Primfaktorzerlegung und Primzahltests

Maximilian Scholz

Proseminar Mathematik

June 24, 2014

Inhalt

Primzahlen

- Natürliche Zahlen > 1 die nur durch sich selbst und 1 teilbar sind.
- Es gibt unendlich viele Primzahlen. (Euklid)
- Jede natürliche Zahl lässt sich als Produkt von Primzalen darstellen. Bis auf die Reihenfolge ist diese Darstellung eindeutig. (Euklid)

Sieb des Eratosthenes

- Der kleinste Teiler > 1 einer zusammengesetzten Zahl n ist eine Primzahl p.

Sieb des Eratosthenes

- Der kleinste Teiler > 1 einer zusammengesetzten Zahl n ist eine Primzahl p.
- Da p der kleinste Teiler ist, gilt $p \leq \frac{n}{p}$, also $p^2 \leq n$.

Sieb des Eratosthenes

- Der kleinste Teiler > 1 einer zusammengesetzten Zahl n ist eine Primzahl p.
- Da p der kleinste Teiler ist, gilt $p \leq \frac{n}{p}$, also $p^2 \leq n$.
- Alle zusammengesetzten Zahlen $n < N$ werden also beim Sieben mit einer Siebzahl q mit $q^2 < n$ gestrichen.

Sieb des Eratosthenes

- Der kleinste Teiler > 1 einer zusammengesetzten Zahl n ist eine Primzahl p.
- Da p der kleinste Teiler ist, gilt $p \leq \frac{n}{p}$, also $p^2 \leq n$.
- Alle zusammengesetzten Zahlen $n < N$ werden also beim Sieben mit einer Siebzahl q mit $q^2 < n$ gestrichen.
- Die übrigen Zahlen sind also Primzahlen.

Sieb des Eratosthenes

BILD

Hase Igel Algorithmus

- Sei M eine endliche Menge mit der Abbildung $f : M \to M$.

Hase Igel Algorithmus

- Sei M eine endliche Menge mit der Abbildung $f : M \to M$.
- Man wähle $x_0 \in M$ und erzeuge die Folge $x_0, x_1, x_2, ...$ mit $x_{i+1} = f(x_i)$.

Hase Igel Algorithmus

- Sei M eine endliche Menge mit der Abbildung $f : M \to M$.
- Man wähle $x_0 \in M$ und erzeuge die Folge $x_0, x_1, x_2, ...$ mit $x_{i+1} = f(x_i)$.
- $\exists\ i, j \in \mathbb{N}$, sodass $i \neq j$ und $x_i = x_j$ gilt.

Hase Igel Algorithmus

- Sei M eine endliche Menge mit der Abbildung $f : M \to M$.
- Man wähle $x_0 \in M$ und erzeuge die Folge $x_0, x_1, x_2, ...$ mit $x_{i+1} = f(x_i)$.
- $\exists\ i, j \in \mathbb{N}$, sodass $i \neq j$ und $x_i = x_j$ gilt.
- Die Folge $y_0, y_1, y_2, ...$ gegeben durch $y_0 = x_0$ und $y_{i+1} = f(f(y_i))$ ist gleich der Folge $x_0, x_2, x_4, ...$

Beweis Teil 1

- $g : \mathbb{N} \to M$ gegeben durch $g(n) = f^n(x_0)$

Beweis Teil 1

- $g : \mathbb{N} \to M$ gegeben durch $g(n) = f^n(x_0)$
- M ist beschränkt also kann g nicht injektiv sein. Daraus folgt: $\exists\ i, j \in \mathbb{N}, i \neq j$ sodass $g(i) = g(j)$ und damit $x_i = x_j$ bei $i \neq j$.

Beweis Teil 2

- Angenommen $x_i = x_j$ für $j > i$.

Beweis Teil 2

- Angenommen $x_i = x_j$ für $j > i$.
- Falls $n \geq i$ und $2n = n + k(j - i) \geq i$ mit $k \geq 0$ muss $x_n = x_2 n$ gelten.

