Aufgabe F17T2A2 (12 Punkte)

(a) Sei G eine multiplikativ geschriebene endliche Gruppe der Ordnung n und sei $g \in G$. Weiter gelte $g^{n/p} \neq 1$ für jeden Primteiler p von n. Zeigen Sie: g erzeugt G.

(b) Zeigen Sie: $4^{3^m} \equiv 1 + 3^{m+1} \bmod 3^{m+2}$ für alle $m \geq 0$

(c) Zeigen Sie, dass die Restklasse von 2 für jedes $e \geq 1$ die Einheitengruppe des Rings $\mathbb{Z}/3^e\mathbb{Z}$ erzeugt.

Lösung:

zu (a) Nehmen wir an, dass $\langle g \rangle$ eine echte Untergruppe von G ist. Dann ist $d = \mathrm{ord}(g) = |\langle g \rangle|$ ein echter Teiler von n. Sei p ein Primteiler von $\frac{n}{d}$. Dann ist p auch ein Primteiler von n, und es gibt ein $k \in \mathbb{N}$ mit $pk = \frac{n}{d}$, also $pkd = n$. Wegen $\mathrm{ord}(g) = d$ folgt $g^{n/p} = g^{kd} = (g^d)^k = 1^k = 1$. Aber dies steht im Widerspruch zur Voraussetzung $g^{n/p} \neq 1$.

zu (b) Wir führen den Beweis durch vollständige Induktion über $m \in \mathbb{N}_0$. Wegen $4^{3^0} \equiv 4 \equiv 1 + 3 \equiv 1 + 3^{0+1} \bmod 9$ ist die Kongruenz für $m = 0$ erfüllt. Sei nun $m \in \mathbb{N}_0$ beliebig, und setzen wir die Kongruenz für dieses m voraus. Dann gibt es ein $k \in \mathbb{Z}$ mit $4^{3^m} = 1 + 3^{m+1} + k \cdot 3^{m+2}$. Rechnen modulo 3^{m+2} und Anwendung des binomischen Lehrsatzes $(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$ auf $a = 1 + 3^{m+1}$ und $b = k \cdot 3^{m+2}$ liefert

$$4^{3^{m+1}} \equiv (4^{3^m})^3 \equiv (1 + 3^{m+1} + k \cdot 3^{m+2})^3 \equiv$$

$$(1 + 3^{m+1})^3 + 3 \cdot (1 + 3^{m+1})^2 k \cdot 3^{m+2} + 3 \cdot (1 + 3^{m+1})(k \cdot 3^{m+2})^2 + (k \cdot 3^{m+2})^3 \equiv$$

$$(1 + 3^{m+1})^3 + (1 + 3^{m+1})^2 k \cdot 3^{m+3} + (1 + 3^{m+1}) \cdot k^2 \cdot 3^{2m+5} + k^3 \cdot 3^{3m+6} \equiv$$

$$(1 + 3^{m+1})^3 \equiv 1^3 + 3 \cdot 1^2 \cdot 3^{m+1} + 3 \cdot 1 \cdot (3^{m+1})^2 + (3^{m+1})^3$$

$$\equiv 1 + 3^{m+2} \bmod 3^{m+3}.$$

wobei im fünften Schritt (Übergang von der dritten zur vierten Zeile) verwendet wurde, dass $2m + 5 \geq m + 3$, $3m + 6 \geq m + 3$ und grundsätzlich $3^r \equiv 3^{r-(m+3)} \cdot 3^{m+3} \equiv 3^{r-(m+3)} \cdot 0 \equiv 0 \bmod 3^{m+3}$ für alle $r \in \mathbb{N}$ mit $n \geq m + 3$ gilt.

zu (c) Laut Vorlesung ist die Einheitengruppe von $\mathbb{Z}/3^e\mathbb{Z}$ eine Gruppe der Ordnung $\varphi(3^e) = 2 \cdot 3^{e-1}$. Wir bezeichnen das Bild der 2 in dieser Gruppe mit $\bar{2}$. Im Fall $e = 1$ ist die Gruppe zweielementig. Wegen $\bar{2} \neq \bar{1}$ in $(\mathbb{Z}/3\mathbb{Z})^\times$ ist $\bar{2}$ damit ein Erzeuger der Gruppe. Setzen wir nun $e \geq 2$ voraus. Dann sind 2 und 3 die einzigen Primteiler der Ordnung von $(\mathbb{Z}/3^e\mathbb{Z})^\times$. Nach Teil (a) genügt es, $\bar{2}^{3^{e-1}} \neq \bar{1}$ und $\bar{2}^{2 \cdot 3^{e-2}} \neq \bar{1}$ zu zeigen. Nehmen wir zunächt $\bar{2}^{3^{e-1}} = \bar{1}$ an. Dann gilt $2^{3^{e-1}} \equiv 1 \bmod 3^e$, also erst recht $2^{3^{e-1}} \equiv 1 \bmod 3$. Aber andererseits gilt $2^3 \equiv 8 \equiv 2 \bmod 3$ und somit auch $2^{3^{e-1}} \equiv 2 \bmod 3$ für alle $e \geq 2$. Wegen $1 \not\equiv 2 \bmod 3$ ist die Gleichung $\bar{2}^{3^{e-1}} = \bar{1}$ also ausgeschlossen.

Nehmen wir nun an, dass $\bar{2}^{2 \cdot 3^{e-2}} = \bar{1}$ gilt. Dann folgt $4^{3^{e-2}} \equiv 1 \bmod 3^e$. Aber nach Teil (b) ist $4^{3^{e-2}} \equiv 1 + 3^{e-1} \bmod 3^e$. Wir erhalten $1 + 3^{e-1} \equiv 4^{3^{e-2}} \equiv 1 \bmod 3^e$. Somit wäre 3^e ein Teiler von $(1 + 3^{e-1}) - 1 = 3^{e-1}$. Weil dies offensichtlich nicht der Fall ist, ist auch $\bar{2}^{2 \cdot 3^{e-2}} = \bar{1}$ ausgeschlossen. Somit sind die Voraussetzungen von Teil (a) erfüllt, und $\bar{2}$ ist tatsächlich ein Erzeuger von $(\mathbb{Z}/3^e\mathbb{Z})^\times$.