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 [4])

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

Abstract **i**

1 Primzahlen **1**
1.1 Primzahlbegriff und geschichtliche Aspekte 1
1.2 Primzahltests 4

2 Satz von Wilson **7**
2.1 Satz von Wilson 7
2.2 Abu Ali al-Hasan ibn al-Haytham 8
2.3 John Wilson 9
2.4 Der Beweis des Satzes von Wilson 9
2.5 Rechnerische Beispiel 10

3 Abschluss **14**

Literatur **15**

Abbildungsverzeichnis **16**

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" ([11], 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.

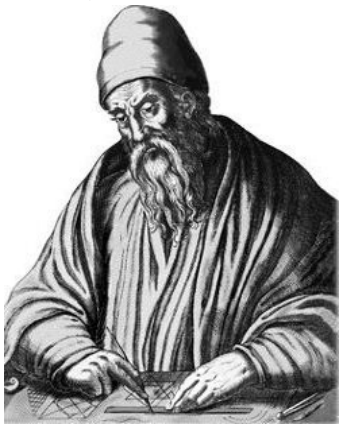

Abbildung 1.1: Bild von Euklid

"Um 300 v. Chr. veröffentlichte Euklid die Bücher der "Elemente", die viele wichtige Erkenntnisse der Primzahlforschung mit korrekt geführten Beweisen beinhalteten" (vgl. [10], 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. [11], 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. [10], 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. [10], 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. [10], S.5).

	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	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80

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“ (siehe [10], 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. [10], 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. [10], 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. [10], 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. [12], 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. [3], 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. [3], 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. [3], 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. [10], S.10). Anhand der echten Primzahltests wie beispielsweise die Probedivision, Sieb des Eratosthenes und Sieb von Atkin können mögliche Teiler einfach gefunden werden (vgl. [7], 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. [10], 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. [3], 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. [10], S.11).
- **Probabilistische Tests**
  Die probabilistische Primzahltests bauen auf Tests auf Zusammengesetztheit bzw. auf Test

auf Primalität auf (vgl. [10], 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. [2], S. 92). Beispiele für probabilistische Tests sind der Fermat-Tests und Miller-Rabin-Test (vgl. [7], 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. [3], 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. [3], S.141).
  Aufgrund der eindeutigen Vorstellung werden in den weiteren Abschnitten zwei Primzahltests kurz näher dargestellt. Es wird (neben dem Sieb von Eratosthenes) ein weiterer "echter" Primzahltest namens Probedivision und ein bekannter probabilistischer Test wie der Fermat-Test in den Vordergrund gebracht.

DIE PROBEDIVISION

Bei diesem Verfahren wird eine ungerade natürliche Zahl n betrachtet. Jeder Faktorisierungsalgorithmus und auch jeder praktische Primzahltest beginnt mit der Probedivision. Es wird überprüft, ob die Zahl n durch bekannte, kleine Primzahlen wie $3, 5, 7, 11, 13$, usw. teilbar ist. Effizient wird das mit der Division mit Rest gemacht. Definiert man bei der Division von n durch p keinen Rest, so gibt es einen Teiler von n und somit ist die Zahl n keine Primzahl. Des Weiteren werden die kleinen Primzahlen in einer Liste geführt und diese Liste ist so geformt, dass alle Elemente in 16-Bit-Wörter gespeichert werden können (vgl. [3], S.142).

Im Falle eines negativen Ergebnisses, d.h. falls der Test negativ ausfällt und keine kleinen Primteiler bestätigt werden, dann wird mit einem anderen Verfahren fortgesetzt und heutzutage ist diese Methodik meistens der Miller-Rabin-Test (vgl. [3], S.142).

Beispiel. Die Zahl $n = 253$ wird mit Rest nacheinander durch die Primzahlen $2, 3, 5, 7$ und 11 geteilt und es wird die Zerlegung festgestellt, dass $n = 11 \cdot 23$ ist (vgl. [3], S.142).

DER FERMAT-TEST

Dieser Primzahltest bezieht sich auf den kleinen Satz von Fermat.

