

Übungen zur Vorlesung Computeralgebra  
Blatt 1

---

Prof. Dr. Klaus Madlener

---

**1. Aufgabe:** [Ringe und Körper]

Wir wollen einige einfache Sätze zeigen:

- a) Sei  $R$  ein Integritätsbereich, ferner seien  $a, b \in R^*$  (die Menge der von 0 verschiedenen Elemente von  $R$ ). Es sind  $a$  und  $b$  genau dann assoziiert, wenn es ein  $u \in E(R)$  (die Einheitengruppe von  $R$ ) mit  $a = ub$  gibt.
- b) Sei  $R$  ein euklidischer Ring und sei  $I$  ein Ideal von  $R$ . Ist  $0 \neq a \in I$ , so ist genau dann  $I = aR$ , wenn  $v(a) \leq v(b)$  für alle  $b \in I \setminus \{0\}$  ist (wobei  $v$  die Bewertungsfunktion von  $R$  sei).  
Zeigen Sie, dass weiter folgt, dass  $R$  ein Hauptidealring ist (d. h., dass alle Ideale von  $R$  Hauptideale sind).
- c) Ist  $K$  ein Körper, so ist  $K[x]$  ein euklidischer Ring.
- d) Ist  $K$  ein Körper und  $L$  eine Erweiterung von  $K$  (also ein Körper, der  $K$  als Teilkörper enthält), ist weiter  $f \in K[x]$  und  $\ell \in L$  eine Nullstelle von  $f$ , so ist  $f$  in  $L[x]$  durch  $x - \ell$  teilbar.

**2. Aufgabe:** [Polynomdivision]

Wir untersuchen die Laufzeit der klassischen Polynomdivision mit Rest. Gegeben sei folgender Algorithmus:

**function** POLYQUOREM( $a, b$ )

$a = \sum_{0 \leq i \leq n} a_i x^i$ ,  $b = \sum_{0 \leq i \leq m} b_i x^i \in R[x]$ ,  $R$  ist ein kommutativer Ring mit 1, alle  $a_i, b_i \in R$ ,  $b_m$  ist eine Einheit in  $R$  und  $n \geq m \geq 0$ .  
Ausgabe:  $q, r \in R[x]$  mit  $a = qb + r$  und  $\deg r < m$  oder  $r = 0$ .

$r \leftarrow a$

**for**  $i \leftarrow n - m, n - m - 1, \dots, 0$  **do**

**if**  $\deg(r) = m + i$  **then**

$q_i \leftarrow \text{lc}(r)/b_m$ ;  $r \leftarrow r - q_i x^i b$

**else**  $q_i \leftarrow 0$

**end if**

**end for**

**return**  $q = \sum_{0 \leq i \leq n-m} q_i x^i$  und  $r$

**end function**

Nehmen Sie an, dass ein Polynom  $p = \sum_{0 \leq i \leq k} p_i x^i$  vom Grad  $k$  durch eine dichte Darstellung gegeben sei, d. h. im Wesentlichen durch einen Koeffizientenvektor  $\vec{p} = (p_0, \dots, p_k)$ .

Geben Sie die Laufzeit, gemessen in der Anzahl von Ringoperationen in  $R$ , im schlechtesten Fall in Abhängigkeit von  $n$  und  $m$  an. Sind  $q$  und  $r$  im Allgemeinen eindeutig? Beweis!

**3. Aufgabe:** [Diophantische Gleichungen]

Gibt es  $s, t \in \mathbb{Z}$ , so dass  $24s + 14t = 1$  bzw. so dass  $61s + 37t = 56$ ? Geben Sie jeweils alle möglichen Lösungen an.

Zeigen Sie allgemeiner: Die lineare diophantische Gleichung  $ax + by = c$  mit  $a, b, c \in \mathbb{Z}$  ist genau dann (in  $\mathbb{Z}$ ) lösbar, wenn für  $d = \text{GGT}(a, b)$  gilt:  $d|c$ . Ist in diesem Fall  $(x_0, y_0)$  eine spezielle Lösung, dann ist

$$\{(x_0 + k \cdot \frac{b}{d}, y_0 - k \cdot \frac{a}{d} \mid k \in \mathbb{Z}\}$$

die Menge alle Lösungen. (Was bedeutet eigentlich die Schreibweise  $\frac{a}{d}$  in diesem Zusammenhang?)

**4. Aufgabe:** [GGT]

a) Berechnen Sie größte gemeinsame Teiler von  $f = x^5 + x^4 + x^3 - x^2 - x + 1$  und  $g = x^3 + x^2 + x + 1$  ( $f, g \in \mathbb{Z}_p[x]$ ) für  $p = 3$  sowie  $p = 5$ . Berechnen Sie jeweils auch Polynome  $s$  und  $t$  mit  $\text{ggT}(f, g) = sf + tg$ .

b) Wir betrachten den folgenden ggT-Algorithmus nach J. Stein (war möglicherweise aber schon im antiken China bekannt):

```

1: function BINARYGCD( $u, v \in \mathbb{N}^+$ )                                ▷ Returns the g.c.d of  $u$  and  $v$ 
2:    $g \leftarrow 1$ 
3:   while ( $u \bmod 2 = 0$ )  $\wedge$  ( $v \bmod 2 = 0$ ) do
4:      $u \leftarrow u/2; v \leftarrow v/2; g \leftarrow 2g$ 
5:   end while
6:   while ( $u \neq 0$ ) do
7:     if ( $u \bmod 2 = 0$ ) then
8:        $u \leftarrow u/2$ 
9:     else if ( $v \bmod 2 = 0$ ) then
10:       $v \leftarrow v/2$ 
11:    else
12:       $t \leftarrow |u - v|/2$ 
13:      if  $u \geq v$  then
14:         $u \leftarrow t$ 
15:      else
16:         $v \leftarrow t$ 
17:      end if
18:    end if
19:  end while
20:  return  $g \cdot v$ 

```

21: **end function**

Zeigen Sie, dass dieser Algorithmus tatsächlich für Eingaben  $u, v \in \mathbb{N}^+$  den Wert  $\text{ggT}(u, v)$  berechnet, und zwar mit  $O((\lambda(uv))^2)$  Bitoperationen im schlechtesten Fall. Dafür nehmen wir an, dass Zahlen aus  $\mathbb{N}^+$  in Binärdarstellung gegeben sind und  $\lambda(x)$  die Länge der Binärdarstellung (ohne führende Nullen) von  $x$  bezeichnet. Zeigen Sie abschließend, dass im schlechtesten Fall  $O(\lambda(u)\lambda(v))$  Bitoperationen *nicht* ausreichen.

