4 Beweise für die Unendlichkeit von Primzahlen

Lukas Raschke

Winf100949

Prof. Dr. Sebastian Iwanowski

Seminar Elegante Beweise

FH Wedel

University of Applied Sciences

Wintersemster 2016/2017

Inhaltsverzeichnis

1. Einleitung

1.1 Grundlagen

1.1.1 Primzahlen allgemein

Eine Primzahl ist eine natürliche Zahl, die nur durch die Zahl 1 und sich selber geteilt werden kann. Eine Ausnahme stellt die 2 als kleinste Primzahl dar.

1.1.2 Hauptsatz der elementaren Zahlentheorie

Jede natürliche Zahl $n \in \mathbb{N}$ mit $n > 1$ lässt sich auf genau eine Weise als Produkt von Primzahlen darstellen:

$$n = \prod_{i=1}^{k} {p_i}^{a_i} = {p_1}^{a_1} \cdot \ldots \cdot {p_k}^{a_k}$$

mit $a_k \in \mathbb{N},\ p_k \in \mathbb{P}\ und\ p_1 < p_2 < \cdots < p_k$.[1]

Sowohl die Existenz des Hauptsatzes (Existenz der Primzahlzerlegung), als auch die Eindeutigkeit (mithilfe vollständiger Induktion) wurden bereits bewiesen und wird im Folgenden somit als gesetzt angenommen.

1.2 Motivation

Im Bereich der Kryptografie und insbesondere bei der Verschlüsselung moderner Kommunikation ist die Unendlichkeit von Primzahlen von zentraler Bedeutung. Die meisten Verschlüsselungsverfahren benutzen heutzutage zwei Schlüssel für die Kommunikation. Der erste Schlüssel (Public Key) wird durch die Verwendung eines Produktes aus (sehr) großen Primzahlen erzeugt. Der zweite Schlüssel (Private Key) wird aus den dazugehörigen Primfaktoren abgeleitet. Da für die Primfaktorzerlegung einer Zahl ein NP-vollständiges Problem ist, ist es für die Zerlegung einer hinreichend großen Zahl, in diesem Fall der Public Key, nicht praktikabel, den Private Key zu errechnen.

Eine Endlichkeit der Primzahlen würde, aufgrund steigender Rechenleistung, Verschlüsselungs-Algorithmen nutzlos machen.

[1] Sebastian Iwanowski, Rainer Lang (2014): Seite 137.

2. Satz des Euklid

Der Beweis von Euklid ist ein indirekter Beweis. Wir nehmen zuerst an, dass die Menge aller Primzahlen $\{P_1, P_2, P_3, \ldots, P_k\}$ endlich sei und dadurch P_k die größte bekannte Primzahl darstellt. Unser Ziel ist es, einen Widerspruch in unserer Beweislogik zu finden, und somit unsere Annahmen zu wiederlegen.

Zunächst überlegen wir uns eine beliebige Zahl n und definieren diese wie folgt:

$$n = P_1 \cdot P_2 \cdot P_3 \cdot \ldots \cdot P_k + 1$$

Durch den Hauptsatz der elementaren Zahlentheorie wissen wir, dass n von einem Primfaktor P_j geteilt wird. Aufgrund unserer Annahmen muss $P_j \in \{P_1, P_2, P_3, \ldots, P_k\}$ sein und teilt diese Menge folglich auch. Wir erhalten also:

$$P_j \mid n \quad \wedge \quad P_j \mid (n-1) \quad \rightarrow \quad P_j \mid 1$$

Der Primfaktor P_j teilt n und $(n-1)$ und somit auch die Differenz. Dies ist der gewünschte Widerspruch. P_j muss von allen P_k verschieden sein. Im Umkehrschluss kann unsere Menge, nie die Menge aller Primzahlen sein.

3. Brief von Christian Goldbach an Euler

3.1 Grundlagen

Dieser Beweis stammt aus einem Brief von Christian Goldbach an Euler aus dem Jahr 1730. Er ist unabhängig von der Goldbachschen Vermutung. In dieser Beweisführung werden die nach dem französischen Mathematiker und Jurist Pierre de Fermat benannten Fermat-Zahlen verwendet. Eine Fermat-Zahl ist eine Zahl der Form

$$F_n = 2^{2^n} + 1$$

Fermat vermutete, dass alle Fermat-Zahlen prim seien. Euler widerlegte diese Behauptung ein Jahrhundert später jedoch, indem er F_5 in ihre Primfaktoren ($F_5 = 641 * 6700417$) zerlegte. Bis heute sind lediglich F_0 bis F_4 als Primzahlen bekannt.