Theorem 1.2.2 (Kleiner Fermatscher Satz). *"Sei p eine Primzahl und a eine beliebige natürliche Zahl mit* $ggT(a,p) = 1$*, so gilt* $a^{p-1} \equiv 1 \mod p$*" ([10], S. 14).*

Wird dieser Ausdruck mit a multipliziert, so erhält man

$$a^p \equiv a \mod p$$

Der Grund dafür ist, dass $ggT(a,p) = 1$ und somit ist der erste Ausdruck identisch zum zweiten Ausdruck (vgl. [10], S.14).

Weitere Hintergründe hinsichtlich dieses Satzes werden in der Arbeit nicht näher vorgestellt. Somit ist der erste Teil der Arbeit bezüglich der allgemeinen Darstellung der Primzahlen abgeschlossen.

2 Satz von Wilson

In diesem Abschnitt der Arbeit werden die ausführlichen Daten hinsichtlich des Satzes, die Mathematiker, die sich mit dem Satz von Wilson beschäftigt haben, in den Vordergrund gebracht, und einige Beweise dieses Satzes näher vorgestellt. Des Weiteren werden kurze Berechnungen bezüglich des Satzes betrachtet.

2.1 Satz von Wilson

Der Satz von Wilson kann auf zwei Varianten definiert werden. Die eine Variante, bei der Kongruenz nicht einbezogen ist, kommt selten in den Literaturen vor, wobei diese Variante - auch bei der Berechnung - viel einfacher zu verstehen ist. Hauptsächlich und in den meisten Büchern und Skripten ist die zweite Variante inklusive der Kongruenz zu sehen. Des Weiteren wird die zweite Variante je nach Autor des Buches oder Skripts unterschiedlich formuliert, wobei alle Formulierungen gleichwertig sind. In den weiteren Paragrafen werden beide Arten des Satzes vorgestellt.

Theorem 2.1.1 (Satz von Wilson). *"Wenn p eine Primzahl ist, dann ist* $1+(p-1)!$ *durch p teilbar" ([6], 2005).*

Theorem 2.1.2 (Satz von Wilson). *"Es ist p genau dann eine Primzahl, wenn* $(p-1)! \equiv -1 \mod p$*" (siehe [9], 2021).*

Außerdem gibt es eine weitere Option des Satzes, nämlich die Umkehrung. Diese lautet:

Theorem 2.1.3 (Umkehrung des Satzes von Wilson). *"Wenn n* $1+(n-1)!$ *teilt, dann ist n eine Primzahl" (vgl. [6], 2005).*

Der Satz von Wilson wurde zuerst von dem arabischen Mathematiker Abu Ali al-Hasan ibn al-Haytham, im Deutschen unter Alhazen bekannt, entdeckt und er wurde mehr als 700 Jahre später von John Wilson wiederentdeckt (vgl. Foco 2009, S.3 & vgl. [1]). Jedoch konnten beide Mathematiker den Satz nicht beweisen (vgl. [6] & vgl. [13], S.116). Der Satz und die Umkehrung wurden erstmals vollständig im Jahr 1773 von Lagrange bewiesen (vgl. [13], S.116).

2.2 Abu Ali al-Hasan ibn al-Haytham

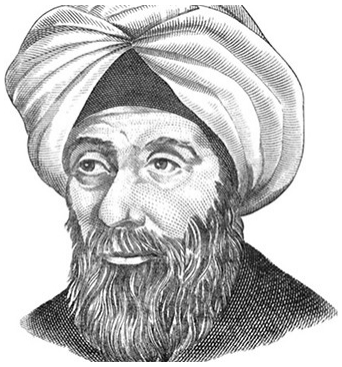

Abbildung 2.1: Ibn al-Haytham

Der arabische Wissenschaftler Abu Ali al-Hasan Ibn al-Haytham, abgekürzt Ibn al-Haytham und im Deutschen unter Alhazen bekannt, war ein engagierter Mathematiker, Physiker, Astronom (vgl. [8]). Geboren ist Alhazen um 965 n. Chr. in Basra (im heutigen Iraq) und er beschäftigte sich neben der Mathematik insbesondere mit der Optik (vgl. [1] & [5]). Aufgrund seiner bedeutenden wissenschaftlichen Beiträge hinsichtlich der Optik wurde er auch der "Vater der Optik" genannt. Beispielsweise war er der Entdecker der Lupe und somit der Mikroskopie (vgl. [1]).

