Modul Computeralgebra mit Gröbnerbasen 21. April 2011
Sommersemester 2011
Schmale

Aufgabenblatt 3

(**7**) Zeigen Sie im Kontext von § 7(a) für ein quadratfreies Polynom f aus $\mathbb{Z}_p[x]$:

Es gibt eine Basis $h_1, \ldots, h_t$ von W derart, dass $\mathsf{ggT}(f, h_i) = u_i$ für $1 \leq i \leq t$.

(**8**) Aus den Übungsaufgaben in [GCL] auf den Seiten 384 bis 387:

(a) Berechne die quadratfreie Zerlegung von $x^{10} + x^6 + x^5 + x^3 + x^2 + 1$ in $\mathbb{Z}_2[x]$.

(b) Zerlege $x^{15} - 1$ aus $\mathbb{Z}_2[x]$ in Primfaktoren mit Hilfe des Berlekamp-Verfahrens für kleine Primzahlen.

(c) Berechne die gleichgradige Zerlegung des Polynoms $x^8 + x^7 + 2x^6 + 3x^5 + 3x^4 + 3x^3 + 2x^2 + 2x + 1$ in $\mathbb{Z}_7[x]$ und zerlegen Sie die erhaltenen Faktoren nach dem Verfahren von Cantor und Zassenhaus.

(**9**) Was vereinfacht sich beim Berlekamp-Verfahren für kleine Primzahlen, wenn die Primteiler $u_1, \ldots, u_t$ alle den gleichen Grad haben, was wenn alle den Grad 1 haben?