BACHELORARBEIT

Titel der Bachelorarbeit

Satz von Wilson

Verfasserin

Esra Solmaz

angestrebter akademischer Grad

Bachelor of Education (BEd.)

Wien, im Monat Februar 2021

Studienkennzahl lt. Studienblatt:	UA 198 410 420 02
Studienrichtung lt. Studienblatt:	Bachelorstudium Lehramt Sek (AB) Lehrverbund UF Mathematik
Betreuer	Herr Mag. Dr. Andreas Ulovec

Abstract

Inwiefern ist eine Zahl eine Primzahl? Wie kann ich wissen oder zeigen, dass sich bei einer Zahl um eine Primzahl handelt? Gibt es dafür eine Formel, eine Methode, eine Theorie bzw. einen Satz?

Im Rahmen dieser Bachelorarbeit beschäftige ich mich mit dem Satz von Wilson, ein Satz aus der Zahlentheorie, der die Primzahlen charakterisiertund definiert. Der Satz, wiederentdeckt und benannt nach John Wilson, lautet kurz und präzise (falls man die Kongruenz einbezieht) folgendermaßen:

$$\textbf{Ist } p \in \mathbb{P} \textbf{ eine Prizahl, so ist } (p-1)! \equiv -1 \pmod{p}$$

(Markwig 2008)

Jedoch kann man den Satz auch anders und sogar noch einfacher formulieren. Diese verschiedenen Formulierungen werde ich in den nächsten Kapiteln und Abschnitten genauer darstellen.

Schon allein durch das Lesen dieses kurzen Satzes stoßen wir auf die verschiedenen "Vokabularen" und Zeichen der Mathematik. Im ersten Teil des Satzes ist die Primzahl angegeben. Des Weiteren ist die Fakultät mit dem Rufzeichen ebenfalls ein Teil des Satzes und im letzten "Abschnitt" kommen die Kongruenzen bzw. Restklassen in den Vordergrund. Aus dieser Tatsache erkennen wir, dass sich der Satz über verschiedene Gebiete der Mathematik erstreckt und anhand dieses Satzes besteht die Möglichkeit der Bestimmung der Primzahlen.

Die Arbeit besteht aus zwei Teilen. Im ersten Teil der Arbeit stelle ich die Primzahlen in den Vordergrund, da sie bezüglich des Satzes eine wichtige Rolle spielen. Dargestellt werden die geschichtlichen Aspekte und der Begriff der Primzahlen, sowie die Primzahltests. Im zweiten Abschnitt der Arbeit wird der Satz von Wilson, die Erfinder und die unterschiedlichen Formulierungen des Satzes, aber auch die Beweise genau untersucht. Außerdem werden mithilfe des Satzes einige Zahlen nach der Primalität überprüft.

Inhaltsverzeichnis

1 Primzahlen

1.1 Primzahlbegriff und geschichtliche Aspekte

Definition 1.1.1 (Primzahl)**.** *"Eine Primzahl ist eine natürliche Zahl $p > 1$, die nur die trivialen Teiler besitzt, d.h. deren einzige Teiler 1 und sie selbst sind" [1], S. 23.*

Die Primzahlen sind nicht vor einer kurzen Zeit erfunden worden. Schon vor mehrere hunderte von Jahren hatten sich die Mathematiker mit den Primzahlen beschäftigt. Hinsichtlich der Mathematiker, die als erste die Primzahlen untersuchten, sind die Mathematiker der pythagoräischen Schule (ab 500 bis 300 v. Chr.). Sie fokussierten sich auf die perfekten und befreundeten Zahlen und infolgedessen untersucheten sie die Primzahlen, aber auch die zusammengesetzten Zahlen. Es wurden viele relevante Entdeckungen von ihnen gemacht, jedoch konnten sie ihre Theorien nicht beweisen.

Abbildung 1.1: Euklid und die Elemente, 2021

"Um 300 v. Chr. veröffentlichte Euklid die Bücher der "Elemente", die viele wichtige Erkenntnisse der Primzahlforschung mit korrekt geführten Beweisen beinhalteten" (vgl. Sas 2002-2008, S. 4). Einer der wichtigen Beweise sind die unendlich vielen Primzahlen.

