

Rechnen mit Zahlen

Taschenrechner

$$\begin{array}{r} 1.23 + 2.25 \\ \hline 3.67 \end{array}$$

0.948229

 $\mathbf{N}[\pi, 1000]$

3.14159265358979323846264338327950288419716939937510582097494459230781640628620899862803
82534211706798214808651328230664709384460955058223172535940812848111745028410270193852
10555964462294895493038196442881097566593344612847564823378678316527120190914564856692
46034861045432664821339360726024914127372458700660631558817488152092096282925409171536
36789259036001133053054882046652138414695194151160943305727036575959195309218611738193
61179310511854807446237996274956735188575272489122793818301194912983367336244065664308
02139494639522473719070217986094370277053921717629317675238467481846766940513200056812
14526356082778577134275778960917363717872146844090122495343014654958537105079227968925
92354201995611212902196086403441815981362977477130996051870721134999999837297804995105
73173281609631859502445945534690830264252230825334468503526193118817101000313783875288
58753320838142061717766914730359825349042875546873115956286388235378759375195778185778
532171226806613001927876611195909216420199

Ganzzahlarithmetik

 $100 !$

9332621544394415268169923885626670049071596826438162146859296389521759999322991560894146
976156518286253697920827223758251185210916864000000000000000000000

 $2^{32} - 1$

4294967295

FactorInteger[60 !]

$$\left(\begin{array}{ll} 2 & 56 \\ 3 & 28 \\ 5 & 14 \\ 7 & 9 \\ 11 & 5 \\ 13 & 4 \\ 17 & 3 \\ 19 & 3 \\ 23 & 2 \\ 29 & 2 \\ 31 & 1 \\ 37 & 1 \\ 41 & 1 \\ 43 & 1 \\ 47 & 1 \\ 53 & 1 \\ 59 & 1 \end{array} \right)$$

Sum $\left[\frac{1}{k}, \{k, 1, 100\}\right]$

$$\frac{14466636279520351160221518043104131447711}{2788815009188499086581352357412492142272}$$

N[%]

5.18738

p = Random[Integer, {1, 10⁵⁰}

27450182362466790947521166099945335659078959027426

FactorInteger[p]

$$\left(\begin{array}{ll} & 2 & 1 \\ & 23 & 2 \\ & 169283 & 1 \\ & 217363 & 1 \\ 705116049342831061977966268520065193 & 1 \end{array} \right)$$

PrimeQ[p]

False

*Rechnen mit Symbolen***Polynome und andere Funktionen****pol** = (x + y)⁶ - (x - y)⁶(x + y)⁶ - (x - y)⁶**Expand**[pol]12 y x⁵ + 40 y³ x³ + 12 y⁵ x**Factor**[pol]4 x y (3 x² + y²) (x² + 3 y²)**rat** = $\frac{1 - x^{10}}{1 - x^4}$ $\frac{1 - x^{10}}{1 - x^4}$ **Together**[rat] $\frac{x^8 + x^6 + x^4 + x^2 + 1}{x^2 + 1}$ **Factor**[rat] $\frac{(x^4 - x^3 + x^2 - x + 1)(x^4 + x^3 + x^2 + x + 1)}{x^2 + 1}$ **Factor**[1 + x⁴]x⁴ + 1

Factor [1 + x⁴, GaussianIntegers → True]

$$(x^2 - i)(x^2 + i)$$

Factor [1 + x⁴, Extension → {√2}]

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

Factor [1 + x⁴, Extension → {√2, i}]

$$\frac{1}{4} (\sqrt{2} - (1+i)x)(\sqrt{2} - (1-i)x)((1-i)x + \sqrt{2})((1+i)x + \sqrt{2})$$

Gleichungen

s = Solve [x² - 3x - 1 == 0, x]

$$\left\{ \left\{ x \rightarrow \frac{1}{2} (3 - \sqrt{13}) \right\}, \left\{ x \rightarrow \frac{1}{2} (3 + \sqrt{13}) \right\} \right\}$$

