Zahlentheorie und Restklassen in MuPAD

Prof. Dr. Dörte Haftendorn, Mathematik mit MuPAD 4.02,
(ex. in 2.5 vom Nov.02 und in 3.11 Sept. 05) Feb.07
http://haftendorn.uni-lueneburg.de **www.mathematik-verstehen.de**

##

Weitere inhaltliche Notebooks------> teiler-prim.mn, restklassen.mn,
Programmierung von zahlentheoretischen Funktionen
---->zahltheo-prg.mn, umwandlungen.mn,
powermod.mn

----------eigene Zahlentheorie Ergänzungen----------/

```
delete PACKAGEPATH:endml:=strmatch(NOTEBOOKPATH,"mathe-lehramt", Index)[2]:
gesamtpackpfad:=substring(NOTEBOOKPATH,1..endml+1).pathname("computer","mupad", "packages"):
PACKAGEPATH:=gesamtpackpfad,PACKAGEPATH://Tipps zu Packages siehe unten auf der Seite.
```

```
package("zahltheo", Forced):zahltheo::init():export(zahltheo):
```

----------eigene Zahlentheorie Ergänzungen----------

```
info(zahltheo);
```

```
Eine Library fuer den Zahlentheorie- und Kryptographie- U

-- Exported:
caesar, ggt,    ggte,       ggtex,   ordo,       pmod,
raseac, teiler, textToZahl, txToZoo, zahlToText, zooToTx,
zstern
```

Zahlentheoretische Funktionen aus dem eigenen zahltheo-package

```
ggt(26,65);ggte(26,65); ggtex(26,65);
```

$$13$$

$$[13, -2, 1]$$

```
26=0*65+26 und es ist  VSD  26= 1*26+ (0)*65
65=2*26+13 und es ist  VSD  13= -2*26+ (1)*65
ggT(26,65)= 13       VSD  13= -2*26+ (1)*65
```

$$[13, -2, 1]$$

```
teiler(15);
```

$$[1, 15, 3, 5]$$

```
zstern(15);
```

$$[1, 2, 4, 7, 8, 11, 13, 14]$$

```
ordo(7,15)
```

$$4$$

```
7^k mod 15 $ k=1..14
```

$$7, 4, 13, 1, 7, 4, 13, 1, 7, 4, 13, 1, 7, 4$$

```
pmod(13,k,15) $ k=1..15  //alle Potenzen von 13 mod 15
```

13, 4, 7, 1, 13, 4, 7, 1, 13, 4, 7, 1, 13, 4, 7

```
pmod(13,-1,15) //das Inverse von 13 mod 15
```

7

Umwandlungen aus dem eigenen zahltheo-package
################

```
mes:="Krytpo ist prima":
cmes:=textToZahl(mes);
```

751141211161121110321051151160321121141051090 97

```
zahlToText(cmes);
```

"Krytpo ist prima"

```
c2mes:=txToZoo(mes); //von ASCII 30 abziehen
```

[75, 114, 121, 116, 112, 111, 32, 105, 115, 116, 32, 112, 114, 1

458491868281027585860282847579 67

```
zooToTx(c2mes);//zerlegen für  ASCII 30 addieren
```

[45, 84, 91, 86, 82, 81, 2, 75, 85, 86, 2, 82, 84, 75, 79, 67]
[75, 114, 121, 116, 112, 111, 32, 105, 115, 116, 32, 112, 114, 1

"Krytpo ist prima"

```
mescaesar:="KRYPTOGRAPHIE";
```

"KRYPTOGRAPHIE"

```
cmescaesar:=caesar(11,mescaesar);
```

[75, 82, 89, 80, 84, 79, 71, 82, 65, 80, 72, 73, 69]
[86, 67, 74, 65, 69, 90, 82, 67, 76, 65, 83, 84, 80]

"VCJAEZRCLASTP"

```
raseac(11,cmescaesar);
```

"KRYPTOGRAPHIE"

Das war MuPAD-eigenes Zahlentheorie-package
####################

---------- MuPAD 4 Vorhandene besondere Funktionen

```
info(numlib);
```

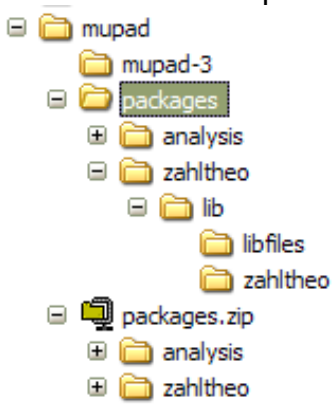
Library 'numlib': the package for elementary number theory

-- Interface:

numlib::Lambda, numlib::Omega, numlib::contfr
numlib::cornacchia, numlib::decimal, numlib::divisc
numlib::ecm, numlib::factorGaussInt, numlib::fibona

```
numlib::ecm,                numlib::factorGaussInt, numlib:
numlib::fromAscii,          numlib::g_adic,         numlib:
numlib::igcdmult,           numlib::invphi,         numlib:
numlib::isquadres,          numlib::issqr,          numlib:
numlib::lambda,             numlib::legendre,       numlib:
numlib::mersenne,           numlib::moebius,        numlib:
numlib::mroots,             numlib::msqrts,         numlib:
numlib::numprimedivisors,   numlib::omega,          numlib:
numlib::phi,                numlib::pi,             numlib:
numlib::prevprime,          numlib::primedivisors,  numlib:
numlib::proveprime,         numlib::sigma,          numlib:
numlib::sqrtmodp,           numlib::sumOfDigits,    numlib:
numlib::tau,                numlib::toAscii
```

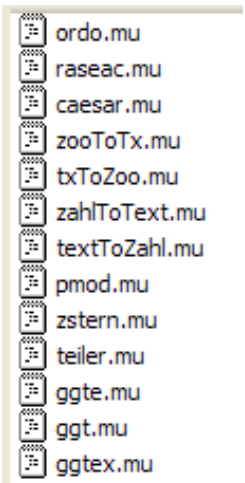
Tipps zur Installation und dem Gebrauch des Krypto-packages von dieser Website.
1. Stellen Sie alles, was Sie von Krypto haben in ein Verzeichnis
mathe-lehramt/krypto
Hinter krypto kann auch noch mehr stehen.
vor mathe-lehramt kann auch Beliebiges stehen.
2. Laden Sie package.zip und entpacken Sie es in einem Verzeichnis
mathe-lehramt/computer/mupad/packages



in lib ist dann 

in libfiles ist dann 

wie die einzeln mu-Dateien aufgebaut sind können Sie in MuPAD
oder jedem Texteditor lesen.

im unteren zahltheo ist dann 

3. Öffnen Sie diese Datei, schicken Sie die beiden obersten Befehle ab.
Dann sollte alles klappen. Sie beeinträchtigen damit nicht die Funktion anderer MuPAD-Dateien.
Übrigens muss das Notebook mit einem Namen geladen sein.
Sie können die Befehle also nicht in ein unbenanntes Notebokk kopieren
und ausprobieren.