Theorem 1.1.2 (Satz von Euklid)**.** *Es gibt unendlich viele Primzahlen.*

Beweis. Angenommen gäbe es nur endlich viele Primzahlen. So bezeichnet man sie mit $p_1, ..., p_n$ und n ist die endliche Anzahl von Primzahlen. Also bildet man die Zahl $m = p_1 p_2 \dots p_n + 1$. "Weiters verwenden wir die Tatsache, dass jede natürliche Zahl größer 1 in Primfaktoren zerlegt, d.h. als Produkt von Primzahlen geschrieben werden kann". Jede solche Zahl ist durch mindestens eine Primzahl teilbar. Hinsichtlich dieser Tatsache muss es eine Primzahl geben, die m teilt. "Dies ist jedoch nicht möglich, da m durch keine der Primzahlen p_i $(1 \leq i \leq n)$ teilbar ist. (Es bleibt ja immer ein Rest von 1). Die logische Schlusskette endet in einem Widerspruch (vgl. [1], S. 25). □

CHINESISCHE VERMUTUNG

Ungefähr um die Lebzeit von Konfuzius ist eine Vermutung aufgestellt worden, die besagt, dass eine Zahl n dann und nur dann eine Primzahl ist, falls diese $2^n - 2$ teilt. Diese Vermutung stellte sich aber falsch heraus, denn $2^{341} - 2$ ist durch 341 teilbar und 341 ist eine zusammengesetzte Zahl. Häufig gab es Bezweiflungen, ob die Chinesen diese Vermutung tatsächlich aufgestellt hätten und man dachte auch, dass sie das Konzept der Primzahlen nie verfasst haben.

Diese Vermutung wird als Chinesische Hypothese bezeichnet (vgl. Sas 2002-2008, S.4ff).

SIEB DES ERATOSTHENES

Um 200 v. Chr. erfand Eratosthenes einen Algorithmus zur Anfertigung einer Tabelle mit allen Primzahlen bis zu einer bestimmten Zahl. Seine Methode wurde nach ihm benannt und sie heißt heute "Sieb des Eratosthenes" (vgl. Sas 2002-2008, S.5).

Kurze Erklärung zur Funktionsweise des Algorithmus

Zu Beginn wird eine Liste bestehend aus natürlichen Zahlen erstellt. Die Liste beginnt mit 2 und endet bei einer gewünschten Zahl n. Es wird die erste Zahl (die 2) durch das Umkreisen markiert und alle Vielfachen von 2 werden durchgestrichen. Danach wird die nächste nicht durchgestrichene Zahl, also die 3 markiert und ebenfalls die Vielfachen von 3 durchgestrichen. Diese Methode wird solange fortgesetzt, bis tatsächlich nur noch Zahlen in der Liste überbleiben, die markiert sind bzw. die keine Teiler (abgesehen von 1 und sich selbst) aufweisen. Diese Zahlen sind die Primzahlen. Alle durchgestrichenen Zahlen sind die Vielfachen von den markierten Zahlen und diese sind teilbar (vgl. Sas 2002-2008, S.5).

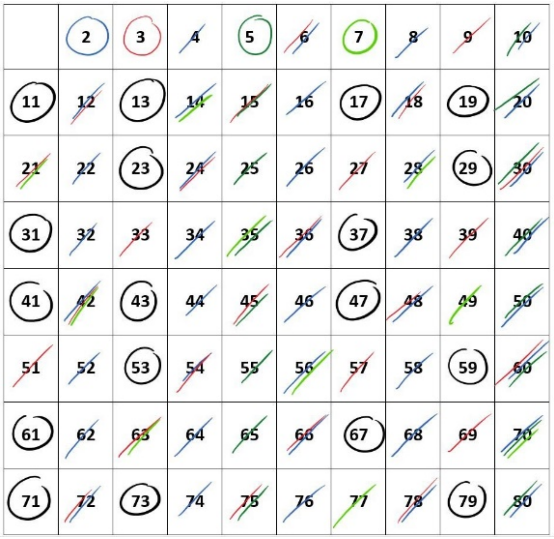

Abbildung 1.2: Sieb des Eratosthenes

Diese Technik ist bis zu einer bestimmten Zahl zwar gut gedacht, jedoch ist sie als Primzahltest

nicht geeignet. ”Um die Primalität einer Zahl n mit dem Sieb von Eratosthenes festzustellen, muß die Primalität aller Zahlen kleiner als n festgestellt werden“ (Sas 2002-2008, S.5).

