Aufgabe H16T1A4 (12 Punkte)

Sei $a \in \mathbb{N}_0$. Wir definieren eine Folge $(x_n)_{n\in\mathbb{N}_0}$ durch

$$x_n \quad = \quad a^{2^n} + 1.$$

(a) Sei $n < m$. Zeigen Sie, dass x_n ein Teiler von $x_m - 2$ ist.

(b) Berechnen Sie den größten gemeinsamen Teiler von x_n und x_m.

(c) Folgern Sie, dass es unendlich viele Primzahlen gibt.

Lösung:

zu (a) Sei $n \in \mathbb{N}_0$ vorgegeben. Wir beweisen durch vollständige Induktion, dass x_n für jedes $r \in \mathbb{N}$ ein Teiler von $x_{n+r} - 2$ ist. Es gilt $x_{n+1} - 2 = a^{2^{n+1}} - 1 = (a^{2^n} + 1)(a^{2^n} - 1) = x_n \cdot (a^{2^n} - 1)$, also ist die Aussage für $r = 1$ erfüllt. Sei nun $r \in \mathbb{N}$ beliebig, und setzen wir die Aussage für dieses r voraus. Es gilt

$$x_{n+(r+1)} - 2 \quad = \quad a^{2^{n+r+1}} - 1 \quad = \quad (a^{2^{n+r}} + 1)(a^{2^{n+r}} - 1) \quad = \quad x_{n+r} \cdot (x_{n+r} - 2)$$

Auf Grund der Induktionsvoraussetzung ist $x_{n+r} - 2$ ein Vielfaches von x_n, also ist auch $x_{n+(r+1)} - 2$ ein Vielfaches von x_n.

zu (b) Sei $d \in \mathbb{N}$ ein gemeinsamer Teiler von x_m und x_n. Nach Teil (a) gilt $x_n \mid (x_m - 2)$. Also ist d auch ein gemeinsamer Teiler von x_m und $x_m - 2$, also auch ein Teiler von $2 = -(x_m - 2) + x_m$. Daraus folgt, dass der ggT von x_m und x_n ein Teiler von 2 ist, es gilt also $\mathrm{ggT}(x_m, x_n) \in \{1, 2\}$. Ist a ungerade, dann ist x_ℓ für jedes $\ell \in \mathbb{N}_0$ gerade. In diesem Fall gilt also $\mathrm{ggT}(x_m, x_n) = 2$. Ist a dagegen gerade, dann ist jedes x_ℓ gerade, und wir erhalten $\mathrm{ggT}(x_m, x_n) = 1$.

zu (c) Sei $a = 2$ und die Folge $(x_n)_{n\in\mathbb{N}_0}$ wie in der Aufgabenstellung definiert. Wir zeigen, dass für jedes $m \in \mathbb{N}$ eine ungerade Primzahl p_m existiert, so dass jeweils $p_m \mid x_m$ und $p_m \nmid x_n$ für alle $n < m$ gilt. Eine solche Folge $(p_m)_{m\in\mathbb{N}}$ besteht dann offenbar aus lauter verschiedenen Primzahlen, woraus folgt dass unendlich viele Primzahlen existieren.

Nach Definition ist $x_1 = a^{2^1} + 1 = 2^2 + 1 = 5$. Wir können also $p_1 = 5$ setzen. Sei nun $m \in \mathbb{N}$ mit $m > 1$. Es gilt $x_m = a^{2^m} + 1 \geq 2^{2^{m+1}} + 1 > 4 + 1 = 5$, und x_m ist ungerade. Somit besitzt x_m einen ungeraden Primteiler p_m. Da nach Teil (b) x_m zu jedem x_n mit $n < m$ teilerfremd ist, gilt $p_m \nmid x_n$ für alle $n < m$.