**5. Aufgabe:** [GGT]

- a) Zu Satz 2.13: Sei  $F_i$  für  $i \in \mathbb{N}$  die  $i$ -te Fibonacci-Zahl (also  $F_0 = 0$ ,  $F_1 = 1$  und  $F_i = F_{i-1} + F_{i-2}$  für  $i \geq 2$ ). Zeigen Sie, dass  $\lfloor F_{i+2}/F_{i+1} \rfloor = 1$  und  $F_{i-1} = F_{i+1} \bmod F_i$  für alle  $i \geq 2$ .
- b) Sei  $F[x]$  der euklidische univariate Polynomring über einem Körper  $F$ . Seien weiter  $a, b \in F[x] \setminus \{0\}$  und  $g = \text{ggT}(a, b) \in F[x]$ . Zeigen Sie, dass es dann für jedes Polynom  $c \in F[x]$  mit  $g \mid c$  eindeutige Polynome  $\sigma, \tau \in F[x]$  gibt, so dass  $\sigma a + \tau b = c$  und  $\deg(\sigma) < \deg(b) - \deg(g)$  gilt; wenn zudem noch  $\deg(c) < \deg(a) + \deg(b) - \deg(g)$  ist, so gilt  $\deg(\tau) < \deg(a) - \deg(g)$ .
- c) Seien  $a, b \in \mathbb{N}^+$  und  $a > b$ . Wir wollen entscheiden, ob es  $i, j \in \mathbb{N}^+$  gibt, so dass  $a^i = b^j$  ist. Betrachten Sie dazu folgendes Entscheidungsverfahren für dieses Problem:

Teste zuerst, ob  $b \mid a$ . Wenn nicht, so antworte „nein“. Ansonsten ersetze  $(a, b)$  durch  $(a/b, b)$ , wenn  $a \geq b^2$ , bzw. durch  $(b, a/b)$ , wenn  $a < b^2$ . Wenn durch Iterieren schließlich ein Paar  $(a', 1)$  erreicht wird, antworte „ja“.

Zeigen Sie, dass dieses Verfahren das Problem für jede Eingabe korrekt löst (und terminiert) und im schlechtesten Fall  $O(\lambda(a)^2)$  Bitoperationen benötigt.

**6. Aufgabe:** [Division in  $\mathbb{Z}$ ]

- a) Wir betrachten noch einmal den Algorithmus zur Division mit Rest nicht negativer ganzer Zahlen zur Basis  $b \geq 2$ . Es seien  $u = (u_0 \cdots u_n)_b$  sowie  $v = (v_1 \cdots v_n)_b$  mit  $\lfloor u/v \rfloor < b$ . Es sei wie in der Vorlesung  $\hat{q} = \min \left( \left\lfloor \frac{u_0 b + u_1}{v_1} \right\rfloor, b - 1 \right)$  die Schätzung für  $q = \lfloor u/v \rfloor$  mit  $u = qv + r$  und  $0 \leq r < v$ .

Zeigen Sie, dass  $\hat{q} \geq q$  und für  $v_1 \geq \lfloor b/2 \rfloor$  auch  $\hat{q} - 2 \leq q$ .

- b) Finden Sie ein Beispiel für  $u$  und  $v$  bei Basis 10, so dass die Notwendigkeit der bedingten Anweisung

**if**  $(u_j \cdots u_{j+n})_b < \hat{q} \cdot (v_1 \cdots v_n)_b$  **then**  $\hat{q} := \hat{q} - 1$

im Algorithmus aus der Vorlesung klar wird.

Übungen zur Vorlesung Computeralgebra  
Blatt 3

Prof. Dr. Klaus Madlener

---

**7. Aufgabe:** [Ringe]

- a) Ist für Integritätsbereiche  $R, S$  der Ring  $R+S$  (die direkte Summe) ebenfalls immer ein Integritätsbereich? Zeigen oder widerlegen Sie.
- b) Sei  $I = \{f \in \mathbb{R}[x] \mid f(5) = 0\}$  die Menge der reellen Polynome, die 5 als eine Nullstelle haben. Zeigen Sie, dass  $I$  ein Ideal in  $\mathbb{R}[x]$  ist. Geben Sie einen Isomorphismus  $\mathbb{R}[x]/I \rightarrow \mathbb{R}$  an.

**8. Aufgabe:**

- a) Bestimmen Sie in  $\mathbb{Z}[[x]]$  das Inverse zur formalen Potenzreihe

$$a(x) = \sum_{k=0}^{\infty} a_k x^k = 1 + x + 2x^2 + 3x^3 + 5x^4 + \dots$$

mit  $a_k = a_{k-1} + a_{k-2}$  für  $k \geq 2$ .

**9. Aufgabe:** [Simplifikation]

- a) Betrachten Sie die folgende „Definition“ einer *expandierten kanonischen Form* für multivariate Polynom-Ausdrücke über einem Integritätsbereich  $D$ :
1. Ausmultiplizieren aller Produkte von Polynomen
  2. Terme gleichen Grades zusammenfassen
  3. Terme nach fallenden Grad ordnen

Ist dies ein kanonischer Simplifikator gemäß der Definition aus der Vorlesung? Welche Angaben brauchen Sie, um diese Frage beantworten zu können? Ist die obige Definition eindeutig?

Wenden Sie die Vorschrift auf folgenden Ausdruck an:

$$a(x, y) = ((x^2 - xy + x) + (x^2 + 3) \cdot (x - y + 1)) \cdot ((y^3 - 3y^2 - 9y - 5) + x^4 \cdot (y^2 + 2y + 1))$$

- b) Finden Sie „einfachste“ Ausdrücke, die äquivalent zu den folgenden Ausdrücken sind:

$$- a(x, y) = \frac{1}{x^9 + x^8y + x^7y^2 + x^6y^3 + x^5y^4 + x^4y^5 + x^3y^6 + x^2y^7 + xy^8 + y^9}$$

$$- b(x, y) = \frac{x - 4}{x^5 + x^4y + x^3y^2 + x^2y^3 + xy^4 + y^5} - \frac{x^2 - xy + y^2}{x^6 - y^6}$$

- c) Wir betrachten ein freies Monoid  $M = (\Sigma, \circ)$ , wobei die Monoid-Elemente die Wörter über dem Alphabet  $\Sigma$  sind, das neutrale Element  $\epsilon$  das leere Wort über dem Alphabet  $\Sigma$  ist und  $\circ$  eine assoziative Abbildung von Paaren auf Wörtern auf ein Wort ist mit  $a \circ b = ab, a, b \in \Sigma^*$ . Für ein  $w \in M$  sei  $(w)^n, n \in \mathbb{N}_+$  definiert durch  $(w)^1 = w$  und  $(w)^n = w(w)^{n-1}$ . Überlegen Sie sich, wie hier Normalformen minimaler Länge von Wörtern aus  $M$  aussehen, d.h. es sollen Terme mit möglichst wenige Symbolen gefunden werden, die dasselbe Wort darstellen. Können Sie einen effizienten Algorithmus angeben, der diese Normalformen berechnet?

### 10. Aufgabe: [Potenzen]

Sei  $n \in \mathbb{N}^+$ . Eine Additions-kette für  $n$  ist eine endliche Folge positiver ganzer Zahlen  $a_0, \dots, a_r$  mit  $a_0 = 1, a_r = n$ , und für alle  $i = 1, \dots, r$  gibt es  $j$  und  $k$  mit  $k \leq j < i$ , so dass  $a_i = a_j + a_k$ ;  $r$  bezeichnen wir als die Länge der Additions-kette. Es bezeichne weiter  $l(n)$  die minimale Länge einer Additions-kette für  $n$ .

- a) Welcher Zusammenhang besteht zwischen  $l(n)$  und der Berechnung von  $x^n$ ? Ist die Anzahl der Multiplikationen der binären Potenzierungsmethode zur Berechnung von  $x^n$  immer minimal?
- b) Sei  $s(n)$  die Summe der Bits in der Binärdarstellung von  $n$  (also die Anzahl der Einsen). Zeigen Sie:  $l(n) \leq \lfloor \log_2 n \rfloor + s(n) - 1$  und  $l(mn) \leq l(m) + l(n)$ .
- c) Seien  $a > b \geq 0$  ganze Zahlen. Zeigen Sie, dass  $l(2^a) = a$  und  $l(2^a + 2^b) = a + 1$ .

