MASTERARBEIT | MASTER'S THESIS

Titel | Title

Elementare Beweise für die Unendlichkeit der Menge der Primzahlen

verfasst von | submitted by

Viktoria Rafael BEd

angestrebter akademischer Grad | in partial fulfilment of the requirements for the degree of

Master of Education (MEd)

Wien | Vienna, 2025

Studienkennzahl lt. Studienblatt | Degree programme code as it appears on the student record sheet:	UA 199 520 525 02
Studienrichtung lt. Studienblatt | Degree programme as it appears on the student record sheet:	Masterstudium Lehramt Sek (AB) Unterrichtsfach Mathematik Unterrichtsfach Psychologie und Philosophie
Betreut von | Supervisor:	ao. Univ.-Prof. Mag. Dr. Christoph Baxa

Danksagung

Diese Arbeit markiert einen wichtigen Meilenstein in meiner akademischen Laufbahn. Ich bin überaus dankbar für die Unterstützung, die ich auf diesem Weg erfahren durfte. Ich möchte mich herzlichst bei meinem Betreuer Univ.-Prof. Mag. Dr. Christoph Baxa für seine fachkundige Anleitung und hilfreiche Betreuung bei der Erstellung meiner Masterarbeit bedanken.

Ich danke meiner Familie, besonders meiner Mutter Andrea Rafael-Zak und meiner Cousine Magdalena Zak für ihre jahrelange Unterstützung in jeder Hinsicht.

Diese Masterarbeit war eine herausfordernde, aber auch erfüllende Erfahrung. Ich bin dankbar für die wertvollen Lektionen auf dieser akademischen Reise. Es wäre zu viel alles zu nennen, dennoch möchte ich nur ein Wort sagen. Das Wort heißt DANKE, und es kommt vom Herzen.

Kurzfassung

In der vorliegenden Arbeit werden verschiedene mathematische Beweise zur Unendlichkeit der Primzahlen untersucht. Nach einer Einführung in die Grundlagen der Zahlentheorie und wichtigen Definitionen wird erläutert, dass Primzahlen fundamentale Bausteine der Mathematik sind. Es folgen historische und modernere Beweise zur Unendlichkeit der Primzahlen, darunter der bekannte Beweis von Euklid. Die weiteren Beweise von Mathematikern wie Euler, Erdös oder Furstenberg liefern andere Zugänge zur Thematik und unterschiedliche Einsichten in die Struktur der Primzahlen. Die Beweise reichen dabei von klassischen Widerspruchsbeweisen bis hin zu topologischen Ansätzen und zeigen die Vielseitigkeit und Bedeutung der Primzahlen in der Mathematik. In der Arbeit werden außerdem Beweisansätze zur Unendlichkeit von Primzahlen mithilfe arithmetischer Progressionen präsentiert. Darüber hinaus wird ein fehlerhafter Beweis des Mathematikers Zignano angeführt, um zu veranschaulichen, wie wichtig eine exakte und genaue Beweisführung ist und welche Herausforderungen mathematische Beweise mit sich bringen können.

Abstract

This paper examines various mathematical proofs of the infinite nature of prime numbers. After introducing the basics of number theory and key definitions, it explains why prime numbers are fundamental building blocks of mathematics. Next, it presents historical and modern proofs of the infinity of prime numbers, including Euclid's well-known proof. Further proofs by mathematicians such as Euler, Erdös, and Furstenberg offer alternative approaches to the topic and different insights into the structure of prime numbers. These proofs range from the classical proof by contradiction to topological approaches, demonstrating the versatility and importance of prime numbers in mathematics. The paper also presents proof approaches to the infinity of prime numbers using arithmetic progressions. Additionally, it cites a flawed proof by the mathematician Zignano to illustrate the importance of precise and accurate reasoning, as well as the challenges that mathematical proofs can pose.

Inhaltsverzeichnis

1 Einleitung

Diese Arbeit beschäftigt sich mit der Unendlichkeit von Primzahlen, denn eine der zentralsten Fragestellungen in der Zahlentheorie ist die Existenz und Verteilung von Primzahlen. Die zahlreichen, teils unterschiedlichen Methoden und Beweise zur Unendlichkeit von Primzahlen sind seit den frühen mathematischen Überlieferungen bis in die moderne Mathematik hinein von großer Bedeutung. Bereits im 3. Jahrhundert vor Chr. bewies Euklid die Unendlichkeit von Primzahlen, doch bis heute sind viele Details ihres Verhaltens nicht ausreichend geklärt, insbesondere für arithmetische Progressionen der Form

$$a, a + d, a + 2d, a + 3d, \ldots$$

Im Jahr 1837 hat Dirichlet bereits bewiesen, dass jede arithmetische Progression dieser Form unendlich viele Primzahlen enthält.

Die Arbeit zeigt in ihrem Hauptteil, wie sich die Unendlichkeit von Primzahlen durch elementare Widerspruchsargumente, kombinatorische Ungleichungen und analytische Überlegungen zeigen lässt. Ein weiterer Schwerpunkt der Arbeit sind Beweise für die Unendlichkeit von Primzahlen in speziellen arithmetischen Progressionen. Beispielsweise lässt sich mithilfe des Reziprozitätsgesetzes und des Legendre-Symbols zeigen, dass in bestimmten Restklassen unendlich viele Primzahlen existieren, was eine Annäherung an den Dirichletschen Primzahlsatz darstellt. Abschließend wird mit einem kritischen Blick auf einen historischen Beweisversuch von Zignano aus dem Jahr 1893 aufgezeigt, wie empfindlich mathematische Argumentationen gegenüber kleinen logischen Unstimmigkeiten sind.

Jedoch werden zunächst einige Grundlagen der Zahlentheorie sowie grundlegende Eigenschaften von Primzahlen und weitere wichtige Definitionen und Sätze thematisiert, welche im weiteren Verlauf der Arbeit von Bedeutung sind. Da es sich bei der Zahlentheorie um ein sehr altes Gebiet in der Mathematik handelt, können eben diese Sätze und Definitionen in einer Vielzahl von Quellen vorgefunden werden. Im folgenden Kapitel werden Werke der Fachliteratur, wie unter anderem „Einführung in die Zahlentheorie (2008)“ von P. Bundschuh, „Basiswissen Zahlentheorie (2014)“ von K. Reiss, sowie die jeweiligen Vorlesungsskripte der „VO Zahlentheorie“ von C. Baxa und M. Fulmek an der Universität Wien, für die Erarbeitung des Vorwissens herangezogen.

Die elementare Zahlentheorie beschäftigt sich überwiegend mit den natürlichen Zahlen

$$\mathbb{N} = \{1, 2, 3, 4, ...\}.$$

Erweitert man den Bereich um die Zahl 0 und die negativen Zahlen, ergibt sich die Menge der ganzen Zahlen

$$\mathbb{Z} = \{... - 3, -2, -1, 0, 1, 2, 3, ...\}.$$

Betrachtet man nun die ganzen Zahlen $\mathbb{Z}$ so sind Addition, Subtraktion und Multiplikation unbeschränkt ausführbar. Das heißt: Addiert, subtrahiert oder multipliziert man ganze Zahlen, so erhält man wieder eine ganze Zahl.
Bei der Division kommen die ganzen Zahlen jedoch an ihre Grenzen. Nicht bei jeder beliebigen Division einer ganzen Zahl erhält man wieder eine ganze Zahl. Daher wird für die Division in $\mathbb{Z}$ der Begriff der Teilbarkeit definiert.

Definition 1.1 (Teiler und Komplementärteiler)**.** Seien $m, n \in \mathbb{Z}$.
Man sagt m teilt n, wenn es ein $d \in \mathbb{Z}$ gibt, sodass $n = m \cdot d$. Man schreibt dafür $m \mid n$.
Ist m kein Teiler von n, so schreibt man $m \nmid n$.
Ist $n = m \cdot d$, so wird d der Komplementärteiler von n zu m genannt.

Im Zusammenhang mit der Teilbarkeit lässt sich eine besondere Menge der ganzen Zahlen abgrenzen, die sogenannten Primzahlen.

2 Die Primzahlen

Seit den frühen Anfängen der Mathematik ist den Primzahlen großes Interesse entgegengebracht worden. Primzahlen sind fundamentale Bausteine der Mathematik, sie beginnen mit der kleinsten Primzahl 2, und setzen sich unendlich fort, wobei sie zunehmend seltener auftreten. Folgende Abbildung zeigt alle Primzahlen zwischen 1 und 1000.

2	3	5	7	11	13	17	19	23	29	31	37	41	43
47	53	59	61	67	71	73	79	83	89	97	101	103	107
109	113	127	131	137	139	149	151	157	163	167	173	179	181
191	193	197	199	211	223	227	229	233	239	241	251	257	263
269	271	277	281	283	293	307	311	313	317	331	337	347	349
353	359	367	373	379	383	389	397	401	409	419	421	431	433
439	443	449	457	461	463	467	479	487	491	499	503	509	521
523	541	547	557	563	569	571	577	587	593	599	601	607	613
617	619	631	641	643	647	653	659	661	673	677	683	691	701
709	719	727	733	739	743	751	757	761	769	773	787	797	809
811	821	823	827	829	839	853	857	859	863	877	881	883	887
907	911	919	929	937	941	947	953	967	971	977	983	991	997

Abbildung 1: Primzahlen von 1 bis 1000

Definition 2.1 (Primzahlen.)**.** Sei p $\in \mathbb{Z}$, $p > 1$. Wenn p nur die Teiler 1, -1, p,$-p$ besitzt, dann heißt p Primzahl.

Bemerkung 2.2. Beachte, dass die Zahl 1 keine Primzahl ist.
Wenn nicht anders definiert, ist die Menge der Primzahlen in aufsteigender Ordnung

$$\mathbb{P} = \{p_1, p_2, p_3, \dots\}.$$

Definition 2.3 (Primteiler)**.** Eine Zahl $q \in \mathbb{N}$ heißt Primteiler von $n \in \mathbb{N}$, wenn q eine Primzahl und Teiler von n ist. Eine natürliche Zahl, die keine Primzahl ist, heißt zusammengesetzte Zahl.
Kann man $n \in \mathbb{N}$ in der Form $n = p \cdot m$ schreiben, wobei p eine Primzahl ist, dann nennt man p einen Primfaktor von n.

Einer der wichtigsten Sätze der Zahlentheorie ist der Fundamentalsatz der Arithmetik (oder auch Fundamentalsatz der Zahlentheorie). Dieser besagt, dass jede von 1 verschiedene natürliche Zahl als Produkt endlich vieler Primzahlen darstellbar ist. Diese Darstellung ist, wenn die vorkommenden Primzahlen der Größe nach geordnet sind, eindeutig.

Satz 2.4 (Fundamentalsatz der Aritmetik)**.** *Jede ganze Zahl* $n \in \mathbb{Z} \setminus \{0, 1, -1\}$ *hat eine eindeutige Darstellung*

$$n = (\pm 1) \cdot p_1^{r_1} \cdot \dots \cdot p_s^{r_s}$$

mit Primzahlen $p_1 < \dots < p_s$ *und* $r_i \in \mathbb{N}$*. Die* p_i *heißen Primfaktoren von* n *und die Darstellung bezeichnet man als Primfaktorzerlegung von* n*.*

Beweis*.*

- Existenz:
  Durch Induktion nach n:
  Für $n = 2$, ist die Behauptung wahr, da 2 eine Primzahl ist. Ist $n > 2$ und keine Primzahl, dann kann n geschrieben werden, als $n = a \cdot b$ mit $a, b \neq 1$. Da $a, b < n$ haben a und b Zerlegungen, und durch Sortieren der Primfaktoren erhält man die Primfaktorzerlegung von n.

- Eindeutigkeit:
  Der Fall $n = 2$ ist erneut wahr, da 2 selbst eine Primzahl ist. Angenommen, es gäbe zwei verschiedene Primfaktorzerlegungen für $n > 2$,

  $$n = p_1 \cdot \dots \cdot p_s = q_1 \cdot \dots \cdot q_t$$

  mit $p_1 \leq \dots \leq p_s$ und $q_1 \leq \dots \leq q_t$ als Primzahlen. Ist $s = 1$ oder $t = 1$, dann ist n prim und die Behauptung klar. Seien als $s, t \geq 2$.
  Ist $p_1 = q_1$, so hat

  $$p_2 \cdot \dots \cdot p_s = q_2 \cdot \dots \cdot q_t < n$$

  nach Induktionsvorraussetzung eine eindeutige Primfaktorzerlegung und die Behauptung folgt.
  Angenommen es wäre $p_1 < q_1$. Dann gilt

  $$n > \underbrace{p_1 \cdot (p_2 \cdot \dots \cdot p_s - q_2 \cdot \dots \cdot q_t)}_{=:N_1} = \underbrace{(q_1 - p_1) \cdot q_2 \cdot \dots \cdot q_t}_{=:N_2} \geq 2,$$

  also hat $N_1 = N_2$ nach Induktionsvorraussetzung eine eindeutige Primfaktorzerlegung. Wegen $p_1 < q_1 \leq \dots \leq q_t$ ist $p_1 \neq q_i$, und p_1 ist kein Teiler von $q_1 - p_1$, denn sonst würde p_1 auch q_1 teilen. Somit ist p_1 ein Primfaktor von N_1, jedoch keiner von N_2, dies ist ein Widerspruch.

□

Definition 2.5 (Primfaktorzerlegung)**.** Für $n \in \mathbb{N}$ heißt eine Zerlegung der Form

$$n = p_1 \cdot p_2 \cdot \dots \cdot p_k = \prod_{i=1}^{k} p_i$$

mit $p_1, p_2, \dots, p_k \in \mathbb{P}$ und $k \in \mathbb{N}$ eine Primfaktorzerlegung von n.

Bemerkung 2.6. Fasst man gleiche Faktoren unter der Verwendung der Potenzschreibweise zusammen, so erhält man die *kanonischen Primfaktorzerlegung*:

$$n = p_1^{r_1} \cdot p_2^{r_2} \cdot \dots \cdot p_k^{r_k} = \prod_{i=1}^{k} p_i^{r_i}$$

Der nächste Satz stellt eine Folgerung aus dem Fundamentalsatz der Arithmetik dar.

Satz 2.7. *Sind $n, a, b \in \mathbb{N}$ mit $n = a \cdot b$ und ist p ein Primteiler von n, so ist p auch ein Primteiler von a oder b.*

Beweis. Es seien $a = a_1 \cdot a_2 \cdots a_m$ und $b = b_1 \cdot b_2 \cdots b_k$, dann existieren nach dem Fundamentalsatz der Arithmetik, bis auf die Reihenfolge der Faktoren, eindeutige Primfaktorzerlegungen von a und b. Die Zerlegung von n ist daher gegeben durch

$$n = a_1 \cdot a_2 \cdots a_m \cdot b_1 \cdot b_2 \cdots b_k.$$

Da $p \mid n$ muss p eine der Primzahlen in $a_1 \cdot a_2 \cdots a_m$ oder $b_1 \cdot b_2 \cdots b_k$ sein, da ansonsten eine weitere Zerlegung von n mit p als Faktor gefunden werden könnte. Dies steht im Widerspruch zur Eindeutigkeit der Primfaktorenzerlegung.
Somit ergibt sich, dass jede Primzahl die n teilt eine der Primzahlen in $a_1 \cdot a_2 \cdots a_m$ oder $b_1 \cdot b_2 \cdots b_k$ sein muss.

□

Die Menge der Primzahlen (in $\in \mathbb{N}$) kann in drei Gruppen unterteilt werden. Dabei beinhaltet die erste Gruppe alle geraden Primzahlen, das ist nur eine Zahl, nämlich $p = 2$. Alle anderen Primzahlen sind ungerade und bilden die anderen beiden Gruppen. Diese Primzahlen lassen sich in der Form $p = 4m + 1$ oder $p = 4m + 3$ darstellen: Ist p ungerade, dann gibt es ein $k \in \mathbb{N}$ mit der Eigenschaft $p = 2k + 1$.

- Ist k gerade, so gibt es ein $m \in \mathbb{N}$ mit $k = 2m$. Daher ist

$$p = 2 \cdot 2m + 1 = 4m + 1.$$

- Ist k ungerade, so gibt es ein $m \in \mathbb{N}_0$ (da für $p = 3$ ist $k = 1$ und somit $m = 0$) mit $k = 2m + 1$. Daher ist

$$p = 2 \cdot (2m + 1) + 1 = 4m + 3.$$

Definitionen und Sätze

Es werden nun einige weitere Definitionen und wichtige Sätze dargestellt, welche in weiteren Beweisen dieser Arbeit von Bedeutung sind.

Definition 2.8 (Größter gemeinsamer Teiler, ggT)**.** Sind $n_1, \ldots, n_k \in \mathbb{Z}$, so heißt $m \in \mathbb{Z}$ gemeinsamer Teiler von $n_1, \ldots, n_k$, wenn $m \mid n_i$ für $1 \leq i \leq k$.
Sind $n_1, \ldots, n_k \in \mathbb{Z}$, nicht alle gleich 0, so sei

$$\text{ggT}(n_1, \ldots, n_k) := \max \left\{ m \in \mathbb{Z} \;\middle|\; m \mid n_i \text{ für } 1 \leq i \leq k \right\}$$

Definition 2.9 (Kleinstes gemeinsames Vielfaches)**.** Sind $n_1, \ldots, n_k \in \mathbb{Z}$, dann heißt $m \in \mathbb{Z}$ gemeinsames Vielfaches von $n_1, \ldots, n_k$, wenn $n_i \mid m$ für $1 \leq i \leq k$.
Sind $n_1, \ldots, n_k \in \mathbb{Z} \setminus \{0\}$, so sei

$$\text{kgV}(n_1, \ldots, n_k) = \min \left\{ m \in \mathbb{N} \;\middle|\; n_i \mid m \text{ für } 1 \leq i \leq k \right\}.$$

Definition 2.10 (Minimum)**.** Seien a und b natürliche Zahlen, dann bezeichnet $\min(a, b)$ das Minimum (das kleinste) der beiden Zahlen.

