Aufgabe H13T3A5 (6 Punkte)

Es sei p eine Primzahl. Man zeige, dass außer 3 jeder Primteiler von $2^p + 1$ größer als p ist.
Hinweis: Betrachten Sie die multiplikative Ordnung von 2 modulo eines Primteilers von $2^p + 1$.

Lösung:

Sei q ein Primteiler von $2^p + 1$ ungleich 3. Weil $2^p + 1$ ungerade ist, gilt $q \neq 2$ und somit $q \geq 5$. Aus $q \mid (2^p + 1)$ folgt $2^p \equiv -1 \bmod q$. Bezeichnen wir mit $\bar{2}$ das Bild von 2 in $\mathbb{Z}/q\mathbb{Z}$, dann gilt also $\bar{2}^p = -\bar{1}$ und $\bar{2}^{2p} = \bar{1}$. Dies zeigt, dass das Element $\bar{2}$ in der Einheitengruppe $(\mathbb{Z}/q\mathbb{Z})^\times$ enthalten ist, und dass es sich bei $\mathrm{ord}(\bar{2})$ um einen Teiler von $2p$ handelt. Es gilt also $\mathrm{ord}(\bar{2}) \in \{1, 2, p, 2p\}$, denn dies sind die einzigen Teiler von $2p$ in $\mathbb{N}$.

Betrachten wir zunächst den Fall $\mathrm{ord}(\bar{2}) \in \{1, 2\}$. Dann gilt $\bar{2}^2 = \bar{1}$, also $\bar{3} = \bar{0}$ in $\mathbb{Z}/q\mathbb{Z}$. Dies ist nur möglich, wenn $q = 3$ ist, was wir aber ausgeschlossen hatten. Im Fall $\mathrm{ord}(\bar{2}) = p$ wäre $\bar{1} = \bar{2}^p = -\bar{1}$ und somit $\bar{2} = \bar{0}$. Daraus würde sich $q = 2$ ergeben, was aber ebenfalls ausgeschlossen war. Also muss $\mathrm{ord}(\bar{2}) = 2p$ gelten. Nach dem Satz von Lagrange bedeutet dies, dass die Ordnung $q - 1$ der Gruppe $(\mathbb{Z}/q\mathbb{Z})^\times$ ein Vielfaches von $2p$ ist. Es folgt $q \geq q - 1 \geq 2p > p$.