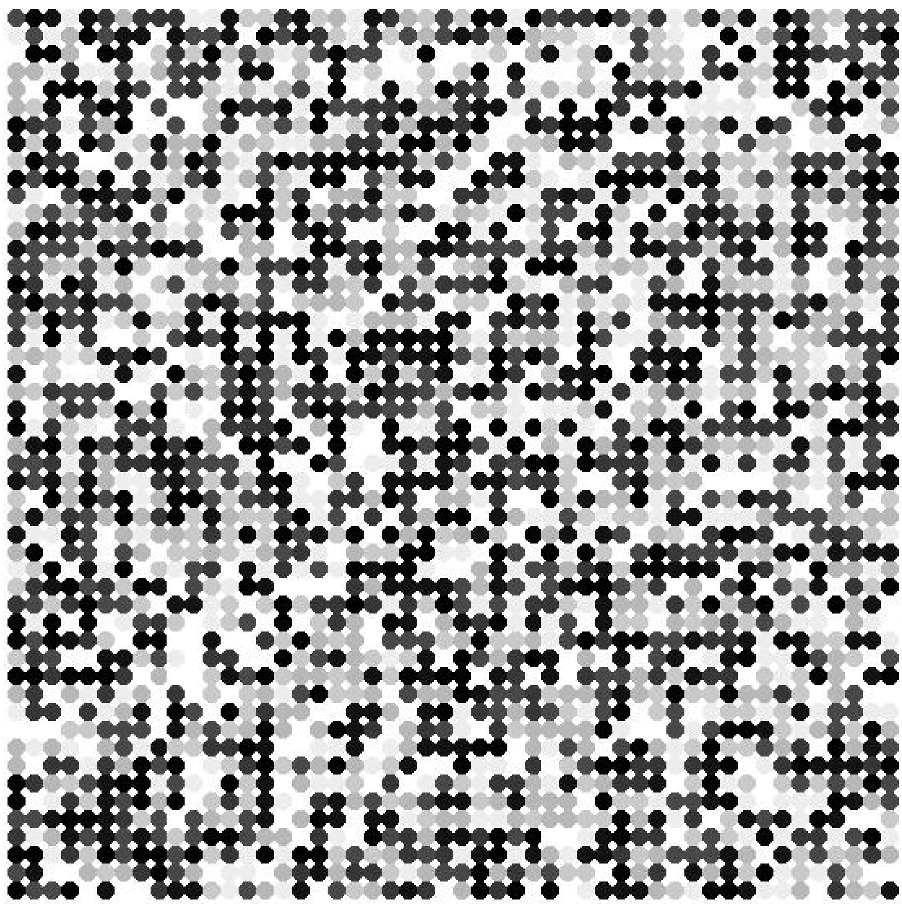
Algorithmen der Computeralgebra und Schulmathematik

Prof. Dr. Wolfram Koepf
Fachbereich Mathematik/Informatik
Universität Kassel

koepf@mathematik.uni-kassel.de

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



Online-Vorführung und Programmierung

- Ich benutze das Computeralgebrasystem *Mathematica* zur Demonstration und zur Programmierung der Algorithmen. Aber wir könnten auch jedes andere System verwenden. Auf DERIVE wird auch eingegangen. Wir beginnen mit ganz leichten Aufgaben ...

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 (mod 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:

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

Faktorisierung von Polynomen

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

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?

■ ganzzahlige Arithmetik

```
50!
```

30414093201713378043612608166064768844377641568960512000000000000

$$\frac{50!}{2^{100}}$$

216105129892080882169214875191192738017616943359375/9007199254740992

■ größte gemeinsame Teiler und Faktorisierung

```
GCD[50!, 2^100]
```

140737488355328

```
FactorInteger[50!]
```

$$\begin{pmatrix} 2 & 47 \\ 3 & 22 \\ 5 & 12 \\ 7 & 8 \\ 11 & 4 \\ 13 & 3 \\ 17 & 2 \\ 19 & 2 \\ 23 & 2 \\ 29 & 1 \\ 31 & 1 \\ 37 & 1 \\ 41 & 1 \\ 43 & 1 \\ 47 & 1 \end{pmatrix}$$