Beweis Teil 2

- Angenommen $x_i = x_j$ für $j > i$.
- Falls $n \geq i$ und $2n = n + k(j - i) \geq i$ mit $k \geq 0$ muss $x_n = x_2 n$ gelten.
- Man wähle $k \geq 0$ sodass $n = k(j - 1) \geq i$ und erhält das gesuchte n.

Beweis Teil 2

- Angenommen $x_i = x_j$ für $j > i$.
- Falls $n \geq i$ und $2n = n + k(j - i) \geq i$ mit $k \geq 0$ muss $x_n = x_2 n$ gelten.
- Man wähle $k \geq 0$ sodass $n = k(j - 1) \geq i$ und erhält das gesuchte n.
- Aus $x_{m+2} = f(f(x_m))$ folgt $y_m = x_{2m}$.

Konkruenz modulo p

- $a \equiv b \pmod{p} \Leftrightarrow p|(a-b)$

Konkruenz modulo p

- $a \equiv b \pmod{p} \Leftrightarrow p|(a-b)$
- $a = p \cdot x + c, \quad b = p \cdot y + c$

Konkruenz modulo p

- $a \equiv b \pmod{p} \Leftrightarrow p|(a-b)$
- $a = p \cdot x + c, \quad b = p \cdot y + c$
- $a - b = p(x-y) + (c-c) = p(x-y)$

Konkruenz modulo p

- $a \equiv b \pmod{p} \Leftrightarrow p|(a-b)$
- $a = p \cdot x + c, \quad b = p \cdot y + c$
- $a - b = p(x-y) + (c-c) = p(x-y)$
- $p|p(x-y)$

Pollard Rho Methode

- Sei N eine zusammengesetzte Zahl und p ein Primfaktor von N.

Pollard Rho Methode

- Sei N eine zusammengesetzte Zahl und p ein Primfaktor von N.
- Gesucht sind $0 \leq a, b < N$ sodass $a \equiv b \pmod{p}$. Dann gilt $p|a - b$

Pollard Rho Methode

- Sei N eine zusammengesetzte Zahl und p ein Primfaktor von N.
- Gesucht sind $0 \leq a, b < N$ sodass $a \equiv b \pmod{p}$.
  Dann gilt $p|a - b$
- Daraus folgt $1 < ggT(a - b, N) \leq N$.
  Wenn $a \neq b$ gilt, ist $ggT(a - b, N)$ ein nichttrivialer Faktor von N.

Pollard Rho Algorithmus

- Sei $f(x)$ eine ganzzahlige Polynomfunktion und $S \in \mathbb{Z}$.

Pollard Rho Algorithmus

- Sei $f(x)$ eine ganzzahlige Polynomfunktion und $S \in \mathbb{Z}$.
- Man erzeuge eine Folge von Pseudozufallszahlen mit:
  $x_0 = S,\ x_{i+1} = f(x_i) \mod N$.

Pollard Rho Algorithmus

- Sei $f(x)$ eine ganzzahlige Polynomfunktion und $S \in \mathbb{Z}$.
- Man erzeuge eine Folge von Pseudozufallszahlen mit: $x_0 = S,\ x_{i+1} = f(x_i) \mod N$.
- Wird schlielich periodisch, da beschränkt.

Pollard Rho Algorithmus

- Sei $f(x)$ eine ganzzahlige Polynomfunktion und $S \in \mathbb{Z}$.
- Man erzeuge eine Folge von Pseudozufallszahlen mit: $x_0 = S,\ x_{i+1} = f(x_i) \mod N$.
- Wird schlielich periodisch, da beschränkt.
- Anstatt $x_k =^? y_k$ suchen wir nach $ggT(x_k - y_k) >^? 1$

Pollard Rho Beispiel

Gesucht: Primfaktorzerlegung von N=143

Parameter: $x_0 = y_0 = 0,\ f(x) = (x^2 + 1) \mod N$

k	$x_k = f(x_{k-1})$	$y_k = f(f(y_{k-1}))$	$ggT(x_k - y_k, N)$
0	0	0	0
1	1	2	1
2	2	26	1
3	5	15	1
4	26	26	0
5	105	15	1
6	15	26	11

Gebutstagsproblem

-

Pollard Rho Komplexitt

-