N[s]

$$\{ \{x \rightarrow -0.302776\}, \{x \rightarrow 3.30278\} \}$$

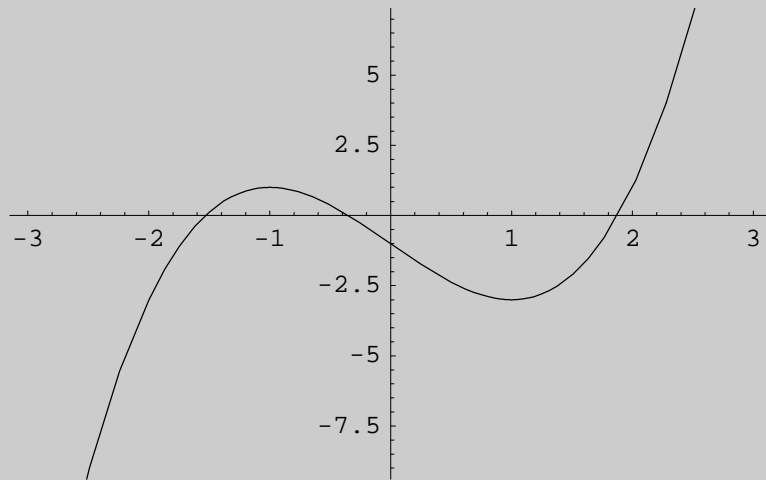
s = Solve [x³ - 3x - 1 == 0, x]

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

N[s]

$$\{ \{x \rightarrow 1.87939 + 0.i\}, \{x \rightarrow -1.53209 + 0.i\}, \{x \rightarrow -0.347296 + 3.33067 \times 10^{-16}i\} \}$$

```
Plot[x3 - 3 x - 1, {x, -3, 3}]
```



- Graphics -

s = Solve[$x^4 - 3x - 1 == 0$, **x**]

$$\left\{ \left\{ x \rightarrow -\frac{1}{2} \sqrt{-4 \sqrt[3]{\frac{2}{3(81 + \sqrt{7329})}} + \frac{\sqrt[3]{\frac{1}{2}(81 + \sqrt{7329})}}{3^{2/3}}} - \frac{1}{2} \sqrt{\left(4 \sqrt[3]{\frac{2}{3(81 + \sqrt{7329})}} - \frac{\sqrt[3]{\frac{1}{2}(81 + \sqrt{7329})}}{3^{2/3}} - \frac{6}{\sqrt{-4 \sqrt[3]{\frac{2}{3(81 + \sqrt{7329})}} + \frac{\sqrt[3]{\frac{1}{2}(81 + \sqrt{7329})}}{3^{2/3}}}} \right)} \right\}, \right.$$

$$\left\{ x \rightarrow -\frac{1}{2} \sqrt{-4 \sqrt[3]{\frac{2}{3(81 + \sqrt{7329})}} + \frac{\sqrt[3]{\frac{1}{2}(81 + \sqrt{7329})}}{3^{2/3}}} + \frac{1}{2} \sqrt{\left(4 \sqrt[3]{\frac{2}{3(81 + \sqrt{7329})}} - \frac{\sqrt[3]{\frac{1}{2}(81 + \sqrt{7329})}}{3^{2/3}} - \frac{6}{\sqrt{-4 \sqrt[3]{\frac{2}{3(81 + \sqrt{7329})}} + \frac{\sqrt[3]{\frac{1}{2}(81 + \sqrt{7329})}}{3^{2/3}}}} \right)} \right\},$$

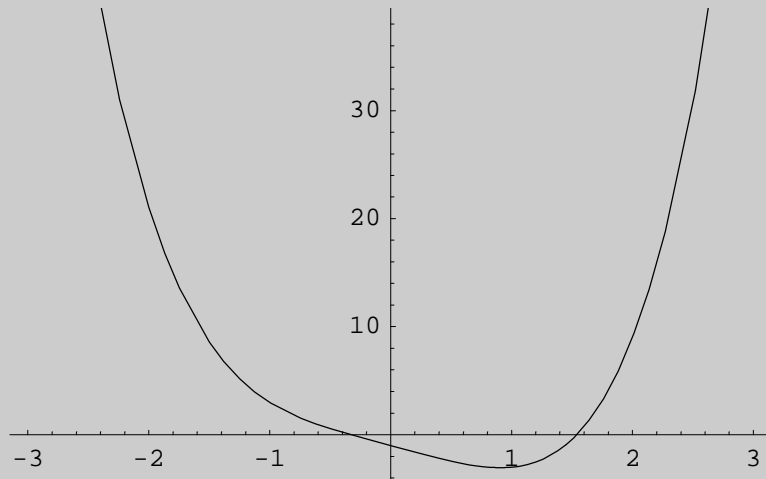
$$\left\{ x \rightarrow \frac{1}{2} \sqrt{-4 \sqrt[3]{\frac{2}{3(81 + \sqrt{7329})}} + \frac{\sqrt[3]{\frac{1}{2}(81 + \sqrt{7329})}}{3^{2/3}}} - \frac{1}{2} \sqrt{\left(4 \sqrt[3]{\frac{2}{3(81 + \sqrt{7329})}} - \frac{\sqrt[3]{\frac{1}{2}(81 + \sqrt{7329})}}{3^{2/3}} + \frac{6}{\sqrt{-4 \sqrt[3]{\frac{2}{3(81 + \sqrt{7329})}} + \frac{\sqrt[3]{\frac{1}{2}(81 + \sqrt{7329})}}{3^{2/3}}}} \right)} \right\},$$

