

7. November 2014

## 10. Übungsblatt Computeralgebra

### Aufgabe 1: (6 Punkte)

- a) Bestimmen Sie (mit Maple oder Maxima) die Resultante der beiden ganzzahligen Polynome  
 $f = x^4 + 182x^3 - 3788x^2 + 6282x + 10251$  und  $g = x^4 - 174x^3 - 2812x^2 - 4386x + 7371$ !  
Der Befehl lautet in beiden Systemen `resultant(f, g, x)`.
- b) Was können daraus auf den ggT der beiden Polynome in  $\mathbb{Z}[x]$  schließen?
- c) Bestimmen Sie alle Primzahlen  $p$ , für die der ggT von  $f \bmod p$  und  $g \bmod p$  positiven Grad hat!
- d) Finden Sie zwei Polynome  $f, g \in \mathbb{Z}[x]$  mit einem linearen Polynom als ggT derart, daß der ggT von  $f \bmod p$  und  $g \bmod p$  in  $\mathbb{F}_p[x]$  für  $p = 17$  quadratisch und für  $p = 5$  kubisch ist!

### Aufgabe 2: (5 Punkte)

- a) Berechnen Sie die LANDAU-MIGNOTTE-Schranke für den ggT der beiden Polynome  
 $f = x^5 + 3x^3 + x^2 + 3x + 2$  und  $g = x^5 - 2x^4 + 2x^3 - 3x + 2$ !
- b) Wählen Sie eine Primzahl  $p$  mit der Eigenschaft, daß der ggT von  $f$  und  $g$  durch seine Reduktion modulo  $p$  eindeutig bestimmt ist, und berechnen Sie den ggT von  $f \bmod p$  und  $g \bmod p$ !
- c) Welchen ggT haben  $f$  und  $g$  in  $\mathbb{Z}[x]$ ?

### Aufgabe 3: (6 Punkte)

- a) Bestimmen Sie mit der modularen Methode und mit höchstens zweistelligen Primzahlen den ggT in  $\mathbb{Z}[x]$  der beiden Polynome  
 $f = 72x^5 + 12x^4 + 84x^3 - 72x^2 - 24x + 48$  und  $g = 189x^4 + 252x^3 + 21x^2 + 210x + 168$ !  
Die ggT über endlichen Körpern können Sie durch ein Computeralgebrasystem bestimmen lassen. (Maple: `Gcd(f, g) mod p`; Maxima: `modulus : p`; schaltet die Arithmetik um auf Rechnen modulo  $p$ ; danach `gcd(f, g)`; Mit `modulus : false`; kommen Sie zurück zur gewöhnlichen Arithmetik.)
- b) Für welche Primzahlen  $p$  hat  $\text{ggT}(f \bmod p, g \bmod p) \in \mathbb{F}_p[x]$  einen anderen Grad als  $\text{ggT}(f, g) \in \mathbb{Z}[x]$ ?

### Aufgabe 4: (3 Punkte)

- a) Der Maple-Befehl zur Berechnung des ggT zweier Polynome heißt `gcd(f, g)`, der zur Berechnung des Divisionsrests von  $f$  modulo  $g$  heißt `rem(f, g, x)`. Warum muß die Variable  $x$  beim `rem`-Befehl angegeben werden, nicht aber bei `gcd`?
- b) Finden Sie zwei Polynome  $f, g \in \mathbb{Z}[x]$  der Grade zwei und drei, die in  $\mathbb{Q}[x]$  teilerfremd sind, nicht aber in  $\mathbb{Z}[x]$ ! Lassen Sie  $\text{ggT}(f, g)$  auch von Maple oder Maxima berechnen, und spekulieren Sie darüber, ob hier der ggT in  $\mathbb{Z}[x]$  oder der in  $\mathbb{Q}[x]$  berechnet wurde!

Abgabe bis zum Donnerstag, dem 13. November 2014, um 12.00 Uhr