



Der kleine Satz des Fermat

Inhalt

- Problemstellung
- Der kleine Satz des Fermat
- Einfluss von Leonhard Euler
- weiterführenden Informationen

Problemstellung

Kann man für eine Zahl möglichst schnell und mit wenig Aufwand feststellen, ob es sich um eine Primzahl handelt?

Ist **11** eine **Primzahl**?

Lösungsvorschläge

Mögliche Ansätze zum Lösen der Problemstellung sind:

- Primzahltests
- Primfaktorenzerlegung

Der kleine Satz des Fermat

$$a^p \equiv a \pmod{p}$$

Teilt man diese Kongruenz durch „a“, so erhält man die bekanntere Version:

$$a^{p-1} \equiv 1 \pmod{p}$$

$$a^{p-1} \equiv 1 \pmod{p}$$

Es gilt:

1. $a, p \in \mathbb{N}$
2. a ist kein Vielfaches von p

Beispielaufgabe:

Ist 11 prim?

Wir nehmen für a eine beliebige natürliche Zahl.

$$2^{10} \equiv 1 \pmod{11}$$

$$2^{10} \equiv 1024 \equiv 93 \cdot 11 + 1 \equiv 1 \pmod{11}$$

Heisst das 11 ist prim?

Dieser Schluss kann aus dem Ergebnis der vorhandenen Kongruenz **nicht** gezogen werden.

Man kann allerdings behaupten, dass 11 pseudoprim ist. (nähere Infos in den „weiterführenden Informationen“)

Da wir wissen, dass 11 eine Primzahl ist, kann man den Umkehrschluss ziehen:

Da 11 prim ist, erfüllt es die Kongruenz.

Einfluss von Leonhard Euler

Sei p eine ungerade Primzahl und
 a eine beliebige ganze Zahl

Wenn gilt: $\text{ggT}(p;a)=1$, dann ist $a^{p-1} - 1$
ein Vielfaches von p .

Über die 3 Binomische Formel gilt:

$$\left(a^{\frac{p-1}{2}} - 1\right) \cdot \left(a^{\frac{p-1}{2}} + 1\right) = a^{p-1} - 1$$

Deshalb gilt:

$$a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$$

Verallgemeinerung des kleinen fermatschen Satz zum Satz von Euler

$a^{\varphi(n)} \equiv 1 \pmod{n}$ mit $\text{ggT}(a;n)=1 \Rightarrow$ Satz von Euler

$\varphi(n)$ liefert Anzahl teilerfremder Zahlen
zu n zwischen 1 und $n-1$

Ist n eine Primzahl, gilt: $\varphi(n) = n - 1$

und der kleine Fermat ist ein Spezialfall
des Satzes von Euler.

Weiterführende Informationen

- Was sind Pseudoprimzahlen?
- Beweis des „kleinen Fermat“
- Quellcode (für Aribas)

Was sind Pseudoprimzahlen?

Es gibt einige verschiedene Arten von Pseudoprimzahlen, welche allerdings alle darauf hinauslaufen, dass die Pseudoprimzahl zu einer (oder mehreren) Basis (Basen) a den kleinen Satz des Fermat erfüllt, **ohne** jedoch eine Primzahl zu sein.

Beispiel:

15 zur Basis 4 $\longrightarrow 4^{14} \equiv 1 \pmod{15}$

$$4^{14} \equiv 268435456$$

$$\equiv 17895697 * 15 + 1 \equiv 1 \pmod{15}$$

Die Kongruenz wird erfüllt, obwohl die Zahl **15** in die Primfaktoren **3** und **5** zerlegt werden kann.

Beweis

Induktionsanfang (a=1):

$$1^p \equiv 1 \pmod{p} \Leftrightarrow 1 \equiv 1 \pmod{p}$$

Induktionsschluss:

$$(a+1)^p \equiv a^p + 1 \equiv a+1 \pmod{p}$$

Quellcode

(implementiert für Aribas)

```
function kleiner_fermat(a,N:integer):boolean; (* a ist eine beliebige ganze Zahl grösser als 1,  
                                             N ist die Zahl, deren Primaität geprüft werden soll*)  
  
begin  
  if a=1 then (* a^1 ist immer 1 => keine Primzahl => wird ausgeschlossen*)  
    return false;  
  end;  
  if a**(N-1) mod N = 1 then (*Ist die kongruenz erfüllt ist N höchstwahrscheinlich prim!*)  
    writeln(N," ist höchstwahrscheinlich eine Primzahl!");  
    return true;  
  end;  
  writeln(N," ist keine Primzahl!"); (*wenn Bedingung oben nicht erfüllt ist Zahl nicht prim!*)  
  return false;  
end.
```

Quellen

www.wikipedia.de (10.06.07)

<http://www.mathematik.uni-dortmund.de> (10.06.2007)

Die Musik der Primzahlen – Paulo Ribenboim
(Springer Verlag, 2. Auflage)