $n = \prod_{i=1}^{r} p_i^{e_i}$ die Primfaktorzerlegung von n, mit verschiedenen Primzahlen $p_1, ..., p_r$ und $e_1, ..., e_r \in \mathbb{N}$. Dann gilt $p_i^{e_i} < n$ und somit $p_i^{e_i} | (n-1)!$, also $(n-1)! \equiv 0 \mod p_i^{e_i}$ für alle i. Mit dem Chinesischen Restsatz erhalten wir $(n-1)! \equiv 0 \mod n$, damit auch $((n-1)!)^2 + (n-1)! \equiv 0 \mod n$.