# Primfaktorzerlegung und Primzahltests

Maximilian Scholz
Technische Universität Hamburg-Harburg

8. Juli 2014

**Zusammenfassung**

Mit dieser Ausarbeitung im Rahmen des Proseminars Mathematik will ich eine Einleitung in die Welt der Primzahlen im Allgemeinen und der Primfaktorzerlegung im besonderen schaffen.
Ich beginne mit einer Einleitung zu den Primzahlen und zeige anhand von Beispielen wie sich die Problematik der Primfaktorzerlegung auf verschiedene Wege angehen lässt. Hierzu beleuchte ich nicht nur die Algorithmen im einzelnen sondern zeige auch, welche Werkzeuge benutzt werden und erkläre auch diese detaillierter, da mir diese Herleitungen in der Fachliteratur oft zu kurz kommen.
Letztendlich ist mein Ziel vor Verständnis in einem sehr begrenzten Bereich zu schaffen anstatt in die Breite zu gehen, denn nur durch wirkliches Verständnis können neue Entdeckungen wie der zum Beispiel der AKS-Algorithmus gemacht werden.

# Inhaltsverzeichnis

# 1 Einführung in Primzahlen

Die wichtigsten Dinge die es zu Primzahlen im Bezug auf diesen Text gibt lassen sich wie folgt zusammenfassen:

- Definition: Jede natürliche Zahl $> 1$, die nur von sich selber und 1 geteilt wird, ist eine Primzahl. Dies lässt sich auch so beschreiben, dass eine Primzahl nur beim Teilen durch 1 und sich selber keinen Rest hat.

- Der griechische Mathematiker Euklid hat bewiesen, dass es unendlich Primzahlen gibt. Würde dies nicht gelten, könnte es zu Problemen bei modernen Kryptographischen Verfahren kommen, da diese auf immer gröÃ§er werdenden Primzahlen beruhen.

- Ebenfalls von Euklid kommt der Beweis dafür, dass sich jede natürliche Zahl als Produkt von Primzahlen darstellen lässt, wobei man hierfür die triviale Multiplikation mit der 1 hinzufügen muss. Später fand Gauss heraus, dass diese sogenannte Zerlegung bis auf die Reihenfolge der einzelnen Elemente eindeutig ist.
  Dies ist besonders interessant weil es uns ermöglicht zusammengesetzte Zahlen (also Zahlen, die nicht prim sind) daran zu erkennen, dass wir einen Faktor ungleich der Zahl oder 1 gefunden haben. AuÃ§erdem birgt dies die Grundlage zu manchen Angriffen auf Kryptografische Verfahren wie RSA, auf die in diesem Text allerdings nicht weiter eingegangen werden.

Dieser Text wird sich im weiteren Verlauf vor allem mit der Zerlegung von Zahlen in deren Primfaktoren befassen.

# 2 Sieb des Eratosthenes

Das Sieb des Eratosthenes ist ein etwa 2000 Jahre altes Verfahren, um alle Primzahlen in einem gegebenen Zahlenbereich zu finden.

## 2.1 Funktionsweise

Das Sieb des Eratosthenes bestimmt alle Primzahlen N, indem es alle zusammengesetzten Zahlen streicht, daher der Name: Sieb.
Das Abbruchkriterium ist ein schÃűnes Beispiel wie unnÃűtiger Aufwand vermieden werden kann.

## 2.2 Beispiel

Bevor die genaue Funktionsweise behandelt wird, hier einmal ein Beispiel fÃijr die Funktionsweise der Methode.

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 |
| 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 |
| 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 |
| 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 |
| 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 |
| 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 |
| 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 |

Tabelle 1: Caption

## 2.3 Mathematik

Derbe die Referenz 1

- article
- book
- report
- letter

1. article
2. book
3. report
4. letter

**article** Article ist ...

**book** Die book Klasse ist ...

**report** Die Klasse report ermöglicht es ...

**letter** Wenn man einen Breif schreiben sollte man eine andere Klasse nutzen, da diese für ein anderes als das deutsche Briefformat ausgelegt ist.

# 3 Pollard Rho Methode

Keine Arbeit ohne eine Tabelle!

## 3.1 Geburtstagsproblem

## 3.2 Hase Igel Algorithmus

### 3.2.1 Beispiel

### 3.2.2 Mathematik

## 3.3 Pollard Rho Algorithmus

### 3.3.1 Kongruenz modulo p

### 3.3.2 Idee

### 3.3.3 Beispiel

### 3.3.4 Mathematik

## 3.4 Komplexität

| erste Spalte | zweite Spalte | dritte Spalte | vierte Spalte |
|---|---|---|---|
| l steht für links | c für zentriert | r für rechts | und p für eine vordefinierte Größe |

# 4 Fazit

Nach langer Suche hat sich herausgestellt, dass es kein längeres LaTeX Beispiel, als das von [Lauritzen] geschriebene gibt.

# Literatur

[Lauritzen] *Niels Lauritzen. Concrete Abstract Algebra. Reptrinted with corrections 2006*

[bk2boint] *blub*