Definition 2.11 (Maximum)**.** Sind a und b natürliche Zahlen, dann bezeichnet $\max(a, b)$ das Maximum (das größte) der beiden Zahlen.

Definition 2.12 (Relativ prim, teilerfremd)**.**

1) $n_1, \ldots, n_k \in \mathbb{Z}$ heißen relativ prim (oder teilerfremd), wenn ihr größter gemeinsamer Teiler 1 ist.

2) $n_1, \ldots, n_k$ heißen paarweise relativ prim (oder paarweise teilerfremd), wenn $\text{ggT}(n_i, n_j) = 1$, für $1 \leq i, j \leq k$, $i \neq j$.

Definition 2.13 (Fakultät)**.** Für eine natürliche Zahl $n > 1$ wird durch $n! = n \cdot (n-1)!$ die Zahl $n!$ (Fakultät) definiert. Weiters sei $1! = 1$ und $0! = 1$.

Definition 2.14 (Primfakultät)**.** Für jede Primzahl p bezeichnet $p\#$ das Produkt aller Primzahlen q mit $q \leq p$. Der Ausdruck $p\#$ wird auch Primfakultät von p genannt.

Definition 2.15 (Quadratfrei)**.** Eine natürliche Zahl heißt quadratfrei, wenn es außer der Zahl 1 keine weitere Quadratzahl gibt, die diese Zahl teilt.
In der Primfaktorzerlegung

$$n = p_1 \cdots p_k$$

einer quadratfreien Zahl tritt keine Primzahl mehr als einmal auf.

Definition 2.16 (Folge)**.** Eine Folge mit Werten in $\mathbb{R}$ ist eine Abbildung

$$a : \mathbb{N} \to \mathbb{R}.$$

Folgen werden mit $(a_n)_{n\in\mathbb{N}}$ bezeichnet (oder kurz (a_n)), sie können auch aufzählend $a_1, a_2, \ldots$ geschrieben werden.

Bemerkung 2.17. Es gibt besondere Folgen:

- Konstante Folgen: alle Folgenglieder sind die gleiche Zahl $a_n = a \in \mathbb{R}$.
- Alternierende Folge: Folgenglieder ändern fortlaufend das Vorzeichen, z.B.

  $$a_n = (-1)^n.$$

- Arithmetische Folge: Folge $(a_n)_{n=0}^{\infty}$, die für eine konstante Zahl d und alle $n \in \mathbb{N}_0$ gebildet wird über

  $$a_n = a_0 + n \cdot d.$$

- Geometrische Folge: Folge $(a_n)_{n=0}^{\infty}$ zu einer reellen Zahl $q \neq 0$ mit $a_0 \neq 0$ und

  $$a_n = a_0 \cdot q^n.$$

  Wobei q konstant und $q = \dfrac{a_{n+1}}{a_n}$ für alle $n \geq 0$.

Definition 2.18 (Reihe)**.** Sei $(a_n)_{n\in\mathbb{N}}$ eine Folge reeller Zahlen. Die Folge

$$s_n := \sum_{k=1}^{n} a_k$$

ist die Folge der Partialsummen (Partialsummenfolge). Diese wird als Reihe über (a_n) bezeichnet. Falls die Folge (s_n) konvergiert, dann sei $\sum_{k=1}^{\infty} a_k$ ihr Grenzwert.

Bemerkung 2.19. Es gibt besondere Reihen:

- Geometrische Reihe: Wird über die geometrische Folge $(p^k)_{k=0}^{\infty}$ gebildet und ist konvergent.
  Für $p \neq 0$, $|p| < 1$ gilt:

$$\lim_{n\to\infty} \sum_{k=0}^{n} p^k = \lim_{n\to\infty} \frac{1-p^{n+1}}{1-p} = \frac{1}{1-p}$$

- Harmonische Reihe: Ist divergent.

$$\sum_{k=1}^{\infty} \frac{1}{k} = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \dots$$

- Alternierende harmonische Reihe: Ist konvergent.

$$\sum_{k=1}^{\infty} (-1)^k \frac{1}{k} = -1 + \frac{1}{2} - \frac{1}{3} \pm \dots$$

Definition 2.20 (Fermat-Zahlen)**.** Sei $n \geq 0$. Definiert man

$$F(n) = 2^{2^n} + 1.$$

Die Zahl $F(n)$ nennt man die Fermat-Zahl mit dem Exponenten n. Ist die Zahl $F(n)$ prim, so heißt $F(n)$ eine $Fermat - Primzahl$.

Die ersten Fermat-Zahlen lauten

n	0	1	2	3	4
$F(n)$	3	5	17	257	65537

Bemerkung 2.21. Alle Fermat-Zahlen sind ungerade.

Definition 2.22 (Kongruent modulo m)**.** Es seien $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$ und $m \geq 2$. Man sagt a und b seien kongruent modulo m, wenn $m \mid (a-b)$ gilt. Man schreibt dafür

$$a \equiv b \pmod{m} \text{ oder kurz } a \equiv b \ (m).$$

Die Zahl m heißt dabei Modul. Falls $m \nmid (a-b)$, so schreibt man $a \not\equiv b \pmod{m}$ und sagt, a und b seien inkongruent modulo m.

Gilt $m \mid (a-b)$, so gelten alle Bedingungen des folgenden Satzes:

Satz 2.23. *Es seien $a, b \in \mathbb{Z}$ und $m \in \mathbb{N}, m \geq 2$. Dann sind äquivalent:*

(i) *a und b haben bei der Division durch m denselben Rest.*

(ii) *$m \mid (a - b)$.*

(iii) *Es gibt ein $k \in \mathbb{Z}$, derart dass $a = b + k \cdot m$.*

Beweis.
(i) $\Rightarrow$ (ii): Es seien $q_1, q_2, r \in \mathbb{Z}$, sodass $a = q_1 \cdot m + r$ und $b = q_2 \cdot m + r$ mit $0 \leq r < m$. Dann ist

$$\begin{aligned} a - b &= (q_1 \cdot m + r) - (q_2 \cdot m + r) \\ &= q_1 \cdot m + r - q_2 \cdot m - r \qquad = m \cdot (q_1 - q_2) \end{aligned}$$

und daher gilt $m \mid (a - b)$.

(ii) $\Rightarrow$ (iii): Da $m \mid (a - b)$ gilt, gibt es laut Definition der Teilbarkeit ein $k \in \mathbb{Z}$ mit $a - b = k \cdot m$ woraus sofort $a = b + k \cdot m$ folgt.
(iii) $\Rightarrow$ (i): Die Division von b durch m mit Rest liefert $b = q \cdot m + r$ für $q, r \in \mathbb{Z}$ und $0 \leq r < m$. Damit folgt

$$\begin{aligned} a &= b + k \cdot m \\ &= q \cdot m + r + k \cdot m \\ &= m \cdot (q + k) + r \end{aligned}$$

Die Division von a durch m liefert daher ebenfalls den Rest r. □

Definition 2.24 (Limes)**.** Konvergiert eine Folge $(a_n)_{n \in \mathbb{N}}$ gegen ein $a \in \mathbb{R}$, so heißt a der Limes (oder Grenzwert) der Folge und man schreibt $a_n \to a$ oder

$$a = \lim_{n \to \infty} a_n$$

Definition 2.25 (Quadratische Reste und Nichtreste)**.**
Es sei $p > 2$ eine Primzahl und $a \in \mathbb{Z}$, $p \nmid a$.. Es kann zwischen zwei Fällen unterschieden werden:

- Fall 1: a heißt quadratischer Rest modulo p, wenn

  $$\exists\, x, k \in \mathbb{Z} : x^2 = a + kp,$$

  das heißt $x^2 \equiv a \pmod{p}$ lösbar ist.

- Fall 2: a heißt quadratischer Nichtrest modulo p, wenn solche $x, k \in \mathbb{Z}$ nicht existieren und die Kongruenz nicht lösbar ist.

Definition 2.26 (Legendre-Symbol)**.** Unter diesen Voraussetzungen kann das Legendre-Symbol $\left(\frac{a}{p}\right)$ definiert werden durch

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{wenn } p \mid a \\ 1 & \text{wenn } a \text{ quadratischer Rest modulo } p \text{ ist} \\ -1 & \text{wenn } a \text{ quadratischer Nichtrest modulo } p \text{ ist} \end{cases}$$

Man spricht für $\left(\frac{a}{p}\right)$ "a nach p".

Proposition 2.27. *Aus der Definition 2.25 (Quadratischer Rest und Nichtreste) folgt unmittelbar: Unterscheiden sich $a, b \in \mathbb{Z}$ um ein Vielfaches von p, so sind entweder beide quadratische Reste modulo p oder beide quadratische Nichtreste modulo p.*
Das heißt, ist $a - b = lp$ für ein $l \in \mathbb{Z}$ bzw. $a \equiv b \pmod{p}$, so gilt

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$$

Korollar 2.28. *Für $p > 2$, $a_1 \cdot a_2 \cdots a_n, b \in \mathbb{Z}$ gelten für das Legendre-Symbol weiters folgende Eigenschaften*

(i) $\left(\frac{a_1 \cdot a_2 \cdots a_n}{p}\right) = \left(\frac{a_1}{p}\right) \cdot \left(\frac{a_2}{p}\right) \cdots \left(\frac{a_n}{p}\right)$.

(ii) $\mathrm{ggT}(b, p) = 1 \Longrightarrow \left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$.

(iii) $\left(\frac{1}{p}\right) = 1$.

Beweis. (i) Aus dem Euler-Kriterium (Lemma 2.34) folgt

$$\begin{aligned} \left(\frac{a_1 \cdot a_2 \cdots a_n}{p}\right) &\equiv (a_1 \cdot a_2 \cdots a_n)^{\frac{p-1}{2}} = a_1^{\frac{p-1}{2}} \cdot a_2^{\frac{p-1}{2}} \cdots a_n^{\frac{p-1}{2}} \\ &\equiv \left(\frac{a_1}{p}\right) \cdot \left(\frac{a_2}{p}\right) \cdots \left(\frac{a_n}{p}\right) \pmod{p} \end{aligned}$$

(ii) Es gilt $\left(\frac{c}{p}\right) \cdot \left(\frac{c}{p}\right) = 1$, denn entweder $\left(\frac{c}{p}\right) = 1$ oder $\left(\frac{c}{p}\right) = -1$. Aus (i) folgt somit

$$\left(\frac{a \cdot c^2}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{c}{p}\right)^2 = \left(\frac{a}{p}\right) \cdot 1 = \left(\frac{a}{p}\right)$$

(iii) $\left(\frac{1}{p}\right) = \left(\frac{1^2}{p}\right) = \left(\frac{1}{p}\right)^2 = 1.$

□

Bemerkung 2.29. Eine Erweiterung des bereits beschriebenen Legendre-Symbols ist das Jacobi-Symbol $\left(\frac{a}{m}\right)$, dieses wird folgendermaßen definiert:

Definition 2.30 (Jacobi-Symbol)**.** Sei $m \in \mathbb{N}$ ungerade und $m = p_1 \cdots p_k$ die Primfaktorzerlegung von m. Dabei sind $p_1, \ldots, p_k$ nicht notwendigerweise verschiedene Primzahlen und $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, m) = 1$. Dann sei

$$\left(\frac{a}{m}\right) := \prod_{i=1}^{k} \left(\frac{a}{p_i}\right),$$

wobei $\left(\frac{a}{p_i}\right)$ das Legendre-Symbol bezeichnet, für $1 \leq i \leq k$.

Satz 2.31 (Euklidischer Algorithmus)**.** *Sind $a, b \in \mathbb{N}$ und $b \leq a$, so führe wiederholt Division mit Rest durch.*

$$\begin{aligned} a &= bq_1 + r_1, & 0 \leq r_1 < b \\ b &= r_1 q_1 + r_2, & 0 \leq r_2 < r_1 \\ r_1 &= r_2 q_2 + r_3, & 0 \leq r_3 < r_2 \\ &\vdots & \vdots \\ r_{m-1} &= r_m q_m + r_{m+1}, & 0 \leq r_{m+1} < r_m \end{aligned}$$

Setze $r_0 := b$. Wegen $b = r_0 > r_1 > r_2 > r_3 > \cdots > r_m > r_{m+1} > \cdots \geq 0$ gibt es ein kleinstes $n \geq 0$ mit $r_{n+1} = 0$. Dann gilt $r_n = ggT(a, b)$.

Beweis. Zunächst wird gezeigt, dass r_n ein gemeinsamer Teiler von a und b ist.
Wegen $r_{n-1} = r_n \cdot q_n$ gilt $r_n \mid r_{n-1}$.
Wegen $r_{n-2} = r_{n-1} \cdot q_{n-1} + r_n$ (und dem Satz: wenn $m \mid n_i$ $(1 \leq i \leq k)$, so folgt $m \mid (l_1 n_1 + \cdots + l_k n_k)$ $\forall l_1, \ldots, l_k \in \mathbb{Z}$) folgt, dass $r_n \mid r_{n-2}$.
Führe das Verfahren weiter fort. Ist $r_n \mid r_{m+1}$ und $r_n \mid r_m$ bereits gezeigt, so folgt wegen $r_{m-1} = r_m \cdot q_m + r_{m+1}$, dass $r_n \mid r_{m-1}$.
Es folgt $r_n \mid b$ wegen $b = r_1 \cdot q_1 + r_2$ und $r_n \mid a$ wegen $a = b \cdot q_0 + r_1$.
Sei nun d ein beliebiger positiver Teiler von a, b.
Wegen $r_1 = a - b \cdot q_0$ folgt $d \mid r_1$ und wegen $r_2 = b - r_1 \cdot q_1$ folgt $d \mid r_2$.
Führe das Verfahren auch hier weiter fort. Ist $d \mid r_{m-1}$ und $d \mid r_m$ gezeigt, so folgt wegen $r_{m+1} = r_{m-1} - r_m \cdot q_m$, dass $d \mid r_{m+1}$.
Es folgt $d \mid r_n$ $(\Rightarrow d \leq r_n)$.

□

Satz 2.32 (Kleiner Satz von Fermat)**.** *Falls p eine Primzahl ist und a eine ganze Zahl, so gilt $p \mid (a^p - a)$ beziehungsweise*

$$a^p \equiv a \pmod{p}.$$

Insbesondere gilt: Wenn p kein Teiler von a ist, dann ist $a^{p-1} \equiv 1 \pmod{p}$.

Beweis. Für $a = 0$ gilt $p \mid (0^p - 0)$, da $p \mid 0$.
Für $a \geq 1$ kann die Behauptung mit Induktion nach a gezeigt werden:
Für $a = 1$ gilt $p \mid (1^p - 1)$, da $p \mid 0$.
Für $a + 1$ gilt:

$$\begin{aligned}(a+1)^p - (a+1) &= \sum_{j=0}^{p} \binom{p}{j} a^j - a - 1 \\ &= a^p + \sum_{j=1}^{p-1} \binom{p}{j} a^j + 1 - a - 1 \\ &= a^p - a + \sum_{j=1}^{p-1} \binom{p}{j} a^j\end{aligned}$$

Es gilt $p \mid (a^p - a)$ und $p \mid \binom{p}{j}$ für $1 \leq j \leq p-1$.
Für $a < 0$ kann unterschieden werden:

- Ist $p = 2$, so ist entweder a gerade, das heißt $a = 2b$ für ein $b \in \mathbb{Z}$ und somit

  $$a^p - a = (2b)^2 - 2b = 4b^2 - 2b = 2(2b^2 - b),$$

  oder a ist ungerade, also $a = 2b + 1$ für ein $b \in \mathbb{Z}$ und daher

  $$a^p - a = (2b+1)^2 - (2b+1) = 4b^2 + 4b + 1 - 2b - 1 = 4b^2 + 2b = 2(2b^2 + b).$$

- Ist $p \neq 2$, so ist die Behauptung für $-a$ bereits bewiesen, das heißt

  $$p \mid ((-a)^p - (-a)) \Rightarrow p \mid (-a^p + a) \Rightarrow p \mid -(a^p - a) \Rightarrow p \mid (a^p - a)$$

- Ist $p \nmid a$, so gilt $p \mid (a^p - a) \Rightarrow p \mid a(a^{p-1} - 1) \Rightarrow p \mid a$ oder $p \mid (a^{p-1} - 1)$. Nach Voraussetzung ist $p \nmid a$, daher muss $p \mid (a^{p-1} - 1)$ gelten.

□

Korollar 2.33. *Ist $p > 2$ eine Primzahl, $a \in \mathbb{Z}$ und $p \nmid a$, so gilt entweder $p \mid (a^{\frac{p-1}{2}} - 1)$ oder $p \mid (a^{\frac{p-1}{2}} + 1)$ beziehungsweise*

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

oder

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

Beweis. Es gilt

$$p \mid (a^{p-1} - 1) \Rightarrow p \mid (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \Rightarrow p \mid (a^{\frac{p-1}{2}} - 1) \text{ oder } p \mid (a^{\frac{p-1}{2}} + 1).$$

□

Einige Sätze werden nun ohne Beweis angegeben, sie werden in der Arbeit angewandt und verwendet. Die Beweise selbst würden jedoch teilweise den Rahmen der Arbeit sprengen.

Satz 2.34 (**Euler-Kriterium**)**.** *Ist $p > 2$ eine Primzahl, a eine ganze Zahl und $p \nmid a$, so gilt*

$$p \mid \left(a^{\frac{p-1}{2}} - \left(\frac{a}{p}\right)\right)$$

beziehungsweise

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$$

Satz 2.35 (1. Ergänzungssatz)**.** *Ist $p > 2$ eine Primzahl, so ist*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

Das heißt -1 ist quadratischer Rest modulo p, wenn $p = 4k + 1$ (bzw. $p \equiv 1 \pmod 4$) und quadratischer Nichtrest, wenn $p = 4k + 3$ (bzw. $p \equiv 3 \pmod 4$)

Satz 2.36 (2. Ergänzungssatz)**.** *Ist $p > 2$ eine Primzahl, so ist*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Das heißt 2 ist ein quadratischer Rest modulo p, wenn $p = 8k + 1$ oder $p = 8k + 7$ für ein $k \in \mathbb{Z}$ (bzw. $p \equiv 1 \pmod 8$ oder $p \equiv 7 \pmod 8$).
Und 2 ist ein quadratischer Nichtrest modulo p, wenn $p = 8k + 3$ oder $p = 8k + 5$ für ein $k \in \mathbb{Z}$ (bzw. $p \equiv 3 \pmod 8$ oder $p \equiv 5 \pmod 8$).

