Aufgabe F18T2A4 (12 Punkte)

(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.

Lösung:

zu (a) Für alle $n \in \mathbb{N}_0$ gilt die Äquivalenz $3 \mid (2^n + 3) \Leftrightarrow 2^n + 3 \equiv 3 \bmod 3 \Leftrightarrow 2^n \equiv 0 \bmod 3$, und die letzte Kongruenz ist äquivalent zu $\bar{2}^n = \bar{0}$ in $\mathbb{F}_3$. Weil 3 eine Primzahl ist, ist $\mathbb{F}_3$ ein Körper, und aus $\bar{2} \neq \bar{0}$ folgt $\bar{2}^n \neq \bar{0}$ für alle $n \in \mathbb{N}_0$. Also ist $2^n + 3$ für kein $n \in \mathbb{N}_0$ durch 3 teilbar. Ebenso gilt

$$3 \mid (2^n + 5) \quad \Leftrightarrow \quad 2^n + 5 \equiv 0 \bmod 3 \quad \Leftrightarrow \quad 2^n \equiv -5 \bmod 3 \quad \Leftrightarrow \quad 2^n \equiv 1 \bmod 3.$$

Dies ist gleichbedeutend mit $\bar{2}^n = \bar{1}$ in $\mathbb{F}_3$. Die Ordnung von $\bar{2}$ in der multiplikativen Gruppe $\mathbb{F}_3^\times$ ist 2, denn es gilt $\bar{2}^1 = \bar{2} \neq \bar{1}$ und $\bar{2}^2 = \bar{4} = \bar{1}$. Daraus folgt $\bar{2}^n = \bar{1} \Leftrightarrow 2 \mid n \Leftrightarrow n \equiv 0 \bmod 2$. Also ist $2^n + 5$ für alle geraden $n \in \mathbb{N}_0$ durch 3 teilbar.

Entsprechend interpretieren wir Kongruenzen modulo 5 als Gleichungen im Körper $\mathbb{F}_5$. Für alle $n \in \mathbb{N}_0$ gilt

$$5 \mid (2^n + 3) \quad \Leftrightarrow \quad 2^n \equiv -3 \bmod 5 \quad \Leftrightarrow \quad 2^n \equiv 2 \bmod 5 \quad \Leftrightarrow \quad \bar{2}^n = \bar{2} \quad \Leftrightarrow \quad \bar{2}^{n-1} = \bar{1}.$$

Es gilt $\mathrm{ord}(\bar{2}) = 4$ in $\mathbb{F}_5^\times$, denn der einzige Primteiler q von 4 ist 2, und es gilt $\bar{2}^4 = \overline{16} = \bar{1}$ und $\bar{2}^{4/q} = \bar{2}^2 = \bar{4} \neq \bar{1}$. Somit gilt $\bar{2}^{n-1} = \bar{1} \Leftrightarrow 4 \mid (n-1) \Leftrightarrow n \equiv 1 \bmod 4$. Die Zahl $2^n + 3$ ist also für alle $n \in \mathbb{N}_0$ mit $n \equiv 1 \bmod 4$ durch 5 teilbar. Für die Zahl $2^n + 5$ gilt entsprechend

$$5 \mid (2^n + 5) \quad \Leftrightarrow \quad 2^n + 5 \equiv 0 \bmod 5 \quad \Leftrightarrow \quad 2^n \equiv 0 \bmod 5 \quad \Leftrightarrow \quad \bar{2}^n = \bar{0}.$$

Wegen $\bar{2} \neq \bar{1}$ in $\mathbb{F}_5$, und weil $\mathbb{F}_5$ ein Körper ist, gilt $\bar{2}^n \neq \bar{0}$ für alle $n \in \mathbb{N}_0$. Also ist $2^n + 5$ für kein $n \in \mathbb{N}_0$ durch 5 teilbar.

Betrachten wir nun Kongruenzen modulo 7 und entsprechend Gleichungen im Körper $\mathbb{F}_7$. Für alle $n \in \mathbb{N}_0$ gilt

$$7 \mid (2^n + 3) \quad \Leftrightarrow \quad 2^n \equiv -3 \bmod 7 \quad \Leftrightarrow \quad 2^n \equiv 4 \bmod 7 \quad \Leftrightarrow \quad \bar{2}^n = \bar{4} \quad \Leftrightarrow \quad \bar{2}^{n-2} = \bar{1}.$$

In der multiplikativen Gruppe $\mathbb{F}_7^\times$ gilt $\mathrm{ord}(\bar{2}) = 3$ wegen $\bar{2}^1 = \bar{2} \neq \bar{1}$ und $\bar{2}^3 = \bar{8} = \bar{1}$. Daraus folgt $\bar{2}^{n-2} = \bar{1} \Leftrightarrow 3 \mid (n-2) \Leftrightarrow n \equiv 2 \bmod 3$. Also ist $2^n + 3$ genau dann durch 7 teilbar, wenn $n \equiv 2 \bmod 3$ gilt. Entsprechend gilt

$$7 \mid (2^n + 5) \quad \Leftrightarrow \quad 2^n \equiv -5 \bmod 7 \quad \Leftrightarrow \quad 2^n \equiv 2 \bmod 7 \quad \Leftrightarrow \quad \bar{2}^n = \bar{2} \quad \Leftrightarrow$$
$$\bar{2}^{n-1} = \bar{1} \quad \Leftrightarrow \quad 3 \mid (n-1) \quad \Leftrightarrow \quad n \equiv 1 \bmod 3$$

wobei im vorletzten Schritt wieder $\mathrm{ord}(\bar{2}) = 3$ verwendet wurde. Also ist $2^n + 5$ genau dann durch 7 teilbar, wenn $n \equiv 1 \bmod 3$ gilt.