### 11. Aufgabe: [Fibonacci]

- a) Wir wollen die Fibonacci-Zahlen  $F_k$  modulo  $n \in \mathbb{N}$  berechnen. Geben Sie eine asymptotische obere Schranke für die Anzahl der Bitoperationen eines naiven Verfahrens zur Berechnung von  $F_k$  modulo  $n$  im schlechtesten Fall an.

Ein anderes Verfahren benutzt die Tatsache, dass  $F_{k+1}$  sich wie folgt gewinnen lässt:

$$\begin{pmatrix} F_{k+1} & F_k \\ F_k & F_{k-1} \end{pmatrix} = \begin{pmatrix} F_k & F_{k-1} \\ F_{k-1} & F_{k-2} \end{pmatrix} \cdot X,$$

wobei  $X$  von Ihnen anzugeben ist. Konkretisieren Sie nun dieses Verfahren zur Berechnung von  $F_k$  modulo  $n$  und geben Sie ebenfalls eine asymptotische obere Schranke für die Anzahl der Bitoperationen im schlechtesten Fall an.

- b) Zeigen Sie, wie man  $1 + x + \dots + x^{n-1} \bmod m$  für  $x, n, m \in \mathbb{N}^+$  mit  $O(\lambda(n)\lambda(m)^2)$  Bitoperationen im schlechtesten Fall berechnet. Beachten Sie besonders den Fall, dass  $m$  keine Primzahl ist.

Übungen zur Vorlesung Computeralgebra  
Blatt 4

---

Prof. Dr. Klaus Madlener

---

**12. Aufgabe:** [Potenzreihen]

Gegeben sei ein Körper  $F$  der Charakteristik 0. Zeigen Sie: Die Koeffizienten  $a_k \in F$  für  $k \geq K$  ( $K$  fest) einer Potenzreihe  $a(x) = \sum_{k=0}^{\infty} a_k x^k$  können genau dann durch eine lineare Rekurrenzgleichung mit konstanten Koeffizienten  $a_k = u_1 a_{k-1} + u_2 a_{k-2} + \dots + u_n a_{k-n}$  ( $n$  fest) über  $F$  dargestellt werden, wenn  $a(x)$  als rationale Funktion in  $x$  über  $F$  dargestellt werden kann.

**13. Aufgabe:** [Pseudo-Restefolgen]

Untersuchen Sie, ob die polynomialen Pseudo-Restefolgen aus der Vorlesung tatsächlich zur ggT-Berechnung verwendet werden können. Zeigen Sie dazu:

Sind  $a(x)$  und  $b(x)$  primitive Polynome über einem ZPE-Ring  $D$  und ist  $f_1(x) = a(x)$ ,  $f_2(x) = b(x)$ ,  $f_3(x), \dots, f_{k-1}(x), f_k(x)$  eine polynomiale Restefolge für  $a(x)$  und  $b(x)$ , wobei  $f_k(x) = 0$  sei, so gilt:

$$\text{ggT}(a(x), b(x)) = \text{pp}(f_{k-1}(x)).$$

**14. Aufgabe:** [Anwendung]

Sei  $D$  ein euklidischer Ring mit Bewertungsfunktion  $\nu$ . Entwerfen Sie einen Algorithmus, der der folgenden Spezifikation genügt:

**Eingabe:** Eine positive ganze Zahl  $n$  sowie  $a, d_1, \dots, d_n \in D \setminus \{0\}$  mit  $\text{ggT}(d_i, d_j) = 1$  für  $i \neq j$ .

**Ausgabe:**  $a_0, a_1, \dots, a_n \in D$ , so dass

$$\frac{a}{d_1 \cdots d_n} = a_0 + \sum_{i=1}^n \frac{a_i}{d_i}$$

und entweder  $a_i = 0$  oder  $\nu(a_i) < \nu(d_i)$  für  $i \geq 1$ .

Begründen Sie auch, weshalb Ihr Algorithmus korrekt ist. Ist Ihnen dieser Algorithmus schon einmal begegnet?

**15. Aufgabe:** [Nachrichtenverifikation]

Nehmen Sie an, Alice und Bob hätten jeweils eine Nachricht von  $n$  Bit,  $M_A$  und  $M_B$ . Sie würden gerne verifizieren, dass ihre Nachrichten identisch sind, und zwar einerseits mit einer großen Wahrscheinlichkeit und andererseits mit wenig Kommunikationsaufwand. Insbesondere sei  $n$  so groß, dass ein Nachrichtenaustausch ausscheide.

Alice und Bob wählen  $k$  Primzahlen  $p_1, \dots, p_k$  uniform aus der Menge der ersten  $2n$  Primzahlen und prüfen dann, ob  $M_A \equiv M_B \pmod{p_i}$  für  $1 \leq i \leq k$ . Zeigen Sie, dass, wenn  $M_A = M_B$ , so ist  $M_A \equiv M_B \pmod{p_i}$  für alle  $i$ , während, wenn  $M_A \neq M_B$ , so ist  $M_A \not\equiv M_B \pmod{p_i}$  für ein  $i$  mit Wahrscheinlichkeit mindestens  $1 - 2^{-k}$ .

**16. Aufgabe:** [Karatsuba]

- a) Machen Sie sich klar, dass der Multiplikationsalgorithmus nach Karatsuba und Ofman (in der Vorlesung für Langzahlarithmetik eingeführt) auch für univariate Polynome funktioniert. Formulieren Sie eine entsprechende rekursive Prozedur.
- b) Zeigen Sie, dass dieser Algorithmus eine Multiplikation zweier Polynome vom Grade höchstens  $n$  (wobei  $n$  eine Zweierpotenz sei) mit höchstens  $9n^{\log_2 3} + O(n)$  Ringoperationen durchführt.

Zeigen Sie dazu folgendes Lemma:

Seien  $b, d \in \mathbb{N}$  mit  $b > 0$ , und seien  $S, T : \mathbb{N} \rightarrow \mathbb{N}$  Funktionen mit  $S(2n) \geq 2S(n)$  sowie  $S(n) \geq n$  für alle  $n \in \mathbb{N}$ . Es gelte  $T(1) = d$  und  $T(n) \leq bT(n/2) + S(n)$  für  $n = 2^i$  und  $i \in \mathbb{N}^+$ . Dann gilt für  $i \in \mathbb{N}$  und  $n = 2^i$ :

$$T(n) \leq \begin{cases} (2 - 2/n)S(n) + d \in O(S(n)) & \text{falls } b = 1, \\ S(n) \log_2 n + dn \in O(S(n) \log_2 n) & \text{falls } b = 2, \\ \frac{2}{b-2}(n^{\log_2 b-1} - 1)S(n) + dn^{\log_2 b} \in O(S(n)n^{\log_2 b-1}) & \text{falls } b \geq 3. \end{cases}$$

- c) überzeugen Sie sich, dass der Algorithmus nach Karatsuba und Ofman für „kleine“ Eingaben langsamer ist als der klassische Multiplikationsalgorithmus für Polynome.

Untersuchen Sie nun einen hybriden Algorithmus, der rekursiv die Karatsuba/Ofman-Idee anwendet, bis die Grade kleiner als eine Grenze  $2^d \in \mathbb{N}$  werden, und dann die klassische Multiplikation verwendet.

