Wolfgang K. Seiler
Tel. 2515

B6, B4.18

16. März 2020

4. Übungsblatt Computeralgebra

Aufgabe 1: *(5 Punkte)*
Das Polynom $f \in \mathbb{Z}[X]$ vom Grad d habe einen Faktor g vom Grad e mit $1 \leq e < d$.

a) Benutzen Sie die Methode, die zur Landau-Mignotte-Schranke führten, um eine Schranke für die Höhe von g zu finden unter der Voraussetzung, daß e bekannt ist!

b) Wie verschlechtert sich diese Schranke, wenn Sie nur wissen, daß $1 \leq e < d$ ist?

c) Welche Schranke können Sie für einen nichttrivialen Faktor vom Grad d angeben?

Aufgabe 2: *(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)` 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?

Aufgabe 3: *(4 Punkte)*
Berechnen Sie den ggT der beiden Polynome

$$f = X^8 + X^6 - 3X^4 - 3X^3 + 8X^2 + 2X - 5$$

und

$$g = 3X^6 + 5X^4 - 4X^2 - 9X + 21$$

nach dem EZ GCD Algorithmus mit der Primzahl $p = 11$!

Aufgabe 4: *(6 Punkte)*

a) Berechnen Sie den ggT der beiden Polynome

$$f = X^5 - 2X^4 - X^3 + 2X^2 + X - 2$$

und

$$g = X^4 - 2X^3 - X^2 + X + 2$$

nach dem EZ GCD Algorithmus mit der Primzahl $p = 11$!

b) Für welche Primzahlen p hat dieses ggT-Problem schlechte Reduktion?

Abgabe bis zum Donnerstag, dem 19. März 2020, um 15.30 Uhr