In vielen Literaturen ist Alhazen für seine bedeutenden optischen Experimente und Arbeiten bekannt. Eine seiner wichtigen Leistungen war die Forschung hinsichtlich der "Sehstrahlen". Die bekannten Wissenschaftler wie Euklid und Ptolemäus sind damals davon ausgegangen, dass die sogenannten "Sehstrahlen", die das menschliche Auge verlassen sollten, die Umgebung anfühlten bzw. abtasteten und so zur Erzeugung des visuellen Eindrucks im Gehirn führten. Alhazen begann mit seiner Forschung bezüglich der "Sehstrahlen" mit der genauen Untersuchung des Aufbaues des Auges. Infolgedessen entdeckte er die Wichtigkeit bzw. die Bedeutung der Linse im Auge und aufgrund dessen konnte er anhand wissenschaftlicher Experimente die "Sehstrahlen"-Theorie widerlegen (vgl. [1]).

Bezüglich der Mathematik fokussierte sich Alhazen besonders auf die Geometrie und er schrieb sämtliche Bücher hinsichtlich dieses mathematischen Gebietes. Beispielsweise untersuchte er das Problem der Quadratur des Kreises und die Theorie der Kegelschnitte (vgl. [5] & vgl. [8]). Des Weiteren konnte er anhand seiner Ergebnisse über die Summation von Potenzen natürlicher Zahlen die Rauminhalte von Rotationskörpern berechnen (vgl. [13], S.13).

Außerdem beschäftigte sich Alhazen mit der Zahlentheorie und entdeckte den nach John Wilson benannten Satz. Anhand dieses Satzes löste Alhazen die Probleme mit Kongruenzen und der Satz lautet: wenn p eine Primzahl ist, dann ist $1+(p-1)!$ durch p teilbar.

Alhazen konnte den Satz jedoch nicht beweisen (vgl. [5]).

2.3 John Wilson

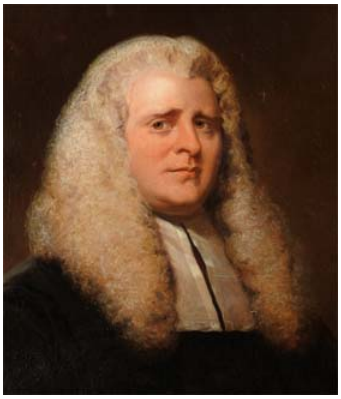

Abbildung 2.2: John Wilson

John Wilson, geboren am 06. August 1741 in Applethwaite, war ein englischer Mathematiker und Jurist, der für den nach ihm benannten Satz in der Geschichte der Mathematik bekannt ist. Studiert hat Wilson von 1757 bis 1761 in Cambridge und beendete sein Mathematikstudium mit erfolgreichen Noten. Genauer beschrieben, besaß Wilson die besten Noten unter den Studenten. Des Weiteren lehrte Wilson ab 1764 Mathematik in Cambridge und zwei Jahre später wurde Wilson in die Anwaltskammer berufen und hörte somit mit der Universitätslehre auf (vgl. [6]).

Wie es im ersten Absatz beschrieben ist, ist John Wilson unter den Mathematikern für seinen Satz berühmt, den er 1770 wiederentdeckte, da dieser Satz mehr als 700 Jahre davor von Alhazen zuerst erfunden worden ist (vgl. Foco 2009, S. 3). John Wilson hat die Vermutung getroffen, dass die Aussage "wenn p eine Primzahl ist, dann ist $1+(p-1)!$ durch p teilbar" tatsächlich existiert, jedoch konnte er keinen Beweis für diese Aussage bzw. für diesen Satz verfassen (vgl. [6]).

