Aufgabe F14T2A1 (8 Punkte)

Es seien die Polynome $p = x^{500} - 2x^{301} + 1$ und $q = x^2 - 1$ in $\mathbb{Q}[x]$ gegeben. Berechnen Sie den Rest der Division von p durch q.

Lösung:

Sei $R = \mathbb{Q}[x]/(q)$. Zwei Elemente $f_1 + (q)$ und $f_2 + (q)$ dieses Rings sind genau dann gleich, wenn die Differenz $f_1 - f_2$ der beiden Polynome $f_1, f_2 \in \mathbb{Q}[x]$ durch q teilbar ist. Setzen wir $\alpha = x + (q)$, dann gilt deshalb $\alpha^2 = (x + (q))^2 = x^2 + (q) = 1 + (q)$. Für die bessere Lesbarkeit bezeichnen wir die Elemente aus R der Form $a + (q)$ mit $a \in \mathbb{Q}$ einfach mit a, wir identifizieren also $\mathbb{Q}$ mit seinem Bild in R unter der Abbildung $\mathbb{Q} \to R$, $a \mapsto a + (q)$. Mit dieser Notation gilt dann $\alpha^2 = 1$.

Sei nun $r \in \mathbb{Q}[x]$ der Rest, der bei Division von p durch q entsteht. Dann ist auch $p - r$ durch q teilbar, es gilt also $r + (q) = p + (q)$. Wir erhalten

$$r + (q) \quad = \quad p + (q) \quad = \quad (x^{500} - 2x^{301} + 1) + (q) \quad = \quad \alpha^{500} - 2\alpha^{301} + 1 \quad =$$
$$(\alpha^2)^{250} - 2(\alpha^2)^{150}\alpha + 1 \quad = \quad 1 - 2\alpha + 1 \quad = \quad -2\alpha + 2 \quad = \quad -2x + 2 + (q).$$

Somit ist die Differenz $r - (-2x + 2)$ durch q teilbar. Weil r und $-2x + 2$ beide vom Grad < 2 sind, folgt $r - (-2x + 2) = 0$ und $r = -2x + 2$.