Pseudo-Primzahlen und Carmichael-Zahlen

Prof. Dr. Dörte Haftendorn, Mathematik mit MuPAD 4 Okt.08
http://haftendorn.uni-lueneburg.de www.mathematik-verstehen.de

##

Alle Zahlen, die a^(p-1)mod p=1 für mindestens ein a>1 erfüllen, heißen **Pseudoprimzahlen**.

Es sind also die Primzahl-Kandidaten, die der Kleine Fermat bei einmaliger Prüfung liefert.

1.) Es werden die Basen 2,3,...8 genommen und jedesmal eine Liste der
Pseudoprimzahlen bis 1000 erzeugt.
Die Primfaktorzerlegung dieser Pseudoprimzahlen wird angezeigt.
2.) Es wird die Carmichael-Zahl 561 untersucht.

##

Kleiner Fermat: Wenn p prim und ggt(a,p)=1, dann gilt: a^(p-1) mod p=1

```
li:=[]:a:=2:
for p from 2 to 1000 do
 if  powermod(a,p-1,p)=1 and not isprime(p)
then
   li:=li.[p]:
 end_if:
 end_for:
["a=",a,"p=",li];
map(li,factor);
```

$$["a=", 2, "p=", [341, 561, 645]]$$

$$[11 \cdot 31, 3 \cdot 11 \cdot 17, 3 \cdot 5 \cdot 43]$$

Also sieht man hier 2^340 mod 341 =1 und 341 ist die kleinste Pseudoprimzahl zur Basis 2.

```
li:=[]:a:=3:
for p from 2 to 1000 do
 if  powermod(a,p-1,p)=1 and not isprime(p) then
   li:=li.[p]:
 end_if:
 end_for:
["a=",a,"p=",li];
map(li,factor);
```

$$["a=", 3, "p=", [91, 121, 286, 671, 703, 949]]$$

$$[7 \cdot 13, 11^2, 2 \cdot 11 \cdot 13, 11 \cdot 61, 19 \cdot 37, 13 \cdot 73]$$

Also sieht man hier 2^90 mod 91 =1 und 91 ist die kleinste Pseudoprimzahl zur Basis 3.

```
li:=[]:a:=4:
for p from 2 to 1000 do
 if  powermod(a,p-1,p)=1 and not isprime(p) then

   li:=li.[p]:
```

```
    li:=li.[p]:
  end_if:
  end_for:
["a=",a,"p=",li];
map(li,factor);
```

$$["a=", 4, "p=", [15, 85, 91, 341, 435, 451, 561, 645, 703]]$$

$$[3 \cdot 5, 5 \cdot 17, 7 \cdot 13, 11 \cdot 31, 3 \cdot 5 \cdot 29, 11 \cdot 41, 3 \cdot 11 \cdot 17, 3 \cdot 5 \cdot 43, 19 \cdot 37]$$

Also sieht man hier 4^14 mod 15 =1 und 15 ist die kleinste Pseudoprimzahl zur Basis4.

```
li:=[]:a:=5:
for p from 2 to 1000 do
  if  powermod(a,p-1,p)=1 and not isprime(p) then
    li:=li.[p]:
  end_if:
  end_for:
["a=",a,"p=",li];
map(li,factor);
```

$$["a=", 5, "p=", [4, 124, 217, 561, 781]]$$

$$[2^2, 2^2 \cdot 31, 7 \cdot 31, 3 \cdot 11 \cdot 17, 11 \cdot 71]$$

Also sieht man hier 5^3 mod 4 =1 und 4 ist die kleinste Pseudoprimzahl zur Basis 5.

```
li:=[]:a:=6:
for p from 2 to 1000 do
  if  powermod(a,p-1,p)=1 and not isprime(p) then
    li:=li.[p]:
  end_if:
  end_for:
["a=",a,"p=",li];
map(li,factor);
```

$$["a=", 6, "p=", [35, 185, 217, 301, 481]]$$

$$[5 \cdot 7, 5 \cdot 37, 7 \cdot 31, 7 \cdot 43, 13 \cdot 37]$$

```
li:=[]:a:=7:
for p from 2 to 1000 do
  if  powermod(a,p-1,p)=1 and not isprime(p) then
    li:=li.[p]:
  end_if:
  end_for:
["a=",a,"p=",li];
map(li,factor);
```

$$["a=", 7, "p=", [6, 25, 325, 561, 703, 817]]$$

$$[2 \cdot 3, 5^2, 5^2 \cdot 13, 3 \cdot 11 \cdot 17, 19 \cdot 37, 19 \cdot 43]$$

```
li:=[]:a:=8:
for p from 2 to 1000 do
 if  powermod(a,p-1,p)=1 and not isprime(p) then
   li:=li.[p]:
 end_if:
 end_for:
["a=",a,"p=",li];
map(li,factor);
```

$$["a=", 8, "p=", [9, 21, 45, 63, 65, 105, 117, 133, 153, 231, 273, 341, 481, 511, 561, 585,$$

$$[3^2, 3\cdot 7, 3^2\cdot 5, 3^2\cdot 7, 5\cdot 13, 3\cdot 5\cdot 7, 3^2\cdot 13, 7\cdot 19, 3^2\cdot 17, 3\cdot 7\cdot 11, 3\cdot 7\cdot 13, 11\cdot 31, 13\cdot$$

```
8^8, 8^8/9.0, powermod(8,8,9)
```

$$16777216,\ 1864135.111,\ 1$$

561 ist Carmichael-Zahl, das ist eine Zahl, die nicht Primzahl ist,
aber dennoch für alle a, die teilerfremd sind erfüllt: a^(p-1) mod p=1.
561 ist die kleinste Carmichael-Zahl.

```
li:=[]:p:=561:
factor(561);
for a from 2 to 35 do
 if  powermod(a,p-1,p)=1 then
   li:=li.[a]:
 end_if:
 end_for:
["p=",p,"a=",li];
```

$$3\cdot 11\cdot 17$$

$$["p=", 561, "a=", [2, 4, 5, 7, 8, 10, 13, 14, 16, 19, 20, 23, 25, 26, 28, 29, 31, 32, 35]]$$

In dieser Liste fehlen also nur die Zahlen mit gcd(a,p)<>1, die also nicht teilerferemd zu 561 sind.
Dies zeigt auch die folgende Liste, die nämlich leer bleibt.

```
li:=[]:p:=561:
factor(561);
for a from 2 to 1000 do
 if  powermod(a,p-1,p)=1 and gcd(a,p)<>1
then
   li:=li.[a]:
 end_if:
 end_for:

["p=",p,"a=",li];
```

```
["p=",p,"a=",li];
```

$$3 \cdot 11 \cdot 17$$

```
["p=", 561, "a=", []]
```