$$\left\{ x \rightarrow \frac{1}{2} \sqrt{-4 \sqrt[3]{\frac{2}{3(81 + \sqrt{7329})}} + \frac{\sqrt[3]{\frac{1}{2}(81 + \sqrt{7329})}}{3^{2/3}}} + \frac{1}{2} \sqrt{\left(4 \sqrt[3]{\frac{2}{3(81 + \sqrt{7329})}} - \frac{\sqrt[3]{\frac{1}{2}(81 + \sqrt{7329})}}{3^{2/3}} + \frac{6}{\sqrt{-4 \sqrt[3]{\frac{2}{3(81 + \sqrt{7329})}} + \frac{\sqrt[3]{\frac{1}{2}(81 + \sqrt{7329})}}{3^{2/3}}}} \right)} \right\} \right\}$$

```
N[s]
```

```
{{x → -0.605102 - 1.26713 i}, {x → -0.605102 + 1.26713 i}, {x → -0.329409}, {x → 1.53961}}
```

```
Plot[x4 - 3 x - 1, {x, -3, 3}]
```



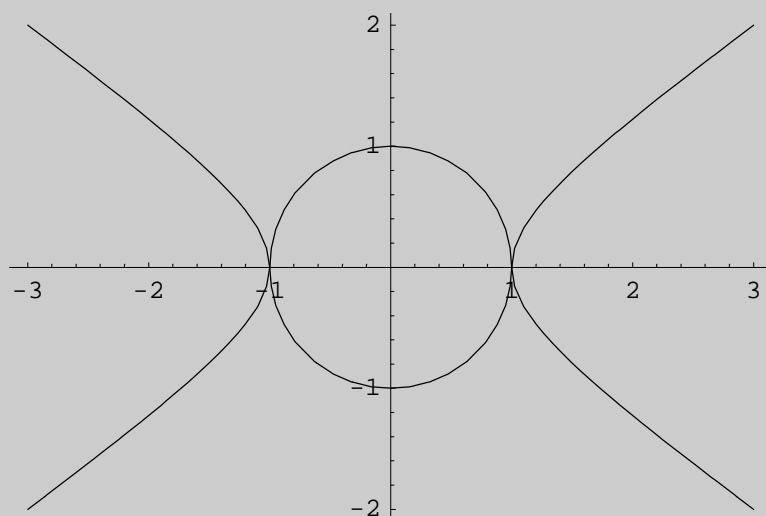
- Graphics -

```
Solve[{x2 + y2 == 1, -x2 + 2 y2 + 1 == 0}, {x, y}]
```

```
{{x → -1, y → 0}, {x → -1, y → 0}, {x → 1, y → 0}, {x → 1, y → 0}}
```

```
Needs["Graphics`ImplicitPlot`"]
```

```
ImplicitPlot[{x^2 + y^2 == 1, -x^2 + 2 y^2 + 1 == 0}, {x, -3, 3}, {y, -3, 3}]
```