Satz 2.37 (Quadratisches Reziprozitätsgesetz)**.** *Sind $p, q > 2$ zwei verschiedene Primzahlen, so ist*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

Das heißt, ist $p = 4k+1$ ODER $q = 4k+1$ für ein $k \in \mathbb{Z}$
(bzw. $p \equiv 1 \pmod 4$ ODER $q \equiv 1 \pmod 4$), so ist $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = 1$.
Ist aber $p = 4k+3$ UND $q = 4l+3$ für $k, l \in \mathbb{Z}$
(bzw. $p \equiv 3 \pmod 4$ UND $q \equiv 3 \pmod 4$), so ist $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = -1$.

Bemerkung 2.38. Außerdem ist zu sagen

1. Das quadratische Reziprozitätsgesetz wird meist in der Form

   $$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

   angewandt.

2. Satz 2.35. impliziert, dass $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$, wenn $p \equiv 1 \pmod 4$ oder $q \equiv 1 \pmod 4$ und $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$, wenn $p \equiv q \equiv 3 \pmod 4$.

Satz 2.39 (Primzahlsatz)**.** *Sei für $x \in \mathbb{R}_{>0}$*

$$\pi(x) = \Big|\{p \leq x \mid p \in \mathbb{N}\, prim\}\Big|.$$

Dann gilt

$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\ln(x)}} = 1.$$

Im Jahr 1793 wurde der Primzahlsatz von C.F. Gauß formuliert. Bewiesen wurde der Satz von Hadamard und unabhängig auch von de la Vallée-Poussin im Jahr 1896. Der Beweis selbst benutzt analytische Hilfsmittel, welche den Rahmen dieser Arbeit sprengen würden.

Nachdem die Definitionen und grundlegenden Eigenschaften der Primzahlen dargestellt wurden, widmet sich das nächste Kapitel einigen, teils verschiedenen Beweisen für die Unendlichkeit der Primzahlen. Dabei wird als Literatur beispielsweise „Das BUCH der Beweise (2010)“ von M. Aigner und G. Ziegler, und „Die Welt der Primzahlen (2011)“ von P. Ribenboim herangezogen.

3 Es gibt unendlich viele Primzahlen

3.1 Beweis von Euklid

Im alten Griechenland, bereits im 3. Jahrhundert vor Chr., hat Euklid von Alexandria viele bedeutende Beiträge zur Mathematik geleistet. Die Grundlagen der damals bekannten Mathematik hat er in den, aus 13 Bänden bestehenden, Elementen zusammengefasst.
Den Beweis der Unendlichkeit der Primzahlen hat Euklid im Buch „Die Elemente: Buch IX, Prop 20“ folgendermaßen formuliert:

„Es gibt mehr Primzahlen als jede vorgelegte Anzahl von Primzahlen.“

Euklid führt einen Widerspruchsbeweis durch, aufgrund der Kürze und der Einfachheit, gilt er als einer der schönsten Beweise in der Zahlentheorie.

Satz 3.1 (**Satz von Euklid**). *Es gibt unendlich viele Primzahlen.*

Beweis. Angenommen, $p_1 = 2 < p_2 = 3 < \cdots < p_r$ würde die Gesamtheit aller Primzahlen darstellen. Betrachtet man

$$P = p_1 \cdot p_2 \cdots p_r + 1.$$

Sei p eine Primzahl, die P teilt. Dann kann p keine der Zahlen $p_1, p_2, \ldots, p_r$ sein, denn andernfalls müsste p auch die Differenz $P - p_1 \cdot p_2 \cdots p_r = 1$ teilen, was jedoch unmöglich ist. Daher ist p eine zusätzliche Primzahl, so dass $p_1, p_2, \ldots, p_r$ nicht schon alle Primzahlen gewesen sein können. □

Euklids Beweis ist recht einfach, jedoch gibt er keine Auskunft über die Beschaffenheit der neuen Primzahlen. Man weiß lediglich, dass sie in der Größe höchstens gleich $P = p_1 \cdot p_2 \cdots p_n + 1$ ist. Für manche $p_1, \ldots, p_n$ ist die Zahl P selbst eine Primzahl, für andere $p_1, \ldots, p_n$ ist die Zahl P jedoch zerlegbar, z.B. ist

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509$$

Im Laufe der Jahrhunderte haben einige Mathematiker ihre eigenen Varianten des euklidischen Beweises formuliert.
Der folgende Beweis von Kummer aus dem Jahre 1878 ist eine dieser Varianten. Ribenboim bezeichnet ihn in seinem Buch ”Die Welt der Primzahlen (2011)” als rund, glanzvoll und schön in seiner Einfachheit.

***Beweis** (Kummer).* Angenommen, es gäbe nur endlich viele Primzahlen $p_1 < p_2 < \cdots < p_r$. Es sei $N = p_1 \cdot p_2 \cdots p_r$, wobei $N > 2$. Die Zahl $N - 1$ ist ein Produkt von Primzahlen und muss mit N einen gemeinsamen Primteiler p_i haben. Dieser wiederum müsste die Differenz $N - (N - 1) = 1$ teilen, was nicht sein kann und zu einem Widerspruch führt. □

Eine weiterere ähnliche, einfache und schöne Beweisvariation folgte 1890 von Stieltjes. [Not Always Buried Deep: A second course of elementary Number Theory Paul Pollak, 2009, S.2]

***Beweis** (Stieltjes).* Angenommen $p_1, p_2, \ldots, p_r$ sei eine endliche Liste paarweise verschiedene Primzahlen und man betrachtet das Produkt $P = p_1 \cdots p_r$. Es sei $P = AB$ eine Zerlegung in positive ganze Zahlen A und B. Ist p_i einer der Primteiler von P, dann gilt $p_i \mid AB$. Wenn $p_i \mid A$ und $p_i \mid B$ gelten würde, dann würde $p_i^2 \mid P$ gelten. Dies widerspricht dem Fundamentalsatz der Arithmetik und ist somit falsch.
Daraus folgt, p_i muss genau eine der beiden Zahlen A oder B teilen, woraus weiter folgt, dass $p_i \nmid (A + B)$. Jedoch hat $A + B \geq 2$ einen Primteiler, weshalb es mehr Primzahlen in der Liste geben muss. □

Die folgende rekursive Abwandlung dieser Beweisidee stammt von F. Saidak aus "Biscuits of Number Theory (2009)" und basiert auf dem größten gemeinsamen Teiler.

Beweis. Es sei $n > 1$ eine natürliche Zahl. Da $\mathrm{ggT}(n, n + 1) = 1$, besitzt die Zahl $n \cdot (n + 1)$ mindestens zwei verschiedene Primteiler. Da auch

$$\mathrm{ggT}(n \cdot (n + 1), n \cdot (n + 1) + 1) = 1,$$

besitzt die Zahl $n \cdot (n + 1)(n \cdot (n + 1) + 1)$ mindestens drei verschiedene Primteiler.
Da man diesen Prozess beliebig fortsetzen kann, erhält man auf diese Weise unendlich viele Primzahlen. □

3.2 Beweis von Goldbach

Der deutsche Mathematiker Christian Goldbach wurde vor allem durch seine berühmte und bis heute unbewiesene Goldbachsche Vermutung im Jahr 1742 bekannt.
Eine Überlegung von Goldbach zur Unendlichekeit der Primzahlen ist einfach und ergiebig zugleich [Ribenboim, Die Welt der Primzahlen, 2011].
Es genügt eine unendliche Folge natürlicher Zahlen $1 < a_1 < a_2 < a_3 < \cdots$ zu finden, die paarweise teilerfremd sind. Falls also p_1 eine Primzahl ist, die a_1 teilt, die Primzahl p_2 die Zahl a_2 teilt, und so weiter, dann sind $p_1, p_2, \ldots$ alle verschieden.
Durch den euklidischen Algorithmus kann der größte gemeinsame Teiler ermittelt werden, ohne dass die Primfaktoren der Zahlen bekannt sein müssen. Der folgende Beweis von Goldbach beruht auf den Fermat Zahlen. Es wird gezeigt, dass Fermat-Zahlen paarweise relativ prim sind und es daher unendlich viele Primzahlen geben muss.

Satz 3.2. *Die Fermat-Zahlen $F_n = 2^{2^n} + 1$ (für $n \geq 0$) sind paarweise teilerfremd.*

Beweis. Ist m ein gemeinsamer Teiler von F_k und F_n mit $k < n$. Es folgt aus der Rekursion

$$\prod_{k=0}^{n-1} F_k = F_n - 2 \quad (n \geq 1),$$

dass m auch 2 teilt, das heißt $m = 1$ oder $m = 2$.
Der Fall $m = 2$ ist aber ausgeschlossen, da alle Fermat Zahlen ungerade sind.
Die Rekursionsrelation beweist man mit Induktion nach n.
Für $n = 1$ gilt $F_0 = 3$ und $F_1 - 2 = 3$. Mit Induktion erhält man

$$\begin{aligned}\prod_{k=0}^{n} F_k = \Big(\prod_{k=0}^{n-1} F_k\Big) F_n = \Big(F_n - 2\Big) F_n = \\ = (2^{2^n} - 1)(2^{2^n} + 1) = 2^{2^{n+1}} - 1 = F_{n+1} - 2.\end{aligned}$$

□

Eine weitere Beweisvariante mit diesem Gedankengang, jedoch mit der Verwendung des größten gemeinsamen Teilers, ist von Schorn, ebenfalls aus Ribenboim, „Die Welt der Primzahlen (2011)“.

Beweis*(Schorn).* Angenommen, es gibt nur eine endliche Anzahl von Primzahlen $p_1, p_2, \ldots, p_m$. Wenn n eine natürliche Zahl ist und $1 \leq i < j \leq n$, betrachte nun die Zahlen $i \cdot n! + 1$ und $j \cdot n! + 1$. Dann gilt:

$$\mathrm{ggT}(i \cdot n! + 1, j \cdot n! + 1) = 1.$$

Denn wenn man $j = i + d$ setzt, wobei $1 \leq d < n$ ist, kann die Teilerfremdheit wie folgt gezeigt werden:

$$\begin{aligned} \text{ggT}(i \cdot n! + 1, j \cdot n! + 1) &= \text{ggT}(i \cdot n! + 1, (i + d) \cdot n! + 1) \\ &= \text{ggT}(i \cdot n! + 1, d \cdot n!) \end{aligned}$$

Für $n > 2$ ist $d \cdot n!$ keine Primzahl. Jede Primzahl, die $d \cdot n!$ teilt, ist daher höchstens gleich n. Da keine Primzahl, die $d \cdot n!$ teilt, auch $i \cdot n! + 1$ teilen kann, gilt:

$$\text{ggT}(i \cdot n! + 1, d \cdot n!) = 1.$$

Falls nun die Anzahl aller Primzahlen m wäre und man $n = m + 1$ wählt, folgt aus obiger Bemerkung, dass die $m + 1$ Zahlen $i \cdot (m + 1)! + 1$ $(1 \leq i \leq m + 1)$ paarweise teilerfremd sind, so dass es mindestens $m + 1$ verschiedene Primzahlen geben muss. Ein Widerspruch zur obigen Annahme, daher gibt es unendlich viele Primzahlen.

□

3.3 Beweis von Thue

Um zu zeigen, dass es unendlich viele Primzahlen gibt, verwendet Thue lediglich den Fundamentalsatz der Arithmetik.

Beweis. Es seien $n, k \geq 1$ natürliche Zahlen, welche die Ungleichung

$$(1+n)^k < 2^n$$

erfüllen. Es seien $p_1 = 2$, $p_2 = 3, \cdots, p_r$ alle Primzahlen $\leq 2^n$.
Aufgrund des Fundamentalsatzes der Arithmetik lässt sich jede Zahl m $(1 \leq m \leq 2^n)$ in eindeutiger Weise schreiben als

$$m = 2^{e_1} \cdot 3^{e_2} \cdots p_r^{e_r},$$

wobei $0 \leq e_i \leq n$ und $1 \leq i \leq r$. Die Anzahl der möglichen Kombinationen für die Exponenten $e_1, e_2, \ldots, e_r$ ist höchstens $(n+1)n^{r-1}$. Wäre $r \leq k$, so ergäbe das

$$2^n \leq (n+1)n^r < (n+1)^r \leq (n+1)^k < 2^n,$$

was unmöglich ist. Also ist $r \geq k+1$.
Es wird $n = 2k^2$ gewählt. Aus $1 + 2k^2 < 2^{2k}$ folgt daraus

$$(1+2k^2)^k < 2^{2k^2} = 4^{k^2}.$$

Daher gibt es bis 4^{k^2} mindestens $k+1$ Primzahlen. Da k aber beliebig gewählt werden kann, kann dadurch gezeigt werden, dass es unendlich viele Primzahlen gibt. □

Bemerkung 3.3. Die verwendete Ungleichung folgt z.B. aus

$$\begin{aligned} 2^{2k} = (1+1)^{2k} \geq 1 + \binom{2k}{1} + \binom{2k}{2} &= 1 + 2k + k(2k-1) \\ &= 1 + 2k + 2k^2 - k \\ &= 1 + k + 2k^2 > 1 + 2k^2. \end{aligned}$$

3.4 Beweis von Euler

Leonard Euler war im 18. Jahrhundert einer der einflussreichsten Mathematiker, dessen Beiträge die Mathematik nachhaltig geprägt haben. Im Jahr 1737 veröffentlichte Euler in seiner Schrift Introductio in analysin infinitorum einen Beweis für die Unendlichkeit der Menge der Primzahlen. Er nutzte dazu den Satz über die Eindeutigkeit der Primfaktorenzerlegung und die Tatsache, dass die harmonische Reihe $(\sum_{i=1}^{n} \frac{1}{i})_{n\in\mathbb{N}}$ für $n \to \infty$ divergiert.
2011 beschreibt Ribenboim den Beweis in „Die Welt der Primzahlen“ folgendermaßen: Er führt folgende Überlegungen durch:
Es muss unendlich viele Primzahlen geben, weil ein bestimmter, aus allen Primzahlen gebildeter Ausdruck unbeschränkt wächst.
Es sei p eine beliebige Primzahl, so ist $\frac{1}{p} < 1$, und die geometrische Reihe summiert sich zu

$$\sum_{k=0}^{\infty} \frac{1}{p^k} = \frac{1}{1-\frac{1}{p}}$$

Für eine weitere Primzahl q ergibt sich analog

$$\sum_{k=0}^{\infty} \frac{1}{q^k} = \frac{1}{1-\frac{1}{q}}$$

Indem man diese Gleichungen miteinander multipliziert, erhält man:

$$1 + \frac{1}{p} + \frac{1}{q} + \frac{1}{p^2} + \frac{1}{pq} + \frac{1}{q^2} + \cdots = \frac{1}{1-\frac{1}{p}} \cdot \frac{1}{1-\frac{1}{q}}$$

Die linke Seite ist genau die Summe der Inversen aller natürlichen Zahlen der Form $p^h q^k$ für $h, k \geq 0$. Dabei wird $p^h q^k$ genau einmal gezählt, denn jede natürliche Zahl besitzt eine eindeutige Darstellung als Produkt von Primfaktoren.
Diese Überlegung zeigt, dass die Unendlichkeit von Primzahlen direkt aus den Eigenschaften der geometrischen Reihe und der Eindeutigkeit der Primfaktorenzerlegung folgt und ist die Basis des folgenden Beweises aus Ribenboims „Die Welt der Primzahlen“.

Beweis. Zunächst wird die geometrische Reihe $\sum_{k=0}^{\infty} \frac{1}{p_i^k}$ für eine beliebige Primzahl p_i betrachtet. Da einzelne Terme mit wachsendem k exponentiell kleiner werden, hat die Reihe einen endlichen Wert. Angenommen, es gäbe nur endlich viele Primzahlen $p_1, p_2, \ldots, p_n$. Für jedes $i = 1, \ldots, n$ gilt

$$\sum_{k=0}^{\infty} \frac{1}{p_i^k} = \frac{1}{1-\frac{1}{p_i}}$$

Wenn man diese n Gleichungen miteinander multipliziert, erhält man

$$\prod_{i=1}^{n}\left(\sum_{k=0}^{\infty}\frac{1}{p_i^k}\right)=\prod_{i=1}^{n}\frac{1}{1-\frac{1}{p_i}}$$

Die linke Seite des Ausdrucks ist äquivalent zur Summe der Inversen aller natürlichen Zahlen, jeweils einmal gezählt, was sich aus der Eindeutigkeit der Primfaktorenzerlegung ergibt. Die Reihenfolge der Summation ist beliebig und hat daher keinen Einfluss auf das Ergebnis, da die Summanden der Reihe positiv sind. Daher ist die linke Seite gleich der harmonischen Reihe $\sum_{n=1}^{\infty}\frac{1}{n}$, und diese Reihe ist divergent.
Die rechte Seite des Ausdrucks ist endlich, da es sich um das Produkt endlich vieler Brüche mit endlichem Wert handelt.
Dies führt zu einem Widerspruch der Annahme und beweist damit, dass es tatsächlich unendlich viele Primzahlen gibt.

□

Aus dem Buch der Beweise (2002), von Aigner und Ziegler, folgt ein weiterer, ausführlicherer Beweis für die Unendlichkeit der Primzahlen. Dieser Beweis stammt ebenfalls von Leonard Euler und beinhaltet neben der geometrischen Reihe auch den natürlichen Logarithmus.

