

Übersicht über Primzahltests

Primzahltest 1

Gilt für alle Zahlen $a \in \mathbb{N}$ ($1 < a < n$): $\text{ggT}(a, n) = 1 \Rightarrow n$ ist Primzahl

- ```
isprime1:=proc(n) local a;
begin
 if n < 2 then return(FALSE); end_if;
 for a from 2 to n-1 do
 if igcd(a, n) > 1 then return(FALSE); end_if;
 end_for;
 return(TRUE);
end_proc;
```

### Primzahltest 2

Gilt für alle Zahlen  $a \in \mathbb{N}$  ( $1 < a \leq \lfloor \sqrt{n} \rfloor$ ):  $\text{ggT}(a, n) = 1 \Rightarrow n$  ist Primzahl.

- ```
isprime2:=proc(n)    local a;
begin
  if n < 2 then return(FALSE); end_if;
  for a from 2 to trunc(sqrt(n)) do
    if igcd(a, n) > 1 then return(FALSE); end_if;
  end_for;
  return(TRUE);
end_proc;
```

Kleiner Satz von Fermat

Ist $a \in \mathbb{N}$ kein Vielfaches der Primzahl p , so ist $a^{p-1} \equiv 1 \pmod{p}$.

Folgerung

Gibt es ein $a \in \mathbb{N}$ mit $\text{ggT}(a, n) = 1$ und $a^{n-1} \not\equiv 1 \pmod{n} \Rightarrow n$ ist zusammengesetzt

Primzahltest 3

Gilt für alle $a \in \mathbb{N}$ ($1 < a < n$) mit $\text{ggT}(a, n) = 1$: $a^{n-1} \equiv 1 \pmod{n} \Rightarrow n$ ist Primzahl oder Carmichaelzahl.

Carmichaelzahlen

Sei $n \in \mathbb{N}$ eine zusammengesetzte Zahl.

Gilt für alle $a \in \mathbb{N}$ mit $\text{ggT}(a, n) = 1$: $a^{n-1} \equiv 1 \pmod{n}$, so heißt n Carmichaelzahl.

Primzahltest 4

Gilt für einige $a \in \mathbb{N}$ ($1 < a < n-1$): $\text{ggT}(a, n) = 1$ und $a^{n-1} \equiv 1 \pmod{n} \Rightarrow n$ ist Primzahl oder Pseudoprimzahl.

Pseudoprimzahlen

Sei n eine ungerade zusammengesetzte Zahl.

Gibt es ein $a \in \mathbb{N}$ mit $a^{n-1} \equiv 1 \pmod{n}$, so heißt n Pseudoprimzahl zur Basis a .