Auch Wilsons Professor Waring konnte den Satz nicht beweisen, jedoch wurde der Satz von ihm veröffentlicht und nach Wilson benannt (vgl. [6]). Im Jahr 1773 bewies Lagrange erstmals diesen Satz (vgl. [13], S.116).

2.4 Der Beweis des Satzes von Wilson

Der Satz von Wilson wird in vielen Büchern und Skripten gleichwertig, aber verschieden formuliert. Aus diesem Grund gibt es auch viele verschiedene Beweise. In diesem Unterkapitel der Arbeit möchte ich zwei Formulierungen des Satzes und die dazugehörigen Beweise vorstellen.

Einer von vielen Beweisen ist im Buch namens "Algorithmische Zahlentheorie" von Otto Forster (2. Auflage) vorgestellt. Dieser Beweis ist im Vergleich zu den anderen Beweisen etwas kurz, jedoch nach meiner Ansicht verständlich erklärt worden. Wie im ersten Paragrafen erwähnt ist, ist der Satz in dem Buch gleichwertig, aber anders definiert.

Theorem 2.4.1 (Wilson). *"Eine natürliche Zahl $p \geq 2$ ist genau dann eine Primzahl, wenn $(p-1)! \equiv -1 \mod p$" (vgl. [2], S. 56).*

Beweis. "Sei p keine Primzahl, sondern besitze einen Teiler q mit $1 < q < p$. Dann ist auch $(p-1)!$ durch q teilbar, also nicht teilerfremd zu p. Aber -1 ist teilerfremd zu p, Widerspruch!" ([2], S. 56). □

Des Weiteren wurde ein längerer Beweis hinsichtlich des Satzes von Wilson von Gábor Sas in seiner Arbeit präsentiert worden.

Theorem 2.4.2 (Wilson). *"$(p-1)! \equiv -1 \mod p$ gilt dann und nur dann, wenn p eine Primzahl ist" (siehe [10], S.12f).*
Beweis. Dieser Beweis wird in zwei Schritten geführt.

- p prim $\Rightarrow$ $(p-1)! \equiv -1 \mod p$
  Das Produkt über alle Elemente der multiplikativen Gruppe des Körpers $\mathbb{Z}_p$ steht links. "Da mit jedem $a \in \mathbb{Z}_p^\star$ auch $a^{-1} \in \mathbb{Z}_p^\star$ ist, lassen sich die Faktoren zu Paaren $a \cdot a^{-1} = 1$ zusammenfassen mit Ausnahme der Elemente, welche zu sich selbst invers sind, d.h. $a^2 = 1$ erfüllen". Aufgrund dass die Gleichung $x^2 = 1$ im Körper $\mathbb{Z}_p$ genau die Lösung ± 1 hat, folgt somit die Behauptung (vgl. [10], S.12f).
- $(p-1)! \equiv -1 \mod p \Rightarrow p$ prim
  "Ist $p = n \cdot m$, wobei n und m echte Teiler von p mit $m \neq n$ sind, dann sind beide Faktoren in $(p-1)!$ vorhanden und damit ist $(p-1)!$ durch $m \cdot n$ teilbar, also ist $(p-1)! \equiv 0 \mod p$. Sei nun $p = c^2$, so ist $(p-1)! = (p-1) \cdot (p-2) \cdot \ldots \cdot (2c) \cdot \ldots \cdot c \cdot \ldots \cdot 2 \cdot 1$. Ist nun $(p-1) > 2c = 2\sqrt{p}$, dann enthält $(p-1)!$ mindestens zweimal den Faktor c, und damit gilt auch $(p-1)! \equiv 0 \mod p$. Die Ungleichung $(p-1) > 2c = 2\sqrt{p}$ ist für alle $p \geq 6$ erfüllt, da $6-1 > 2\sqrt{6} \approx 4{,}9$ und die linke Seite wächst schneller als die rechte. Damit ist die einzige noch zu behandelnde Quadratzahl die 4, für $p = 4$ gilt jedoch $(p-1)! \equiv 3! \equiv 6 \equiv 2 \mod 4$" ([10], S 12).