Beweis. Die Anzahl der Primzahlen, die kleiner oder gleich der reellen Zahl x sind, wird als $\pi(x) := \#\{p \leq x : p \in \mathbb{P}\}$ beschrieben. Dabei bezeichne $\mathbb{P}$ die Menge der Primzahlen. Es sei $\log x$ der natürliche Logarithmus, das heißt

$$\log x=\int_{1}^{x}\frac{dt}{t}.$$

Anschließend wird die Fläche unter dem Graphen der Funktion $f(t)=\frac{1}{t}$, mit einer oberen Treppenfunktion (siehe Abb.1) verglichen.
Für $n \leq x < n+1$ erhält man daher

$$\begin{aligned}\log x &\leq 1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n-1}+\frac{1}{n}\\ &\leq \sum{}'\frac{1}{m},\end{aligned}$$

wobei die Summe $\sum'\frac{1}{m}$ über alle natürlichen Zahlen m läuft, deren Primfaktoren p höchstens x sind.
Jede solche Zahl m lässt sich aufgrund des Fundamentalsatzes der Arithmetik auf

eindeutige Weise, als ein Produkt der Form

$$\prod_{p \leq x} p^{k_p}$$

darstellen, wobei nur endlich viele Exponenten k_p ungleich 0 sind.
Daraus kann geschlossen werden, dass

$$\sum\nolimits' \frac{1}{m} = \prod_{p \leq x} \Big(\sum_{k \geq 0} \frac{1}{p^k} \Big)$$

gilt. Die innere Summe dessen ist eine geometrische Reihe mit Faktor $\frac{1}{p}$, woraus

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

folgt. Weiters gilt aufgrund der Menge der Primzahlen $\mathbb{P}$ und $\pi(x)$,

$$\log x \leq \prod_{p \leq x} \frac{p}{p-1} = \prod_{k=1}^{\pi(x)} \frac{p_k}{p_k - 1}$$

Da offensichtlich $p_k \geq k + 1$ gilt, erhält man

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

Somit folgt daraus:

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

Die Funktion $\log x$ ist nicht beschränkt, daraus kann geschlossen werden, dass $\pi(x)$ ebenfalls unbeschränkt ist, also gibt es unendlich viele Primzahlen.

□

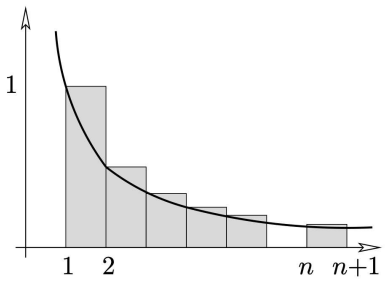

Abbildung 2: Eine obere Treppenfunktion für $f(t) = \frac{1}{t}$

3.5 Beweis von Erdös

Der ungarische Mathematiker Paul Erdös trug im 20. Jahrhundert ebenfalls einen der wichtigsten Beweise für die Unendlichkeit der Primzahlen bei. Dieser Beweis aus dem Buch der Beweise (2011), von Aigner und Zieger, betrachtet die Reihe der Inversen der Primzahlen und geht dabei noch wesentlich tiefer.

Beweis. Sei $p_1 < p_2 < p_3 < \cdots$ die Folge aller Primzahlen in aufsteigender Ordnung. Angenommen die Reihe $\sum \frac{1}{p_i}$ konvergiert, dann gibt es eine natürliche Zahl l, sodass

$$\sum_{i \geq l+1} \frac{1}{p_i} < \frac{1}{2}. \tag{1}$$

Das bedeutet, dass die Primzahlen, die nach p_l kommen, weniger als die Hälfte der Gesamtsumme beitragen. Die Primzahlen $p_1, \ldots, p_l$ werden als die „kleinen“ Primzahlen und $p_{l+1}, p_{l+2}, \ldots$ als die „großen“ Primzahlen bezeichnet. Aus (1) folgt für jede natürliche Zahl N

$$\sum_{i \geq l+1} \frac{N}{p_i} < \frac{N}{2}. \tag{2}$$

Die Menge der natürlichen Zahlen $1, \ldots, N$ wird in zwei Teile geteilt. Es sei N_g die Anzahl der Zahlen in $\{1, \ldots, N\}$, welche mindestens einen großen Primteiler haben und N_k die Anzahl der Zahlen in $\{1, \ldots, N\}$, die nur kleine Primteiler haben. Offenbar gilt

$$N = N_g + N_k.$$

Es soll N_g und N_k abgeschätzt werden. Die Anzahl der Vielfachen von p_i, welche $\leq N$ sind, ist $[\frac{N}{p_i}]$, und man erhält daraus mit (2) für N_g

$$N_g \leq \sum_{i \geq l+1} \left[\frac{N}{p_i} \right] < \frac{N}{2}. \tag{3}$$

Um N_k abschätzen zu können, wird jede Zahl $n \leq N$ in der Form $n = a_n b_n^2$ geschrieben, wobei a_n quadratfrei ist. Jedes a_n ist dann ein Produkt verschiedener kleiner Primzahlen (Fundamentalsatz). Daraus und weil es nach Annahme nur l kleine Primzahlen gibt, folgt, dass es genau 2^l verschiedene quadratfreie Teile gibt.
Für die nicht quadratfreien Teile b_n gilt,

$$b_n \leq \sqrt{n} \leq \sqrt{N}.$$

Also ist die Anzahl der möglichen b_n^2 höchstens $\sqrt{N}$. Insgesamt ergibt dies durch Kombination

$$N_k \leq 2^l \sqrt{N}. \tag{4}$$

Um den Widerspruch zu $N = N_g + N_k$ herzustellen, muss aufgrund von (2) nun lediglich ein N gefunden werden, für das $N_k \leq 2^l \sqrt{N}$ und somit $2^l \sqrt{N} \leq \frac{N}{2}$ gilt.
Wählt man z.B. $N = 2^{2l+2}$, so ist

$$\sqrt{N} = \sqrt{2^{2l+2}} = \sqrt{2^{2\cdot(l+1)}} = 2^{l+1}$$

und damit ist

$$2^l \sqrt{N} = 2^{2l+1} \leq \frac{N}{2}.$$

Dies führt schlussendlich zu einem Widerspruch, da die Ungleichung $N_g + N_k < N$ mit $N = 2^{2l+2}$ gilt. Daher divergiert die Reihe $\sum \frac{1}{p_i}$ und es muss unendlich viele Primzahlen geben.

□

Das Besondere an diesem Beweis ist, dass Paul Erdös damit nicht nur die Unendlichkeit der Primzahlen nachweisen kann, sondern eben auch, dass die Reihe $\sum \frac{1}{p}$ divergiert.

3.6 Beweis von Perott

Der Beweis von Perott, aus dem Jahr 1881, ist einer von drei Beweisen, welche zwar zu keinen neuen Erkenntnissen führen, jedoch trotzdem originell und einfallsreich sind. Sie werden von Ribenboim im Buch "Die Welt der Primzahlen (2011)" als "Die drei vergessenen Beweise" bezeichnet.
Für den ersten Beweis von Perott muss man wissen, dass die Reihe $\sum_{n=1}^{\infty} \frac{1}{n^2}$ konvergiert mit einer Summe $\sum_{n=1}^{\infty} \frac{1}{n^2} < 2$. Tatsächlich ist

$$\sum_{n=1}^{\infty} \frac{1}{n^2} < 1 + \sum_{n=1}^{\infty} \frac{1}{n(n+1)} = 1 + \sum_{n=1}^{\infty} \Big(\frac{1}{n} - \frac{1}{n+1} \Big) = 1 + 1 = 2.$$

Beweis. Angenommen, es gäbe nur r Primzahlen $p_1 < p_2 < \cdots < p_r$. Es sei N eine beliebige Zahl mit $p_1 \cdot p_2 \cdots p_r < N$. Die Anzahl derjenigen $m \leq N$, die quadratfrei sind, ist 2^r, dies entspricht genau der Anzahl der möglichen Mengen verschiedener Primzahlen, da jede Zahl in eindeutiger Weise das Produkt von Primzahlen ist. Da nur höchstens $\frac{N}{p_i^2}$ Zahlen $m \leq N$ durch p_i^2 teilbar sind, ist die Anzahl derjenigen $m \leq N$, welche sich durch irgendein Quadrat teilen lassen, höchstens gleich $\sum_{i=1}^{r} \frac{N}{p_i^2}$. Da die Reihe $\sum_{n=1}^{\infty} \frac{1}{n^2}$ konvergiert und $\sum_{n=1}^{\infty} \frac{1}{n^2} < 2$, folgt

$$\begin{aligned} N &\leq 2^r + \sum_{i=1}^{r} \frac{N}{p_i^2} \\ &< 2^r + N \left(\sum_{n=1}^{\infty} \frac{1}{n^2} - 1 \right) \end{aligned}$$

Der letzte Faktor auf der rechten Seite dieser Ungleichung ist von N unabhängig, wählt man ein N so, dass $N\big(2 - \sum_{n=1}^{\infty} \frac{1}{n^2}\big) \geq 2^r$, führt dies zu einem Widerspruch, da dann $N\Big(1 - \big(\sum_{n=1}^{\infty} \frac{1}{n^2} - 1\big)\Big) \geq 2^r$ und daher $2^r + N\big(\sum_{n=1}^{\infty} \frac{1}{n^2} - 1\big) \leq N$.

Daraus folgt, dass es tatsächlich unendlich viele Primzahlen geben muss. □

3.7 Beweis von Auric

Der zweite "vergessene" Beweis nach Ribenboim "Die Welt der Primzahlen (2011)" ist von Auric und wurde 1915 veröffentlicht.

Beweis. Angenommen, es gäbe nur r Primzahlen $p_1 < p_2 < \cdots < p_r$.
Es sei $t \geq 1$ eine beliebige ganze Zahl und $N = p_r^t$. Aufgrund der Eindeutigkeit der Primfaktorzerlegung lässt sich jede Zahl m $(1 \leq m \leq N)$ als

$$m = p_1^{f_1} \cdot p_2^{f_2} \cdots p_r^{f_r}$$

schreiben, wobei die Folge $(f_1, f_2, \ldots, f_r)$, $f_i \geq 0$, eindeutig festgelegt ist. Aus

$$p_1^{f_i} \leq p_i^{fi} \leq m \leq N = p_r^t$$

ergibt sich für $i = 1, 2, \ldots, r$, dass $f_i \leq tE$, wobei $E = \dfrac{\log p_r}{\log p_1}$.
Daher ist die Anzahl N der ganzen Zahlen m, die im Bereich $1 \leq m \leq N$ liegen, höchstens gleich der Anzahl von Folgen $(f_1, f_2, \ldots, f_r)$ und somit ist

$$p_r^t = N \leq (tE + 1)^r \leq t^r (E + 1)^r.$$

Für ein genügend großes t wird diese Ungleichung unwahr, damit ist gezeigt, dass die Anzahl der Primzahlen bis ins Unendliche wachsen muss. □

3.8 Beweis von Métrod

Der letzte der drei "vergessenen" Beweise nach Ribenboim "Die Welt der Primzahlen (2011)" ist ebenfalls sehr kurz und stammt aus dem Jahr 1917 von Méthod.

Beweis. Angenommen, es gäbe nur r Primzahlen $p_1 < p_2 < \cdots p_r$.
Es sei für $i = 1, 2, \ldots, r$

$$N = p_1 \cdot p_2 \cdots p_r \quad \text{und} \quad Q_i = \frac{N}{p_i}.$$

Für kein i gilt $p_i \mid Q_i$, aber $p_i \mid Q_j$, sofern $j \neq i$.
Man setze nun

$$S = \sum_{i=1}^{r} Q_i$$

und bezeichne mit q einen beliebigen Primteiler von S.
Dann ist q verschieden von allen p_i, denn $p_i \mid Q_j$ für alle $i \neq j$, doch p_i ist kein Teiler von Q_i. Daher muss q eine weitere Primzahl sein, welche nicht in der ursprünglichen Menge von Primzahlen enthalten ist, dies führt zu einem Widerspruch.
Es folgt daraus, dass es unendlich viele Primzahlen gibt. □

3.9 Beweis von Furstenberg

Im Jahr 1955 veröffentlichte Harry Furstenberg, geboren Fürstenberg, einen Beweis im American Mathematical Monthly. Dieser Beweis für die Unendlichkeit der Primzahlen basiert auf topologischen Überlegungen und verbindet abstrakte mathematische Konzepte mit der Zahlentheorie. Der Beweis wird hier zunächst wörtlich wiedergegeben, bevor er diskutiert wird.

Beweis. In this note we would like to offer an elementary "topological" proof of the infinitude of the prime numbers. We introduce a topology into the space of integers S, by using the arithmetic progressions (from $-\infty$ to $+\infty$) as a basis. It is not difficult to verify that this actually yields a topological space. In fact, under this topology, S may be shown to be normal and hence metrizable. Each arithmetic progressions is closed as well as open, since its complement is the union of other arithmetic progressions (having the same difference). As a result the union of any finite number of arithmetic progressions is closed. Consider now the set $A = \cup A_p$, where A_p consists of all multiples of p, and p runs through the set of primes ≥ 2. The only numbers not belonging to A are -1 and 1, and since the set $\{-1, 1\}$ is clearly not an open set, A cannot be closed. Hence A is not a finite union of closed sets which proves that there are an infinity of primes. □

Der Beweis von Furstenberg mittels Topologie wird im Buch der Beweise als "fünfter Beweis" vereinfacht dargestellt.

Beweis*(Furstenberg).* Es wird eine Topologie auf der Menge $\mathbb{Z}$ betrachtet.
Für $a, b \in \mathbb{Z}$, $b > 0$ setzen wir

$$N_{a,b} = \{a + nb : n \in \mathbb{Z}\}.$$

Jede Menge $N_{a,b}$ ist eine in beide Richtungen unendliche arithmetische Folge. Wir nennen nun eine Menge $O \subseteq \mathbb{Z}$ offen, wenn entweder O leer ist oder wenn zu jedem $a \in O$ ein $b > 0$ existiert mit $N_{a,b} \subseteq O$. Offensichtlich ist dann jede Vereinigung von offenen Mengen wieder offen. Falls O_1 und O_2 offen sind und $a \in O_1 \bigcap O_2$ mit $N_{a,b_1} \subseteq O_1$ und $N_{a,b_2} \subseteq O_2$, so ist $a \in N_{a,b_1 b_2} \subseteq O_1 \bigcap O_2$. Daraus folgt, dass jeder Durchschnitt von endliche vielen offenen Mengen wiederum offen sein muss. Es werden die Axiome einer Topologie auf $\mathbb{Z}$ erfüllt, es gilt:

(A) Jede nicht-leere offene Menge ist unendlich.

(B) Jede Menge $N_{a,b}$ ist auch abgeschlossen.

Das erste Resultat folgt direkt aus der Definition. Zu (B) wird bemerkt:

$$N_{a,b} = \mathbb{Z} \setminus \bigcup_{i=1}^{b-1} N_{a+i,b}$$

Daher ist also $N_{a,b}$ das Kompliment einer offenen Menge und somit abgeschlossen. Nun kommen die Primzahlen ins Spiel: Da jede Zahl $n \neq 1, -1$ einen Primteiler p besitzt und daher in der Menge $N_{0,p}$ enthalten ist, kann geschlossen werden

$$\mathbb{Z} \setminus \{1, -1\} = \bigcup_{p \in \mathbb{P}} N_{0,p}.$$

Wäre nun $\mathbb{P}$ endlich, so wäre $\bigcup\limits_{p \in \mathbb{P}} N_{0,p}$ eine endliche Vereinigung von abgeschlossenen Mengen (nach (B)) und daher ebenfalls abgeschlossen. Folglich wäre $\{1, -1\}$ eine offenen Menge, was ein Widerspruch zu (A) wäre.

□

Es folgt nun eine detailliertere Analyse dieses Beweises, dafür zu Beginn eine Erinnerung an die Topologie im $\mathbb{R}^n$ (wie sie in der Analysis behandelt wird):

Definition 3.4. Es sei $x \in \mathbb{R}^n$ und $r > 0$. Eine Menge der Gestalt

$$B_r(x) = \left\{ y \in \mathbb{R}^n \middle| \|y - x\| < r \right\}$$

wird als offene Kugel mit Radius r um x bezeichnet.

Definition 3.5. Eine Menge $U \subseteq \mathbb{R}^n$ heißt offen, wenn für jedes $x \in U$ ein $\epsilon > 0$ existiert, derart dass $B_\epsilon(x) \subseteq U$.

Bemerkung 3.6. Gemäß dieser Definition ist die leere Menge $\varnothing$ ($\subseteq \mathbb{R}^n$) eine offene Menge.

Lemma 3.7. *Es sei $U \subseteq \mathbb{R}^n$ und $U \neq \varnothing$. Dann sind folgende Aussagen äquivalent:*

(i) U ist offen,

(ii) U ist die Vereinigung offener Kugeln.

Beweis.
$(i) \Rightarrow (ii)$: Für jedes $x \in U$ existiert ein $\epsilon_x > 0$, sodass $B_{\epsilon_x}(x) \subseteq U$. Daher ist

$$U = \bigcup_{x \in U} \{x\} \subseteq \bigcup_{x \in U} B_{\epsilon_x}(x) \subseteq U$$

und somit $U = \bigcup_{x \in U} B_{\epsilon_x}(x)$, U ist eine Vereinigung offener Kugeln.

$(ii) \Rightarrow (i)$: Es gibt eine Menge $\{x_i | i \in I\} \subseteq U$ und für jedes $i \in I$ ein $\epsilon_i > 0$, so dass

$$U = \bigcup_{x \in I} B_{\epsilon_i}(x_i).$$

Ist nun $x \in U$, so existiert $i_0 \in I$, derart dass $x \in B_{\epsilon_{i_0}}(x_{i_0})$.
Ist $x = x_{i_0}$, so ist

$$B_{\epsilon_{i_0}}(x) = B_{\epsilon_{i_0}}(x_{i_0}) \subseteq U.$$

Ist $x \neq x_{i_0}$, so ist

$$B_{\epsilon_{i_0} - \|x - x_{i_0}\|}(x) \subseteq B_{\epsilon_{i_0}}(x_{i_0}) \subseteq U.$$

Ist $y \in B_{\epsilon_{i_0} - \|x - x_{i_0}\|}(x)$, so ist $\|y - x\| < \epsilon_{i_0} - \|x - x_{i_0}\|$ und daher

$$\|y - x_{i_0}\| \leq \|y - x\| + \|x - x_{i_0}\| < \epsilon_{i_0},$$

also $y \in B_{\epsilon_{i_0}}(x_{i_0})$. Daher ist U offen.