MERSENNEZAHLEN UND DER KLEINE FERMATSCHE SATZ

Lange Zeit nach Eratosthenes wurde keine mathematische Forschung betrieben. Man begann sich mit der Mathematik und somit auch mit den Primzahlen wieder während der Renaissance zu beschäftigen. ”Dabei mussten viele Erkenntnisse aus der Zeit der Griechen erst wieder neu entdeckt werden“. Bezüglich der ersten Erforschungen der Neuzeit wurden die Zahlen der Form $2^n - 1$ untersucht und diese Zahlen werden Mersennezahlen genannt. Die abgekürzte Form ist M_n. ”Es ist leicht zu zeigen, daß n prim sein muß, damit M_n prim sein kann, daß nicht alle Zahlen dieser Form mit einer Primzahl n wieder eine Primzahl ist, wurde 1536 entdeckt ($211 - 1 = 2047 = 23 \cdot 89$)“. Im Jahr 1588 wurde von Cataldi bewiesen, dass $2^{19} - 1$ eine Primzahl ist und sie blieb ungefähr 200 Jahre lang die größte Primzahl (vgl. Sas 2002-2008, S.6f).

Zu Beginn des 17. Jahrhundert hat Fermat die erste wirklich andeutende Entdeckung seit Eratosthenes gemacht und eine neue Technik zur Zerlegung von größeren Zahlen gefunden. Hinsichtlich der Primzahlen gibt es den bekannten und nach ihm benannten Kleinen Fermatschen Satz, der besagt, dass falls p eine Primzahl ist, gilt für jede ganze Zahl a, daß $a^p \equiv a \mod p$. Dieser Satz unterstütz als Grundidee viele weitere Erkenntnisse in der Zahlentheorie und zahlreiche von Computern verwendete Verfahren zum Überprüfen von Primzahlen beziehen sich auf diesen Satz (vgl. Sas 2002-2008, S.6f).

DIE ZEIT AB DEM 20. JAHRHUNDERT

Ab Mitte des 20. Jahrhunderts haben die Computer in der Wissenschaft und auch in der Mathematik eine wichtige Rolle gespielt. Zwar hat diese neue Technik kaum neue Erkenntnisse hinsichtlich des Gebietes der Zahlentheorie gebracht, aber einen Primzahlrekord nach dem anderen. Der Amerikaner Robinson war der erste, den Computer zum Finden von Primzahlen verwendete und M_{2281} war die größte Primzahl, die er fand. Diese Entdeckung passierte im Jahr 1952. In den weiteren Jahren bzw. in der Folgezeit sind alle paar Jahre ein neuer Rekord gefunden worden (vgl. Sas 2002-2008, S.7f).

Im Rahmen des Projekts Great Internet Mersenne Prime Search (GIMPS) ist im Jahr 2018 die aktuell größte Primzahl $M_{82589933}$ entdeckt worden. Der US-amerikanische IT-Fachmann Patrick Laroche identifizierte die neue größte Primzahl mit ungefähr 25 Millionen Stellen und diese Zahl ist um mehr als 1,5 Millionen Ziffern länger als der bisherige Rekordhalter (vgl. ”Neue größte Primzahl hat 25 Millionen Stellen“, 2018)

1.2 Primzahltests

Wie im ersten Unterkapitel beschrieben, sind die Primzahlen unendlich. Das heißt, dass es auch große Primzahlen existieren, die für viele Verschlüsselungsverfahren immens bedeutend sind.

Jedoch gibt es keine Konstruktionsmethode hinsichtlich der Primzahlen, etwa wie eine effizient berechenbare Funktion $f : \mathbb{N} \to \mathbb{P}$ mit unendlicher Bildmenge (vgl. Karpfinger & Kiechle 2010, S.141). In diesem Abschnitt ist $\mathbb{P}$ die Menge aller Primzahlen.

In der Praxis wird eine ungerade natürliche Zahl n ausgesucht und auf Primalität geprüft. Es wird also geprüft, ob die Zahl n eine Primzahl ist und dazu werden die Primzahltests benutzt. Wird anhand eines solchen Tests festgestellt, dass die Zahl n keine Primzahl ist, so wird eine zu n nächstgelegene ungerade natürliche Zahl überprüft. Der Primzahlsatz garantiert dabei, dass mit hoher Wahrscheinlichkeit in der Nähe von n eine Primzahl liegt (vgl. Karpfinger & Kiechle 2010, S.141). Des Weiteren definiert der Primzahlsatz eine asymptotische Aussage über die Anzahl der Primzahlen (vgl. Schürz 2016, S.3).

