Modulares Wurzelziehen

Kryptographie mit MuPAD 4, Prof. Dr. Dörte Haftendorn, Juni 07

http://haftendorn.uni-lueneburg.de **www.mathematik-verstehen.de**

##

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

Im Dateimenu bei "Eigenschaften" steht die Prozeduren zur Berechnung von zstern, daher kann sie hier ausgeführt werden.

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

```
n:=19;  // 19, 123, 12345, geht nicht mehr: 123456789
zstern(n)
```

19

[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18]

```
factor(n)
```

19

```
quadrate:=modp(i^2,n) $ i in zstern(n);
mengeQ:={%}
```

1, 4, 9, 16, 6, 17, 11, 7, 5, 5, 7, 11, 17, 6, 16, 9, 4, 1

{1, 4, 5, 6, 7, 9, 11, 16, 17}

```
nops(quadrate); nops(mengeQ);
```

18

9

```
modp(11^2,n)
```

7

Definition einer Prozedur, die modular Wurzeln zieht.

```
wurzel:=proc(v,n)
        begin
          ZS:=zstern(n);
          ord:=nops(ZS);
          wu:=[];
          for i from 1 to ord do
            if modp(ZS[i]^2,n)=v then wu:=wu.[ZS[i]];
            end_if;
          end_for;
          return(wu);
        end_proc:
```

Hier eine der oben erzeugten Quadratzahlen eintragen.

```
wurzel(11,n)
```

[7, 12]

Betrachtung der geraden Potenzen einer passenden Wurzel

```
modp((5^2)^i,n) $ i=1..5
```

```
6, 17, 7, 4, 5
```