Schulmathematik und Algorithmen der Computeralgebra

Prof. Dr. Wolfram Koepf

Fachbereich Mathematik/Informatik

Universität Gh Kassel

koepf@mathematik.uni-kassel.de

http://www.mathematik.uni-kassel.de/~koepf

Kleiner Satz von Fermat

- Für eine Primzahl $p \in \mathbb{P}$ und $a \in \mathbb{Z}$ gilt

$$a^p = a \pmod{p}$$

- Fermattest: Ist diese Beziehung für eine Zahl $a \in \mathbb{Z}$ nicht erfüllt, so ist p keine Primzahl!

Effiziente Berechnung von Potenzen

- Die modulare Potenz $a^n \pmod p$ berechnet man am besten durch Zurückführen auf Exponenten der Größe $n/2$ (Divide-and-Conquer-Algorithmus):

- $a^0 \bmod p = 1$
- $a^n \bmod p = (a^{n/2} \bmod p)^2 \bmod p$ für gerade n
- $a^n \bmod p = (a^{n-1} \bmod p) \cdot a \bmod p$

Euklidischer Algorithmus

- Den größten gemeinsamen Teiler von a und b berechnet man so:

- $ggT(a,b) = ggT(|a|,|b|)$, falls $a<0$ oder $b<0$
- $ggT(a,b) = ggT(b,a)$, falls $a<b$
- $ggT(a,0) = a$
- $ggT(a,b) = ggT(b, a \bmod b)$

Faktorisierung von Polynomen

- Polynome mit rationalen Koeffizienten können algorithmisch faktorisiert werden!
- Dies funktioniert sogar, wenn mehrere Variablen im Spiel sind.
- Algorithmische Faktorisierungen über $\mathbb{R}$ dagegen sind nur unter Verwendung algebraischer Zahlen möglich, z. B. $x^4+1 = (x^2+\sqrt{2}\,x+1)(x^2-\sqrt{2}\,x+1)$.
- Moderne schnelle Faktorisierungsalgorithmen gibt es in *Mathematica* und Maple, aber nicht in DERIVE bzw. dem TI 92/89.

Wo ist der zweite Pol?

- Während graphische Taschenrechner und Computeralgebrasysteme im Allgemeinen auf Anhieb Funktionsgraphen darstellen, gibt es auch Fälle, wo hierzu Kurven-untersuchungen nötig sind.
- Wo ist der zweite Pol der Funktion

$$\frac{1000(x-1)}{(101x-100)(100x-99)}$$

Differentiation

- Ableiten ist algorithmisch, wenn wir die üblichen Ableitungsregeln verwenden:
- Konstantenregel $c' = 0$ falls c konstant ist
- Potenzregel $(x^n)' = n\, x^{n-1}$
- Linearität $(f + g)' = f' + g'$ und $(c \cdot f)' = c \cdot f'$
- Produktregel $(f \cdot g)' = f' \cdot g + g' \cdot f$
- Quotientenregel $(f / g)' = (f' \cdot g - g' \cdot f)/g^2$
- Kettenregel $f(g)' = f'(g) \cdot g'$
- Ableitungen spezieller Funktionen

Integration

- Auch für die Integration gibt es Algorithmen, welche entscheiden, ob ein Integral eine elementare Funktion ist.
- Die übliche Methode zur rationalen Integration benötigt eine reelle Faktorisierung des Nenners und ist daher kein guter Algorithmus.
- Der Risch-Algorithmus und seine Verwandten sind erheblich komplizierter, verwenden aber nur quadratfreie Faktorisierungen.

Vereinfachung

- Rationale Funktionen lassen sich durch Bestimmung des ggT vereinfachen.
- Trigonometrische Polynome lassen sich durch Anwendung der Additionstheoreme vereinfachen.
- Man kann zeigen, dass es für allgemeine Terme keinen generellen Vereinfachungsalgorithmus geben kann.

Das Hofstadterproblem

- Hofstadters geometrische Vermutung ist richtig, wenn die Determinante der Matrix

$$\begin{pmatrix} \frac{\sin(r\alpha)}{\sin((1-r)\alpha)} & \frac{\sin(2\alpha)}{\sin(-\alpha)} & \frac{\sin((2-r)\alpha)}{\sin((r-1)\alpha)} \\ \frac{\sin(r\beta)}{\sin((1-r)\beta)} & \frac{\sin(2\beta)}{\sin(-\beta)} & \frac{\sin((2-r)\beta)}{\sin((r-1)\beta)} \\ \frac{\sin(r\gamma)}{\sin((1-r)\gamma)} & \frac{\sin(2\gamma)}{\sin(-\gamma)} & \frac{\sin((2-r)\gamma)}{\sin((r-1)\gamma)} \end{pmatrix}$$

gleich 0 ist, sofern $\alpha + \beta + \gamma = \pi$.

Reihenentwicklungen

- In der speziellen Relativitätstheorie ergibt sich die Energie aus der Formel

$$E(v) = \frac{mc^2}{\sqrt{1-\frac{v^2}{c^2}}}$$

- Wie erhält man hieraus die klassische Formel $E = \frac{1}{2}mv^2$ für die kinetische Energie?