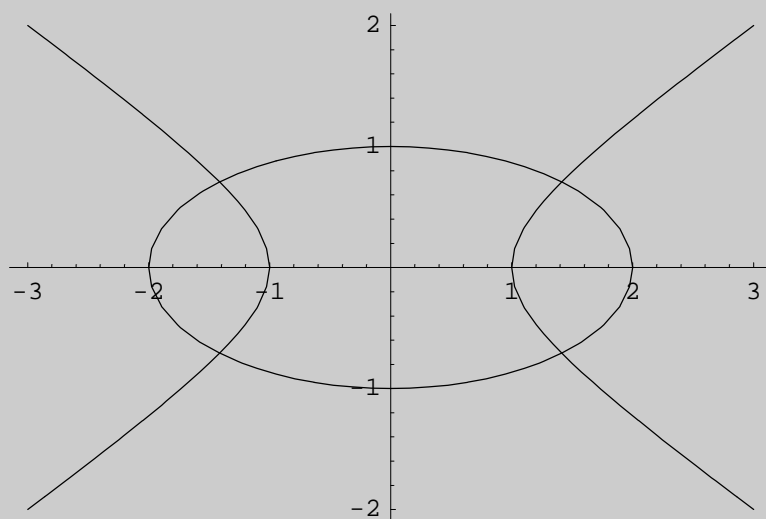


- Graphics -

```
Solve[{ $\frac{x^2}{4} + y^2 == 1$ ,  $-x^2 + 2 y^2 + 1 == 0$ }, {x, y}]
```

```
{{x -> - $\sqrt{2}$ , y -> - $\frac{1}{\sqrt{2}}$ }, {x -> - $\sqrt{2}$ , y ->  $\frac{1}{\sqrt{2}}$ }, {x ->  $\sqrt{2}$ , y -> - $\frac{1}{\sqrt{2}}$ }, {x ->  $\sqrt{2}$ , y ->  $\frac{1}{\sqrt{2}}$ }}
```

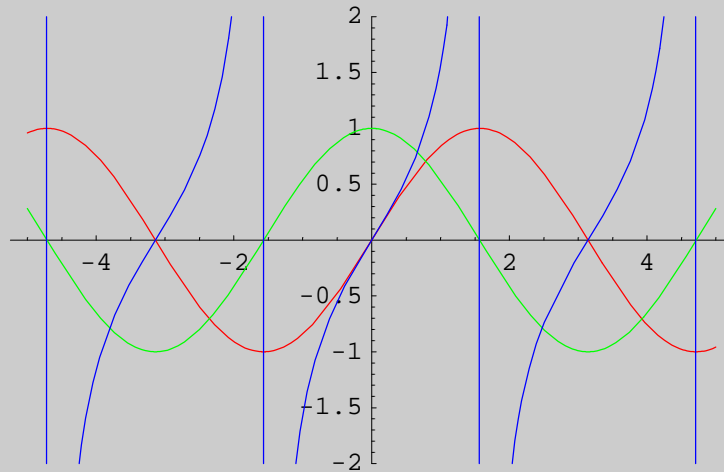
```
ImplicitPlot[{ $\frac{x^2}{4} + y^2 == 1$ ,  $-x^2 + 2 y^2 + 1 == 0$ }, {x, -3, 3}, {y, -3, 3}]
```



- Graphics -

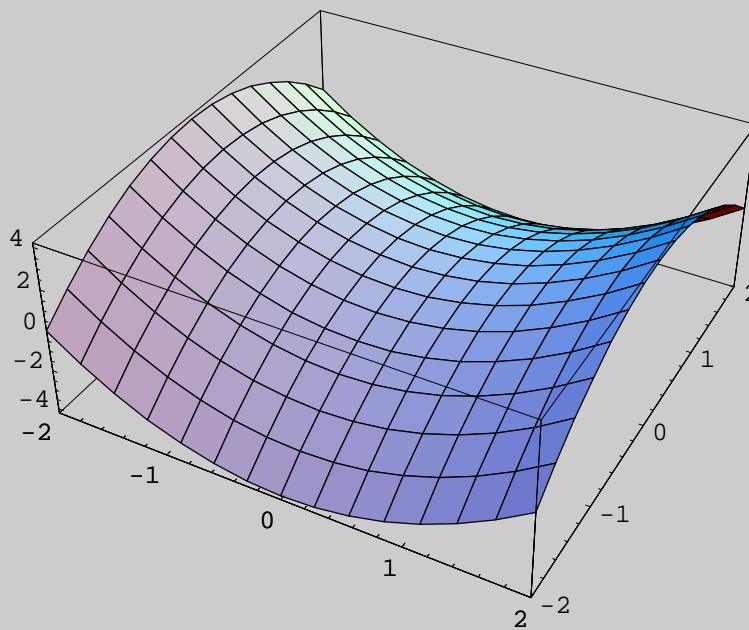
Graphische Darstellungen

```
Plot[{Sin[x], Cos[x], Tan[x]}, {x, -5, 5},  
PlotStyle -> {RGBColor[1, 0, 0], RGBColor[0, 1, 0], RGBColor[0, 0, 1]},  
PlotRange -> {-2, 2}]
```