Zeigen Sie, dass dieser hybride Algorithmus höchstens  $\gamma(d)n^{\log_2 3} + O(n)$  Ringoperationen durchführt, wobei  $\gamma(d)$  nur von  $d$  abhängt. Finden Sie  $d$ , so dass  $\gamma(d)$  minimal ist. (Dazu brauchen Sie eine recht genaue Abschätzung für die Anzahl der Ringoperationen im klassischen Multiplikationsalgorithmus.)

Übungen zur Vorlesung Computeralgebra  
Blatt 5

Prof. Dr. Klaus Madlener

---

**17. Aufgabe:**

Entwickeln Sie Möglichkeiten, um diophantische Gleichungen auch in nicht-euklidischen Bereichen zu lösen. Betrachten Sie

1.  $ax + by \equiv c \pmod{n}$ , wobei  $n \in \mathbb{N}$ .
2. Beliebige diophantische Gleichungen über  $\mathbb{Z}[x]$ . (Vorsicht!)

**18. Aufgabe:**

Nehmen Sie an, dass ungerade und teilerfremde Moduli  $m_j$  gegeben seien. Außerdem sei  $u = (u_1, \dots, u_r)$  als Restvektor bezüglich der  $m_j$  dargestellt. Wie kann man (unter der Annahme, dass  $u$  ein Vielfaches von 2 ist)  $u/2$  modular berechnen?

**19. Aufgabe:**

- a) Sei  $F$  ein Körper,  $f(x)$  ein univariates Polynom über  $F$  und  $u \in F$ . Geben Sie eine Methode zur Berechnung von  $f(u)$  an, die mit möglichst wenigen Operationen in  $F$  auskommt.
- b) Verallgemeinern Sie diese Methode auf Polynome aus  $F[x, y]$  und geben Sie auch hier Abschätzungen für die Anzahl der Körperoperationen an.

**20. Aufgabe:**

- a) Geben Sie für  $n = 4$  und  $n = 8$  jeweils primitive Einheitswurzeln in  $\mathbb{C}$  an und berechnen Sie die Fouriertransformierten von  $(0, 1, 2, 3)$  und  $(1, 2, 0, 2, 0, 0, 0, 1)$ .
- b) Seien  $a(x) = -x^3 + 3x + 1$  und  $b(x) = 2x^4 - 3x^3 - 2x^2 + x + 1$  Polynome aus  $\mathbb{Z}_{17}[x]$ . Bestimmen Sie das Produkt dieser Polynome mit Hilfe der schnellen Fourier-Transformation.

**21. Aufgabe:**

Sei  $a(x)$  ein Polynom vom Grade  $3^n - 1$  mit  $n \geq 0$ .

- a) Zeigen Sie, dass  $a(x)$  als

$$a(x) = b(x^3) + x \cdot c(x^3) + x^2 \cdot d(x^3)$$

geschrieben werden kann; dabei sind  $b(x)$ ,  $c(x)$  und  $d(x)$  Polynome vom Grade kleiner oder gleich  $3^{n-1} - 1$ .

- b) Finden Sie Symmetriebedingungen ähnlich zu denen aus der Vorlesung, die es erlauben,  $a(x)$  an  $3^n$  Stellen auszuwerten, indem man drei geeignete Polynome jeweils an  $3^{n-1}$  geeigneten Stellen auswertet.
- c) Zeigen Sie, dass für eine primitive  $3^n$ -te Einheitswurzel  $\omega$  eines Körpers die Elemente  $1, \omega, \dots, \omega^{3^n-1}$  die Symmetriebedingungen aus b) erfüllen.
- d) Welches sind die Kosten der Auswertung von  $a(x)$  an den  $3^n$  in c) genannten Stellen?
- e) Verwenden Sie a) bis d), um einen 3-FFT-Algorithmus zu entwickeln und eine Abschätzung der Anzahl der Multiplikationen im Koeffizientenkörper anzugeben.

Übungen zur Vorlesung Computeralgebra  
Blatt 6

Prof. Dr. Klaus Madlener

**22. Aufgabe:**

- a) Seien  $f(x) = x^3 - x^2 + 2$  und  $g(x) = x^2 + x + 1$  Polynome über  $\mathbb{Q}$ . Berechnen Sie eine Darstellung von  $h(x) = x^4 + 2x$  als  $h(x) = p(x)f(x) + q(x)g(x)$  mit  $\deg p < 2$  und  $\deg q < 3$ .
- b) Berechnen Sie das Polynom  $r(x) \in \mathbb{Q}[x]$  kleinsten Grades, das die Kongruenzen

$$\begin{aligned} r(x) &\equiv 2x^2 + 1 \pmod{x^3 + x^2 - 1} \\ r(x) &\equiv x + 2 \pmod{x^2 + 2x + 2} \end{aligned}$$

erfüllt.

**23. Aufgabe:**

Wir betrachten den Algorithmus von Garner aus der Vorlesung.

- a) Der zweite Schritt benutzt die Formeln

$$\begin{aligned} \nu_0 &\equiv u_0 \pmod{m_0} \\ \nu_k &\equiv \left( u_k - \left( \nu_0 + \nu_1 m_0 + \cdots + \nu_{k-1} \prod_{i=0}^{k-2} m_i \right) \right) \left( \prod_{i=0}^{k-1} m_i \right)^{-1} \\ &\pmod{m_k} \text{ für } k \geq 1. \end{aligned}$$

Zeigen Sie, dass man die gemischten Basiskoeffizienten  $\nu_k$  auch mit Hilfe der Formeln

$$\begin{aligned} \nu_0 &\equiv u_0 \pmod{m_0} \\ \nu_k &\equiv \left( \cdots \left( (u_k - \nu_0)m_0^{-1} - \nu_1 \right) m_1^{-1} - \cdots - \nu_{k-1} \right) m_{k-1}^{-1} \\ &\pmod{m_k} \text{ für } k \geq 1 \end{aligned}$$

berechnen kann. (Beachten Sie: Die Inversen in dieser Formel sind Inverse modulo  $m_k$ .)

- b) Wenn man den zweiten Schritt wie in a) realisiert, welche Menge von Inversen muss dann im ersten Schritt berechnet werden? Wie viele Inverse werden benötigt?

- c) Vergleichen Sie die Zeitkomplexität beider Varianten. Betrachten Sie einmal den Fall, dass die Menge  $\{m_i\}$  der Reste fest ist, d. h. die Inversenbildung im ersten Schritt ein einen Vorberechnungsschritt ausgelagert werden kann, und auch den Fall, dass dies nicht möglich ist.

**24. Aufgabe:**

Bestimmen Sie mit Hilfe der 7-adischen linearen Newton-Iteration die dritte Wurzel des Polynoms

$$a(x) = x^6 - 531x^5 + 94137x^4 - 5598333x^3 + 4706850x^2 - 1327500x + 125000$$

mit  $a(x) \in \mathbb{Z}[x]$ . Führen Sie diese Rechnung mit Hilfe eines Computeralgebra-Systems durch.

