F18-T2-A4

a) Bestimmen Sie alle ganzen Zahlen $n \geq 0$, für die $2^n + 3$ bzw. $2^n + 5$ durch 3, 5, 7, bzw. 13 teilbar ist.

b) Bestimmen Sie alle ganzen Zahlen $n \geq 0$ mit der Eigenschaft, dass sowohl $2^n + 3$ als auch $2^n + 5$ Primzahlen sind.

Lösungsvorschlag. Zu a). Zuerst zu $2^n + 3$. Offenbar ist $2^n + 3$ genau dann durch eine Primzahl p teilbar, wenn gilt $2^n = -3 = p - 3 \mod p$. Im Folgenden soll $\mathrm{ord}_p(a)$ für eine Primzahl p und ein $a \in \mathbb{Z}$, welches nicht von p geteilt wird, die Ordnung von $[a]$ in $\mathbb{Z}_p^\times$ bezeichnen.

- Es ist $2^n \neq 0 \mod 3$ für alle $n \geq 0$.
- $2^n = -3 = 2 \mod 5 \;\Leftrightarrow\; 2^{n-1} = 1 \mod 5 \;\Leftrightarrow\; n - 1 \in \mathrm{ord}_5(2)\mathbb{Z} = 4\mathbb{Z}$.
- $2^n = -3 = 4 = 2^2 \mod 7 \;\Leftrightarrow\; 2^{n-2} = 1 \mod 7 \;\Leftrightarrow\; n - 2 \in \mathrm{ord}_7(2)\mathbb{Z} = 3\mathbb{Z}$.
- $$\begin{aligned} 2^n = -3 = 10 \mod 13 \;&\Leftrightarrow\; 2^{n+2} = 4 \cdot 2^n = 4 \cdot 10 = 1 \mod 13 \\ &\Leftrightarrow\; n + 2 \in \mathrm{ord}_{13}(2)\mathbb{Z} = 12\mathbb{Z}. \end{aligned}$$

Für $2^n + 5$ gehen wir ganz genauso vor:

- $2^n = -5 = 1 \mod 3 \;\Leftrightarrow\; n \in \mathrm{ord}_3(2)\mathbb{Z} = 2\mathbb{Z}$.
- Für kein $n \geq 0$ ist $2^n = -5 = 0 \mod 5$.
- $2^n = -5 = 2 \mod 7 \;\Leftrightarrow\; 2^{n-1} = 1 \mod 7 \;\Leftrightarrow\; n - 1 \in \mathrm{ord}_7(2)\mathbb{Z} = 3\mathbb{Z}$.
- $2^n = -5 = 8 = 2^3 \mod 13 \;\Leftrightarrow\; 2^{n-3} = 1 \mod 13 \;\Leftrightarrow\; n - 3 \in \mathrm{ord}_{13}(2)\mathbb{Z} = 12\mathbb{Z}$.

Zu b). Seien $p_n := 2^n + 3$ und $q_n := 2^n + 5$. Sei $M := \{3, 5, 7, 13\}$. Nach Teil a) wissen wir, dass gilt

$$\begin{aligned} \forall m \in M\colon m \text{ teilt nicht } p_n \;&\Longleftrightarrow\; \begin{cases} n \neq 2 \mod 3 \\ n \neq 1 \mod 4 \\ n \neq 10 \mod 12 \end{cases} \\ &\Longleftrightarrow [n] \in \{[0], [3], [4], [6], [7]\} \subset \mathbb{Z}_{12} \end{aligned}$$

und ebenso

$$\begin{aligned} \forall m \in M\colon m \text{ teilt nicht } q_n \;&\Longleftrightarrow\; \begin{cases} n = 1 \mod 2 \\ n \neq 1 \mod 3 \\ n \neq 3 \mod 12 \end{cases} \\ &\Longleftrightarrow [n] \in \{[1], [5], [9], [11]\} \subset \mathbb{Z}_{12} \end{aligned}$$

Insbesondere haben wir also gezeigt:

$$p_n \text{ und } q_n \text{ prim} \quad \Longrightarrow \quad p_n \in M \text{ oder } q_n \in M$$

Somit genügt es, alle n mit $p_n \leq 13$ zu testen (da $q_n > p_n$ für alle n).

- Für $n = 0$: $p_0 = 4$ ist nicht prim.
- Für $n = 1$: $p_1 = 2 + 3 = 5$ und $q_1 = 2 + 5 = 7$ sind beide prim.
- Für $n = 2$: $p_2 = 4 + 3 = 7$, aber $q_2 = 4 + 5 = 9$ ist nicht prim.
- Für $n = 3$: $p_3 = 8 + 3 = 11$ und $q_3 = 8 + 5 = 13$ sind beide prim.
- Für $n = 4$: $p_4 = 16 + 3 = 17 > 13$. (Entsprechend: $q_4 = 16 + 5 = 21$ nicht prim.)

Die p_n und q_n sind also genau dann beide prim, wenn $n \in \{1, 3\}$ gilt.