Zahlentheorie

Alexander May

Fakultät für Mathematik
Ruhr-Universität Bochum

Sommersemester 2013

Organisatorisches

- Vorlesung: **Mo 12–14** in HZO 70, **Mi 10–12** in HZO 60 (9 CP)
- Übung: **Mo 12–14**, **Mi 08–10, 12–14, 14–16**
- Assistenten: **Gottfried Herold, Dr. Martin Wendler, Anne Wald**
- SHKs: **Katharina Schütte, Puya Jafari, Lisa Koppka**
- Übungsbetrieb:
  - Präsenzübung, Start 08. April
  - Zentralübung, Start 15. April, **Mo 14–16** in NC 5/99
- Übungsaufgaben werden korrigiert.
- Gruppenabgaben bis 3 Personen
- Bonussystem: Zusätzlich zu den 100 Punkten in der Klausur können Bonuspunkte über die Übungen erworben werden.
  - 1 Punkt ab 5%, 2 Punkte ab 15%, . . . , 10 Punkte ab 95% der Übungspunkte.
- Klausurtermin: voraussichtlich Mitte Juli

Literatur

Vorlesung richtet sich nach

- Stefan Müller-Stach, Jens Piontkowski, “Elementare und algebraische Zahlentheorie”, Vieweg+Teubner, 2. Auflage, 2011.

Weitere Literatur:

- Peter Bundschuh, “Einführung in die Zahlentheorie”, Springer, 2002
- Alexander Schmidt, “Einführung in die algebraische Zahlentheorie”, Springer, 2007
- Rainer Schulze-Pillot, “Einführung in Algebra und Zahlentheorie”, Springer, 2008
- Helmut Koch, “‘Zahlentheorie”, Vieweg, 1997
- Reinhold Remmert, Peter Ullrich, “Elementare Zahlentheorie”, Birkhäuser, 1995
- Friedhelm Padberg, “Elementare Zahlentheorie”, Spektrum, 2008

Primzahlen

Definition Primzahl

Wir definieren die Menge der *Primzahlen*

$$\mathbb{P} = \{x \in \mathbb{N} \setminus \{1\} \mid x \text{ ist nur durch sich selbst und 1 teilbar.}\}$$

- Können wir effizient entscheiden, ob $x \in \mathbb{P}$?

Algorithmus Naiver Primzahltest

EINGABE: $x \in \mathbb{N}$

1. Falls x durch eine der Zahlen $2, \ldots, \lceil \sqrt{x} \rceil$ teilbar, Ausgabe "$x \notin \mathbb{P}$".
2. Sonst Ausgabe "$x \in \mathbb{P}$".

- **Korrektheit:** Falls x zusammengesetzt ist, so besitzt es einen Teiler der Größe höchstens $\sqrt{x}$.
- **Laufzeit:** Algorithmus benötigt höchstens $\sqrt{x} - 1$ Divisionen.
- Später: Primzahltests mit Laufzeit polynomiell in $\log_2(x)$.

Landau-Notation

Definition Landau-Notation

Seien $f, g : \mathbb{N} \to \mathbb{N}$ Funktionen. Es gilt

1. $f(n) = \mathcal{O}(g(n))$ gdw
   $\exists n_0 \in \mathbb{N}, c \in \mathbb{R}, c > 0$ mit $f(n) \leq c \cdot g(n)$ für alle $n \geq n_0$.
2. $f(n) = \Omega(g(n))$ gdw
   $\exists n_0 \in \mathbb{N}, c \in \mathbb{R}, c > 0$ mit $f(n) \geq c \cdot g(n)$ für alle $n \geq n_0$.
3. $f(n) = \Theta(g(n))$ gdw $f(n) = \mathcal{O}(g(n))$ und $f(n) = \Omega(g(n))$

Bsp:

- $2n = \mathcal{O}(n^2)$ und $2n = \mathcal{O}(n)$.
- $3n^2 + n \log n + 7 = \mathcal{O}(n^2)$
- $\sum_{i=1}^{n} i = \frac{n(n+1)}{2} = \mathcal{O}(n^2)$
- $\sum_{i=0}^{n} \frac{1}{i} = \mathcal{O}(\log n)$
- $n! = \mathcal{O}(n \left(\frac{n}{e}\right)^n)$

Sieb des Erasthostenes

Ziel: Berechne alle Primzahlen bis n.