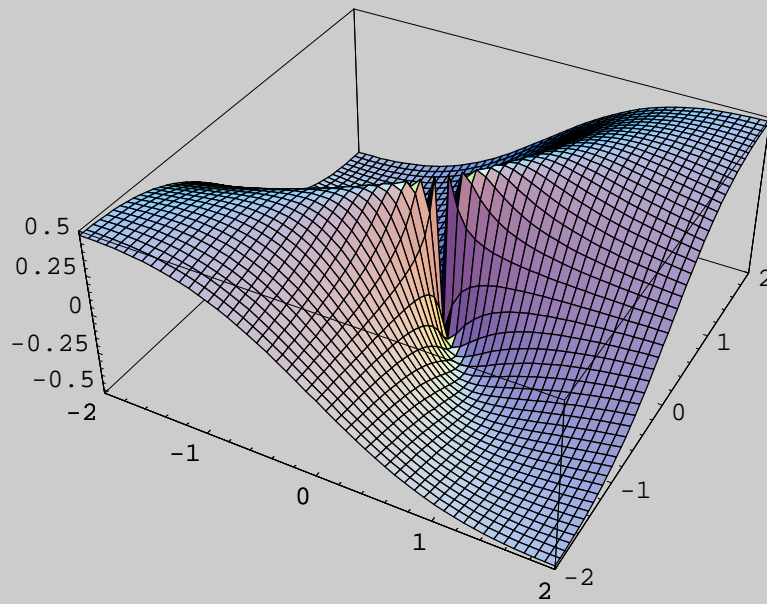
- Graphics -

```
Plot3D[x2 - y2, {x, -2, 2}, {y, -2, 2}]
```



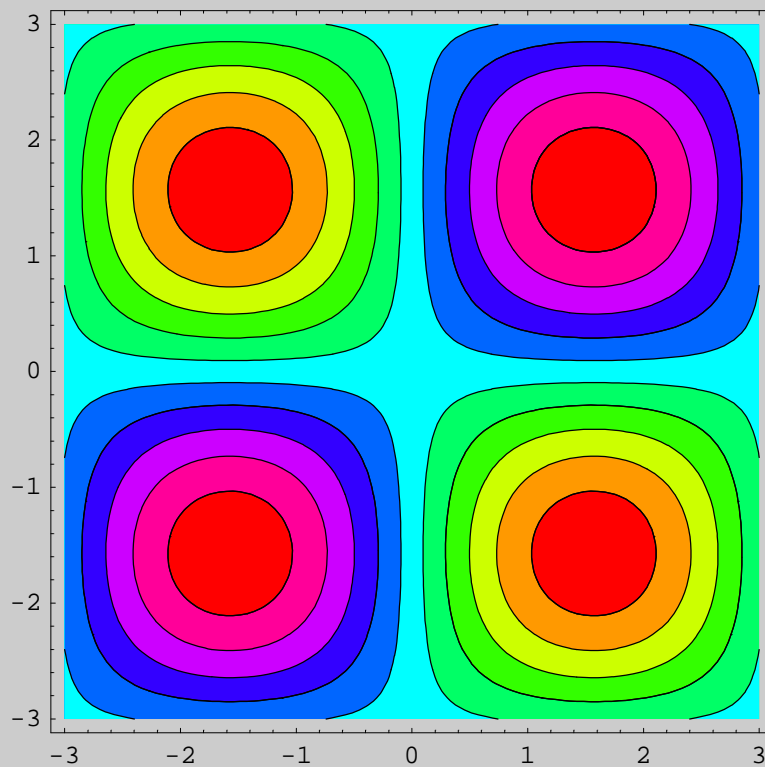
- SurfaceGraphics -

```
Plot3D[ $\frac{xy}{x^2 + y^2}$ , {x, -2, 2}, {y, -2, 2}, PlotPoints -> 50]
```