$2^{67} - 1$

147573952589676412927

```
FactorInteger[2^67 - 1]
```

$$\begin{pmatrix} 193707721 & 1 \\ 761838257287 & 1 \end{pmatrix}$$

$10^{51} - 1$

999999999999999999999999999999999999999999999999999

```
FactorInteger[10^51 - 1]
```

$$\begin{pmatrix} 3 & 3 \\ 37 & 1 \\ 613 & 1 \\ 210631 & 1 \\ 2071723 & 1 \\ 52986961 & 1 \\ 5363222357 & 1 \\ 13168164561429877 & 1 \end{pmatrix}$$

```
p = Random[Integer, {1, 10^100}]
```

7746875075893487571983873875103160620026983008936959708351628523763481918144068043747811511769730\
711

```
FactorInteger[p]
```

$Aborted

```
PrimeQ[p]
```

False

■ Wie stellt man fest, dass Zahlen keine Primzahlen sind, ohne ihre Faktoren zu bestimmen?

```
NextPrime[n_] := n + 1 /; PrimeQ[n + 1]
NextPrime[n_] := NextPrime[n + 1]
```

```
NextPrime[10^100]
```

1000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000\
0267

■ Fermattest

```
2^p
```

General::ovfl : Overflow occurred in computation.

Overflow[]

```
p
```

2005399547141541688765830535611234414357181434873934635102343178860996494342920282862864229565590\
40

```
Mod[2^p, p]
```

General::ovfl : Overflow occurred in computation.

Overflow[]

```
PowerMod[2, p, p]
```

2135987035920910082395021706169552114602704522356652769947041607822219725780640550022962086936576

■ Schnelles Potenzieren

```
powermod[a_, 0, p_] := 1
powermod[a_, n_, p_] := Mod[powermod[a, n/2, p]^2, p] /; EvenQ[n]
powermod[a_, n_, p_] := Mod[a * powermod[a, n - 1, p], p] /; OddQ[n]
$RecursionLimit = ∞;
```

```
powermod[2, p, p]
```

2135987035920910082395021706169552114602704522356652769947041607822219725780640550022962086936576

```
PowerMod[2, p, p]
```

2135987035920910082395021706169552114602704522356652769947041607822219725780640550022962086936576

■ Euklidischer Algorithmus

```
ggt[a_, b_] := ggt[|a|, |b|] /; a < 0 || b < 0
ggt[a_, b_] := ggt[b, a] /; a < b
ggt[a_, 0] := a
ggt[a_, b_] := ggt[b, Mod[a, b]]
```

```
ggt[50!, 2^100]
```

140737488355328

■ Rechnen mit Polynomen

```
(x + y)^10 - (x - y)^10
```

$(x+y)^{10}-(x-y)^{10}$

```
p = Expand[(x + y)^10 - (x - y)^10]
```

$20\,y\,x^9+240\,y^3\,x^7+504\,y^5\,x^5+240\,y^7\,x^3+20\,y^9\,x$

```
Factor[p]
```

$4\,x\,y\,(5\,x^4+10\,y^2\,x^2+y^4)\,(x^4+10\,y^2\,x^2+5\,y^4)$

```
Integrate[1/(1 + x^4), x]
```

$$\frac{\tan^{-1}\left(\frac{2x-\sqrt{2}}{\sqrt{2}}\right)}{2\sqrt{2}}+\frac{\tan^{-1}\left(\frac{2x+\sqrt{2}}{\sqrt{2}}\right)}{2\sqrt{2}}-\frac{\log\left(-x^2+\sqrt{2}\,x-1\right)}{4\sqrt{2}}+\frac{\log\left(x^2+\sqrt{2}\,x+1\right)}{4\sqrt{2}}$$

$$\texttt{Factor}\left[1+x^4,\ \texttt{Extension}\to\left\{\sqrt{2}\right\}\right]$$

$$-\left(-x^2+\sqrt{2}\,x-1\right)\left(x^2+\sqrt{2}\,x+1\right)$$

■ Differentiation

$$\texttt{f} = \texttt{Sin}\left[2\,x^2-\frac{1}{1-x}\right]*\texttt{Cos}\left[\frac{1}{1+x}\right]$$