Algorithmus Sieb des Erasthostenes

EINGABE: $n \in \mathbb{N}$

1. Schreibe alle Zahlen $2, \ldots, n$ in eine Liste L.
2. For $i = 2$ to n: Falls $i \in L$, entferne alle Vielfachen $2i, 3i, \ldots$ aus L.

AUSGABE: $L = \{x \in \mathbb{P} \mid x \leq n\}$

Korrektheit:

- Alle aus L entfernten Zahlen sind nicht in $\mathbb{P}$.
- Jede Nicht-Primzahl wird entfernt, sobald i ihr kleinster Teiler ist.
- Damit verbleiben in L nur Primzahlen.

Laufzeit:

- Schritt 1: $\mathcal{O}(n)$
- Schritt 2: höchstens $\frac{n}{2} + \frac{n}{3} + \ldots + 1 = \mathcal{O}(n \log n)$ Operationen.
- D.h. die Gesamtlaufzeit ist $\mathcal{O}(n \log n)$.

Unendlich viele Primzahlen

Satz von Euklid

Es existieren unendlich viele Primzahlen.

Beweis:

- Annahme: Sei $\mathbb{P} = \{p_1, \ldots, p_n\}$ endlich mit $p_1 < \ldots < p_n$.
- Sei $P = \prod_{i=1}^{n} p_i + 1$. Da $P > p_n$ folgt $P \notin \mathbb{P}$.
- D.h. P besitzt einen nicht-trivialen kleinsten Teiler a, $1 < a < P$.
- Sei $a \notin \mathbb{P}$. Dann besitzt a einen nicht-trivialen Teiler a', $1 < a' < a$, der ein Teiler von P ist (Widerspruch zur Minimalität von a).
- Es folgt $a \in \mathbb{P}$. Damit lässt $P = \prod_{p \in \mathbb{P}} p + 1$ bei Teilung durch a Rest 1. (Widerspruch: a teilt P.)

Wie konstruiert man Primzahlen?

Vermutung von Fermat: $F_k = 2^{2^k} + 1 \in \mathbb{P}$. Falsch schon für $k = 5$.

Lemma

Falls $b > 1$ ungerade oder $m \neq 2^k$, $m \geq 3$ so ist $b^m + 1$ nicht prim.

Beweis:

- Falls $b > 1$ ungerade, ist auch $b^m > 1$ ungerade. Damit ist $b^m + 1 > 2$ gerade und kann keine Primzahl sein.
- Ist $m \neq 2^k$, so gilt $m = pm'$ für einen ungeraden Faktor $3 \leq p \leq m$.
- Damit gilt $b^m + 1 = (b^{m'})^p + 1$. Wir wollen $(b^{m'})^p + 1$ faktorisieren.
- Betrachte dazu das Polynom $X^p + 1$ mit Nullstelle (-1). Es gilt
$$X^p + 1 = (X + 1)(X^{p-1} - X^{p-2} + X^{p-3} - \ldots - X + 1).$$
- Einsetzen von $X = b^{m'}$ liefert den nicht-trivialen ersten Faktor
$$1 < b^{m'} + 1 < b^m + 1.$$

Mersenne Primzahlen

Mersenne-Primzahlen sind Primzahlen der Form $2^p - 1$ für $p \in \mathbb{P}$.

Lemma

Falls m zusammengesetzt ist, so ist auch $2^m - 1$ zusammengesetzt.

Beweis:

- Sei $m = pq$ mit $1 < p, q < m$. Damit ist $2^m - 1 = (2^p)^q - 1$. Es gilt
$$X^q - 1 = (X - 1)(X^{q-1} + \ldots + X + 1).$$
- Einsetzen von $X = 2^p$ liefert nicht-trivialen Faktor
$$1 < 2^p - 1 < 2^m - 1.$$

Anmerkung:
Die größten *bekannten* Primzahlen sind oft von der Mersenne-Form.