Übungsblatt № 10

Aufgabe 64

Beweisen Sie, dass für jede Primzahl mit $p \geq 5$ gilt: $p^2 - 1$ ist durch 24 teilbar.

Da p eine Primzahl ist, sind $p-1$ und $p+1$ gerade. Eine der beiden muss dann durch 4 teilbar sein. Daraus folgt aber direkt, dass $(p+1)(p-1) = p^2 - 1$ durch 8 teilbar ist. Sei dazu z.B. $p+1$ durch 4 teilbar und damit $p-1$ gerade. Da p auch nicht durch 3 teilbar ist, folgt somit, dass entweder $p+1$ oder $p-1$ durch drei teilbar ist. Das ist eine Folgerung daraus, dass Vielfache von 3 immer einen Abstand von 3 haben. Somit muss in $p-1$, p, $p+1$ ein Vielfaches von 3 auftauchen. Ist etwa $p+1$ durch 3 und 4 teilbar, so gilt $p+1 = 3k_1 = 4k_2$. Wählen wir nun $k = \mathrm{ggT}(k_1, k_2)$ so folgt $p+1 = 12k$. Daraus erhalten wir aber

$$p^2 - 1 = (p+1)(p-1) = 12k \cdot 2l = 24kl$$

womit $p^2 - 1$ ein Vielfaches von 24 ist. Analog behandeln wir den Fall, dass $p-1$ durch 3 und 4 teilbar ist. Es verbleiben noch die Fälle, dass $p+1$ oder $p-1$ durch 2 und 3 teilbar ist. Ist $p+1$ durch 2 und 3 teilbar, so ist $p+1 = 2k_1 = 3k_1$. Mit $k = \mathrm{ggT}(k_1, k_2)$ folgt $p+1 = 6k$ und dadurch

$$p^2 - 1 = (p+1)(p-1) = 6k \cdot 4l = 24kl$$

Aufgabe 66

Zeigen Sie, dass die Zahl

$$z_n = 5^{2n+1} \cdot 2^{n+2} + 3^{n+2} \cdot 2^{2n+1}$$

für alle $n \in \mathbb{N}_0$ von 19 geteilt wird.

Wir führen einen Induktionsbeweis. Für z_0 gilt

$$z_0 = 5 \cdot 2^2 + 3^2 \cdot 2 = 20 + 18 = 38 = 2 \cdot 19 \implies z_0 \equiv 0 \mod 19$$

Wir verwenden nun die Schreibweise $[x]_k = \{z \in \mathbb{Z} \colon z \equiv x \mod k\}$ für die Kongruenzklassen. Die Addition $[x+y]_k [x]_k + [y]_k$ und Multiplikation $[xy]_k = [x]_k [y]_k$ sind wohldefiniert. Ist $x \in \mathbb{Z}$ durch k teilbar, so folgt direkt $[x]_k = [0]_k$, da $\exists l \in \mathbb{Z}$ sodass $x = lk$. Wir wollen im Induktionsschritt also zeigen, dass $[z_{n+1}]_{19} = [0]_{19}$:

$$\begin{aligned}
z_{n+1} &= 5^{2n+3} \cdot 2^{n+3} + 3^{n+3} \cdot 2^{2n+3} = 2 \cdot 5^2 \cdot 5^{2n+1} \cdot 2^{n+2} + 3 \cdot 2^2 \cdot 3^{n+2} \cdot 2^{2n+1} \\
&= 50 \cdot 5^{2n+1} \cdot 2^{n+1} + 12 \cdot 3^{n+2} 2^{2n+1} \\
&\implies [z_{n+1}]_{19} = [50]_{19} [5^{2n+1} \cdot 2^{n+2}]_{19} + [12]_{19} \cdot [3^{n+2} \cdot 2^{2n+1}]_{19}
\end{aligned}$$

Da $2 \cdot 19 = 38$ folgt $50 \equiv 12 \mod 19$, sprich:

$$\begin{aligned}
[z_{n+1}]_{19} &= [12]_{19} \left([5^{2n+1} \cdot 2^{n+2}]_{19} + [3^{n+2} \cdot 2^{2n+1}]_{19} \right) \\
&= [12]_{19} \left([5^{2n+1} \cdot 2^{n+2} + 3^{n+2} \cdot 2^{2n+1}]_{19} \right) = [12]_{19} \left([z_n]_{19} \right) = [12]_{19} \cdot [0]_{19} = [0]_{19}
\end{aligned}$$