Aufgabe H19T2A1 (12 Punkte)

(a) Seien $k, \ell \in \mathbb{N}_0$ mit $k < \ell$. Betrachte die Polynome $x^{2^k} + 1$ und $x^{2^\ell} - 1$ aus $\mathbb{Q}[x]$. Man zeige, dass $x^{2^k} + 1$ ein Teiler von $x^{2^\ell} - 1$ ist.

(b) Für $m \in \mathbb{N}$ setze $n = 2^{2^m} + 1$. Man beweise, dass $2^{n-1} \equiv 1 \bmod n$ gilt.

Hinweis/Kommentar:

Teil (a) kann man elementar durch vollständige Induktion mit Hilfe der Dritten Binomischen Formel beweisen. Schneller geht es aber, wenn man im Faktorring $R_k = \mathbb{Q}[x]/(x^{2^k} + 1)$ rechnet. (Und natürlich ist es sinnvoll, jede Gelegenheit zu nutzen, um den Umgang mit Faktorstrukturen zu üben, da diese erfahrungsgemäß die meisten Probleme bereiten.) Teil (b) ergibt sich aus Teil (a), indem man $m = k$ und $n = 2^m$ setzt.