Wolfgang K. Seiler
Tel. 2515

B6, B4.18

21. Februar 2020

1. Übungsblatt Computeralgebra

Aufgabe 1: *(15 Punkte)*

a) Berechnen Sie nach dem klassischen Euklidischen Algorithmus in $\mathbb{Q}[X]$ den ggT der beiden Polynome

$$f = X^5 + 2X^4 + 4X^3 + 3X^2 + 5X + 3 \quad \text{und} \quad g = X^4 + 3X^3 + 6X^2 + 5X + 3\,!$$

Lösung:

$$(X^5+2X^4+4X^3+3X^2+5X+3) : (X^4+3X^3+6X^2+5X+3) = X-1 \text{ Rest } -3X^3+4X^2+7X+6$$
$$(X^4+3X^3+6X^2+5X+3) : (-3X^3+4X^2+7X+6) = -\frac{X}{3} - \frac{13}{9} \text{ Rest } \frac{127}{9}X^2 + \frac{154}{9}X + \frac{35}{3}$$
$$(-3X^3+4X^2+7X+6) : \left(\frac{127}{9}X^2 + \frac{154}{9}X + \frac{35}{3}\right) = -\frac{27}{127}X + \frac{8739}{16129} \text{ Rest } \frac{3528}{16129}X - \frac{5076}{16129}$$
$$\left(\frac{127}{9}X^2 + \frac{154}{9}X + \frac{35}{3}\right) : \left(\frac{3528}{16129}X - \frac{5076}{16129}\right) = \frac{2048383}{31753}X + \frac{532240871}{3111696} \text{ Rest } \frac{629031}{9604}$$

Da der letzte Rest eine von Null verschiedene Konstante ist, geht die nächste Division ohne Rest auf, d.h. dieser Rest ist ein ggT. Da größte gemeinsame Teiler im Polynomring über einem Körper nur bis auf multiplikative Konstanten bestimmt sind, ist dann natürlich auch eins ein ggT von f und g.

b) Überprüfen Sie, ob das so berechnete Polynom auch in $\mathbb{Z}[X]$ ein gemeinsamer Teiler von f und g ist!

Lösung: Da der *berechnete* ggT keine ganze Zahl ist, also nicht in $\mathbb{Z}[X]$ liegt, ist er dort natürlich kein ggT.

c) Was ist der größte gemeinsame Teiler von f und g in $\mathbb{Z}[X]$?

Lösung: Dieser kann keinen positiven Grad haben, denn sonst hätte auch der in $\mathbb{Q}[X]$ berechnete ggT positiven Grad. Er ist daher die größte ganze Zahl, die alle Koeffizienten von f und von g teilt, also eins. (-1 wäre auch eine Lösung.)

d) Berechnen Sie in $\mathbb{F}_3[X]$ nach dem klassischen Euklidischen Algorithmus den ggT von f mod 3 und g mod 3, und überprüfen Sie, ob er mit der Reduktion modulo drei von $\text{ggT}(f, g) \in \mathbb{Z}[X]$ übereinstimmt!

Lösung: $f \equiv X^5 + 2X^4 + 2X \bmod 3$ und $g \equiv X^4 + 2X \bmod 3$. Damit ist schon klar, daß der ggT durch X teilbar sein muß. In $\mathbb{F}_3[X]$ ist

$$(X^5 + 2X^4 + 2X) : (X^4 + 2X) = X + 2 \text{ Rest } X^2 + X$$
$$(X^4 + 2X) : (X^2 + X) = X^2 + 2X + 1 \text{ Rest } X$$
$$(X^2 + X) : X = X + 1 \text{ Rest } 0$$

Der ggT ist also gleich X.

e) Berechnen Sie in $\mathbb{F}_7[X]$ nach dem klassischen EUKLIDischen Algorithmus den ggT von $f \bmod 7$ und $g \bmod 7$, und bestimmen Sie einen ggT mit führendem Koeffizienten eins aus $\mathbb{F}_7[X]$!

Lösung: Da alle Koeffizienten zwischen 0 und 6 liegen, können wir auch in $\mathbb{F}_7[X]$ problemlos mit der angegebenen Darstellung rechnen.

$$(X^5 + 2X^4 + 4X^3 + 3X^2 + 5X + 3) : (X^4 + 3X^3 + 6X^2 + 5X + 3) = X + 6 \text{ Rest } 4X^3 + 4X^2 + 6$$
$$(X^4 + 3X^3 + 6X^2 + 5X + 3) : (4X^3 + 4X^2 + 6) = 2X + 4 \text{ Rest } 4X^2$$
$$(4X^3 + 4X^2 + 6) : 4X^2 = X + 1 \text{ Rest } 6$$

Da dies eine Einheit ist, sind die Polynome auch in $\mathbb{F}_7[X]$ teilerfremd; der ggT ist also eins.

f) p sei eine Primzahl, und $f, g \in \mathbb{F}_p[X]$ seien zwei Polynome. Wie viele größte gemeinsame Teiler von f und g gibt es in $\mathbb{F}_p[X]$?

Lösung: Der ggT ist bestimmt bis auf eine von Null verschiedene multiplikative Konstante; davon gibt es in $\mathbb{F}_p$ genau $p - 1$ Stück, und somit gibt es auch $p - 1$ verschiedene größte gemeinsame Teiler.

Aufgabe 2: *(5 Punkte)*
Berechnen Sie für das Polynom $f = (X^2 + 5X + 6)(4X^2 + 1)$ die Höhe, L^1- und L^2-Norm, sowie das Maß!

Lösung: Ausmultipliziert ist $f = 4X^4 + 20X^3 + 25X^2 + 5X + 6$. Die Höhe ist der größte Betrag eines Koeffizienten, also 25. Die L^1-Norm ist die Summe der Beträge der Koeffizienten, also $4 + 20 + 25 + 5 + 6 = 60$.

$$\|f\|_2 = \sqrt{4^2 + 20^2 + 25^2 + 5^2 + 6^2} = \sqrt{1102} \approx 33{,}196\,,$$

Der erste Faktor von f hat die Nullstellen -2 und -3, deren Betrag jeweils größer eins ist; der zweite hat $\pm\frac{1}{2}i$ als Nullstellen; deren Betrag ist kleiner als eins. Der führende Koeffizient ist vier, also ist $\mu(f) = 4 \cdot 2 \cdot 3 = 24$.