□

Somit sind der Satz und die Beweise von zwei unterschiedlichen Autoren bzw. Verfassern auch unterschiedlich beschrieben. Es gibt jedoch viele weitere Formulierungen hinsichtlich dieses Satzes und der Beweise, jedoch werden nur diese in dieser Arbeit in den Vordergrund gebracht.

2.5 Rechnerische Beispiel

Der Satz von Wilson wird im Rahmen der Primzahltests auch als Wilsontest bezeichnet, denn auch anhand dieses Satzes können die Primzahlen festgestellt werden (vgl. [10], S.10ff). Da die Feststellung der Primzahlen heute nur noch mit den Computern geführt werden, ist es meistens ungünstig bzw. aufwändig, eine Menge von Primzahlen schriftlich mit der Hand zu definieren. Hinsichtlich des effektiven Verständnisses des Satzes werden in diesem Teil der Arbeit einige Primzahlen mithilfe der beiden Arten des Satzes Wilson festgestellt.

- **"Wenn p eine Primzahl ist, dann ist $1+(p-1)!$ durch p teilbar".**
  Wir setzen für p beliebige natürliche Zahlen ein und untersuchen das Ergebnis.

Wenn 2 eine Primzahl ist, dann ist $1+(2-1)!$ durch 2 teilbar	$2 \mid 2$	2 ist eine Primzahl
Wenn 3 eine Primzahl ist, dann ist $1+(3-1)!$ durch 3 teilbar	$3 \mid 3$	3 ist eine Primzahl
Wenn 4 eine Primzahl ist, dann ist $+(4-1)!$ durch 4 teilbar	$4 \nmid 7$	4 ist keine Primzahl
Wenn 10 eine Primzahl ist, dann ist $1+(10-1)!$ durch 10 teilbar	$10 \nmid 362881$	10 ist keine Primzahl
Wenn 11 eine Primzahl ist, dann ist $1+(11-1)!$ durch 11 teilbar	$11 \mid 3628801$	11 ist eine Primzahl
Wenn 12 eine Primzahl ist, dann ist $1+(12-1)!$ durch 12 teilbar	$12 \nmid 39916801$	12 ist keine Primzahl

Anhand des Einsetzens von natürlichen Zahlen besteht die Möglichkeit zur Untersuchung, ob die Zahl tatsächlich eine Primzahl ist. Die hellrot hinterlegten Zeilen weisen auf die Zahlen hin, die keine Primzahlen sind.

- **"Es ist p genau dann eine Primzahl, wenn** $(p-1)! \equiv -1 \mod p$**"**.

  Bei der zweiten Form des Satzes ist die Kongruenz miteinbezogen und bevor die Zahlen nach der Primalität überprüft werden, wird die Definition der Kongruenz in den Vordergrund gebracht.

Definition 2.5.1 (Kongruenz). *"Gegeben sei ein Modul $m \in \mathbb{N}$. Zwei ganze Zahlen a und b heißen kongruent modulo m, wenn die Division von a und b durch m den gleichen Rest r lässt" (http://www.math.uni-bremen.de, 2021).*

Im Zuge eines deutlichen Vergleiches der Formen und der Methodik werden die gleichen Zahlen in die zweite Art des Satzes eingesetzt und ebenfalls nach der Primalität untersucht.

Es ist 2 genau dann eine Primzahl, wenn $(2-1)! \equiv -1 \mod 2$	$1 \equiv -1$? $1 = 0 \cdot 2 + 1$ (Rest) $-1 = -1 \cdot 2 + 1$ (Rest)
Es ist 3 genau dann eine Primzahl, wenn $(3-1)! \equiv -1 \mod 3$	$2 \equiv -1$? $2 = 0 \cdot 3 + 2$ $-1 = -1 \cdot 3 + 2$
Es ist 4 genau dann eine Primzahl, wenn $(4-1)! \equiv -1 \mod 4$	$6 \equiv -1$? $6 = 0 \cdot 4 + 2$ $-1 = -0,75 \cdot 4 + 2$
Es ist 10 genau dann eine Primzahl, wenn $(10-1)! \equiv -1 \mod 10$	$362880 \equiv -1$? $362880 = 36288 \cdot 10 + 0$ $-1 = -0,1 \cdot 10 + 0$
Es ist 11 genau dann eine Primzahl, wenn $(11-1)! \equiv -1 \mod 11$	$3628800 \equiv -1$? $3628800 = 329890 \cdot 11 + 10$ $-1 = -1 \cdot 11 + 10$
Es ist 12 genau dann eine Primzahl, wenn $(12-1)! \equiv -1 \mod 12$	$39916800 \equiv -1$? $39916800 = 3326400 \cdot 12 + 0$ $-1 = -0,083 \cdot 12 + 0$