**25. Aufgabe:**

- a) Es seien  $I = \langle x, y \rangle$  und  $J = \langle x \rangle$  Ideale in  $\mathbb{Z}[x, y]$ . Beschreiben Sie zunächst die Elemente von  $I$  und  $J$  sowie die Teilmengenbeziehung zwischen  $I$  und  $J$ . Beschreiben Sie dann die Elemente von  $I + J$ ,  $I \cdot J$  und  $I^2$  und geben Sie erzeugende Elemente dieser Ideale an. Untersuchen Sie schließlich die Teilmengenbeziehungen zwischen  $I + J$ ,  $I \cdot J$  und  $I^2$ .
- b) Beschreiben Sie das Ideal  $\langle x^e \rangle$ , wobei  $e \in \mathbb{N}$  fest sei, in  $\mathbb{Q}[[x]]$ .
- c) Betrachten Sie den kanonischen Homomorphismus

$$\phi_{\langle x^e \rangle} : \mathbb{Q}[[x]] \rightarrow \mathbb{Q}[[x]]/\langle x^e \rangle.$$

Beschreiben Sie die Elemente des homomorphen Bildes in  $\mathbb{Q}[[x]]/\langle x^e \rangle$ . Geben Sie auch eine praktische Darstellung dieser Elemente an.

- d) Geben Sie eine Darstellung der Elemente von  $\mathbb{Q}[x]/\langle x^2 + 1 \rangle$  an. Zeigen Sie, dass dieser Quotientenring ein Körper ist.
- e) Beschreiben Sie  $\mathbb{R}[x]/\langle x^2 + 1 \rangle$ .
- f) Ist  $\mathbb{Z}[x]/\langle x^2 + 1 \rangle$  ein Körper? Ein Integritätsbereich? Beschreiben Sie den Zusammenhang zwischen diesem Quotientenring und den ganzen Gaußschen Zahlen  $G = \{a + b \cdot \sqrt{-1} \mid a, b \in \mathbb{Z}\}$ .

Übungen zur Vorlesung Computeralgebra  
Blatt 7

Prof. Dr. Klaus Madlener

---

**26. Aufgabe:**

Betrachten Sie den Algorithmus aus der Vorlesung (F 102) zur Bestimmung eines polynomialen Inversen  $g \in D[x]$  modulo  $x^\ell$  ( $\ell \in \mathbb{N}$ ) zu gegebenem  $f \in D[x]$  mit  $f(0) = 1$ . Zeigen Sie, dass, wenn  $\ell = 2^r$  eine Zweierpotenz ist, die Rechenzeit des Algorithmus höchstens  $3M(\ell) + \ell \in O(M(\ell))$  Operationen in  $D$  beträgt. ( $M(n)$  bezeichne die Rechenzeit einer Multiplikation zweier Polynome vom Grade  $\leq n$ .)

Wie könnte man vorgehen, um im Falle, dass  $\ell$  keine Zweierpotenz ist, die Berechnung zu vieler Koeffizienten des polynomialen Inversen zu vermeiden?

Zeigen Sie weiter, dass die Rechenzeit des Algorithmus aus der Vorlesung auf  $2M(\ell)$  Operationen in  $D$  fällt wenn  $\text{char}(D) = 2$  ist.

**27. Aufgabe:**

Sei  $R$  ein kommutativer Ring mit 1,  $F \in R[y]$ ,  $g \in R$ , wobei  $F(g) \equiv 0 \pmod{p}$  und  $F'(g)$  invertierbar modulo  $p$  sei, sei eine Anfangslösung, und  $\ell \in \mathbb{N}^+$ .

Zeigen Sie: Wenn  $h, h^* \in R$  Lösungen modulo  $p^\ell$  mit  $h \equiv g \equiv h^* \pmod{p}$  sind und  $F(h) \equiv 0 \equiv F(h^*) \pmod{p^\ell}$  gilt, so ist  $h \equiv h^* \pmod{p^\ell}$ .

**28. Aufgabe:**

Berechnen Sie in  $\mathbb{Z}_3[x, y, z]$  mit Hilfe der ideal-adischen Iteration und dem Ideal

$$I = \langle y - 1, z \rangle \subseteq \mathbb{Z}_3[x, y, z]$$

die Lösung der Gleichung

$$u^2 - u = x^6 + x^4y^2 + 2x^3z + x^2y^4 + xy^2z + z^2 + 2.$$

Bestimmen Sie dazu zunächst die  $I$ -adische Darstellung des Polynoms auf der rechten Seite.

Übungen zur Vorlesung Computeralgebra  
Blatt 8

Prof. Dr. Klaus Madlener

**29. Aufgabe:**

Zeigen Sie den Satz 5.18 auf Folie 260: Der Algorithmus für den quadratischen Hensel-Lifting-Schritt ist korrekt.

**30. Aufgabe:**

Betrachten Sie das Faktorisierungsbeispiel aus der Vorlesung: Sei  $a(x) = 12x^3 + 10x^2 - 36x + 35 \in \mathbb{Z}[x]$ ; eine Faktorisierung modulo 5 ist

$$\phi_5(a(x)) = 2 \cdot x \cdot (x^2 + 2) \in \mathbb{Z}_5[x].$$

Wenden Sie quadratisches Hensel-Lifting (s. F 257f.) an, um eine Faktorisierung von  $a(x)$  in  $\mathbb{Z}[x]$  zu berechnen.

**31. Aufgabe:**

Wir definieren für ein Polynom  $f = \sum_{0 \leq i \leq n} f_i x^i = f_n \prod_{1 \leq i \leq n} (x - z_i) \in \mathbb{C}[x]$  das Landau-Maß  $M(f)$  durch

$$M(f) = |f_n| \cdot \prod_{1 \leq i \leq n} \max\{1, |z_i|\},$$

wobei  $f_0, \dots, f_n, z_1, \dots, z_n \in \mathbb{C}$ . Weiter definieren wir noch die Maximumsnorm  $\|f\|_\infty$ , die 1-Norm  $\|f\|_1$  und die 2-Norm  $\|f\|_2$  durch

$$\begin{aligned} \|f\|_\infty &= \max_{0 \leq i \leq n} |f_i| \\ \|f\|_1 &= \sum_{0 \leq i \leq n} |f_i| \\ \|f\|_2 &= \sqrt{\sum_{0 \leq i \leq n} |f_i|^2}. \end{aligned}$$

Dabei ist  $|a| = \sqrt{a\bar{a}}$  für  $a \in \mathbb{C}$  ( $\bar{a}$  ist die  $\mathbb{C}$ -Konjugierte zu  $a$ ).

- a) Zeigen Sie, dass für jedes  $f \in \mathbb{C}[x]$  gilt: (a.1)  $M(f) \geq |f_n|$ , (a.2)  $M(f) = M(g)M(h)$ , falls  $f = gh$  mit  $g, h \in \mathbb{C}[x]$ , und (a.3)  $M(f) \leq \|f\|_2$ .
- b) Wenn  $h = \sum_{0 \leq i \leq m} h_i x^i \in \mathbb{C}[x]$  vom Grad  $m$  ein Teiler von  $f = \sum_{0 \leq i \leq n} f_i x^i \in \mathbb{C}[x]$  vom Grad  $n \geq m$  ist, so gilt:

$$\|h\|_2 \leq \|h\|_1 \leq 2^m M(h) \leq 2^m \left| \frac{h_m}{f_n} \right| \|f\|_2.$$

- c) Nun zum eigentlichen Ziel: Seien  $f, g, h \in \mathbb{Z}[x]$  mit  $\deg f = n \geq 1$ ,  $\deg g = m$ ,  $\deg h = k$  und es sei  $gh$  ein Teiler von  $f$  in  $\mathbb{Z}[x]$ . Zeigen Sie

$$\|g\|_{\infty} \|h\|_{\infty} \leq 2^{m+k} \|f\|_2 \leq \sqrt{n+1} \cdot 2^{m+k} \|f\|_{\infty}$$

sowie

$$\|h\|_{\infty} \leq \sqrt{n+1} \cdot 2^k \|f\|_{\infty}.$$

**32. Aufgabe:**

Sei  $f(x, y) = f_0x^d + f_1x^{d-1}y + f_2x^{d-2}y^2 + \dots + f_dy^d$  ein bivariates homogenes Polynom. Geben Sie eine Reduktion des Faktorisierungsproblems für solche Polynome auf das Faktorisierungsproblem für univariate Polynome an.