3.2 Idee

Unter der Annahme, dass zwei Fermat-Zahlen immer teilerfremd seien, „verbraucht" jede Fermat-Zahl Primfaktoren. Jede Fermat-Zahl besitze somit eindeutige Primfaktoren, die in keiner anderen Fermat-Zahl auftauchen. Durch die Unendlichkeit der natürlichen Zahlen, ist die Menge der Fermat-Zahlen ebenso unendlich, wodurch es dann auch unendlich Primzahlen gäbe.

Beispiel bis F_5: $F_0 = 3;$ $F_1 = 5;$ $F_2 = 17;$ $F_3 = 257;$

$F_4 = 65537;$ $F_5 = 641 * 6700417$

Es ist deutlich zu erkennen, dass die Vermutung in diesem kleinen Beispiel zutrifft.

3.3 Beweis

Es ist lediglich die Tatsache, dass zwei Fermat-Zahlen teilerfremd sind zu beweisen, da die restliche Argumentation des Beweises, wie oben beschrieben, trivial daraus folgt. Der Zusammenhang zwischen zwei Fermat-Zahlen F_k und F_n lässt sich durch folgende Rekursion beschreiben:

$$\prod_{k=0}^{n-1} F_k = F_n - 2; \qquad mit\ (n \geq 1)\ und\ (k < n)$$

Im nächstes Schritt überlegen wir uns einen gemeinsamen Teiler m von F_k und F_n, um zu zeigen, dass diese zwei Zahlen relativ prim sind. Aus der Rekursion ist zu erkennen, dass m neben F_k und F_n auch die Differenz (2) teilen muss. m kann also lediglich die Werte $m = 1$ oder $m = 2$ besitzen.

$m = 2$ können wir ausschließen, da jede Fermat Zahl ungerade ist und m somit keine geraden Werte annehmen kann.

Mit $m = 1$ ist die Teilerfremdheit zwischen F_k und F_n bewiesen, sofern die o.g. Rekursion korrekt ist. Um den Beweis also abzuschließen, beweisen wir diese Rekursion anhand vollständiger Induktion.

Verankerung $n = 1$:

$$\prod_{k=0}^{n-1} F_k = F_n - 2 \quad \rightarrow \quad 2^{2^0} + 1 = \left(2^{2^1} + 1\right) - 2 \quad \rightarrow \quad 3 = 5 - 2$$

Induktionsschluss $n \rightarrow (n+1)$:

Induktionsannahme

$$\prod_{k=0}^{n} F_k = \left(\prod_{k=0}^{n-1} F_k\right) \cdot F_n = (F_n - 2) \cdot F_n$$

$$= \left(2^{2^n} - 1\right)\left(2^{2^n} + 1\right) = 2^{2^{n+1}} - 1 = F_{n+1} - 2$$

4. Mersenne Zahl

4.1 Grundlagen

Der nachfolgende Beweis verwendet Mersenne-Zahlen und benötigt zum Verständnis den Satz von Lagrange.

4.1.1 Satz von Lagrange

Sei G eine endliche Gruppe.

(1) Ist H eine Untergruppe von G, so gilt |H| | |G|.

(2) Die Ordnung eines Elementes x von G teilt die Gruppenordnung. Also für $x \in G$ gilt |x| | |G|.[2]

4.1.2 Mersenne-Zahlen

Mersenne-Zahlen sind Zahlen der Form:

$$M_n = 2^n - 1$$

Die ersten Mersenne-Zahlen sind: $M = \{1, 3, 7, 15, 31, 63, 127, \dots\}$

4.2 Idee

Wie bereits im ersten Beweis von Euklid, nimmt man zunächst eine größte bekannte Primzahl P an. Mithilfe dieser Primzahl erzeugt man nun eine Mersenne-Zahl $M_P = 2^P - 1$. Im Verlauf des Beweises versuchen wir nun zu zeigen, dass jeder Primteiler q von M_P größer P ist und P somit nicht die größte bekannte Primzahl sein kann.

