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!

Lösung: Sind a_d und b_e die führenden Koeffizienten von f und g, so gilt zunächst für die Maße, daß

$$\mu(g) \leq \left|\frac{b_e}{a_d}\right| \cdot \mu(f) \,.$$

Von b_e wissen wir nur, daß es ein Teiler von a_d sein muß, der Vorfaktor ist also auf jeden Fall kleiner oder gleich eins, so daß wir von der Ungleichung $\mu(g) \leq \mu(f)$ ausgehen müssen. Das Maß von f ist im Allgemeinen nur schwer zu berechnen; wir wissen aber, daß es höchstens gleich der L^2-Norm von f ist. Von der Höhe wissen wir, daß sie höchstens gleich dem größten Binomialkoeffizienten zum Grad mal dem Maß ist, so daß wir insgesamt die Abschätzung

$$H(g) \leq \binom{e}{[e/2]}\mu(g) \leq \binom{e}{[e/2]}\mu(f) \leq \binom{e}{[e/2]}\|f\|_2$$

erhalten.

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

Lösung: Da der Binomialkoeffizient strikt monoton mit e ansteigt, muß man vom größtmöglichen Grad ausgehen, also von $e = d-1$. Die Schranke wird also zu

$$H(g) \leq \binom{d-1}{[(d-1)/2]}\|f\|_2 \,.$$

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

Lösung: Ist g ein Teiler gleichen Grad, so ist der Kofaktor eine ganze Zahl c; es gibt also ein $c \in \mathbb{Z}$, so daß $f = cg$ ist. Damit ist $H(f) = |c| \cdot H(g)$, also insbesondere $H(g) \leq H(f)$. Da g ein nichttrivialer Teiler sein soll, ist $|c| \neq 1$, so daß $|c|$ mindestens gleich dem kleinsten Primteiler p des Inhalts von f ist und sich die Abschätzung in diesem (nicht sonderlich interessanten) Fall auf $H(g) \leq H(f)/p$ verbessern läßt.

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 HENSELschen 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 $[a, b, ggT]$.)

Lösung: Sei $g = X^4 + 21X^2 + 22X + 5$ und $h = X^3 + 13X + 16$. Wir suchen Polynome $g', h' \in \mathbb{Z}[X]$, so daß

$$f \equiv (g + 23g')(h + 23h') = gh + 23(gh' + hg') + 23^2 g'h' \bmod 23^2$$

ist. Dabei soll natürlich $\deg g' \leq \deg g = 4$ und $\deg h' \leq \deg h = 3$ sein.

$$gh = X^7 + 34X^5 + 38X^4 + 278X^3 + 622X^2 + 417X + 80$$

ist offensichtlich ungleich f; die Differenz ist

$$f - gh = -23X^5 - 46X^4 - 299X^3 - 621X^2 - 345X - 115 = -23(X^5 + 2X^4 + 13X^3 + 27X^2 + 15X + 5)\,.$$

Die gesuchten Polynome müssen also die Kongruenz

$$gh' + hg' \equiv f_0 = -(X^5 + 2X^4 + 13X^3 + 27X^2 + 15X + 5) \bmod 23$$

erfüllen.
Falls $g \bmod 23$ und $h \bmod 23$ teilerfremd sind, liefert der erweiterte EUKLIDische Algorithmus in $\mathbb{F}_{23}[X]$ Polynome $a, b \in \mathbb{F}_{23}[X]$, so daß dort gilt

$$a(g \bmod 23) + b(h \bmod 23) = 1\,.$$

Anwendung mit einem Computeralgebrasystem (oder eigenes Rechnen) zeigt, daß der ggT in $\mathbb{F}_{23}[X]$ tatsächlich gleich eins ist; für die Koeffizienten erhalten wir $a = 2X + 10$ und $b = 21X^2 + 13X + 7$. Wenn wir diese mit f_0 multiplizieren, erhalten wir Kandidaten für h' und g', allerdings haben diese einen viel zu hohen Grad:

$$af_0 = -2X^6 - 14X^5 - 46X^4 - 184X^3 - 300X^2 - 160X - 50 \equiv 21X^6 + 9X^5 + 22X^2 + X + 19 \bmod 23$$

und

$$\begin{aligned} bf_0 &= -21X^7 - 55X^6 - 306X^5 - 750X^4 - 757X^3 - 489X^2 - 170X - 35 \\ &\equiv 2X^7 + 14X^6 + 16X^5 + 9X^4 + 2X^3 + 17X^2 + 14X + 11 \bmod 23\,. \end{aligned}$$

Die Gleichung $gh' + hg' = f_0$ bleibt gültig, wenn wir ein Vielfaches von h zu h' addieren und das entsprechende Vielfache von g von g' subtrahieren, denn $gh - hg = 0$. Division mit Rest in $\mathbb{F}_{23}[X]$ zeigt, daß

$$af_0 : h = 21X^3 + 9X^2 + 3X + 7 \quad \text{Rest } 22\,;$$

wir subtrahieren also $21X^3 + 9X^2 + 3X + 7$ mal h von af_0, was auf den Rest 22 führt, und wir addieren das entsprechende Vielfache von g zu bf_0:

$$bf_0 + (21X^3 + 9X^2 + 3X + 7)g = 22X^2 + 22X\,.$$

Wir bekommen die einfachere Gleichung

$$22g + (22X^2 + 22X)h = f_0 \quad \text{in } \mathbb{F}_{23}$$

und können $h' = 22$ und $g' = 22X^2 + 22X$ setzen. Damit erhalten wir die neuen Faktoren

$$\widetilde{g} = g + 23g' = X^4 + 527X^2 + 528X + 5 \quad \text{und} \quad \widetilde{h} = h + 23h' = X^3 + 13X + 522\,.$$

Nachrechnen zeigt, daß

$$\widetilde{g}\widetilde{h} - f = 23^2(X^5 + 2X^4 + 13X^3 + 533X^2 + 521X + 5)$$

ist, so daß wir tatsächlich eine Faktorisierung modulo 23^2 haben.

b) Versuchen Sie, daraus eine Faktorisierung von $f \in \mathbb{Z}[x]$ zu erraten, und überprüfen Sie, ob diese korrekt ist!

Lösung: Wie wir gesehen haben, weicht $\widetilde{g} \cdot \widetilde{h}$ stark von f ab. Das liegt sicher auch daran, daß wir Restklassen modulo 23^2 durch Zahlen zwischen 0 und $23^2 - 1 = 528$ repräsentieren. Modulo 23^2 ist $\widetilde{g}$ kongruent zu dem deutlich einfacheren Polynom $X^4 - 2X^2 - X + 5$ und $\widetilde{h}$ zu $X^3 + 13X - 7$. Das Produkt dieser beiden Polynome ist in der Tat gleich f.

c) Wie groß können die Koeffizienten eines irreduziblen Faktors von f höchstens werden?

Lösung: Dazu können wir die Ergebnisse von Aufgabe 1 verwenden: Die L^2-Norm von f ist

$$\|f\|_2 = \sqrt{1^2 + 11^2 + 8^2 + 21^2 + 1^2 + 72^2 + 35^2} = \sqrt{7037} \approx 83{,}8868\,;$$

wenn wir nichts über den Grad des Faktors wissen, müssen wir von einem Grad bis zu sechs, müssen also noch mit dem Binomialkoeffizienten $\binom{6}{3} = 20$ multiplizieren, was auf eine Zahl mit 1677 vor dem Komma führt. Nach unserer allgemeinen Abschätzung wissen wir also nur, daß der Betrag jedes Koeffizienten höchstens gleich 1677 sein kann.

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 $p = 11$!