- SurfaceGraphics -

```
ContourPlot[Sin[x] Sin[y], {x, -3, 3},
  {y, -3, 3}, ColorFunction -> Hue, PlotPoints -> 100]
```



• ContourGraphics •

Analysis

$$\text{Limit}\left[\frac{x^2 - 1}{x - 1}, x \rightarrow 1\right]$$

2

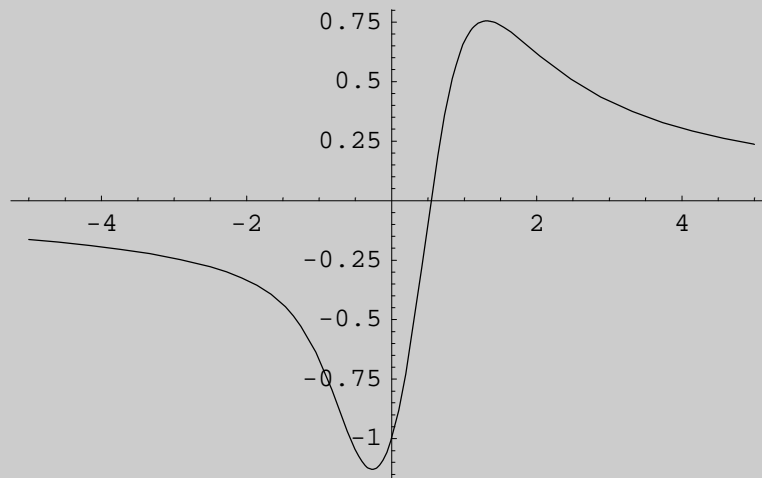
$$\text{ableitung} = D\left[\frac{x^2 + x - 1}{x - 1}, x\right]$$

$$\frac{2x + 1}{x - 1} - \frac{x^2 + x - 1}{(x - 1)^2}$$

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

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

Plot[eingabe, {x, -5, 5}]



- Graphics -

integral = Integrate[eingabe, x]

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

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

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

resultat = D[integral, x]

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

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

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

Vereinfachung

```
resultat // Simplify
```

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

Kryptographie

Caesars Geheimschrift

```
nachricht = "DIES IST MEINE NACHRICHT"
```

```
DIES IST MEINE NACHRICHT
```

```
CaesarV[nachricht_, e_] := Module[{liste, L},
  liste = ToCharacterCode[nachricht];
  liste = liste /. {32 -> L};
  liste = liste - 65;
  liste = liste + e;
  liste = Mod[listete, 26];
  liste = liste /. {Mod[x_, y_] -> L};
  liste = liste + 65;
  liste = liste /. {L + 65 -> 32};
  FromCharacterCode[listete]
]
```

```
CaesarV[nachricht_] := CaesarV[nachricht, 3]
```

```
CaesarE[nachricht_, d_] := CaesarV[nachricht, -d]
```

```
CaesarE[nachricht_] := CaesarE[nachricht, 3]
```

— *General::spell1* : Possible spelling error: new symbol name "CaesarE" is similar to existing symbol "CaesarV".

```
resultat = CaesarV[nachricht]
```

```
GLHV LVW PHLQH QDFKULFKW
```

```
CaesarV["ABCDEFGHIJKLMNOPQRSTUVWXYZ"]
```

```
DEFGHIJKLMNOPQRSTUVWXYZABC
```

```
CaesarE[resultat]
```

```
DIES IST MEINE NACHRICHT
```

```
CaesarV["CAESAR IST DOOF"]
```

```
FDHVDU LVW GRRI
```

```
CaesarE[CaesarV["CAESAR IST DOOF"]]
```

```
CAESAR IST DOOF
```

■ Text zum Entziffern

```
test = "QXIIT TCIOXUUTGC"
```

```
QXIIT TCIOXUUTGC
```

```
Do[Print[CaesarE[test, n]], {n, 1, 26}]
```

```
PWHHS SBHNWTTSTFB
```

```
OVGGR RAGMVSSREA
```

```
NUFFQ QZFLURRQDZ
```

```
MTEEP PYEKTQQPCY
```

```
LSDDO OXDJSPPOBX
```

```
KRCCN NWCIROONAW
```

```
JQBBM MVBHQNNMZV
```

```
IPAAL LUAGPMMLYU
```

```
HOZZK KTFOLLKXT
```

```
GNYYJ JSYENKKJWS
```