Analyse der Rechenschritte und des Ergebnisses

Die zweite Form des Satzes ist im Vergleich zur ersten Form ein wenig umständlich, denn bei dieser Methode sind zwei Gleichungen für jede überprüfende Zahl aufzustellen. Anhand der Zahl 2 werden die Schritte näher beschrieben.

Zahl 2: “Es ist 2 genau dann eine Primzahl, wenn $(2-1)! \equiv -1 \mod 2$”.
$(2-1)! = 1$ und ist $1 \equiv -1 \mod 2$?

Zur Überprüfung stellen wir die Gleichungen auf:

(I) $1 = 0 \cdot 2 + 1$ (Rest) $\qquad 1 : 2 = 0 \rightarrow 1$ Rest

(II) $-1 = -1 \cdot 2 + 1$ (Rest)

Die zweite Gleichung muss “ähnlich” wie die erste Gleichung aufgestellt werden, d.h. mit dem gleichen Teiler und Rest. Der erste Faktor kann bei beiden Gleichungen verschieden sein, jedoch muss er zur Menge der ganzen Zahlen gehören.

Dadurch, dass die beiden Gleichungen die Bedingungen erfüllen, ist $(2-1)! \equiv -1 \mod 2$ und daraus folgt, dass die Zahl 2 eine Primzahl ist.

Wenn die Berechnungen der Primzahlen genau untersucht werden, so ist es ersichtlich, dass die zweite Gleichung (mit -1) immer mit dem Faktor -1 beginnt und mit dem gleichen Teiler und Rest endet. Steht aber anstatt von -1 ein anderer Faktor, so folgt, dass diese Zahlen keine Primzahlen sind.

3 Abschluss

Abschließend wird erforscht, ob der Wilsontest als Primzahltest geeignet bzw. praktisch ist. Wie es in den Unterkapiteln des zweiten Abschnittes beschrieben ist, kann man auch anhand dieses Satzes Primzahlen definieren. Jedoch werden in den Büchern und Skripten hervorgehoben, dass der Wilsontest hinsichtlich des Primzahltests ungeeignet ist.

Otto Forster argumentiert in seinem Buch "Algorithmische Zahlentheorie", dass obwohl der Satz von Wilson eine notwendige und hinreichende Bedingung für die Primalität von p liefert, ist er trotzdem für praktische Primzahltest ungeeignet, weil es für die Berechnung von $(p-1)!$ mod p keinen schnellen Algorithmus gibt, der mit dem Potenzierungs-Algorithmus vergleichbar wären (vgl. [2], S.57).

Auch Gábor Sas erwähnt in seinem Skriptum, dass dieser Test sehr ineffizient ist, da wiederum für die Berechnung der Fakultät keine schnellen Methoden bekannt sind und müsste $p-2$ Multiplikationen durchführen, um eine Zahl als Primzahl zu "entlarven". Aus diesem Grund wird der Test praktisch unanwendbar (vgl. [10], S.13).

Als angehende Lehrerin aber werde ich diesen Satz auf jeden im Unterricht einsetzen, da anhand dieses Satzes und einer praktischen Tabelle (Kapitel 2.7) die Zahlen nach der Primalität einfach überprüft werden können.