Lösung: Beide Polynome sind primitiv, wir können also direkt mit ihnen rechnen. Als erstes berechnen nach dem Euklidischen Algorithmus in $\mathbb{F}_{11}[X]$ den ggT von

$$f \bmod 11 = X^8+X^6+8X^4+8X^3+8X^2+2X+6 \quad \text{und} \quad g \bmod 11 = 3X^6+5X^4+7X^2+2X+10\,.$$

Das multiplikative Inverse von drei modulo elf ist vier, bei der Division durch drei müssen wir also mit vier multiplizieren:

$$\begin{gathered}(X^8+X^6+8X^4+8X^3+8X^2+2X+6) : (3X^6+5X^4+7X^2+2X+10) = 4X^2+1 \quad \text{Rest } 8X^4+5X^2+7 \\ (3X^6 + 5X^4 + 7X^2 + 2X + 10) : (8X^4 + 5X^2 + 7) = 10X^2 + 4 \quad \text{Rest } 5X^2 + 2X + 4 \\ (8X^4 + 5X^2 + 7) : (5X^2 + 2X + 4) = 6X^2 + 2X + 2 \quad \text{Rest } 10X + 10 \\ (5X^2 + 2X + 4) : (10X + 10) = 6X + 3 \quad \text{Rest } 7\end{gathered}$$

Da sieben in $\mathbb{F}_{11}$ eine Einheit ist, ist der ggT in $\mathbb{F}_{11}[X]$ gleich eins. Da elf die führenden Koeffizienten von f und g nicht teilt und beide Polynome primitiv sind, folgt, daß auch der ggT von f und g in $\mathbb{Z}[X]$ eins ist.

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 $p = 11$!

Lösung: Beide Polynome sind primitiv; wir müssen also keine Inhalte ausklammern.

Wir berechnen zunächst die LANDAU-MIGNOTTE-Schranke:

$$\|f\|_2 = \sqrt{1^1 + 2^2 + 1^2 + 2^2 + 1^2 + 2^2} = \sqrt{15}$$

und

$$\|g\|_2 = \sqrt{1^2 + 2^2 + 1^2 + 1^2 + 2^2} = \sqrt{11}\,,$$

beide führenden Koeffizienten sind eins und das Minimum der Grade ist vier. Somit ist

$$\mathrm{LM}(f,g) = 2^4\sqrt{11} \approx 53{,}066\,,$$

die Höhe des ggT ist also höchstens 53. Da $11^2 = 121$ größer als das Doppelte davon ist, kennen wir den ggT, wenn wir ihn modulo 11^2 kennen.
Dazu müssen zunächst den ggT von f mod 11 und g mod 11 bestimmen:

$$(X^5 + 9X^4 + 10X^3 + 2X^2 + X + 9) : (X^4 + 9X^3 + 10X^2 + X + 2) = X \quad \text{Rest } X^2 + 10X + 9$$
$$(X^4 + 9X^3 + 10X^2 + X + 2) : (X^2 + 10X + 9) = X^2 + 10X \quad \text{Rest } 10X + 2$$
$$(X^2 + 10X + 9) : (10X + 2) = 10X + 10 \quad \text{Rest } 0$$

Der ggT ist also $10X + 2$ oder, da es auf Einheiten aus $\mathbb{F}_{11}[X]$ nicht ankommt, $X + 9$.
Polynomdivision zeigt, daß

$$f \equiv (X+9)(X^4 + 10X^2 + 1) \bmod 11 \quad \text{und} \quad g \equiv (X+9)(X^3 + 10X + 10) \bmod 11$$

ist. $X+9$ hat in $\mathbb{F}_{11}$ die Nullstelle $x = 2$, bei der keiner der beiden Kofaktoren verschwindet. Wir haben also in beiden Fällen Produkte zweier in $\mathbb{F}_{11}[X]$ teilerfremder Polynome, die wir nach dem HENSELschen Lemma zu einer Faktorisierung modulo 11^2 hochheben können. Da g den kleineren Grad hat, empfiehlt es sich, diese Faktorisierung zu betrachten. Wir setzen also $h = X + 9$ und $k = X^3 + 10X + 10$; dann ist $g \equiv hk \bmod 11$, und wir suchen Polynome $\widetilde{h} = h + 11h'$ sowie $\widetilde{k} = k + 11k'$, so daß $g \equiv \widetilde{h} \cdot \widetilde{k} \bmod 11^2$ ist, d.h.