4.3 Beweis

Sei q ein beliebiger Primteiler von M_P. Zunächst überlegen wir uns die multiplikative Gruppe $\mathbb{Z}_q \backslash \{0\}$ des Körpers $\mathbb{Z}_q$. Die Anzahl der Elemente dieser Gruppe beträgt $q - 1$, da wir mit der {0} ein Element aus der Gruppe nehmen. Wäre die {0} mit einbezogen, hätten wir das Inverse Element verletzt und es würde sich nicht mehr um eine Gruppe handeln. Weil wir q als Primteiler von M_P definiert haben, ergibt sich $2^P mod\ q \equiv 1$.

Um zu beweisen, dass der Primteiler q größer als die Primzahl P ist, müssen wir uns die Ordnung eines

[2] Marc Richter (2013): Seite 4.

Elementes der Gruppe $\mathbb{Z}_q\backslash\{0\}$ überlegen. Aufgrund der Tatsache, dass P eine Primzahl ist und wir uns $2^P mod\ q \equiv 1$ überlegt haben, muss die Ordnung des Elementes 2 genau P sein.

$$o\big(2 \in \mathbb{Z}_q\backslash\{0\}\big) = P$$

Es ist nun also die Gruppenordnung $q - 1$ und die Ordnung eines Elementes bekannt. Aufgrund des o.g. Satz von Lagrange wissen wir, dass die Ordnung eines Elementes der Gruppe die Gruppenordnung teilt. Folglich muss P also q teilen: $P|q - 1$. Unschwer zu erkennen ist, dass $P < q - 1$ sein muss. Dies steht jedoch im Widerspruch zu unserer ursprünglichen Definition.

Jeder Primteiler einer Mersennen-Zahl ist größer, als die erzeugende Primzahl.

5. Beweis nach Euler

5.1 Idee

Im Gegensatz zu den anderen Beweisen aus dem Gebieten der Zahlentheorie und Algebraischen Strukturen nutzt Euler in seinem Beweis die Analysis. Seine Idee ist es, die Anzahl aller Primzahlen kleiner einer reellen Zahl x mit dem Logarithmus $\log(x)$ dieser Zahl zu vergleichen. Der Trick seines Beweises liegt in der Tatsache, dass der Logarithmus unendlich ist.

5.2 Beweis

Zu Beginn des Beweises definieren wir uns eine Funktion $R(x)$, die alle Primzahlen $\{p_1, p_2, p_3, \dots\}$ kleiner gleich einer reellen Zahl x angibt:

$$R(x) := \#(p \leq x | p \in \mathbb{P}),\ x \in \mathbb{R}$$

Außerdem sei die Menge der Primzahlen aufsteigend sortiert ($\mathbb{P} := \{p_1, p_2, p_3, \dots\}$) und $\log(x)$ als natürlicher Logarithmus $\log(x) = \int_1^x \frac{1}{t} dt$ definiert. Zusätzlich benötigen wir für die obere Treppenfunktion, welche wir mithilfe der harmonischen Reihe modellieren, noch eine natürliche Zahl $n \in \mathbb{N}$ als Endpunkt. n sei in unserem Beweis als $n \leq x \leq n+1$ definiert.

Im nächsten Schritt wird nun der natürliche Logarithmus mit der harmonischen Reihe bis n vergleichen. Wie man auf Abbildung 1 unschwer erkennen kann, ist der Logarithmus immer kleiner gleich der oberen Treppenfunktion:

$$log(x) \leq 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n-1} + \frac{1}{n} \leq \cdots$$

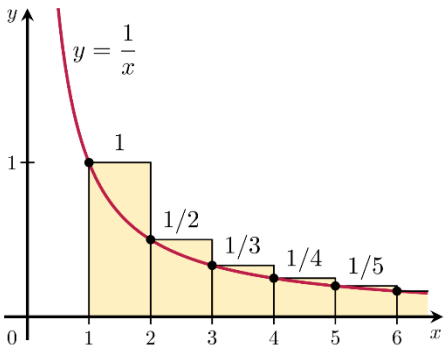

Abbildung 1

Die obere Treppenfunktion ist wiederum kleiner als die Summe aller Kehrwerte der natürlichen Zahlen m, die nur Primfaktoren p enthalten, welche kleiner gleich x sind:

$$\dots \leq \sum{}' \frac{1}{m}; \qquad m \in \mathbb{N}, \qquad p \leq x$$

Diese Summe ist immer größer gleich der oberen Treppenfunktion, da mindestens alle Brüche der oberen Treppenfunktion auch hier enthalten sind. Jede natürliche Zahl $m \leq x$ kann nur Primfaktoren besitzen, die ebenfalls $p \leq x$ sind.