Allgemein möchte ich andeuten, dass ich diesen Satz aus dem Grund gewählt habe, da bestimmte Sätze in der Mathematik für eine (lange) Zeit verloren gegangen sind und viele Jahre später wiederentdeckt waren. Auch der Satz von Wilson ist mehr als 700 Jahre später wiedererfunden worden und somit habe ich mich für diesen Satz entschieden. Ich wollte mich erkundigen, warum dieser Satz für mehr als 700 Jahre in Vergessenheit geraten ist und hinsichtlich der Recherche kam ich auf den Punkt, dass dieser Satz von Alhazen nicht bewiesen werden konnte und das könnte ein Anlass für die Vergessenheit gewesen sein. Außerdem habe ich den Satz aufgrund der Methodik mit der Fakultät und Kongruenz sehr interessant gefunden.

Ich bedanke mich beim Herrn Mag. Dr. Andreas Ulovec für die großartige Unterstützung meiner Bachelorarbeit und des Weiteren möchte ich in den Vordergrund bringen, dass ich den Herrn Professor immer weiterempfehlen werde.

Literatur

[1] Eslam.de. „Abu Ali al-Hasan Ibn al-Haitham“. In: *Enzyklopädie des Islam* (). Online: http://www.eslam.de/begriffe/a/ai/alhazen.htm. Abgerufen am 2021.

[2] Otto Forster. *“Algorithmische Zahlentheorie”*. Springer Spektrum, 2015. ISBN: 978-3-658-06539-3. DOI: 10.1007/978-3-658-06540-9.

[3] Christian Karpfinger und Hubert Kiechle. *“Kryptologie, Algebraische Methoden und Algorithmen”*. Vieweg + Teubner, 2010. ISBN: 978-3-8348-0884-4. DOI: 10.1007/978-3-8348-9356-7.

[4] Thomas Markwig. „Elementare Zahlentheorie“. In: *Vorlesungsskript. TU Kaiserslautern* (Apr. 2008). Online: https://studylibde.com/doc/6581953/elementare-zahlentheorie. Abgerufen am 2021.

[5] O’Connor und Robertson. „Abu Ali al-Hasan ibn al-Haytham“. In: *Mac Tutor* (1999). Online: https://mathshistory.st-andrews.ac.uk/Biographies/Al-Haytham/. Abgerufen am 2021.

[6] O’Connor und Robertson. „Abu Ali al-Hasan ibn al-Haytham“. In: *Mac Tutor* (2005). Online: https://mathshistory.st-andrews.ac.uk/Biographies/Wilson_John/. Abgerufen am 2021.

[7] Primzahle.net. „Primzahltests“. In: *Primzahlen.net* (). Online: https://primzahlen.net/primzahltests/. Abgerufen am 2021.

[8] Roshdi Rashed. „Ibn Al-Haytham“. In: (). Abgerufen am 2021.

[9] „Rechnen mit Restklassen“. In: *Grundlagen der elementaren Zahlentheorie* (). Moodle: https://wuecampus2.uni-wuerzburg.de/moodle. Abgerufen am 2021.

[10] Gábor SAS. „Primzahltests“. In: *https://dmg.tuwien.ac.at/drmota/Sas_primetests_endversion.pdf (2002-2008)* (). Abgerufen am 2021. Mirror: https://docplayer.org/18085267-Primzahltests-g-abor-sas-2002-2008.html.

[11] 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.

[12] Der Standard. „Neue größte Primzahl hat 25 Millionen Stellen“. In: *Der Standard - Wissenschaft - Welt* (Dez. 2018). Online: https://www.derstandard.at/story/2000094950656/neue-groesste-primzahl-hat-25-millionen-stellen. Abgerufen im Jänner 2021.

[13] Jochen Ziegenbalg. *“Elementare Zahlentheorie”*. Springer Spektrum, 2015. ISBN: 978-3-658-07170-7. DOI: 0.1007/978-3-658-07171-4.

Abbildungsverzeichnis

1.1 Bild von Euklid (Kurz-Info: Euklid und die Elemente, 2021 1
1.2 Das Sieb des Eratosthenes, 2021 2

2.1 Ibn al-Haytham (Ibn al-Haytham's scientific method, 2015) 8
2.2 John Wilson (John Wilson (mathematician), 2020) 9