Übungen zur Vorlesung Computeralgebra  
Blatt 9

---

Prof. Dr. Klaus Madlener

---

**33. Aufgabe:**

Zeigen oder widerlegen Sie:

- Das Polynom  $x^{1000} + 2 \in \mathbb{Z}_5[x]$  ist quadratfrei.
- Sei  $F$  ein Körper und seien  $f, g \in F[x]$ . Dann ist der quadratfreie Anteil von  $fg$  das Produkt der quadratfreien Anteile von  $f$  und  $g$ .

Der quadratfreie Anteil eines Polynoms  $h = \prod_{1 \leq i \leq r} h_i^{e_i}$  ist dabei  $\prod_{1 \leq i \leq r} h_i$  (mit paarweise verschiedenen irreduziblen  $h_i$ ).

**34. Aufgabe:**

Faktorisieren Sie das Polynom  $x^8 + x^7 + 2x^6 + 3x^5 + 3x^4 + 3x^3 + 2x^2 + 2x + 1$  mit der Distinct-Degree-Methode jeweils über  $\mathbb{Z}_7[x]$ ,  $\mathbb{Z}_{19}[x]$  und  $\mathbb{Z}_{23}[x]$ .

**35. Aufgabe:**

Wie viele Faktoren hat  $a(x) = x^4 + 1 \in \mathbb{Z}_p[x]$  ( $p$  prim), wenn (i)  $p = 2$ , (ii)  $p \equiv 1 \pmod{8}$ , (iii)  $p \equiv 3 \pmod{8}$  bzw. (iv)  $p \equiv 5 \pmod{8}$ ?

**36. Aufgabe:**

Machen Sie sich mit den Begriffen Sylvestermatrix und Resultante vertraut, z.B. Modern Computer Algebra, von zur Gathen, Kap. 6.3 S. 142-147, oder Algorithms for Computer Algebra, Geddes, Kap. 7.3, S. 285-288.

Zeigen Sie: Seien  $f, g \in \mathbb{Z}[x]$ ,  $r = \text{res}(f, g) \in \mathbb{Z}$ , und  $u \in \mathbb{Z}$ . Dann gilt  $\text{ggT}(f(u), g(u)) \mid r$ .

**37. Aufgabe:**

Sei  $p \in \mathbb{Z}$  prim und  $n > 1$ . Zeigen Sie die folgenden „pathologischen“ Eigenschaften von  $R = \mathbb{Z}_{p^n}[x]$  ( $f, g \in R$ ):

- Es gilt nicht notwendigerweise  $\deg fg = \deg f + \deg g$ .
- $R$  ist kein ZPE-Ring.
- Es ist  $\text{ggT}(f, g)$  nicht notwendigerweise als Linearkombination von  $f$  und  $g$  darstellbar.

Übungen zur Vorlesung Computeralgebra  
Blatt 10

Prof. Dr. Klaus Madlener

**38. Aufgabe:**

Sei  $p \in \mathbb{N}$  eine Primzahl und  $q = p^k$  für ein positives  $k \in \mathbb{N}$ ,  $f \in \mathbb{F}_q[x]$  ein monisches und quadratfreies Polynom vom Grade  $n$  sowie  $R = \mathbb{F}_q[x]/\langle f \rangle$ . Wir können den Frobenius-Endomorphismus  $\alpha \mapsto \alpha^q$  von  $R$  über  $\mathbb{F}_q$  im Berlekamp-Algorithmus von F 182 durch den absoluten Frobenius-Endomorphismus  $\alpha \mapsto \alpha^p$  von  $R$  über dem Primkörper  $\mathbb{F}_p$  ersetzen. Untersuchen Sie diese Variante und vergleichen Sie ihre Laufzeit mit der des ursprünglichen Algorithmus.

**39. Aufgabe:**

für  $n \in \mathbb{N}^+$  sei

$$\Phi_n = \prod_{\substack{1 \leq k \leq n \\ \text{ggT}(k,n)=1}} (x - e^{2\pi i k/n}) = \prod_{\substack{\omega \in \mathbb{C} \text{ ist eine } n\text{-te} \\ \text{primitive EW}}} (x - \omega) \in \mathbb{C}[x]$$

das  $n$ -te Kreisteilungspolynom (siehe z. B. Heinz Lüneburg, *Galoisfelder, Kreisteilungskörper und Schieberegisterfolgen*, Bibliographisches Institut, 1979). Es gilt  $\deg \Phi_n = \varphi(n)$ .

a) Zeigen Sie:  $x^n - 1 = \prod_{d|n} \Phi_d$ .

b) Die Möbiusfunktion  $\mu : \mathbb{N}^+ \rightarrow \{-1, 0, 1\}$  ist erklärt durch

$$\mu(n) = \begin{cases} 1 & \text{falls } n = 1, \\ (-1)^k & \text{falls } n \text{ das Produkt von } k \text{ verschiedenen Primzahlen ist,} \\ 0 & \text{falls } n \text{ nicht quadratfrei ist.} \end{cases}$$

Es gilt folgende Inversionsformel: Sei  $R$  ein kommutativer Ring mit 1 und  $f, g : \mathbb{N}^+ \rightarrow R$  seien zwei Funktionen mit

$$f(n) = \sum_{d|n} g(d) \text{ für } n \in \mathbb{N}^+.$$

Dann gilt:

$$g(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) f(d) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) \text{ für } n \in \mathbb{N}^+.$$

Geben Sie nun unter Beachtung von a) eine Formel für  $\Phi_n$  an.

c) Seien  $n, k \in \mathbb{N}^+$ . Dann gilt:

- (i)  $\Phi_n = x^{n-1} + x^{n-2} + \dots + x + 1$ , falls  $n$  prim ist.
  - (ii)  $\Phi_{2n} = \Phi_n(-x)$ , falls  $n > 3$  und  $n$  ungerade ist.
  - (iii)  $\Phi_{kn}\Phi_n = \Phi_n(x^k)$ , falls  $k$  prim ist und  $n$  nicht teilt.
  - (iv)  $\Phi_{kn} = \Phi_n(x^k)$ , falls jeder Primteiler von  $k$  auch  $n$  teilt.
- d) Geben Sie unter Verwendung der Ergebnisse aus c) einen Algorithmus an, der aus  $n \in \mathbb{N}^+$  und den verschiedenen Primteilern  $p_1, \dots, p_r$  von  $n$  das Polynom  $\Phi_n$  berechnet. Ihr Algorithmus soll eine Laufzeit von  $O(M(n) \log n)$  Operationen in  $\mathbb{Z}$  haben. (Zusatzfrage: Wieso gilt  $\Phi_n \in \mathbb{Z}[x]$ ?)