□

Satz 3.8.

(i) Sind alle $U_i \subseteq \mathbb{R}^n$ für alle $i \in I$ offen, so ist auch $\bigcup_{i \in I} U_i$ offen.

(ii) Sind $U_1, \ldots, U_k \subseteq \mathbb{R}^n$ offen, so ist auch $U_1 \cap \cdots \cap U_k$ offen.

Beweis.

(i) Ist $x \in \bigcup_{i \in I} U_i$, so gibt es ein $i_0 \in I$, derart dass $x \in U_{i_0}$ und daher ein $\epsilon > 0$ mit

$$B_\epsilon(x) \subseteq U_{i_0} \subseteq \bigcup_{i \in I} U_i.$$

(ii) Ist $x \in U_1, \ldots, U_k$, so existieren $\epsilon_1, \ldots, \epsilon_n > 0$ mit der Eigenschaft $B_{\epsilon_i}(x) \subseteq U_i$ für $1 \leq i \leq n$. Setzt man $\epsilon := \min\{\epsilon_1, \ldots, \epsilon_n\}$, so folgt

$$B_\epsilon(x) \subseteq B_{\epsilon_i}(x) \subseteq U_i,$$

für $1 \leq i \leq n$ und daher $B_\epsilon(x) \subseteq U_1 \cap \cdots \cap U_k$.

□

Definition 3.9. Eine Menge $A \in \mathbb{R}^n$ heißt abgeschlossen, wenn $\mathbb{R}^n \setminus A$ offen ist.

Satz 3.10.

(i) Sind alle $A_i \subseteq \mathbb{R}^n$ für alle $i \in I$ abgeschlossen, so ist auch $\bigcap_{i\in I} A_i$ abgeschlossen.

(ii) Sind $A_1, \ldots, A_k \subseteq \mathbb{R}^n$ abgeschlossen, so ist auch $A_1 \cup \cdots \cup A_k$ abgeschlossen.

Beweis.

(i) $\mathbb{R}^n \setminus \bigcap_{i\in I} A_i = \bigcup_{i\in I}(\mathbb{R}^n \setminus A_i)$ ist nach Satz 3.8 (i) offen.

(ii) $\mathbb{R}^n \setminus (A_1 \cup \cdots \cup A_k) = (\mathbb{R}^n \setminus A_1) \cap \cdots \cap (\mathbb{R}^n \setminus A_k)$ ist nach Satz 3.8 (ii) offen.

□

Es wird nun eine weitgehend analoge Konstruktion auf $\mathbb{Z}$ durchgeführt, wobei hier die arithmetischen Progressionen $a + b\mathbb{Z}$ (mit $a, b \in \mathbb{Z}$ und $b > 0$) die Rolle der offenen Kugeln übernehmen.

Definition 3.11. Eine Menge $U \subseteq \mathbb{Z}$ heißt offen, wenn für jedes $a \in U$ ein $b \in \mathbb{Z}$, $b > 0$ mit der Eigenschaft $a + b\mathbb{Z} \subseteq U$ existiert.

Bemerkung 3.12.

1) Auch nach dieser Definition ist die leere Menge $\varnothing(\subseteq \mathbb{Z})$ eine offene Menge.

2) Ist $U \subseteq \mathbb{Z}$, $U \neq \varnothing$ offen, so muss U unendlich sein.

Lemma 3.13. *Es sei $U \subseteq \mathbb{Z}$, $U \neq \varnothing$. Dann sind äquvalent:*

(i) U ist offen,

(ii) U ist die Vereinigung arithmetischer Progressionen.

Beweis.
$(i) \Rightarrow (ii)$: Für jedes $a \in U$, existiert ein $b_a \in \mathbb{Z}, b_a > 0$, mit $a + b_a\,\mathbb{Z} \subseteq U$.
Daher ist

$$U = \bigcup_{a\in U} \{a\} \subseteq \bigcup_{a\in U} (a + b_a\mathbb{Z}) \subseteq U$$

und somit $U = \bigcup_{a\in U} (a + b_a\mathbb{Z})$, U ist eine Vereinigung arithmetischer Progressionen.

$(ii) \Rightarrow (i)$: Es gibt eine Menge $\{a_i | i \in I\} \subseteq U$ und für jedes $i \in I$ ein $b_i \in \mathbb{Z}$, $b_i > 0$, derart dass $U = \bigcup_{i\in I}(a_i + b_i\mathbb{Z})$.
Ist nun $a \in U$, so existiert $i_0 \in I$ so, dass $a \in a_{i_0} + b_{i_0}\mathbb{Z}$. Die Behauptung folgt aus

$$a \in a + b_{i_0}\mathbb{Z} = a_{i_0} + b_{i_0}\mathbb{Z} \subseteq U.$$

Es ist $a \in a_{i_0} + b_{i_0}\mathbb{Z}$ äquivalent zu $b_{i_0}|(a - a_{i_0})$, d.h. $a - a_{i_0} = n_0 b_{i_0}$ für ein $n_0 \in \mathbb{Z}$.
Ist $x \in a + b_{i_0}\mathbb{Z}$, so ist $x = a + b_{i_0} n$ für ein $n \in \mathbb{Z}$ und daher

$$x = a_{i_0} + (a - a_{i_0}) + b_{i_0} n = a_{i_0} + b_{i_0}(n + n_0) \in a_{i_0} + b_{i_0}\mathbb{Z},$$

d.h. $a + b_{i_0}\mathbb{Z} \subseteq a_{i_0} + b_{i_0}\mathbb{Z}$.
Ist umgekehrt $x \in a_{i_0} + b_{i_0}\mathbb{Z}$, so ist $x = a_{i_0} + b_{i_0} n$ für ein $n \in \mathbb{Z}$ und daher

$$x = a_{i_0} + b_{i_0} n = a - (a - a_{i_0}) + b_{i_0} n = a + b_{i_0}(n - n_0) \in a + b_{i_0}\mathbb{Z},$$

d.h. es gilt auch $a_{i_0} + b_{i_0}\mathbb{Z} \subseteq a + b_{i_0}\mathbb{Z}$. □

Satz 3.14.

(i) Sind alle $U_i \subseteq \mathbb{Z}$ für alle $i \in I$ offen, so ist auch $\bigcup_{i \in I} U_i$ offen.

(ii) Sind $U_1, \ldots, U_k \subseteq \mathbb{Z}$ offen, so ist auch $U_1 \cap \cdots \cap U_k$ offen.

Beweis.

(i) Ist $a \in \bigcup_{i \in I} U_i$, so gibt es ein $i_0 \in I$ so, dass $a \in U_{i_0}$ und daher existiert ein $b \in \mathbb{Z}$, $b > 0$ mit

$$a + b\mathbb{Z} \subseteq U_{i_0} \subseteq \bigcup_{i \in I} U_i.$$

(ii) Ist $a \in U_1 \cap \cdots \cap U_k$, so gibt es positive $b_1, \ldots, b_k \in \mathbb{Z}$ mit der Eigenschaft $a + b_i\mathbb{Z} \subseteq U_i$, für $1 \leq i \leq n$.
Ist $b = b_1 \cdot \cdots \cdot b_k$, so ist

$$a + b\mathbb{Z} \subseteq a + b_i\mathbb{Z} \subseteq U_i$$

für $1 \leq i \leq n$ und daher $a + b\mathbb{Z} \subseteq U_1 \cap \cdots \cap U_k$.

□

Definition 3.15. Eine Menge $A \in \mathbb{Z}$ heißt abgeschlossen, wenn $\mathbb{Z} \setminus A$ offen ist.

Bemerkung 3.16. Jede arithmetische Progression $a + b\mathbb{Z}$ (mit $a, b \in \mathbb{Z}$, $b > 0$) ist nach diesen Definitionen sowohl offen, als auch abgeschlossen. Dass $a + b\mathbb{Z}$ offen ist, folgt aus Lemma 3.13. Offenbar ist

$$\mathbb{Z} \setminus (a + b\mathbb{Z}) = (a + 1 + b\mathbb{Z}) \cup (a + 2 + b\mathbb{Z}) \cup \cdots \cup (a + b - 1 + b\mathbb{Z}).$$

Da die rechte Seite (aufgrund von Satz 3.14. (i)) offen ist, gilt das auch für die linke Seite.

Satz 3.17.

(i) Sind alle $A_i \subseteq \mathbb{Z}$ für alle $i \in I$ abgeschloosen, so ist auch $\bigcap\limits_{i\in I} A_i$ abgeschlossen.

(ii) Sind $A_1, \ldots, A_k \subseteq \mathbb{Z}$ abgeschlossen, so ist auch $A_1 \cup \cdots \cup A_k$ abgeschlossen.

Beweis. Beide Aussagen können, völlig analog zum Beweis von Satz 3.8., aus Satz 3.14. gefolgert werden. □

Beweis für die Unendlichkeit von Primzahlen.
Da ± 1 die einzigen beiden ganzen Zahlen sind, die nicht durch eine Primzahl teilbar sind, ist

$$\mathbb{Z} \setminus \{-1, 1\} = \bigcup_{p\in\mathbb{P}} (0 + p\mathbb{Z}) = \bigcup_{p\in\mathbb{P}} p\mathbb{Z}.$$

Wäre die Menge $\mathbb{P}$ endlich, so wäre $\bigcup\limits_{p\in\mathbb{P}} p\mathbb{Z}$ nach Satz 3.17.(ii) und der Bemerkung 3.16. abgeschlossen. Dann wäre aber auch $\mathbb{Z} \setminus \{-1, 1\}$ abgeschlossen und daher $\{-1, 1\}$ offen. Das ist aber unmöglich, da $\{-1, 1\}$ weder leer noch unendlich ist, was zu einem Widerspruch führt! □

Die folgende Verknüpfung der Beweise von Euklid und Furstenberg stammt von Keith Conrad, er führt diesen an, allerdings ohne Begriffe aus der Topologie zu verwenden:

Beweis. Aus $\bigcup\limits_{p} p\mathbb{Z} = \mathbb{Z}\setminus \{1, -1\}$ folgt mittels Komplementbildung

$$\bigcap_{p} (\mathbb{Z} \setminus p\mathbb{Z}) = \{1, -1\}.$$

Sind $p_1, \ldots, p_k$ paarweise verschiedene Primzahlen, so ist

$$1 + p_1 \ldots p_k \, \mathbb{Z} \subseteq \bigcap_{i=1}^{k} (\mathbb{Z} \setminus p_i\mathbb{Z}),$$

da für $1 \leq i \leq k$ und $n \in \mathbb{Z}$ stets $p_i \nmid (1 + p_1 \ldots p_k n)$ gilt.
Gäbe es nun endlich viele Primzahlen $p_1, \ldots, p_k$, so wäre

$$1 + p_1 \ldots p_k \, \mathbb{Z} \subseteq \bigcap_{i=1}^{k} (\mathbb{Z} \setminus p_i\mathbb{Z}) = \bigcap_{p} (\mathbb{Z} \setminus p\mathbb{Z}) = \{1, -1\},$$

was einen Widerspruch liefert. □

4 Arithmetische Progression

Nachdem verschiedene Beweise zur Unendlichkeit gezeigt wurden, widmet sich dieses Kapitel der Beziehung zwischen Primzahlen und arithmetischen Progressionen, sowie ihrer Verteilung.
Eine arithmetische Progression ist eine endliche oder unendliche Folge von Zahlen, bei der die Differenz zwischen zwei aufeinanderfolgenden Elementen konstant ist. Diese Konstante wird als arithmetische Differenz d bezeichnet.
Die allgemeine Form einer arithmetischen Progression ist:

$$a, a + d, a + 2d, a + 3d, \ldots$$

Peter Gustav Lejeune Dirichlet hat im Jahre 1837 einen wichtigen Satz in der Zahlentheorie bewiesen, den Dirichletsche Primzahlsatz. Dieser trägt zum Verständnis der Verteilung von Primzahlen bei und besagt folgendes:
In jeder gegebenen arithmetischen Progression $a, a+d, a+2d, a+3d, \ldots$ sind unendlich viele Primzahlen enthalten, wenn $a, d \in \mathbb{N}$ und teilerfremd sind.

Satz 4.1 (DIRICHLETscher Primzahlsatz)**.** *Wenn* $\mathrm{ggT}(a, d) = 1$*, dann gibt es unendlich viele Primzahlen der Form* $dk + a$ *(mit* $k \in \mathbb{N}$ *).*

Die Allgemeine Aussage kann mittels Methoden der analytischen Zahlentheorie bewiesen werden, welche diese Arbeit sprengen würde. Andere Formulierungen des Dirichlet'schen Primzahlsatzes sind:

Satz 4.2 (**2. Formulierung:**)**.** *Sind* $a, d \in \mathbb{N}$ *zueinander teilerfremd, so gibt es unendlich viele Primzahlen* p *mit* $p \equiv a \pmod{d}$*.*

Bemerkung 4.3. Angenommen eine Primzahl q teilt sowohl a als auch d, wobei oBdA $a < d$, so gilt $q \mid (a + kd)$ für $k \in \mathbb{Z}$. Daher kann höchstens der kleinste positive Wert von $a + kd$ eine Primzahl (und damit gleich q) sein.

Satz 4.4 (**3. Formulierung:**)**.** *Wenn* $d \geq 2$ *und* $a \neq 0$ *ganze, teilerfremde Zahlen sind, dann enthält die arithmetische Folge*

$$a, a + d, a + 2d, a + 3d, \ldots$$

unendlich viele Primzahlen.

Spezielle arithmetische Progressionen

Für arithmetische Progressionen existieren zahlreiche Spezialfälle, d.h. a und d nehmen bestimmte besondere Werte an. Es folgen elementare Beweise für die Unendlichkeit der Primzahlen in solchen Spezialfällen arithmetischer Progressionen.
Nach kurzen Bemerkungen zur Gestalt von Primzahlen arithmetischer Progressionen wird mit zwei elementaren Beweisen für Primzahlen der Gestalt $4k+3$ bzw. $4k-1$ (oder auch $p \equiv 3 \pmod 4$), noch ohne Verwendung von Kongruenzen, begonnen.

Bemerkung 4.5. Keine Primzahl $p > 2$ ist durch 2 teilbar. Bei der Division von $p > 2$ durch 4 treten also nur die Reste 1 oder 3 auf. Anders ausgedrückt:
Jede Primzahl $p > 2$ ist von der Gestalt $4 \cdot k + 1$ oder $4 \cdot k + 3$ für ein $k \in \mathbb{N}_0$.

Bemerkung 4.6. Das Produkt zweier Zahlen der Gestalt $4l+1$ bzw. $4l+3$ hat stets die Gestalt $4k+1$, denn:

$$\begin{aligned}(4l+1)(4m+1) &= 16lm + 4l + 4m + 1 \\ &= 4 \cdot (4lm + l + m) + 1 \\ (4l+3)(4m+3) &= 16lm + 12l + 12m + 9 \\ &= 4 \cdot (4lm + 3l + 3m + 2) + 1\end{aligned}$$

Satz 4.7. *Es gibt unendlich viele Primzahlen der Gestalt $4k+3$ ($k \in \mathbb{Z}$, $k \geq 0$).*

Beweis. Angenommen, es gibt nur endlich viele Primzahlen $p_1, \ldots, p_s$ der Gestalt $4k+3$. Betrachte $N := p_1^2 \cdots p_s^2 + 2$. Mit Bemerkung 4.6. hat N dann die Gestalt $4k+3$. Sei $N = q_1 \cdots q_r$ die Primfaktorzerlegung von N. Hätten $q_1, \ldots, q_r$ alle die Gestalt $4k+1$, so würde das auch für N gelten. Dies führt zu einem Widerspruch!
Also existiert ein q_j, wobei $j \in \{1, \ldots, r\}$, mit einer anderen Gestalt. Da $q_j = 4k$ und $q_j = 4k+2$ unmöglich sind, muss q_j die Gestalt $4k+3$ haben.
Es existiert also ein $i \in \{1, \ldots, s\}$ mit $q_j = p_i$.
Dieses q_j teilt sowohl N als auch $p_1^2 \cdots p_s^2$, und somit teilt q_i ebenfalls $N - (p_1^2 \cdots p_s^2)$, woraus $q_j \mid 2$ folgt, was $q_i > 2$ widerspricht! □

Satz 4.8. *Es gibt unendlich viele Primzahlen der Form $4k-1$ mit $k \in \mathbb{N}$.*

Beweis. Angenommen es gibt nur endlich viele Primzahlen $p_1, p_2, \ldots, p_n$ der Form $4k-1$. Betrachtet man die Zahl $m = 4 \cdot p_1 \cdot p_2 \cdot \cdots \cdot p_n - 1$, erkennt man, dass sie größer ist als die größte der angenommenen Primzahlen und somit sicherlich keine Primzahl. Die Zahl m ist ungerade, hat also eindeutig bestimmte Primteiler, welche alle ungerade sind. Nach Bemerkung 4.5. kann m in der Form $4i+1$ oder in der Form $4i+3$ für ein

geeignetes $i \in \mathbb{N}$ dargestellt werden.
Da $m = 4 \cdot p_1 \cdot p_2 \ldots p_n - 1$ gewählt wurde, kann m in der Form $4r + 3$ geschrieben werden, wobei $r = p_1 \cdots p_n - 1 \in \mathbb{N}$ ist:

$$\begin{aligned} m = 4r + 3 &= 4 \cdot (p_1 \cdot p_2 \cdots p_n - 1) + 3 \\ &= 4 \cdot p_1 \cdot p_2 \cdots p_n - 4 + 3 \\ &= 4 \cdot p_1 \cdot p_2 \cdots p_n - 1. \end{aligned}$$

Keine der Primzahlen $p_1, p_2, \ldots p_n$ teilt die Zahl m, da

$$m - 4 \cdot p_1 \cdot p_2 \cdots p_n = -1$$

Nach der Annahme sind die Primzahlen $p_1, p_2, \ldots p_n$ alle Primzahlen der Form $4k - 1$, daher muss m ausschließlich Primfaktoren der Form $4k + 1$ haben.
Nach Bemerkung 4.6. lässt sich jedes Produkt aus Faktoren der Form $4k+1$, für wieder in dieser Form schreiben.
Damit ergäbe sich, dass m von der Form $m = 4s + 1$, für ein $s \in \mathbb{N}$, ist. Da m jedoch bereits die Form $m = 4r + 3$ besitzt, ergibt sich

$$\begin{aligned} 4s + 1 &= 4r + 3 \\ 4s - 4r &= 3 - 1 \\ 4 \cdot (s - r) &= 2 \\ 2 \cdot (s - r) &= 1 \end{aligned}$$

Die erhaltene Gleichung ist jedoch für keine ganze Zahl $s - r$ erfüllbar und führt somit zu einem Widerspruch! Damit ist unsere Annahme falsch und es gibt unendlich viele Primzahlen der Form $4k - 1$. □

4.1 Estermann

Um den Beweis von T. Estermann, aus Note on a paper of A Rotkiewiez (1963) vollständig angeben zu können, müssen noch Begriffe definiert und einige Lemmata bewiesen werden, welche uns zum Beweis der Unendlichkeit der Primzahlen der Gestalt $p \equiv 1 \pmod{k}$ führen.

