Modulares Wurzelziehen, ohne zStern

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----------

In dieser Datei wird die Bestimmung von zstern vermieden.

```
n:=1234//56789;  // 19, 123, 12345, geht nicht mehr:
123456789
```

$$1234$$

```
factor(n)
```

$$2 \cdot 617$$

Einige Quadrate sollen berechnet werden.

```
quadrate:=modp(i^2,n) $ i =2*n+30..2*n+50;
mengeQ:={%}
```

$$900, 961, 1024, 1089, 1156, 1225, 62, 135, 210, 287, 366, 447, 530, 615, 702, 791, 882, 9$$

$$\{32, 62, 135, 210, 287, 366, 447, 530, 615, 702, 791, 882, 900, 961, 975, 1024, 1070, 108$$

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

$$21$$

$$21$$

```
modp(25^2,n)
```

$$625$$

Definition einer Prozedur, die modular Wurzeln zieht.

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

Hier eine der oben erzeugten Quadratzahlen eintragen.

```
n;
wurzel(25,n);
```

$$1234$$

$$[5, 1229]$$

```
wurzel(615,n)
```

$$[43, 1191]$$

```
[43, 1191]
```

Betrachtung der geraden Potenzen einer passenden Wurzel

```
modp((5^2)^i,n) $ i=1..15
```

```
25, 625, 817, 681, 983, 1129, 1077, 1011, 595, 67, 441, 1153, 443, 1203, 459
```

Fazit:

Wenn man hier mit etwas größeren Zahlen arbeitet merkt man, dass modulares Wurzelziehen sehr lange dauert.