Wolfgang K. Seiler
Tel. 2515

A5, C201

21. November 2014

12. Übungsblatt Computeralgebra

Aufgabe 1: *(12 Punkte)*
Sei $f = X^5 + X^4 + 1 \in \mathbb{Z}[X]$.

a) Zeigen Sie, daß das Polynom $f^{(2)} \in \mathbb{F}_2[X]$ quadratfrei ist!

b) Finden Sie die irreduziblen Faktoren von $f^{(2)}$!

c) Überprüfen Sie, ob f in $\mathbb{Z}[X]$ irreduzible Faktoren der Höhe eins hat, die modulo zwei zu den in *b)* berechneten werden!

Aufgabe 2: *(3 Punkte)*
In $\mathbb{F}_2[X]$ ist $X^5+X^3+X+1 = (X+1)(X^4+X^3+1)$, und X^4+X^3+1 ist irreduzibel. Folgern Sie (ohne Computerhilfe), daß das Polynom $X^5 + X^3 + X + 1 \in \mathbb{Z}[X]$ irreduzibel ist!

Aufgabe 3: *(5 Punkte)*
Das Polynom $f = X^7 + 11X^5 - 8X^4 - 21X^3 + X^2 + 72X - 35$ erfüllt die Kongruenz

$$f \equiv (X^4 + 21X^2 + 22X + 5)(X^3 + 13X + 16) \bmod 23\,.$$

a) Setzen sie diese Faktorisierung nach dem Hensel'schen Lemma fort zu einer Faktorisierung modulo 23^2. Für den erweiterten Euklidischen Algorithmus können Sie ein Computeralgebrasystem benutzen. In Maple setzt `gcdex(f, g, X, 'a', 'b')` die beiden Variablen a und b so, daß der ggT $af+bg$ ist; in Maxima liefert `gcdex(f, g, X)` die Liste $[a, b, ggT]$.)

b) Versuchen Sie, daraus eine Faktorisierung von $f \in \mathbb{Z}[X]$ zu erraten und überprüfen Sie, ob diese korrekt ist!

c) Wie groß können die Koeffizienten eines irreduziblen Faktors von f höchstens werden?

Abgabe bis zum Donnerstag, dem 27. November 2014, um 12.00 Uhr