#### 40. Aufgabe:

1. Zeigen Sie das Eisenstein-Kriterium: Wenn  $f \in \mathbb{Z}[x]$  und  $p \in \mathbb{N}$  eine Primzahl, so dass  $p \nmid \text{lc}(f)$ ,  $p$  alle anderen Koeffizienten von  $f$  teilt, und  $p^2 \nmid f(0)$ , dann ist  $f$  irreduzibel in  $\mathbb{Q}[x]$ .
2. Folgern Sie, dass für beliebige  $n \in \mathbb{N}$  das Polynom  $x^n - p$  irreduzibel in  $\mathbb{Q}[x]$  ist.

Übungen zur Vorlesung Computeralgebra  
Blatt 11

Prof. Dr. Klaus Madlener

**41. Aufgabe:**

Sei  $f \in \mathbb{Z}[x]$  vom Grad  $n$  und die Maximumsnorm  $\|f\|_\infty = A$  und  $f = (ux + v)g$ , wobei  $u, v \in \mathbb{Z} \setminus \{0\}$  und  $g = \sum_{0 \leq i < n} g_i x^i \in \mathbb{Z}[x]$ .

1. Zeigen Sie, dass  $|g_i| < (i + 1)A/|v|$  für  $0 \leq i < n - 1$ , falls  $|u| = |v|$ , und folgern Sie, dass dann  $\|g\|_\infty \leq nA$ .
2. Angenommen  $\alpha = |u/v| < 1$ . Zeigen Sie  $|g_i| \leq A \frac{1 - \alpha^{i+1}}{1 - \alpha} / |v|$  für  $0 \leq i < n - 1$ , und folgern Sie, dass dann  $\|g\|_\infty \leq A$  gilt. Zeigen Sie, dass letzteres auch im Fall  $|u/v| > 1$  gilt.

**42. Aufgabe:**

Betrachten Sie die deterministische Variante des Berlekamp-Algorithmus in Geddes et al. auf Seite 352 (Algorithm 8.4). Wieso genügt es im letzten Abschnitt, die größten gemeinsamen Teiler  $\text{ggT}(v^{[r]} - s, u)$  für die Basispolynome  $v^{[2]}, \dots, v^{[k]}$  der Nullraumbasis von  $Q - I$  zu berechnen, um eine vollständige Faktorisierung zu erhalten?

**43. Aufgabe:**

Von Kronecker (1882) stammt folgende Methode, das Faktorisierungsproblem für multivariate Polynome über einem ZPE-Ring  $R$  auf das Faktorisierungsproblem für univariate Polynome über  $R$  zu reduzieren.

- a) Sei die Abbildung  $S_d : R[x_1, \dots, x_n] \rightarrow R[y]$  durch

$$h(x_1, \dots, x_n) \mapsto h(y, y^d, \dots, y^{d^{n-1}})$$

definiert (für  $d \in \mathbb{N}$ ). Überzeugen Sie sich, dass  $S_d$  ein Homomorphismus ist, der für diejenigen Polynome invertiert werden kann, die in jeder Variablen einen Grad kleiner als  $d$  haben.

- b) Wir wollen mit  $S_d^{-1}$  die additive Abbildung  $R[y]/\langle y^d \rangle \rightarrow R[x_1, \dots, x_n]$  bezeichnen, die

$$S_d^{-1}(c y^\alpha) = c x_1^{\alpha_1} \cdots x_n^{\alpha_n}$$

erfüllt, wobei  $\alpha_1 + \alpha_2 d + \cdots + \alpha_n d^{n-1}$  die (positive)  $d$ -adische Darstellung von  $\alpha$  sei.

Sei nun  $f \in R[x_1, \dots, x_n]$ ,  $d > \max_{1 \leq i \leq n} \deg_{x_i}(f)$ , und sei  $g$  ein Faktor von  $f$ . Zeigen Sie, dass es dann irreduzible Faktoren  $g_1, \dots, g_s$  von  $S_d(f)$  gibt, so dass  $g = S_d^{-1}(\prod_{j=1}^s g_j)$  ist.

- c) Geben Sie nun einen Algorithmus an, der für ein  $f \in R[x_1, \dots, x_n]$  seine irreduziblen Faktoren  $f_1, \dots, f_s$  berechnet. Untersuchen Sie die Laufzeit Ihres Algorithmus.
- d) Faktorisieren Sie das Polynom  $f = -x^4y + x^3z + xz^2 + yz^2 \in \mathbb{F}_3[x, y, z]$  mit Ihrem Algorithmus.

**44. Aufgabe:**

Betrachten Sie folgenden Spezialfall der polynomialen Faktorisierung: Eingabe ist eine Primzahl  $p$  und  $f \in \mathbb{F}_p[x]$  vom Grad  $n$  und Teiler von  $x^p - x$ , so dass alle monischen irreduziblen Faktoren von  $f$  in  $\mathbb{F}_p[x]$  linear und unterschiedlich sind. Finden Sie mit Hilfe der Methode nach Pollard und Strassen einen deterministischen Algorithmus zur Faktorisierung von  $f$  mit einer oberen Schranke von  $O(n\sqrt{p})$  Operationen in  $\mathbb{F}_p$ , falls  $p^2 > n$ .

**45. Aufgabe:**

Sei  $x_0 = 2$  und  $x_i = x_{i-1}^2 + 1$  für  $i \geq 1$ . Für  $p \in \mathbb{N}$  sei  $e(p) = \min\{i \in \mathbb{N}_{\geq 1} : x_i \equiv x_{2i} \pmod{p}\}$

1. Berechne  $e(p)$  für alle Primzahlen  $p \leq 13$
2. Berechne  $e(p)$  für alle Primzahlen  $p \leq 10^6$ . Es sollte  $e(p) \leq 3680$  für alle diese  $p$  sein. Das vermutete Wachstumsverhalten ist  $\sqrt{p \ln p}$
3. Sei  $N$  die zu faktorisierte Zahl. Angenommen mit Pollard's  $\rho$ -Methode mit Anfangswert  $x_0 = 2$  erhält man  $\text{ggT}(x_i - x_{2i}, N) = 1$  für  $0 \leq i \leq k$ . Zeigen Sie, dass dann  $e(p) > k$  für alle Primteiler  $p$  von  $N$ .
4. Schließen Sie daraus, dass  $N$  keine Faktoren bis  $10^6$  hat, wenn der ggT in 3 in 3680 Schritten trivial ist.

**46. Aufgabe:**

Sei  $E$  eine elliptische Kurve und  $P, Q \in E$ . Erklären Sie, warum  $P + Q = S$ , wobei  $S$  der dritte Schnittpunkt der Geraden durch  $P$  und  $Q$  mit  $E$  ist, keine Gruppenoperation ist.

**47. Aufgabe:**

Sei  $F$  ein Körper, und  $f = x^3 + ax + b \in F[x]$

1. Weisen Sie nach, dass  $r = \text{res}(f, f') = 4a^3 + 27b^2$ .
2. Folgern Sie, dass  $f$  QF genau dann wenn  $r \neq 0$ .
3. Für welche Werte von  $b$  definiert  $y^2 = x^3 - x + b$  keine elliptische Kurve über  $F = \mathbb{R}$ ? Wie sieht die Kurve für diese Werte aus?

**48. Aufgabe:**

Sei  $N = 8051 = 97 \cdot 83$ .

1. Der öffentliche RSA-Schlüssel ist  $K = (N, e) = (8051, 3149)$ . Wie lautet der dazu gehörige private Schlüssel?
2. Eine Nachricht  $x$  ist mit dem Schlüssel  $K$  zu 694 verschlüsselt worden. Was ist  $x$ ?