$$-\cos\left(\frac{1}{x+1}\right)\sin\left(\frac{1}{1-x}-2\,x^2\right)$$

```
D[f, x]
```

$$-\left(\frac{1}{(1-x)^2}-4\,x\right)\cos\left(\frac{1}{x+1}\right)\cos\left(\frac{1}{1-x}-2\,x^2\right)-\frac{\sin\left(\frac{1}{x+1}\right)\sin\left(\frac{1}{1-x}-2\,x^2\right)}{(x+1)^2}$$

```
D[u[x] * v[x] * w[x], x]
```

$$v(x)\,w(x)\,u'(x)+u(x)\,w(x)\,v'(x)+u(x)\,v(x)\,w'(x)$$

■ Integration

$$\texttt{f} = \frac{x^3+x^2+x-1}{x^4+x^2+1}$$

$$\frac{x^3+x^2+x-1}{x^4+x^2+1}$$

$$\texttt{int} = \int \texttt{f}\,dx$$

$$\frac{(4+4\,i)\left(3+i\sqrt{3}\right)\tan^{-1}\left(\left(\frac{1}{2}+\frac{i}{2}\right)\sqrt{-i+\sqrt{3}}\,x\right)}{\left(-i+\sqrt{3}\right)^{5/2}\left(3\,i+\sqrt{3}\right)}-\frac{16\,i\tan^{-1}\left(\frac{\sqrt{-i+\sqrt{3}}\,x}{\sqrt{i+\sqrt{3}}}\right)}{\left(-i+\sqrt{3}\right)^{5/2}\sqrt{\frac{1}{3}\left(i+\sqrt{3}\right)}\left(3\,i+\sqrt{3}\right)}+$$

$$\frac{4\,i\left(1-i\sqrt{3}\right)\tan^{-1}\left(\frac{-x^2-2}{\sqrt{3}\,x^2}\right)}{\left(-i+\sqrt{3}\right)^3\left(3\,i+\sqrt{3}\right)}+\frac{8\,i\tan^{-1}\left(\frac{1-x^2}{\sqrt{3}\,x^2+\sqrt{3}}\right)}{\left(-i+\sqrt{3}\right)^3\left(3\,i+\sqrt{3}\right)}+\frac{2\left(1-i\sqrt{3}\right)\log(x^4+x^2+1)}{\left(-i+\sqrt{3}\right)^3\left(3\,i+\sqrt{3}\right)}+\frac{4\log(x^4+x^2+1)}{\left(-i+\sqrt{3}\right)^3\left(3\,i+\sqrt{3}\right)}$$

```
diff = D[int, x]
```

$$\frac{2\left(1-i\sqrt{3}\right)(4\,x^3+2\,x)}{\left(-i+\sqrt{3}\right)^3\left(3\,i+\sqrt{3}\right)(x^4+x^2+1)}+\frac{4\,(4\,x^3+2\,x)}{\left(-i+\sqrt{3}\right)^3\left(3\,i+\sqrt{3}\right)(x^4+x^2+1)}+$$

$$\frac{8\,i\left(-\frac{2\,x}{\sqrt{3}\,x^2+\sqrt{3}}-\frac{2\sqrt{3}\,(1-x^2)\,x}{\left(\sqrt{3}\,x^2+\sqrt{3}\right)^2}\right)}{\left(-i+\sqrt{3}\right)^3\left(3\,i+\sqrt{3}\right)\left(\frac{(1-x^2)^2}{\left(\sqrt{3}\,x^2+\sqrt{3}\right)^2}+1\right)}+\frac{4\,i\left(3+i\sqrt{3}\right)}{\left(-i+\sqrt{3}\right)^2\left(3\,i+\sqrt{3}\right)\left(\frac{1}{2}\,i\left(-i+\sqrt{3}\right)x^2+1\right)}-$$

$$\frac{16\,i\sqrt{3}}{\left(-i+\sqrt{3}\right)^2\left(i+\sqrt{3}\right)\left(3\,i+\sqrt{3}\right)\left(\frac{\left(-i+\sqrt{3}\right)x^2}{i+\sqrt{3}}+1\right)}+\frac{4\,i\left(1-i\sqrt{3}\right)\left(-\frac{2\,(-x^2-2)}{\sqrt{3}\,x^3}-\frac{2}{\sqrt{3}\,x}\right)}{\left(-i+\sqrt{3}\right)^3\left(3\,i+\sqrt{3}\right)\left(\frac{(-x^2-2)^2}{3\,x^4}+1\right)}$$

```
Simplify[diff]
```