Definition 4.9. Es sei p eine Primzahl, $a \in \mathbb{Z}$ und $p \nmid a$. Dann wird

$$\mathrm{ord}_p(a) := \min \{n \in \mathbb{Z}^+ \mid a^n \equiv 1 \pmod{p}\}$$

als die Ordnung von a bezüglich p (oder a modulo p) bezeichnet.

Bemerkung 4.10. Nach dem kleinen Fermatschen Satz gilt $a^{p-1} \equiv 1 \pmod{p}$, sodass $\mathrm{ord}_p(a)$ stets existiert und $\mathrm{ord}_p(a) \leq p-1$.

Lemma 4.11. *Es sei p eine Primzahl, $a \in \mathbb{Z}^+$, $p \nmid a$ und $m \geq 0$. Dann sind äquivalent:*

(i) $a^m \equiv 1 \pmod{p}$.

(ii) $\mathrm{ord}_p(a) \mid m$.

Beweis.
$(i) \Rightarrow (ii)$: Angenommen $a^m \equiv 1 \pmod{p}$. Sei $m = q \cdot \mathrm{ord}_p(a) + r$ mit $q \geq 0$ und $0 \leq r < \mathrm{ord}_p(a)$. Dann ist

$$a^m = a^{q \cdot \mathrm{ord}_p(a) + r} = (a^{\mathrm{ord}_p(a)})^q \cdot a^r \equiv 1^q \cdot a^r = a^r \pmod{p}$$

Da $a^m \equiv a^r \pmod{p}$ und $a^m \equiv 1 \pmod{p}$, folgt $a^r \equiv 1 \pmod{p}$. Das ist wegen der Minimalität von $\mathrm{ord}_p(a)$ nur für $r = 0$ möglich. Daher gilt

$$\mathrm{ord}_p(a) \mid m.$$

$(ii) \Rightarrow (i)$: Angenommen $m = d \cdot \mathrm{ord}_p(a)$ für ein $d \geq 0$. Dann ist

$$a^m = a^{d \cdot \mathrm{ord}_p(a)} = (a^{\mathrm{ord}_p(a)})^d \equiv 1^d = 1 \pmod{p}.$$

□

Lemma 4.12. *Sind $n_1, \ldots, n_l \in \mathbb{Z}^+$, $m_h \in \{\pm 1\}$ und setze $\prod_{h=1}^{l} n_h^{m_h} = \frac{r}{s}$ mit $r, s \in \mathbb{Z}^+$ und $\mathrm{ggT}(r,s) = 1$, dann gilt*

$$rs \,\Big|\, \prod_{h=1}^{l} n_h$$

Beweis. Aus

$$\prod_{h=1}^{l} n_h^{m_h} \;=\; \frac{\prod\limits_{\substack{1\le h\le l\\ m_h=1}} n_h}{\prod\limits_{\substack{1\le h\le l\\ m_h=-1}} n_h} \;=\; \frac{r}{s},$$

folgt sofort $r \Big| \prod\limits_{\substack{1\le h\le l\\ m_h=1}} n_h$ und $s \Big| \prod\limits_{\substack{1\le h\le l\\ m_h=-1}} n_h$.

Durch Multiplikation beider, ergibt sich wie behauptet $rs \Big| \prod\limits_{h=1}^{l} n_h$. □

Lemma 4.13. *Sei $k \geq 3$, $m_h \in \{\pm 1\}$ $(1 \leq h \leq l)$, und $0 < n_1 < n_2 < \cdots < n_l$, so ist*

$$\prod_{h=1}^{l} (k^{n_h} - 1)^{m_h} \neq 1.$$

Beweis. Es seien

$$S := \Big\{ h \in \{1, \ldots, l\} \,\Big|\, m_h = m_1 \Big\} \text{ und } T := \Big\{ h \in \{1, \ldots, l\} \,\Big|\, m_h = -m_1 \Big\}.$$

Angenommen $\prod\limits_{h=1}^{l} (k^{n_h} - 1)^{m_h} = 1$, da die Faktoren mit $m_h = +1$ die mit $m_h = -1$ aufheben, folgt

$$\prod_{h \in S} (k^{n_h} - 1) = \prod_{h \in T} (k^{n_h} - 1).$$

Für $2 \leq h \leq l$ ist $n_h \geq n_1 + 1$ und daher

$$k^{n_h} - 1 \equiv -1 \pmod{k^{n_1+1}},$$

weil k^{n_h} für $n_h \geq n_1 + 1$ bereits durch k^{n_1+1} teilbar ist. Daraus folgen

$$\prod_{h \in S} (k^{n_h} - 1) \equiv (k^{n_1} - 1) \cdot (-1)^{|S|-1} \pmod{k^{n_1+1}} \text{ und}$$

$$\prod_{h \in T} (k^{n_h} - 1) \equiv (-1)^{|T|} \pmod{k^{n_1+1}}.$$

Aus $\prod\limits_{h=1}^{l} (k^{n_h} - 1)^{m_h} = 1$ würde daher folgen

$$(k^{n_1} - 1) \cdot (-1)^{|S|-1} \equiv (-1)^{|T|} \pmod{k^{n_1+1}}.$$

Multipliziert man nun beidseitig mit $(-1)^{|S|+1}$ und da $|S|+|T|=l$, folgt

$$\begin{aligned}(k^{n_1}-1) &\equiv (-1)^{|T|+|S|+1}\\ (k^{n_1}-1) &\equiv (-1)^{l+1} \pmod{k^{n_1+1}}\end{aligned}$$

Es wird unterschieden:
Ist l gerade, dann ist $l+1$ ungerade und $(-1)^{l+1}=-1$, so wäre $k^{n_1+1} \mid k^{n_1}$, was unmöglich ist.
Ist l ungerade, dann ist $l+1$ gerade und $(-1)^{l+1}=+1$, so wäre $k^{n_1} \equiv 2(k^{n_1+1})$. Daraus folgt, dass ein $d \geq 1$ existiert mit $dk^{n_1+1}=k^{n_1}-2$ und daher $dk^{n_1+1}+2=k^{n_1}$, was wiederum $k^{n_1} > k^{n_1+1}$ bedeutet, was unmöglich ist.
In beiden Fällen erhält man einen Widerspruch, also muss $\prod_{h=1}^{l}(k^{n_h}-1)^{m_h} \neq 1$ gelten.
□

Lemma 4.14. *Es sei $k \geq 3$ mit der Primfaktorzerlegung $k=q_1^{\alpha_1}\cdots q_g^{\alpha_g}$, es sind also $q_1,\ldots,q_g$ sind paarweise verschiedene Primzahlen und $\alpha_1,\ldots,\alpha_g \in \mathbb{Z}^+$. Weiters sei*

$$\frac{r}{s}=\prod_{d\mid(q_1\cdots q_g)}(k^{\frac{k}{d}}-1)^{(-1)^{\omega(d)}}$$

mit $r,s \in \mathbb{Z}^+$ und $\mathrm{ggT}(r,s)=1$, wobei $\omega(d)$ die Anzahl der verschiedenen Primteiler von d bezeichnet. Ist p eine Primzahl mit der Eigenschaft $p \mid (rs)$, so gilt

$$p \equiv 1 \pmod{k}.$$

Beweis. Nach Lemma 4.12. gilt $rs \mid \prod_{d\mid(q_1\cdots q_g)}(k^{\frac{k}{d}}-1)$ und daher nach Voraussetzung

$$p \mid \prod_{d\mid(q_1\cdots q_g)}(k^{\frac{k}{d}}-1).$$

Folglich gibt es ein $d_0 \in \mathbb{Z}^+$ mit den Eigenschaften $d_0 \mid (q_1\cdots q_g)$ und $p \mid (k^{\frac{k}{d_0}}-1)$, woraus sofort $p \nmid k$ folgt.
Es sei nun $b:=\mathrm{ord}_p(k)$. Nach Lemma 4.11. gilt für $m \geq 0$ nun

$$k^m \equiv 1 \pmod{p} \Longleftrightarrow b \mid m.$$

Nach dem kleinen Fermatschen Satz gilt $k^{p-1} \equiv 1 \pmod{p}$ und wegen Lemma 4.11. gilt $b \mid (p-1)$.
Aus $k^{\frac{k}{d_0}} \equiv 1 \pmod{p}$ und Lemma 4.11. folgt $b \mid \dfrac{k}{d_0}$, woraus man sofort $b \mid k$ erhält.

Angenommen $b < k$. Dann wäre $\frac{k}{b} > 1$ und es würde eine Primzahl $q \in \{q_1, \ldots, q_g\}$ geben mit der Eigenschaft $q \mid \frac{k}{b}$, woraus $b \mid \frac{k}{q}$ folgt.
Wenn $q \mid \frac{k}{b}$, dann existiert ein $d \in \mathbb{Z}^+$, sodass

$$q \cdot d = \frac{k}{b} \Rightarrow bd = \frac{k}{q}$$

Wir schreiben nun die Definition von $\frac{r}{s}$ um, zu

$$\frac{r}{s} = \prod_{d \mid \frac{q_1 \cdots q_g}{q}} \left(\frac{k^{\frac{k}{d}} - 1}{k^{\frac{k}{dq}} - 1} \right)^{(-1)^{\omega(d)}}, \text{wobei} \quad \frac{k^{\frac{k}{d}} - 1}{k^{\frac{k}{dq}} - 1} = \sum_{n=0}^{q-1} k^{\frac{nk}{qd}} \in \mathbb{Z}^+.$$

Nach Lemma 4.12. gilt

$$rs \Big| \prod_{d \mid \frac{q_1 \cdots q_g}{q}} \frac{k^{\frac{k}{d}} - 1}{k^{\frac{k}{dq}} - 1} \quad \text{und daher} \quad p \Big| \prod_{d \mid \frac{q_1 \cdots q_g}{q}} \frac{k^{\frac{k}{d}} - 1}{k^{\frac{k}{dq}} - 1}.$$

Folglich gibt es ein $d_1 \in \mathbb{Z}^+$ mit den Eigenschaften

$$d_1 \Big| \frac{q_1 \cdots q_g}{q} \quad \text{und} \quad p \Big| \frac{k^{\frac{k}{d_1}} - 1}{k^{\frac{k}{d_1 q}} - 1}.$$

Daraus folgt

$$p \mid \left(k^{\frac{k}{d_1}} - 1 \right) \Longrightarrow k^{\frac{k}{d_1}} \equiv 1 \pmod{p}$$

daraus und Lemma 4.11. folgt erneut $b \Big| \frac{k}{d_1}$.
Da b sowohl $\frac{k}{q}$ als auch $\frac{k}{d_1}$ teilt, gilt $b \mid \mathrm{ggT}(\frac{k}{q}, \frac{k}{d_1})$.
Aus $d_1 \mid \frac{q_1 \cdots q_g}{q}$ folgt $\mathrm{ggT}(d_1, q) = 1$ und daher

$$\mathrm{ggT}\left(\frac{k}{q}, \frac{k}{d_1} \right) = \frac{k}{qd_1} \mathrm{ggT}(d_1, q) = \frac{k}{qd_1}.$$

Also gilt $b \mid \frac{k}{qd_1}$ und daher $k^{\frac{k}{qd_1}} \equiv 1 \pmod{p}$. Daraus folgt

$$\frac{k^{\frac{k}{d_1}} - 1}{k^{\frac{k}{qd_1}} - 1} = \sum_{n=0}^{q-1} k^{\frac{nk}{qd_1}} \equiv q \pmod{p},$$

also

$$p \mid q \Longrightarrow p = q.$$

Das steht im Widerspruch zu $p \mid k$. Daher kann die Annahme $b < k$ nicht stimmen. Wir behaupten nun $b = k$. Aus $b \mid (p-1)$ folgt sofort $k \mid (p-1)$, also

$$p \equiv 1 \pmod{k}.$$

□

Lemma 4.15. *Es sei $k \geq 3$. Dann gibt es eine Primzahl $p \equiv 1 \pmod{k}$.*

Beweis. Es sei erneut $k = q_1^{\alpha_1} \cdots q_g^{\alpha_g}$ eine Primfaktorzerlegung, d.h. $q_1, \ldots, q_g$ sind paarweise verschiedenen Primzahlen und $\alpha_1, \ldots, \alpha_g \in \mathbb{Z}^+$, sowie

$$\frac{r}{s} = \prod_{d \mid q_1 \cdots q_g} \left(k^{\frac{k}{d}} - 1\right)^{(-1)^{\omega(d)}} \text{ mit } r, s \in \mathbb{Z}^+ \text{ und } \operatorname{ggT}(r, s) = 1.$$

Nach Lemma 4.13. ist $\frac{r}{s} \neq 1$. Daher gibt es eine Primzahl p mit der Eigenschaft $p \mid rs$. Diese hat nach Lemma 4.14. die Eigenschaft $p \equiv 1 \pmod{k}$. □

Satz 4.16. *Es sei $k \geq 2$. Dann gibt es unendlich viele Primzahlen $p \equiv 1 \pmod{k}$.*

Beweis. Für $k = 2$ ist die Aussage trivial, da alle Primzahlen, bis auf die Zahl 2, ungerade sind.
Es sei nun $k \geq 3$. Mit Induktion wird gezeigt, dass es n paarweise verschiedene Primzahlen $p_1, \ldots, p_n$ mit der Eigenschaft $p_1 \equiv \cdots \equiv p_n \equiv 1 \pmod{k}$ gibt.
Für $n = 1$ gibt es nach Lemma 4.15. eine Primzahl $p_1 \equiv 1 \pmod{k}$.
Angenommen, es wurden schon n paarweise verschiedene Primzahlen $p_1, \ldots, p_n$ mit der Eigenschaft $p_1 \equiv \cdots \equiv p_n \equiv 1 \pmod{k}$ gefunden. Nach Lemma 4.15. gibt es eine Primzahl p_{n+1} mit der Eigenschaft

$$\begin{aligned} p_{n+1} &\equiv 1 \pmod{(kp_1 \cdots p_n)} \quad \text{und daher} \\ p_{n+1} &\equiv 1 \pmod{k}. \end{aligned}$$

Dabei existiert ein $d \in \mathbb{Z}^+$ mit $p_{n+1} = 1 + dk \cdot p_1 \cdots p_n > p_i$ für $1 \leq i < n$.
Also wurde eine $(n+1)$-te, von $p_1, \ldots, p_n$ verschiedene Primzahl $p_{n+1} \equiv 1 \pmod{k}$ gefunden, und somit gibt es unendlich viele Primzahlen der Form $p \equiv 1 \pmod{k}$. □

4.2 Robbins

Neville Robbins beweist, dass es unendlich viele Primzahlen der Form $p \equiv 1 \pmod 4$ ($p = 4k + 1$) gibt. Dafür zieht er die Fermat-Zahlen und deren Bedeutung, sowie das Legendre-Symbol für die Existenz unendlich vieler Primzahlen heran.
In Satz 3.2. wurde bereits bewiesen, dass die Fermat-Zahlen

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

mit $n \geq 0$ paarweise teilerfremd sind, also

$$\text{ggT}(F_n, F_m) = \text{ggT}(2^{2^n} + 1, 2^{2^m} + 1) = 1$$

für $m, n \geq 0, m \neq n$. Daraus folgt, dass es unendlich viele Primzahlen gibt.

Damit ist auch gezeigt, dass es unendlich viele Primzahlen $p \equiv 1 \pmod 4$ gibt:
Ist nämlich $n \in \mathbb{Z}^+$ und p ein Primteiler von F_n, so gilt

$$p \mid (2^{2^n} + 1) \Longrightarrow \quad 2^{2^n} \equiv -1 \pmod p$$

Woraus mit dem Legendre-Symbol (Def. 2.26.) $\left(\frac{-1}{p}\right) = 1$ folgt.
Das bedeutet, dass -1 ein quadratischer Rest modulo p ist, was äquivalent ist zu

$$p \equiv 1 \pmod 4.$$

4.3 Lucas

Édouard Lucas bewies nicht nur die Unendlichkeit der Primzahlen der Form

$$4k+1 \ \ (\text{also } p \equiv 1 \pmod 4), \text{ sondern auch der Form}$$

$$4k+3 \ \ (\text{also } p \equiv 3 \pmod 4) \ \text{ und } \ 6k+5 \ \ (\text{also } p \equiv 5 \pmod 6).$$

Dafür verwendete er in moderner Formulierung das Legendre-Symbol (Def. 2.26.) und dessen Eigenschaften.

Satz 4.17. *Es gibt unendlich viele Primzahlen* $p \equiv 1 \pmod 4$.