Nach dem Hauptsatz der elementaren Zahlentheorie, lässt sich jede natürliche Zahl als Produkt ihrer Primzahlpotenzen schreiben (siehe 1.1.2). Schreiben wir m in Form seiner Primzahlpotenzen und kombinieren dies mit unserer Summe, erhalten wir folgendes Produkt:

$$\leq \prod_{p \leq x} \left(\sum_{k \geq 0} \frac{1}{p^k} \right)$$

Die Summe innerhalb der Klammer entspricht einer geometrischen Reihe. Diese konvergiert immer gegen den Grenzwert $\frac{1}{1-\frac{1}{p}}$. Wir erhalten also folgenden Ausdruck:

$$log(x) \leq \prod_{p \leq x} \frac{1}{1 - \frac{1}{p}}$$

Das Produkt lässt sich weiter umformen. Das Umformen wird an dieser Stelle übersprungen, kann aber im Abschnitt 5.3 nachvollziehen. Am Ende der Umformung erhalten wir ein Teleskopprodukt von 1 bis $R(x)$. Aufgrund der besonderen Eigenschaft von Teleskopprodukten, lässt sich das Ergebnis (letzter Faktor + 1) einfach ausrechnen:

$$\log(x) \leq \prod_{k=1}^{R(x)} \frac{k+1}{k} \quad = \quad R(x) + 1$$

An diesem Punkt haben wir nun den gewünschten Zusammenhang zwischen dem Logarithmus von x und unsere Funktion aller Primzahlen kleiner gleich x hergestellt. Man sieht, dass die Anzahl der Primzahlen, die kleiner gleich einer reellen Zahl sind, immer größer gleich dessen Logarithmus sind. Da $\log(x)$ unbeschränkt, also unendlich, ist, muss also die Anzahl der Primzahlen mindestens gleich groß sein. Das bedeutet die Anzahl der Primzahlen ist unendlich.

5.3 Umformung

$$log(x) \leq \prod_{p \leq x} \frac{1}{1 - \frac{1}{p}} = \prod_{p \leq x} \frac{p}{p-1}$$

Die Primzahl p an der Stelle k, wird immer größer gleich k sein, da mit $p = 2$ die erste Primzahl schon größer seines Indizes ist, $2 > 1$. Daraus folgt mit $pk \geq k + 1$:

$$\frac{p_k}{p_k - 1} = 1 + \frac{1}{p_k - 1} \leq 1 + \frac{1}{k} = \frac{k+1}{k}$$

Einsetzen in die Formel:

$$\log(x) \leq \prod_{k=1}^{R(x)} \frac{k+1}{k}$$

5.4 Beispiel

Im Folgenden ein Beispiel für den Beweis nach Euler mit der Zahl $x = 4$.

$$\mathbb{P}_{(bis\ x)} = \{2, 3\}$$

$$R(x) = 2$$

$$\log(x) \leq \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} \leq \sum{}' \frac{1}{m}$$

$$\sum{}' \frac{1}{m} = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{6} + \frac{1}{8} + \frac{1}{9} + \frac{1}{12}$$

$$+ \cdots \ (jede\ Zahl, die\ aus\ 2^k \frac{und}{oder} 3^j gebildet werden\ kann)$$

Umformungen übersprungen.

$$\log(2) \leq R(x)$$

$$0{,}301 \leq 2$$

6. Literaturverzeichnis

Martin Aigner, Günter M. Ziegler (2002): *Das BUCH der Beweise*. 4. Auflage. Berlin, Deutschland: Springer Spektrum.

Sebastian Iwanowski, Rainer Lang (2014): *Disktrete Mathematik mit Grundlagen*. Lehrbuch für Studierende von MINT-Fächern. Wedel, Deutschland: Springer Vieweg.

Kryptographie: https://de.wikipedia.org/wiki/Kryptographie (aufgerufen: 12.02.17)

Marc Richter (2013): *Behauptung: Es gibt unendlich viele Primzahlen*: http://www2.informatik.hu-berlin.de/~koessler/Proseminar/Proseminar2012/Richter_prim.pdf (aufgerufen: 12.02.17)

Abbildung 1: https://de.wikipedia.org/wiki/Integralkriterium#/media/File:Integral_Test.svg (aufgerufen: 12.02.17)