Zum Schluss betrachten wir Kongruenzen modulo 13 und entsprechend Gleichungen im Körper $\mathbb{F}_{13}$. Für alle $n \in \mathbb{N}_0$ gilt

$$13 \mid (2^n + 3) \quad \Leftrightarrow \quad 2^n \equiv -3 \bmod 13 \quad \Leftrightarrow \quad 2^n \equiv 10 \bmod 13 \quad \Leftrightarrow \quad \bar{2}^n = \overline{10} \quad \Leftrightarrow \quad \bar{2}^n = \bar{2}^{10} \quad \Leftrightarrow \quad \bar{2}^{n-10} = \bar{1}.$$

In der multiplikativen Gruppe $\mathbb{F}_{13}^\times$ gilt $\mathrm{ord}(\bar{2}) = 12$, denn die einzigen Primteiler von 12 sind 2 und 3, und es gilt $\bar{2}^{12} = \overline{4096} = \overline{196} = \overline{66} = \bar{1}$, $\bar{2}^{12/2} = \bar{2}^6 = \overline{64} = -\bar{1} \neq \bar{1}$, $\bar{2}^{12/3} = \bar{2}^4 = \overline{16} = \bar{3} \neq \bar{1}$. Wir erhalten $\bar{2}^{n-10} = \bar{1} \Leftrightarrow 12 \mid (n-10) \Leftrightarrow n \equiv 10 \bmod 12$. Die Zahl $2^n + 3$ ist also genau dann durch 13 teilbar, wenn $n \equiv 10 \bmod 12$ gilt. Entsprechend gilt

$$13 \mid (2^n + 5) \quad \Leftrightarrow \quad 2^n \equiv -5 \bmod 13 \quad \Leftrightarrow \quad 2^n \equiv 8 \bmod 11 \quad \Leftrightarrow \quad \bar{2}^n = \bar{8} \quad \Leftrightarrow$$
$$\bar{2}^n = \bar{2}^3 \quad \Leftrightarrow \quad \bar{2}^{n-3} = \bar{1} \quad \Leftrightarrow \quad 12 \mid (n-3) \quad \Leftrightarrow \quad n \equiv 3 \bmod 12$$

wobei im vorletzten Schritt noch einmal $\mathrm{ord}(\bar{2}) = 12$ verwendet wurde. Die Zahl $2^n + 5$ ist also genau dann durch 13 teilbar, wenn $n \equiv 3 \bmod 12$ gilt.

zu (b) Sei $n \in \mathbb{N}_0$ eine Zahl mit der Eigenschaft, dass $2^n + 3$ und $2^n + 5$ beide prim sind, und betrachten wir zunächst den Fall, dass beide Primzahlen > 13 sind. Dann ist weder $2^n + 3$ noch $2^n + 5$ durch eine der Zahlen 3, 5, 7 oder 13 teilbar. Nach Teil (a) folgt daraus, dass n ungerade ist und außerdem folgende Bedingungen erfüllt:

$$n \not\equiv 1 \bmod 4 \quad , \quad n \not\equiv 2 \bmod 3 \quad , \quad n \not\equiv 1 \bmod 3 \quad , \quad n \not\equiv 10 \bmod 12 \quad , \quad n \not\equiv 3 \bmod 12$$

Wir überlegen nun, welche Restklassen modulo 12 für n in Frage kommen. Es gilt $n \equiv a \bmod 12$ für ein $a \in \{0, 1, 2, ..., 11\}$. Im Fall $a \in \{0, 2, 4, 6, 8, 10\}$ wäre n gerade, also ist dieser Fall ausgeschlossen. Berücksichtigen wir auch die letzte Bedindung, so verbleiben die Möglichkeiten $a \in \{1, 5, 7, 9, 11\}$. Im Fall $a \in \{1, 5, 9\}$ wäre $n \equiv a \equiv 1 \bmod 4$. Also bleiben durch die Fälle $a \in \{7, 11\}$ übrig. Aber aus $a = 7$ würde $n \equiv a \equiv 1 \bmod 3$ folgen, und im Fall $a = 11$ wäre $n \equiv a \equiv 2 \bmod 3$, was beides ausgeschlossen ist.

Dass $2^n + 3$ und $2^n + 5$ beide prim sind, ist also nur für $2^n + 3 < 13$ möglich. Damit bleiben für n die Möglichkeiten $n \in \{0, 1, 2, 3\}$, die wir einzeln Durchprobieren können. Wir erhalten für die vier Werte die Zahlenpaare $(2^n + 3, 2^n + 5) \in \{(4, 6), (5, 7), (7, 9), (11, 13)\}$. Die Bedingung, dass $2^n + 3$ und $2^n + 5$ beides Primzahlen sind, ist also nur für $n \in \{1, 3\}$ erfüllt.