**50. Aufgabe:**

Zeigen Sie:

- a) Wenn  $s, t \in T[X]$  und  $s|t$ , dann ist  $s \leq t$  für jede Termordnung  $<$  auf  $T[X]$ .
- b) Sei  $R$  ein Integritätsbereich und  $f, g \in R[X]$  mit  $f, g \neq 0$ . Dann gelten (i)  $\text{lt}(fg) = \text{lt}(f) \cdot \text{lt}(g)$ , (ii)  $\text{lm}(fg) = \text{lm}(f) \cdot \text{lm}(g)$ , (iii)  $\text{lc}(fg) = \text{lc}(f) \cdot \text{lc}(g)$  und (iv)  $\text{lt}(f+g) \leq \max\{\text{lt}(f), \text{lt}(g)\}$  für eine beliebige Termordnung  $<$  auf  $T[X]$ .

**51. Aufgabe:**

Zeigen Sie: Ist  $K$  ein Körper,  $F \subseteq K[X]$ , so gilt:

- a) Sei  $g_1, g_2, h \in K[X]$ . Wenn  $g_1 \rightarrow_F g_2$ , dann  $g_1 + h \downarrow_F^* g_2 + h$ .
- b) Die Idealkongruenz modulo  $\langle F \rangle$  ist die reflexiv-transitiv-symmetrische Hülle von  $\rightarrow_F$ , d. h.  $\equiv_{\langle F \rangle} = \longleftrightarrow_F^*$

**52. Aufgabe:**

Wir betrachten eine wichtige Klasse von Termordnungen bzw. von Ordnungen ihrer Exponentenvektoren, die *Gewichtsordnungen*.

Sei dazu  $u = (u_1, \dots, u_n) \in \mathbb{N}^n$  und  $>_\sigma$  eine zulässige Ordnung auf  $\mathbb{N}^n$ . Definiere dann für  $\alpha, \beta \in \mathbb{N}^n$ :  $\alpha >_{u,\sigma} \beta$  genau dann, wenn

$$u \cdot \alpha > u \cdot \beta \quad \text{oder} \quad u \cdot \alpha = u \cdot \beta \quad \text{und} \quad \alpha >_\sigma \beta.$$

Dabei ist  $\cdot$  das Standardskalarprodukt. Wir nennen dann  $>_{u,\sigma}$  die *durch  $u$  und  $>_\sigma$  induzierte Gewichtsordnung*.

1. Zeigen Sie, dass  $>_{u,\sigma}$  eine zulässige Termordnung ist.
2. Finden Sie ein  $u \in \mathbb{N}^n$ , so dass  $>_{u,\text{lex}}$  die graduierte lexikographische Ordnung ist.
3. In der Definition von  $>_{u,\sigma}$  wird  $>_\sigma$  benötigt, um „Unentschieden“ zu vermeiden. Es stellt sich heraus, dass solche Unentschieden tatsächlich auftreten. Zeigen Sie dazu:

Für gegebenes  $u \in \mathbb{N}^n$  gibt es  $\alpha \neq \beta$  in  $\mathbb{N}^n$ , so dass  $u \cdot \alpha = u \cdot \beta$ .

4. Ein nützliches Beispiel einer Gewichtsordnung ist die *Eliminationsordnung*. Fixiere dazu ein  $1 \leq i \leq n$  und setze  $u = (1, \dots, 1, 0, \dots, 0)$  mit  $i$  Einsen und  $n - i$  Nullen. Die  $i$ -te *Eliminationsordnung*  $>_i$  ist dann die Gewichtsordnung  $>_{u, \text{degrevlex}}$ . Zeigen Sie, dass  $>_i$  die folgende Eigenschaft hat:

Wenn  $x^\alpha$  ein Monom ist, in dem eine der Variablen  $x_1, \dots, x_i$  vorkommt, dann gilt  $x^\alpha >_i x^\beta$  für alle Monome  $x^\beta$ , in denen nur die Variablen  $x_{i+1}, \dots, x_n$  vorkommen.

**53. Aufgabe:**

Zeigen Sie, dass die Menge  $B$ , die im Beweis von Dickson's Lemma erzeugt wird, die bezüglich Inklusion kleinste Menge mit der Eigenschaft  $\langle x^A \rangle = \langle x^B \rangle$  ist.

**54. Aufgabe:**

- a) Zeigen Sie, dass  $\{y - x^2, z - x^3\}$  keine Gröbnerbasis für die lexikographische Ordnung mit  $x > y > z$  ist.
- b) Sei  $\{x + 1, y + 1, xy + z\} \subseteq \mathbb{Q}[x, y, z]$ . Berechnen Sie eine Gröbnerbasis für  $\langle F \rangle$  bezüglich der lexikographischen Ordnung mit  $x > y > z$ . Verwenden Sie auch andere Termordnungen, um ein Gefühl für die Komplexität des Buchberger-Algorithmus zu bekommen.

**55. Aufgabe:**

Man fixiere eine zulässige Termordnung. Seien  $G$  und  $\hat{G}$  minimale Gröbnerbasen des Ideales  $I$ .

- a) Zeigen Sie, dass  $G$  und  $\hat{G}$  die gleichen Leiterterme haben.
- b) Zeigen Sie, dass  $G$  und  $\hat{G}$  gleichviele Elemente besitzen.

**56. Aufgabe:**

Betrachten Sie folgendes polynomiale Gleichungssystem  $f_1 = f_2 = f_3 = f_4 = 0$ , wobei

$$\begin{aligned}f_1 &= x_4 + b - d, \\f_2 &= x_4 + x_3 + x_2 + x_1 - a - c - d, \\f_3 &= x_3x_4 + x_1x_4 + x_1x_3 - ad - ac - cd, \\f_4 &= x_1x_3x_4 - acd\end{aligned}$$

Polynome in den Variablen  $x_1, x_2, x_3, x_4$  sind und die Parameter  $a, b, c, d$  enthalten, d. h.  $f_1, f_2, f_3, f_4 \in \mathbb{Q}(a, b, c, d)[x_1, x_2, x_3, x_4]$ . Sei  $<$  die lexikographische Ordnung mit  $x_1 < x_2 < x_3 < x_4$ . Zeigen oder widerlegen Sie: Das System hat unendlich viele Lösungen. Berechnen Sie eine Lösung des Systems (wenn es überhaupt eine Lösung besitzt).

**57. Aufgabe:**

Seien  $I = \langle f_1, \dots, f_r \rangle$  und  $J = \langle g_1, \dots, g_s \rangle$  Ideale in  $K[X]$ ,  $K$  Körper. Zeigen Sie:

- a)  $I \cap J = (\langle t \rangle \cdot I + \langle 1 - t \rangle \cdot J) \cap K[X]$ , wobei  $t$  eine neue Variable ist.
- b)  $I : J$  ist definiert als  $I : J = \{f \mid f \cdot g \in I \text{ für alle } g \in J\}$ .

Es gilt:  $I : J = \bigcap_{j=1}^s (I : \langle g_j \rangle)$  und  $I : \langle g \rangle = \langle h_1/g, \dots, h_m/g \rangle$ , wobei  $I \cap \langle g \rangle = \langle h_1, \dots, h_m \rangle$ .

Was bedeutet dies für die Berechenbarkeit der obigen Idealoperationen?