Theorem 1.2.1 (Primzahlsatz)**.** *Es gilt* $\pi(x) \sim \frac{x}{\log(x)}$*, d.h.* $\lim_{x\to\infty} \pi(x) \cdot \frac{\log(x)}{x} = 1$ *(vgl. Karpfinger & Kiechle 2010, S.142).*

ARTEN VON PRIMZAHLTESTS

- **Echte Primzahltests**
  Die echten Primzahltests definieren bzw. erkennen immer, ob eine Zahl zusammengesetzt oder prim ist. Des Weiteren beziehen sich diese Tests auf Aussagen der Art "n ist genau dann eine Primzahl, falls folgende Bedingungen gelten" (vgl. Sas 2002-2008, S.10). Anhand der echten Primzahltests wie beispielsweise die Probedivision, Sieb des Eratosthenes und Sieb von Atkin können mögliche Teiler einfach gefunden werden (vgl. Primzahltests, 2021).
- **Tests auf Zusammengesetztheit**
  Bestätigt ein Test dieser Form das Ergebnis "zusammengesetzt", so ist die zu prüfende Zahl mit Sicherheit zusammengesetzt. Es kann aber nicht davon ausgegangen werden, dass falls man nicht zusammengesetzt bekommt, dass die Zahl auch tatsächlich eine Primzahl ist. Die Tests auf Zusammengesetztheit beziehen sich auf die Aussagen der Art "Gelten bestimmte Bedingungen, ist n zusammengesetzt" bzw. "Ist n prim, so gilt das Folgende" (vgl. Sas 2002-2008, S.11).

  Eine natürliche Zahl n wird zusammengesetzt bezeichnet, wenn es Zahlen $a, b \in \mathbb{N} \wedge a, b > 1$ vorhanden sind und $n = a \cdot b$ ist. Somit sind die zusammengesetzten Zahlen keine Primzahlen (vgl. Karpfinger & Kiechle 2010, S.141).
- **Tests auf Primalität**
  Eine weitere Variante hinsichtlich der Primzahltests sind die Tests auf Primalität, die nur mit Sicherheit erkennen, dass eine Zahl prim ist. Die Tests auf Primalität beziehen sich auf die Aussagen der Art "Gelten bestimmte Bedingungen, so ist n prim" bzw. "Ist n zusammengesetzt, so gilt das Folgende" (vgl. Sas 2002-2008, S.11).

- **Probabilistische Tests**
  Die probabilistische Primzahltests bauen auf Tests auf Zusammengesetztheit bzw. auf Test auf Primalität auf (vgl. Sas 2002-2008, S.11). Diese Tests sind gegebenfalls im Vergleich zu anderen Tests schneller, aber nicht vollkommen sicher. Falls eine Zahl n diesen Tests besteht, so ist sie mit großer Wahrscheinlichkeit eine Primazahl. Fällt eine Zahl bei diesen Tests durch, so ist sie sicher zusammengesetzt (vgl. Forster 2015, S. 92). Beispiele für probabilistische Tests sind der Fermat-Tests und Miller-Rabin-Test (vgl. Primzahltests, 2021).

- **Deterministische Tests**
  Eine weitere Form von Tests sind die deterministischen Tests. Ein Test heißt deterministisch, wenn er stets ein richtiges Ergebnis liefert bzw. wenn der Test "$n \in \mathbb{P}$" als Ergebnis ausgibt. So ist die Zahl n auch ganz sicher eine Primzahl (vgl. Karpfinger & Kiechle 2010, S.141).

  Der Unterschied hinsichtlich der oben erwähnten Tests liegt an ihrer Komplexität und ihrer Genauigkeit. Die Probedivision beweist das Vorliegen einer Primzahl. Der Fermat-Test und der Miller-Rabin-Tests zeigen bei positivem Ausgang des Tests nur eine Vermutung darüber, ob eine Primzahl vorkommt. Bei negativem Ausgang des Tests liefern sie einen Beweis, der zeigt, dass n keine Primzahl ist und sind streng genommen Tests auf Zusammengesetztheit. "Der Miller-Rabin-Test ist heutzutage für das Auffinden großer Primzahlen, wie man sie etwa für das RSA-Verfahren benutzt, das Mittel der Wahl". Dadurch dass der Miller-Rabin-Test ein probabilistischer Test ist und die Aussage "$n \in \mathbb{P}$" liefert, so ist n tatsächlich nur mit einer gewissen Wahrscheinlichkeit eine Primzahl. Bei diesem Test kann die Aussage "$n \in \mathbb{P}$" mit einer gewissen, kontrollierbar kleinen Fehlerwahrscheinlichkeit falsch sein (vgl. Karpfinger & Kiechle 2010, S.141).

2 Kapitel 2

Literatur

[1] Hermann Schichl und Roland Steinbauer. *"Einführung in das mathematische Arbeiten"*. Springer-Verlag Berlin Heidelberg, 2012. ISBN: 978-3-642-28646-9. DOI: 10.1007/978-3-642-28646-9.

Abbildungsverzeichnis