Beweis. Es sei $N = (2 \cdot 3 \cdot 4 \cdot 7 \cdots p_n)^2 + 1$ und q ein Primteiler von N.
Offenbar ist jedoch $q \notin \{2, 3, 5, 7, \ldots, p_n\}$. Es gilt

$$\begin{aligned} & N \equiv 0 \pmod q \\ \iff \quad & (2 \cdot 3 \cdot 5 \cdot 7 \cdots p_n)^2 \equiv -1 \pmod q \end{aligned}$$

Daraus folgt, durch Verwendung des Legendre-Symbols,

$$\left(\frac{-1}{q}\right) = 1 \implies q \equiv 1 \pmod 4$$

Somit muss es unendlich viele Primzahlen dieser Form geben. □

Satz 4.18. *Es gibt unendlich viele Primzahlen* $p \equiv 3 \pmod 4$.

Beweis. Es sei $N = 2^2 \cdot 3 \cdot 5 \cdot 7 \cdots p_n - 1 = 4 \cdot 3 \cdot 5 \cdot 7 \cdots p_n - 1$. Offenbar gilt

$$N \equiv 3 \pmod 4 \ \text{ und } \ 2 \nmid N.$$

Ist $N = q_1 \cdots q_n$ die Primfaktorzerlegung, so ist q_i, für $1 \leq i \leq k$, entweder

$$q_i \equiv 1 \pmod 4 \ \text{ oder } \ q_i \equiv 3 \pmod 4.$$

Wären alle $q_i \equiv 1 \pmod 4$ für $1 \leq i \leq k$, so wäre

$$N = q_1 \cdots q_n \equiv 1 \pmod 4.$$

Dies steht im Widerspruch zu $N \equiv 3 \pmod 4$.
Also existiert ein $q_i \in \{1, \ldots, k\}$, sodass $q_i \equiv 3 \pmod 4$.
Da $q_i \notin \{2, 3, 5, 7, \ldots, p_n\}$ muss es unendlich viele Primzahlen dieser Form geben.

□

Satz 4.19. *Es gibt unendlich viele Primzahlen* $p \equiv 5 \pmod 6$.

Beweis. Es sei $N = 2 \cdot 3 \cdot 5 \cdot 7 \cdots p_n - 1 = 6 \cdot 5 \cdot 7 \cdots p_n - 1$. Offenbar gilt

$$N \equiv 5 \pmod 6 \text{ und } 2 \nmid N,\ 3 \nmid N.$$

Ist $N = q_1 \cdots q_k$ die Primfaktorzerlegung, so ist q_i, für $1 \leq i \leq k$, entweder

$$q_i \equiv 1 \pmod 6 \text{ oder } q_i \equiv 5 \pmod 6.$$

Wären alle $q_i \equiv 1 \pmod 6$ für $1 \leq i \leq k$, so wäre

$$N = q_1 \cdots q_k \equiv 1 \pmod 6.$$

Dies steht im Wiederspruch zu $N \equiv 5 \pmod 6$.
Also existiert ein $i \in \{1, \ldots k\}$ sodass $q_i \equiv 5 \pmod 6$.
Da $q \notin \{2, 3, 5, 7, \ldots, p_n\}$ muss es unendlich viele Primzahlen dieser Form geben. □

Satz 4.20. *Es gibt unendlich viele Primzahlen* $p \equiv 5 \pmod 8$.

Beweis. Analog zu Serret (siehe Satz 4.23.) □

4.4 Serret

Joseph-Alfred Serret nutzt in seinen Beweisen für die Unendlichkeit der Primzahlen in speziellen Progressionen in moderner Formulierung das Legendre- Symbol, ebenso wie das quadratische Reziprozitätsgesetz und deren Eigenschaften.

Satz 4.21. *Es gibt unendlich viele Primzahlen* $p \equiv 1 \pmod 8$.

Beweis. Es sei $N = (2 \cdot 3 \cdot 5 \cdot 7 \cdots p_n)^4 + 1$ und q ist somit ein Primteiler von N. Offenbar ist $q \notin \{2, 3, 5, 7, \ldots, p_n\}$. Es gilt

$$\begin{aligned} & N \equiv 0 \pmod q \\ \iff \quad & \left((2 \cdot 3 \cdot 5 \cdot 7 \cdots p_n)^2\right)^2 \equiv -1 \pmod q \end{aligned}$$

Mit dem Legendre-Symbol folgt

$$\left(\frac{-1}{q}\right) = 1 \Rightarrow q \equiv 1 \pmod 4.$$

Daher gilt entweder $q \equiv 1 \pmod 8$ oder $q \equiv 5 \pmod 8$.
Nun wird N genauer betrachtet

$$\begin{aligned} N &= (2 \cdot 3 \cdots p_n)^4 + 1 \\ &= \left((2 \cdot 3 \cdots p_n)^2\right)^2 + 2 \cdot (2 \cdot 3 \cdots p_n)^2 + 1 - 2 \cdot (2 \cdot 3 \cdots p_n)^2 \\ &= \left(\left((2 \cdot 3 \cdots p_n)^2\right)^2 - 2 \cdot (2 \cdot 3 \cdots p_n)^2 + 1\right) + 2 \cdot (2 \cdot 3 \cdots p_n)^2 \\ &= \left((2 \cdot 3 \cdots p_n)^2 - 1\right)^2 + 2 \cdot (2 \cdot 3 \cdots p_n)^2 \end{aligned}$$

$$\implies \quad \left((2 \cdot 3 \cdots p_n)^2 - 1\right)^2 \equiv -2 \cdot (2 \cdot 3 \cdots p_n)^2 \pmod q.$$

Durch Verwendung des Legendre-Symbols

$$1 = \left(\frac{-2 \cdot (2 \cdot 3 \cdots p_n)^2}{q}\right) = \left(\frac{-2}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{2}{q}\right) = \left(\frac{2}{q}\right),$$

woraus weiter folgt

$$q \equiv \pm 1 \pmod 8.$$

Daher kann q entweder $q \equiv 1 \pmod 8$ oder $q \equiv -1 \pmod 8$, was $q \equiv 7 \pmod 8$ entspricht und separat bewiesen werden kann, sein.
Daher gilt insgesamt $q \equiv 1 \pmod 8$ und es gibt unendlich viele Primzahlen dieser Form.

□

Satz 4.22. *Es gibt unendlich viele Primzahlen $p \equiv 3 \pmod 8$.*

Beweis. Es sei $N = (3 \cdot 5 \cdot 7 \cdots p_n)^2 + 2$ und q ein Primteiler von N, wobei offenbar $q \notin \{3, 5, 7, \ldots, p_n\}$ ist. Es gilt

$$\begin{aligned} & N \equiv 0 \pmod q \\ \iff \quad & (3 \cdot 5 \cdot 7 \cdots p_n)^2 \equiv -2 \pmod q. \end{aligned}$$

Mit dem Legendre-Symbol erhält man

$$\left(\frac{-2}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{2}{q}\right) = 1$$

Nach den quadratischen Reziprozitätsgesetzen und den Werten des Legendre-Symbols können folgende Fälle unterschieden und untersucht werden:

Falls $q \equiv 1 \pmod 8$ $(\Rightarrow q \equiv 1 \pmod 4)$
$$\left(\frac{-1}{q}\right)\left(\frac{2}{q}\right) = 1 \cdot 1 = 1$$
Falls $q \equiv 3 \pmod 8$ $(\Rightarrow q \equiv 3 \pmod 4)$
$$\left(\frac{-1}{q}\right)\left(\frac{2}{q}\right) = (-1) \cdot (-1) = 1$$
Falls $q \equiv 5 \pmod 8$ $(\Rightarrow q \equiv 1 \pmod 4)$
$$\left(\frac{-1}{q}\right)\left(\frac{2}{q}\right) = 1 \cdot (-1) = -1$$
Falls $q \equiv 7 \pmod 8$ $(\Rightarrow q \equiv 3 \pmod 4)$
$$\left(\frac{-1}{q}\right)\left(\frac{2}{q}\right) = (-1) \cdot 1 = -1$$

Aus allen Fällen folgt $q \equiv 1 \pmod 8$ oder $q \equiv 3 \pmod 8$.
Ist $N = q_1 \cdots q_k$ die Primfaktorzerlegung, so ist q_i für $1 \leq i \leq k$ entweder

$$q_i \equiv 1 \pmod 8 \quad \text{oder} \quad q_i \equiv 3 \pmod 8.$$

Wäre $q_i \equiv 1 \pmod 8$ für alle $1 \leq i \leq k$, so wäre

$$N = q_1 \cdots q_k \equiv 1 \pmod 8$$

Da $(4k \pm 1)^2 = 16k^2 \pm 8k + 1 = 8 \cdot (2k^2 \pm k) + 1$ und somit $(4k \pm 1)^2 \equiv 1 \pmod 8$, gilt aber $N \equiv 3 \pmod 8$.
Also existiert ein $i \in \{1, \cdots, k\}$ sodass $q_i \equiv 3 \pmod 8$.
Da $q \notin \{3, 5, 7, \ldots, p_n\}$ gibt es unendlich viele Primzahlen dieser Form.

□

Satz 4.23. *Es gibt unendlich viele Primzahlen* $p \equiv 5 \pmod 8$.

Beweis. Es sei $N = (3 \cdot 5 \cdot 7 \cdots p_n)^2 + 2^2$ und q ein Primteiler von N, wobei offenbar $q \notin \{3, 5, 7, \ldots, p_n\}$ ist. Es gilt

$$\begin{aligned} N &\equiv 0 \pmod q \\ \iff (3 \cdot 5 \cdot 7 \cdots p_n)^2 &\equiv -2^2 \pmod q \end{aligned}$$

Mit dem Legendre-Symbol folgt

$$\left(\frac{-2^2}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{2^2}{q}\right) = 1$$

$$\Rightarrow q \equiv 1 \pmod 4.$$

Daher kann q entweder die Form $q \equiv 1 \pmod 8$ oder $q \equiv 5 \pmod 8$ haben.
Ist $N = q_1 \cdots q_k$ die Primfaktorzerlegung, so ist q_i, für $1 \leq i \leq k$, entweder

$$q_i \equiv 1 \pmod 8 \quad \text{oder} \quad q_i \equiv 5 \pmod 8.$$

Wäre $q_i \equiv 1 \pmod 8$ für alle $1 \leq i \leq k$, so wäre

$$N = q_i \cdots q_k \equiv 1 \pmod 8.$$

Dies steht im Widerspruch zu $N \equiv 5 \pmod 8$. Also $\exists\, i \in \{1, \ldots, k\} : q_i \equiv 5 \pmod 8$.
Da $q \notin \{3, 5, 7, \ldots, p_n\}$ muss es unendlich viele Primzahlen dieser Form geben.

□

Satz 4.24. *Es gibt unendlich viele Primzahlen* $p \equiv 7 \pmod 8$.

Beweis. Es sei $N = (3 \cdot 5 \cdot 7 \cdots p_n)^2 - 2$ und q ein Primteiler von N, wobei offenbar $q \notin \{3, 5, 7, \ldots, p_n\}$. Es gilt

$$\begin{aligned} N &\equiv 0 \pmod q \\ \iff (3 \cdot 5 \cdot 7 \cdots p_n)^2 &\equiv 2 \pmod q \end{aligned}$$

Mit dem Legendre-Symbol erhält man

$$\left(\frac{2}{q}\right) = 1 \Longrightarrow q \equiv \pm 1 \pmod 8$$

Ist $N = q_1 \cdots q_k$ die Primfaktorzerlegung, so ist q_i, für $1 \leq i \leq k$, entweder

$$q_i \equiv 1 \pmod 8 \quad \text{oder} \quad q_i \equiv 7 \pmod 8.$$

Wäre $q_i \equiv 1 \pmod 8$ für alle $1 \leq i \leq k$, so wäre

$$N = q_1 \cdots q_k \equiv 1 \pmod 8.$$

Dies führt zu einem Widerspruch, da $N \equiv 7 \pmod 8$. Also $\exists i \in \{1, \ldots, k\}$, sodass gilt $q_i \equiv 7 \pmod 8$ und da $q \notin \{3, 5, 7, \ldots, p_n\}$ gibt es unendlich viele Primzahlen dieser Form.

□

Satz 4.25. *Es gibt unendlich viele Primzahlen* $p \equiv 1 \pmod{12}$

Beweis. Es sei $N = (2 \cdot 3 \cdot 5 \cdot 7 \cdots p_n)^4 - (2 \cdot 3 \cdot 5 \cdot 7 \cdots p_n)^2 + 1$ und q ein Primteiler von N, wobei und offenbar $q \notin \{2, 3, 5, 7, \ldots, p_n\}$. Setzt man $M := 2 \cdot 3 \cdot 5 \cdot 7 \cdots p_n$ und betrachtet N genauer, erhält man

$$N = M^4 - M^2 + 1.$$

Da $(M^2 \pm 1)^2 = M^4 \pm 2M^2 + 1$, durch umformen und ergänzen lässt sich N weiter wie folgt schreiben

$$\begin{aligned} N &= M^4 + 1 - M^2 \\ &= M^4 - 2M^2 + 1 - M^2 + 2M^2 = (M^2 - 1)^2 + M^2 \\ &= M^4 + 2M^2 + 1 - M^2 - 2M^2 = (M^2 + 1)^2 - 3M^2 \end{aligned}$$

Daher gilt sowohl

$$N = ((2 \cdot 3 \cdot 5 \cdot 7 \cdots p_n)^2 - 1)^2 + (2 \cdot 3 \cdot 5 \cdot 7 \cdots p_n)^2 \text{ als auch}$$

$$N = ((2 \cdot 3 \cdot 5 \cdot 7 \cdots p_n)^2 + 1)^2 - 3 \cdot (2 \cdot 3 \cdot 5 \cdot 7 \cdots p_n)^2$$

Für $N = ((2 \cdot 3 \cdot 5 \cdot 7 \cdots p_n)^2 - 1)^2 + (2 \cdot 3 \cdot 5 \cdot 7 \cdots p_n)^2$ gilt

$$\begin{aligned} & & N &\equiv 0 \pmod q \\ \iff & \Big((2 \cdot 3 \cdot 5 \cdots p_n)^2 - 1\Big)^2 + (2 \cdot 3 \cdot 5 \cdots p_n)^2 &\equiv 0 \pmod q \\ & \iff \Big((2 \cdot 3 \cdot 5 \cdots p_n)^2 - 1\Big)^2 &\equiv -(2 \cdot 3 \cdot 5 \cdots p_n)^2 \pmod q \end{aligned}$$

Durch Verwendung des Legendre-Symbols folgt

$$\left(\frac{-(2\cdot 3\cdots p_n)^2}{q}\right) = \left(\frac{-1}{q}\right) = 1$$

$$\Longrightarrow q \equiv 1 \pmod 4$$

Daher kann q entweder $q \equiv 1 \pmod{12}$, $q \equiv 5 \pmod{12}$ oder $q \equiv 9 \pmod{12}$ sein. Da $q \equiv 9 \pmod{12}$ unmöglich ist, folgt

$$q \equiv 1 \pmod{12} \text{ oder } q \equiv 5 \pmod{12}.$$

Für $N = ((2\cdot 3\cdot 5\cdot 7\cdots p_n)^2+1)^2 - 3\cdot(2\cdot 3\cdot 5\cdot 7\cdots p_n)^2$ gilt

$$\begin{aligned} & & N &\equiv 0 \pmod q \\ \iff & ((2\cdot 3\cdot 5\cdots p_n)^2+1)^2 - 3\cdot(2\cdot 3\cdot 5\cdots p_n)^2 &\equiv 0 \pmod q \\ & \iff ((2\cdot 3\cdot 5\cdots p_n)^2+1)^2 &\equiv 3\cdot(2\cdot 3\cdot 5\cdots p_n)^2 \pmod q \end{aligned}$$

Durch Verwendung des Legendre-Symbols folgt

$$\left(\frac{3\cdot(2\cdot 3\cdots p_n)^2}{q}\right) = \left(\frac{3}{q}\right) = 1$$

$$\Longrightarrow q \equiv 1 \pmod 3$$

Daher folgt für q entweder

$$q \equiv 1 \pmod{12} \text{ oder } q \equiv 11 \pmod{12}.$$

Die einzige gemeinsame Möglichkeit ist daher $q \equiv 1 \pmod{12}$, und daraus folgt es gibt unendlich viele Primzahlen dieser Form.

□

Satz 4.26. *Es gibt unendlich viele Primzahlen $p \equiv 5 \pmod{12}$.*

Beweis. Es sei $N = (2\cdot 5\cdot 7\cdot 11\cdots p_n)^2+1$ und q ein Primteiler von N, wobei offenbar $q \notin \{2,3,5,7,\ldots,p_n\}$. Beachte dabei, dass für jede ungerade Zahl a gilt

$$(3k \pm 1)^2 \equiv 1 \pmod 3,$$

sodass

$$N \equiv 2 \pmod 3.$$

Es ist

$$\begin{aligned} N &\equiv 0 \pmod{q} \\ \iff (2 \cdot 5 \cdot 7 \cdot 11 \cdots p_n)^2 + 1 &\equiv 0 \pmod{q} \\ \iff (2 \cdot 5 \cdot 7 \cdot 11 \cdots p_n)^2 &\equiv -1 \pmod{q} \end{aligned}$$

Daraus folgt mit dem Legendre-Symbol

$$\left(\frac{-1}{q}\right) = 1 \implies q \equiv 1 \pmod{4}.$$

Folglich muss für q entweder $q \equiv 1 \pmod{12}$ oder $q \equiv 5 \pmod{12}$ gelten.
Es kann für p unterschieden werden:
Ist $p \in \{5, 7, 11, \ldots, p_n\}$, so ist

$$p \equiv \pm 1 \pmod{12} \quad (\implies p^2 \equiv 1 \pmod{12}), \text{ oder}$$

$$p \equiv \pm 5 \pmod{12} \quad (\implies p^2 \equiv 25 \equiv 1 \pmod{12}).$$

Daher ist $N \equiv 5 \pmod{12}$.
Ist $N = q_1 \cdots q_k$ Primfaktorzerlegung, so ist q_i für $1 \leq i \leq k$ entweder

$$q_i \equiv 1 \pmod{12} \quad \text{oder} \quad q_i \equiv 5 \pmod{12}.$$

Wäre $q_i \equiv 1 \pmod{12}$ für alle $1 \leq i \leq k$, so wäre

$$N = q_1 \cdots q_k \equiv 1 \pmod{12}.$$

Dies ist ein Widerspruch.
Also $\exists\, i \in \{1, \cdots k\} : q_i \equiv 5 \pmod{12}$, und daher gibt es unendlich viele Primzahlen dieser Form.

