Aufgabe H19T2A2 (12 Punkte)

Sei $f \in \mathbb{Z}[x]$ ein Polynom mit ganzzahligen Koeffizienten.

(a) Man zeige für alle $a, c \in \mathbb{Z}$ und $n \in \mathbb{N}$: Aus $a \equiv c \bmod n$ folgt $f(a) \equiv f(c) \bmod n$.

(b) Man zeige: Sind $f(0)$ und $f(2019)$ ungerade, dann hat f keine ganzzahligen Nullstellen.

(c) Seien p und q zwei verschiedene Primzahlen. Man zeige: Gibt es ein $a \in \mathbb{Z}$, so dass $f(a)$ nicht durch p teilbar ist, und ein $b \in \mathbb{Z}$, so dass $f(b)$ nicht durch q teilbar ist, dann gibt es ein $c \in \mathbb{Z}$, so dass $f(c)$ weder durch p noch durch q teilbar ist.
Hinweis: Man verwende den Chinesischen Restsatz.

Lösung:

zu (a) Für jedes $b \in \mathbb{Z}$ bezeichnen wir mit $\bar{b}$ jeweils das Bild von b im Restklassenring $\mathbb{Z}/n\mathbb{Z}$. Aus der Vorlesung ist bekannt, dass die Kongruenz $a \equiv c \bmod n$ äquivalent zur Gleichung $\bar{a} = \bar{c}$ ist. Sei nun $f \in \mathbb{Z}[x]$ gegeben durch $f = \sum_{k=0}^{m} a_k x^k$ mit $a_0, ..., a_m \in \mathbb{Z}$. Aus $\bar{a} = \bar{c}$ folgt offenbar $\sum_{k=0}^{m} \bar{a}_k \bar{a}^i = \sum_{k=0}^{m} \bar{a}_k \bar{c}^i$. Dies wiederum ist äquivalent zu $f(a) \equiv f(c) \bmod n$.

zu (b) Nehmen wir an, $a \in \mathbb{Z}$ ist eine Nullstelle von f. Ist a gerade, dann gilt $a \equiv 0 \bmod 2$, und mit Teil (a) folgt $f(a) \equiv f(0) \bmod 2$. Aber mit $f(0)$ ist dann auch $f(a)$ ungerade, im Widerspruch zu $f(a) = 0$. Ist a andererseits ungerade, dann gilt $a \equiv 1 \equiv 2019 \bmod 2$ und wegen Teil (a) somit $f(a) \equiv f(2019) \bmod 2$. Wieder folgt daraus, dass $f(a)$ ungerade ist, was der Voraussetzung $f(a) = 0$ widerspricht. Somit kann es keine ganzzahlige Nullstelle von f geben.

zu (c) Die Voraussetzung $p \nmid f(a)$ ist gleichbedeutend mit $f(a) \not\equiv 0 \bmod p$, und dies wiederum ist äquivalent zu $f(a) + p\mathbb{Z} \neq p\mathbb{Z}$ im Restklassenring $\mathbb{Z}/p\mathbb{Z}$. Ebenso ist $q \nmid f(b)$ äquivalent zu $f(b) \not\equiv 0 \bmod q$ und zur Ungleichung $f(b) + q\mathbb{Z} \neq q\mathbb{Z}$ im Restklassenring $\mathbb{Z}/q\mathbb{Z}$. Da p und q als verschiedene Primzahlen zueinander teilerfremdsind, gibt es nach dem Chinesischen Restsatz einen Ringisomorphismus $\bar{\phi} : \mathbb{Z}/pq\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ mit $\phi(c+pq\mathbb{Z}) = (c+p\mathbb{Z}, c+q\mathbb{Z})$ für alle $c \in \mathbb{Z}$. Auf Grund der Surjektivität gibt es insbesondere ein $c \in \mathbb{Z}$ mit

$$(c + p\mathbb{Z}, c + q\mathbb{Z}) \quad = \quad \bar{\phi}(c + pq\mathbb{Z}) \quad = \quad (a + p\mathbb{Z}, b + q\mathbb{Z}).$$

Aus $c + p\mathbb{Z} = a + p\mathbb{Z}$ und $c + q\mathbb{Z} = b + q\mathbb{Z}$ folgen die Kongruenzen $c \equiv a \bmod p$ und $c \equiv b \bmod q$. Mit Teil (a) erhalten wir $f(c) \equiv f(a) \not\equiv 0 \bmod p$ und $f(c) \equiv f(b) \not\equiv 0 \bmod q$. Dies ist äquivalent zu $p \nmid (c)$ und $q \nmid f(c)$.