Aufgabe F17T1A4 (12 Punkte)

Sei $N \in \mathbb{N}$ eine natürliche Zahl $N \geq 3$.

(a) Zeigen Sie: Falls $2^{N-1} \not\equiv 1 \mod N$ gilt, ist N keine Primzahl.

(b) Zeigen Sie, dass die Umkehrung der Aussage nicht gilt, indem Sie das Beispiel $N = 341 = 11 \cdot 31$ betrachten.

Lösung:

zu (a) Nehmen wir an, dass N eine Primzahl ist. Laut Vorlesung ist dann $(\mathbb{Z}/N\mathbb{Z})^\times$ eine zyklische Gruppe der Ordnung $N-1$. Weil 2 zur Primzahl $N \geq 3$ teilerfremd ist, gilt $\bar{2} \in (\mathbb{Z}/N\mathbb{Z})^\times$. Mit dem Satz von Langrange erhalten wir $\bar{2}^{N-1} = \bar{1}$ und somit $2^{N-1} \equiv 1 \mod N$.

zu (b) Weil 11 eine Primzahl ist, gilt nach Teil (a) $2^{10} \equiv 1 \mod 11$ und somit auch $2^{340} \equiv (2^{10})^{34} \equiv 1^{34} \equiv 1 \mod 11$. Es gilt auch $2^5 \equiv 32 \equiv 1 \mod 31$ und somit $2^{340} \equiv (2^5)^{68} \equiv 1^{68} \equiv 1 \mod 31$. Die Zahl $2^{N-1}-1$ wird also von 11 und 31 geteilt. Weil 11 und 31 teilerfremd sind, ist somit auch $N = 341 = 11 \cdot 31$ ein Teiler von $2^{N-1} - 1$, und es folgt $2^{N-1} \equiv 1 \mod N$. Aber andererseits ist N keine Primzahl.