FMXXI IRXDMJJIVR

ELWWH HQWCLIIHUQ

DKVVG GPVBKHHGTP

CJUUF FOUAJGGFSO

BITTE ENTZIFFERN

AHSSD DMSYHEEDQM

ZGRRC CLRXGDDCPL

YFQQB BKQWFCCBOK

XEPPA AJPVEBBANJ

WDOOZ ZIOUDAAZMI

VCNNY YHNTCZZYLH

UBMMX XGMSBYYXKG

TALLW WFLRAXXWJF

SZKKV VEKQZWWVIE

RYJJU UDJPYVVUHD

QXIIT TCIOXUUTGC

CaesarE[test, 15]

BITTE ENTZIFFERN

Das RSA-Verfahren

```

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

Combine[liste_] := First[liste] /; Length[liste] == 1

Combine[liste_] := 1000 * Combine[Reverse[Rest[Reverse[liste]]]] + Last[liste]

Convert[string_] := Combine[ToCharacterCode[string]]

makelist[zahl_] := {zahl} /; zahl < 1000

makelist[zahl_] :=
  Append[makelist[(zahl - Mod[zahl, 1000]) / 1000], Mod[zahl, 1000]]
]

ConvertBack[zahl_] := FromCharacterCode[makelist[zahl]]

ExpMod[a_, b_, c_] := PowerMod[a, b, c]

Verschlüssele[nachricht_] := ExpMod[Convert[nachricht], e, n]

Entschlüssele[zahl_] := ConvertBack[ExpMod[zahl, d, n]]

InitialisiereRSA := Module[{},
  p = NextPrime[Random[Integer, {10^100, 10^101}]];
  q = NextPrime[Random[Integer, {10^100, 10^101}]];
  n = p * q;
  phi = (p - 1) * (q - 1);
  e = phi;
  While[Not[GCD[phi, e] == 1],
    e = NextPrime[Random[Integer, {10^35, 10^40}]];
  ];
  findevielfachheit[a_, b_] :=
    PowerMod[a, -1, b];
  d = findevielfachheit[e, phi];
]

```

Erzeugung der Schlüssel

```
InitialisiereRSA
```

öffentlicher Schlüssel

```
{e, n}
```

```
{3145824250788429488299605841561088559001,
 24872885989576999525111616937646388999442193238884810574086287325138392713619208232837.
 2984842316734943803931430594987751081894608141697564934478349438913720947703307776955
 40630552586003913483139955421}
```

```
nachricht = "Dies ist meine Nachricht"
```

```
Dies ist meine Nachricht
```

```
resultat = Verschlüssele[nachricht]
```

```
1990981762862819018856014679517066806294367469978211307200177619572894980599960092690192
 85047034984102576782556876729601076453555394301411783907597390334651075028819755397330
 28106475770317438039837197
```

```
Entschlüssele[resultat]
```

```
Dies ist meine Nachricht
```

```
Entschlüssele[resultat + 1]
```

```
• J°• •úā• •JcΔiδ• qMćp• ¼¼• ç• °• ..
```

Ein paar andere Nachrichten:

```
resultat = Verschlüssele["Wie ist es mit dieser Meldung?"]
```

```
1647376517861854589691967068869643361405938262754525802007220901965557089504062118271659
 06937270964725962066636467850719080876640279346832833198791544523161687493934396211165
 56079770016417482768440874
```

```
Entschlüssele[resultat]
```

```
Wie ist es mit dieser Meldung?
```

Schließlich eine wirklich geheime Nachricht:

```
<< "Eigene Dateien/Koepf/Vorträge/Schülervortrag2002/nachricht"
```

```
resultat = Verschlüssele[nachricht]
```

```
1120587714916845689984203550609662132066951094348505622368347434760571696528491243713502  
68595578472967231897140126192810661358031570797579156283376667966889171572783139684334  
97308238137230545008950195
```

```
Entschlüssele[resultat]
```

```
Dies ist meine allerletzte Nachricht! Herzlichen Dank!
```