$$g \equiv hk + 11(hk' + kh') \bmod 11^2\,.$$

Da $g - hk = -11X^3 - 11X^2 - 99X - 88 = -11(X^3 - X^2 - 9X - 8)$ ist, müssen h' und k' die Kongruenz

$$hk' + kh' \equiv g_0 = -X^3 - X^2 - 9X - 8 \bmod 11$$

erfüllen. Wir stellen zunächst, nach dem erweiterten EUKLIDischen Algorithmus, die Eins als Linearkombination in $\mathbb{F}_{11}[X]$ dar:

$$(X^3 + 10X + 10) : (X + 9) = X^2 + 2X + 3 \quad \text{Rest } 5\,.$$

Somit ist $5 = k - (X^2 + 2X + 3)h$, und da modulo elf $5 \cdot 9 \equiv 1$ ist, folgt

$$1 = 9k + (2X^2 + 4X + 6)h \quad \text{in } \mathbb{F}_{11}[X]\,.$$

Diese Gleichung müssen wir mit g_0 multiplizieren und alle Koeffizienten modulo elf betrachten; wir erhalten

$$g_0 = (2X^3 + 2X^2 + 7X + 5)k + (9x^5 + 5x^4 + 5x^3 + 8x^2 + 2x + 7)h\,.$$

Das ist natürlich noch nicht die Darstellung die wir wollen; durch Addition eines Vielfachen der Gleichung $0 = hk - kh$ können wir erreichen, daß der Faktor vor k kleineren Grad als h hat und der vor h kleineren als k.

$$(2X^3 + 2X^2 + 7X + 5) : (X + 9) = (2X^2 + 6X + 8) \quad \text{Rest } 10\,,$$

wir subtrahieren als das $(2X^2 + 6X + 8)$-fache von $hk - kh$ und erhalten

$$g_0 = 10k + (10X + 10)h\,.$$

Wir setzen also $h' = 10$ und $k' = 10X + 10$; dies führt zu

$$\widetilde{h} = h + 11h' = X + 9 + 11 \cdot 10 = X + 119$$

und

$$\widetilde{k} = k + 11k' = X^3 + 10X + 10 + 110X + 110 = X^3 + 120X + 120\,.$$

Die Koeffizienten hier liegen über der LANDA-MIGNOTTE-Schranke von 53; Polynome, die modulo 121 kongruent $\widetilde{h}$ und $\widetilde{k}$ sind und Koeffuzienten mit einem Betrag von höchstens 53 haben, sind $X-2$ und X^3-X-1. Ihr Produkt in $\mathbb{Z}[X]$ ist gleich g, unser Kandidat $X-2$ für den ggT ist also zumindest ein Teiler von g. Da $f(2) = 0$ ist, teilt er auch f, ist also der gesuchte ggT von f und g.

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

Lösung: Es gibt keine Primzahlen, die beide führenden Koeffizienten teilen; problematisch sind also nur die Primzahlen, modulo derer $f/(X-2) = X^4-X^2+1$ und $g/(X-2) = X^3-X-1$ einen gemeinsamen Teiler positiven Grades haben. Das sind genau die Primteiler der über $\mathbb{Z}$ berechneten Resultante der beiden Polynome. Diese Determinante einer 7×7-Matrix lassen wir besser von einem Computeralgebrasystem berechen; das Eregebnis ist eins. Somit hat dieses ggT-Problem modulo jeder Primzahl gute Reduktion.