

Zirkel 11b, Hausaufgaben vom 05.11.2008

(zum 12.11.2008)

Polynome IV

Genau wie bei den ganzen Zahlen, kann man die Reste der Polynome beim Dividieren durch ein Polynom f addieren und multiplizieren. Es entstehen Additions- und Multiplikationsregeln "modulo f ".

Beispiel: $x \cdot x = x^2 \equiv 1 \pmod{x^2 - 1}$.

1. Zeige: f ist irreduzibel genau dann, wenn aus $ab \equiv 0 \pmod{f}$ entweder $a \equiv 0 \pmod{f}$ oder $b \equiv 0 \pmod{f}$ folgt.
2. Zeige: wenn $\text{ggT}(f, g) = 1$ gilt, dann existiert ein h , sodass

$$gh \equiv 1 \pmod{f}$$

gilt.

3. Schreibe Additions- und Multiplikationsregeln modulo $x^2 + 1$ auf. Kommen sie Dir bekannt vor?