

### Aufgabenblatt 4

Die folgenden Aufgaben sind mit geringfügigen Änderungen dem Buch [GaGe], §15 entnommen.

(10) (Legendre 1785, genaue Quelle siehe bei [GaGe])

Sei  $f = x^3 - 292x^2 + 2170221x + 6656000$  aus  $\mathbb{Z}[x]$ . Bestimmen Sie mit Hilfe des Verfahrens von Satz 1 und ggf. des dazu verteilten Maple-Arbeitsblatt in §8 die linearen Teiler von  $f$  in  $\mathbb{Z}_{13^{2^k}}[x]$ ,  $k = 0, 1, 2$  beginnend mit dem Teiler  $x$  in  $\mathbb{Z}_{13}[x]$ .

(11) Sei  $f = 14x^4 + 15x^3 + 42x^2 + 3x + 1$  aus  $\mathbb{Z}[x]$ .

(i) Bestimmen Sie eine geeignete Primzahl derart, dass  $f$  quadratfrei und vom Grad 4 ist modulo  $p$ .

(ii) Berechnen Sie die Primzerlegung von  $f$  in  $\mathbb{Z}_p[x]$ . Wählen Sie zwei in  $\mathbb{Z}_p[x]$  teilerfremde Polynome  $g_1, h_1$  in  $\mathbb{Z}[x]$  derart, dass  $f \equiv_p g_1 h_1$ , und  $h_1$  modulo  $p$  ein normiertes Primpolynom ist, und bestimmen Sie  $u_1, v_1$  in  $\mathbb{Z}[x]$  derart, dass  $u_1 g_1 + v_1 h_1 \equiv_p 1$ .

(iii) Heben Sie die von Ihnen in (ii) gewählte Zerlegung in zwei Schritten nach  $\mathbb{Z}_{p^4}[x]$ . Kann man nun eine Zerlegung von  $f$  in  $\mathbb{Q}[x]$  ablesen?

(12) Sei  $f$  ein Polynom aus  $\mathbb{Z}[x]$  mit höchstem Koeffizienten 1 und vom Grad 8. Sei weiter  $p$  eine Primzahl derart, dass  $f \equiv_p g_1 g_2 g_3$  mit paarweise verschiedenen normierten Primpolynomen  $g_1, g_2, g_3$  aus  $\mathbb{Z}_p[x]$ . Es gelte dabei  $\deg g_1 = 1$ ,  $\deg g_2 = 2$  und  $\deg g_3 = 5$ .

(i) Was lässt sich über die möglichen Zerlegungen von  $f$  in  $\mathbb{Z}_{p^{100}}[x]$  sagen?

(ii) Was lässt sich über die möglichen Zerlegungen von  $f$  in  $\mathbb{Q}[x]$  sagen?

(iii) Sei  $q$  eine weitere Primzahl und gelte  $f \equiv_q h_1 h_2$  mit normierten Primpolynomen  $h_1, h_2$  aus  $\mathbb{Z}_q[x]$  vom Grad 4. Was lässt sich über mögliche Zerlegungen von  $f$  in  $\mathbb{Q}[x]$  sagen unter Berücksichtigung aller bis hierhin vorliegenden Informationen?