$$\frac{x^3+x^2+x-1}{x^4+x^2+1}$$

```
f = x * Cos[x] * Sin[2 x]
```

$x\cos(x)\sin(2x)$

$$\int f\, dx$$

$$\frac{1}{2}(\sin(x)-x\cos(x))+\frac{1}{2}\left(\frac{1}{9}\sin(3x)-\frac{1}{3}x\cos(3x)\right)$$

$$\int \frac{\mathrm{Sin}[x]}{x}\, dx$$

$\mathrm{Si}(x)$

■ Vereinfachung

■ Vereinfachungsfunktionen: Expand, Factor, Together, Simplify, FullSimplify, TrigExpand, TrigReduce, ...

■ Das Hofstadter-Problem

$$\mathbf{hofstadter} = \left\{\left\{\frac{\mathrm{Sin}[r\,\alpha]}{\mathrm{Sin}[(1-r)\,\alpha]}, \frac{\mathrm{Sin}[2\,\alpha]}{\mathrm{Sin}[(1-2)\,\alpha]}, \frac{\mathrm{Sin}[(2-r)\,\alpha]}{\mathrm{Sin}[(r-1)\,\alpha]}\right\}, \left\{\frac{\mathrm{Sin}[r\,\beta]}{\mathrm{Sin}[(1-r)\,\beta]}, \frac{\mathrm{Sin}[2\,\beta]}{\mathrm{Sin}[(1-2)\,\beta]}, \frac{\mathrm{Sin}[(2-r)\,\beta]}{\mathrm{Sin}[(r-1)\,\beta]}\right\}, \left\{\frac{\mathrm{Sin}[r\,\gamma]}{\mathrm{Sin}[(1-r)\,\gamma]}, \frac{\mathrm{Sin}[2\,\gamma]}{\mathrm{Sin}[(1-2)\,\gamma]}, \frac{\mathrm{Sin}[(2-r)\,\gamma]}{\mathrm{Sin}[(r-1)\,\gamma]}\right\}\right\}$$

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

```
det = Det[hofstadter]
```

General::spell1 : Possible spelling error: new symbol name "det" is similar to existing symbol "Det".

$$\begin{aligned}&\csc((1-r)\,\alpha)\csc((r-1)\,\beta)\csc(\gamma)\sin(r\,\alpha)\sin((2-r)\,\beta)\sin(2\,\gamma)-\\ &\csc((r-1)\,\alpha)\csc((1-r)\,\beta)\csc(\gamma)\sin((2-r)\,\alpha)\sin(r\,\beta)\sin(2\,\gamma)-\\ &\csc((1-r)\,\alpha)\csc(\beta)\csc((r-1)\,\gamma)\sin(r\,\alpha)\sin(2\,\beta)\sin((2-r)\,\gamma)+\\ &\csc(\alpha)\csc((1-r)\,\beta)\csc((r-1)\,\gamma)\sin(2\,\alpha)\sin(r\,\beta)\sin((2-r)\,\gamma)+\\ &\csc((r-1)\,\alpha)\csc(\beta)\csc((1-r)\,\gamma)\sin((2-r)\,\alpha)\sin(2\,\beta)\sin(r\,\gamma)-\\ &\csc(\alpha)\csc((r-1)\,\beta)\csc((1-r)\,\gamma)\sin(2\,\alpha)\sin((2-r)\,\beta)\sin(r\,\gamma)\end{aligned}$$

```
Simplify[det]
```

0

■ Relativistische Energie

$$\text{Energie} = \frac{m\,c^2}{\sqrt{1 - \frac{v^2}{c^2}}}$$

$$\frac{c^2 m}{\sqrt{1 - \frac{v^2}{c^2}}}$$

```
Series[Energie, {v, 0, 3}]
```

$$c^2 m + \frac{m v^2}{2} + O(v^4)$$