□

Satz 4.27. *Es gibt unendlich viele Primzahlen* $p \equiv 7 \pmod{12}$.

Beweis. Es sei $N = (2 \cdot 5 \cdot 7 \cdot 11 \cdots p_n)^2 + 3$ und q ein Primteiler von N, wobei offenbar $q \notin \{2, 3, 5, 7, \ldots, p_n\}$. Es gilt

$$\begin{aligned} N &\equiv 0 \pmod{q} \\ \iff (2 \cdot 5 \cdot 7 \cdot 11 \cdots p_n)^2 + 3 &\equiv 0 \pmod{q} \\ \iff (2 \cdot 5 \cdot 7 \cdot 11 \cdots p_n)^2 &\equiv -3 \pmod{q} \end{aligned}$$

Mit dem Legendre-Symbol folgt

$$\left(\frac{-3}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{3}{q}\right) = 1$$

Nach den quadratischen Reziprozitätsgesetzen und den Werten des Legendre-Symbols können folgende Fälle unterschieden und untersucht werden:

Falls $q \equiv 1 \pmod{12}$ $\quad \Big(\Rightarrow q \equiv 1 \pmod{4} \Rightarrow \left(\frac{-1}{q}\right) = 1 \Big)$

$$\text{und } \left(\frac{3}{q}\right) = \left(\frac{q}{3}\right) = \left(\frac{1}{3}\right) = 1, \qquad \text{d.h. } \left(\frac{-3}{q}\right) = 1$$

Falls $q \equiv 5 \pmod{12}$ $\quad \Big(\Rightarrow q \equiv 1 \pmod{4} \Rightarrow \left(\frac{-1}{q}\right) = 1 \Big)$

$$\text{und } \left(\frac{3}{q}\right) = \left(\frac{q}{3}\right) = \left(\frac{2}{3}\right) = -1, \qquad \text{d.h. } \left(\frac{-3}{q}\right) = -1$$

Falls $q \equiv 7 \pmod{12}$ $\quad \Big(\Rightarrow q \equiv 3 \pmod{4} \Rightarrow \left(\frac{-1}{q}\right) = -1 \Big)$

$$\text{und } \left(\frac{3}{q}\right) = -\left(\frac{q}{3}\right) = -\left(\frac{1}{3}\right) = -1, \qquad \text{d.h. } \left(\frac{-3}{q}\right) = 1$$

Falls $q \equiv 11 \pmod{12}$ $\quad \Big(\Rightarrow q \equiv 3 \pmod{4} \Rightarrow \left(\frac{-1}{q}\right) = -1 \Big)$

$$\text{und } \left(\frac{3}{q}\right) = -\left(\frac{q}{3}\right) = -\left(\frac{2}{3}\right) = 1, \qquad \text{d.h. } \left(\frac{-3}{q}\right) = -1$$

Daher ist q entweder $q \equiv 1 \pmod{12}$ oder $q \equiv 7 \pmod{12}$.
Wie im Beweis von Satz 4.26. kann $N \equiv 7 \pmod{12}$ gezeigt werden.

Ist $N = q_1 \cdots q_k$ die Primfaktorzerlegung, so ist q_i für $1 \leq i \leq k$ entweder

$$q_i \equiv 1 \pmod{12} \quad \text{oder} \quad q_i \equiv 7 \pmod{12}.$$

Wäre $q_i \equiv 1 \pmod{12}$ für alle $1 \leq i \leq k$, so wäre

$$N = q_1 \cdots q_k \equiv 1 \pmod{12}.$$

Dies führt zu einem Widerspruch, also $\exists\, i \in \{1, \cdots, k\}$, sodass $q_i \equiv 7 \pmod{12}$ und daher gibt es unendlich viele Primzahlen dieser Form.

□

Satz 4.28. *Es gibt unendlich viele Primzahlen* $p \equiv 11 \pmod{12}$.

Beweis. Es sei $N = 3 \cdot (2 \cdot 5 \cdot 7 \cdot 11 \cdots p_n)^2 - 1$ und q ein Primteiler von N, wobei offenbar $q \notin \{2, 3, 5, 7, \ldots, p_n\}$, so gilt

$$\begin{aligned} N &\equiv 0 \pmod{q} \\ \iff 3 \cdot (2 \cdot 5 \cdot 7 \cdot 11 \cdots p_n)^2 - 1 &\equiv 0 \pmod{q} \\ \iff 3 \cdot (2 \cdot 5 \cdot 7 \cdot 11 \cdots p_n)^2 &\equiv 1 \pmod{q} \end{aligned}$$

Mit dem Legendre-Symbol folgt

$$\Big(\frac{3 \cdot (2 \cdot 5 \cdot 7 \cdot 11 \cdots p_n)^2}{q}\Big) = \big(\frac{3}{q}\big) = 1.$$

Es können folgende Fälle unterschieden werden:

Falls $q \equiv 1 \pmod{12}$, so gilt

$$\Big(\frac{3}{q}\Big) = \Big(\frac{q}{3}\Big) = \Big(\frac{1}{3}\Big) = 1.$$

Falls $q \equiv 5 \pmod{12}$, so gilt

$$\Big(\frac{3}{q}\Big) = \Big(\frac{q}{3}\Big) = \Big(\frac{5}{3}\Big) = \Big(\frac{2}{3}\Big) = -1.$$

Falls $q \equiv 7 \pmod{12}$, so gilt

$$\Big(\frac{3}{q}\Big) = -\Big(\frac{q}{3}\Big) = -\Big(\frac{7}{3}\Big) = -\Big(\frac{1}{3}\Big) = -1.$$

Falls $q \equiv 11 \pmod{12}$, so gilt

$$\Big(\frac{3}{q}\Big) = -\Big(\frac{q}{3}\Big) = -\Big(\frac{11}{3}\Big) = -\Big(\frac{2}{3}\Big) = -(-1) = 1.$$

Daher kann q entweder $q \equiv 1 \pmod{12}$ oder $q \equiv 11 \pmod{12}$ sein.
Wie oben wird $N \equiv 11 \pmod{12}$ gezeigt.

Ist $N = q_1 \cdots q_k$ die Primfaktorzerlegung, so ist q_i für $1 \leq i \leq k$ entweder

$$q \equiv 1 \pmod{12} \quad \text{oder} \quad q \equiv 11 \pmod{12}.$$

Wäre $q_i \equiv 1 \pmod{12}$ für alle $1 \leq i \leq k$, so wäre

$$N = q_1 \cdots q_k \equiv 1 \pmod{12}.$$

Dies führt zu einem Widerspruch, daher $\exists\, i \in \{1, \cdots k\} : q_i \equiv 11 \pmod{12}$, und es gibt unendlich viele Primzahlen dieser Form.

□

Satz 4.29. *Es gibt unendlich viele Primzahlen* $p \equiv 9 \pmod{10}$.

Beweis. Es sei $N = 5 \cdot (2 \cdot 3 \cdot 7 \cdot 11 \cdots p_n)^2 - 1$ und q ein Primteiler von N, wobei offenbar $q \notin \{2, 3, 5, 7, \ldots, p_n\}$, so gilt

$$\begin{aligned} N &\equiv 0 \pmod{q} \\ \iff \quad 5 \cdot (2 \cdot 3 \cdot 7 \cdot 11 \cdots p_n)^2 - 1 &\equiv 0 \pmod{q} \\ \iff \quad 5 \cdot (2 \cdot 3 \cdot 7 \cdot 11 \cdots p_n)^2 &\equiv 1 \pmod{q} \end{aligned}$$

Mit dem Legendre-Symbol folgt

$$\left(\frac{5 \cdot (2 \cdot 3 \cdot 7 \cdot 11 \cdots p_n)^2}{q}\right) = \left(\frac{5}{q}\right) = 1.$$

Es können folgende Fälle unterschieden werden:

Falls $q \equiv 1 \pmod{10}$, so gilt

$$\left(\frac{5}{q}\right) = \left(\frac{q}{5}\right) = \left(\frac{1}{5}\right) = 1.$$

Falls $q \equiv 3 \pmod{10}$, so gilt

$$\left(\frac{5}{q}\right) = \left(\frac{q}{5}\right) = \left(\frac{3}{5}\right) = \left(\frac{-2}{5}\right) = \left(\frac{-1}{5}\right) \cdot \left(\frac{2}{5}\right) = 1 \cdot (-1) = -1.$$

Falls $q \equiv 7 \pmod{10}$, so gilt

$$\left(\frac{5}{q}\right) = \left(\frac{q}{5}\right) = \left(\frac{7}{5}\right) = \left(\frac{-3}{5}\right) = \left(\frac{-1}{5}\right) \cdot \left(\frac{3}{5}\right) = 1 \cdot (-1) = -1.$$

Falls $q \equiv 9 \pmod{10}$, so gilt

$$\left(\frac{5}{q}\right) = \left(\frac{q}{5}\right) = \left(\frac{-1}{5}\right) = 1.$$

Daher ist q entweder $q \equiv 1 \pmod{10}$ oder $q \equiv 9 \pmod{10}$.
Daher ist $N \equiv 9 \pmod{10}$.

Ist $N = q_1 \cdots q_k$ Primfaktorzerlegung, so ist q_i für $1 \leq i \leq k$ entweder

$$q_i \equiv 1 \pmod{10} \quad \text{oder} \quad q_i \equiv 9 \pmod{10}.$$

Wäre $q_i \equiv 1 \pmod{10}$ für alle $1 \leq i \leq k$, so wäre

$$N = q_1 \cdots q_k \equiv 1 \pmod{10}.$$

Dies führt zu einem Widerspruch, also $\exists\, i \in \{1, \cdots k\} : q_i \equiv 9 \pmod{10}$, daher gibt es unendlich viele Primzahlen dieser Form.

□

5 Zignagos fehlerhafter Beweis

Italo Zignago war im Jahr 1893 noch Student, als er einen elementaren Beweis des Dirichletschen Primzahlsatzes, und somit der Unendlichkeit der Primzahlen der Form $ak+d$, in den Annali di Matematica veröffentlichte. Der Beweis ist jedoch nicht korrekt und fehlerhaft. In diesem Kapitel wird der Beweis in Deutsch übersetzt beschrieben und der Fehler herausgearbeitet.
Alle Größen seien, sofern nichts anderes festgelegt, mindestens positive ganze Zahlen.

Proposition 5.1. *Seien $p_1, \ldots, p_s$ paarweise verschiedene Primzahlen und $a, b > 0$, mit der Eigenschaft $p_i \nmid a$ für $1 \leq i \leq s$. Dann enthalten $p_1 \cdots p_s$ aufeinanderfolgende Glieder der Folge $(b + ka)_{k\geq 0}$ mindestens ein Glied $b + ha$, mit der Eigenschaft, dass $b+ha$ teilerfremd zu allen Primzahlen $p_1, \ldots, p_s$ ist und somit $\mathrm{ggT}(b+ha, p_1 \cdots p_s) = 1$ gilt.*

Beweis. Mittels Induktion nach s.
Für $s = 1$: Da $p_1 \geq 2$ und $p_i \nmid a$, ist zu zeigen, dass von zwei aufeinanderfolgenden Gliedern der Form $b + ka$ mindestens eines nicht durch p_1 teilbar ist.
Angenommen, die aufeinanderfolgenden Glieder $b+(x+1)\cdot a$ und $b+(x+2)\cdot a$ werden beide von p_1 geteilt, so würde auch die Differenz von p_1 geteilt werden. Aus

$$p_1 \Big| \Big(b + (x+1)a\Big) \quad \text{und} \quad p_1 \Big| \Big(b + (x+2)a\Big)$$

folgt

$$\begin{aligned} p_1 \quad &\Big| \quad \Big(\Big(b + (x+2)a\Big) - \Big(b + (x+1)a\Big)\Big) \\ \Longrightarrow p_1 \quad &\Big| \quad a \end{aligned}$$

Dies führt zu einem Widerspruch, da $p_1 \nmid a$.
Induktionsschritt (von $s-1$ auf s): Es wird angenommen, dass die Aussage für $s-1$ paarweise verschiedene Primzahlen $p_1, \ldots, p_{s-1}$ gilt und es soll gezeigt werden, dass sie somit auch für s gilt.
Sei $p_1, \ldots, p_s$ eine Menge von s paarweise verschiedenen Primzahlen und $a, b > 0$ mit der Eigenschaft, dass $p_i \mid a$ für $1 \leq i \leq s$. Es werden die $p_1 \cdots p_s$ aufeinanderfolgenden Glieder der Folge $(b + ka)_{k\geq 0}$ betrachtet, gegeben durch:

$$b + (x+1)\cdot a, b + (x+2)\cdot a, \ldots, b + (x + p_1 \cdots p_s)\cdot a.$$

Nach Induktionsvoraussetzung gibt es ein

$$h \in \{1, 2, \ldots, p_1 \cdots p_{s-1}\} \; (\subsetneq \{1, 2, \ldots, p_1 \cdots p_s\})$$

derart, dass $p_i \nmid \Big(b + (x+h) \cdot a\Big)$ für $1 \leq i \leq s-1$ gilt.
Aus $1 \leq h \leq p_1 \cdots p_{s-1}$ folgt:

$$p_1 \cdots p_{s-1} + 1 \leq h + p_1 \cdots p_{s-1} \leq 2 \cdot p_1 \cdots p_{s-1} \leq p_1 \ldots p_s.$$

Also ist auch $b + (x + h + p_1 \cdots p_{s-1}) \cdot a$ ein (anderes) der $p_1 \cdots p_s$ Folgeglieder, die betrachtet werden. Es gilt

$$p_i \nmid (b + (x + h + p_1 \cdots p_{s-1}) \cdot a) \quad \text{für} \quad 1 \leq i \leq s-1.$$

Angenommen $p_j \mid (b + (x + h + p_1 \cdots p_{s-1}) \cdot a)$ für ein $j \in \{1, 2, \ldots, s-1\}$, dann folgt aufgrund $p_j \mid p_1 \cdots p_{s-1}$, dass p_j auch die Differenz teilt. Wenn

$$\begin{aligned} & p_j \quad | \quad ((b + (x + h + p_1 \cdots p_{s-1}) \cdot a) - (p_1 \cdots p_{s-1}) \cdot a) \\ \text{d.h.} \quad & p_j \quad | \quad (b + (x+h) \cdot a) \end{aligned}$$

Dies führt zu einem Widerspruch, da $p_j \nmid a$.
Nun gilt entweder $p_s \nmid (b + (x+h) \cdot a)$ oder $p_s \nmid (b + (x + h + p_1 \cdots p_{s-1}) \cdot a)$.
Angenommen $p_s \mid (b + (x+h) \cdot a)$ und $p_s \mid (b + (x + h + p_1 \cdots p_{s-1}) \cdot a)$. Dann

$$\begin{aligned} \Longrightarrow p_s \quad & | \quad ((b + (x + h + p_1 \ldots p_{s-1}) \cdot a) - (b + (x+h) \cdot a)) \\ \Longrightarrow p_s \quad & | \quad (p_1 \ldots p_{s-1}) \cdot a \\ \Longrightarrow p_s \quad & | \quad p_1 \ldots p_{s-1} \quad \text{oder} \quad p_s \mid a \end{aligned}$$

Ersteres ist unmöglich, da $p_s \neq p_i$ und zweiteres widerspricht der Voraussetzung.
Somit gibt es mindestens ein n, sodass $b + na$ teilerfremd zu $p_1 \cdots p_s$ ist.

□

Proposition 5.2. *Ist* $\mathrm{ggT}(a, b, c) = 1$*, so enthalten* c *aufeinanderfolgende Glieder der Folge* $(b + ka)_{k \geq 0}$ *mindestens ein Glied* $b + ha$ *mit der Eigenschaft* $\mathrm{ggT}(b + ha, c) = 1$*.*

Beweis. Es werden die c aufeinanderfolgenden Glieder

$$b + (x+1) \cdot a, b + (x+2) \cdot a, \ldots, b + (x+c) \cdot a$$

der Folge $(b+ka)_{k\geq 0}$ für $k \in \{1,\ldots,c\}$ betrachtet. Es sei

$$c = p_1^{\alpha_1} \ldots p_s^{\alpha_s} \cdot p_{s+1}^{\alpha_{s+1}} \ldots p_{s+t}^{\alpha_{s+t}}$$

die Primfaktorzerlegung von c, mit $\alpha_1,\ldots,\alpha_{s+t} \geq 1$. Dabei soll für p_i folgendes gelten:

$$p_i \nmid a \quad \text{für} \quad 1 \leq i \leq s \quad \text{und} \quad p_i \mid a \quad \text{für} \quad s+1 \leq i \leq s+t$$

Ist $p_i \in \{p_{s+1},\ldots,p_{s+t}\}$, dann $p_i \mid a$, aber $p_i \nmid (b+(x+k)\cdot a)$ für $1 \leq k \leq c$.
Angenommen $p \mid (b+(x+k)\cdot a)$ für ein $k \in \{1,\ldots,c\}$, dann würde p auch die Differenz teilen. Denn

$$\begin{aligned} & p \quad \mid \quad ((b+(x+k)\cdot a) - (x+k)\cdot a)) \\ \Longrightarrow\ & p \quad \mid \quad b \end{aligned}$$

Das heißt p wäre ein gemeinsamer Teiler von a, b und c, dies ist ein Widerspruch zur Annahme $\mathrm{ggT}(a,b,c) = 1$.
Es folgt $\mathrm{ggT}\left(b+(x+k)\cdot a, p_{s+1}^{\alpha_{s+1}} \ldots p_{s+t}^{\alpha_{s+t}}\right) = 1$ für $1 \leq k \leq c$.
Wäre $\mathrm{ggT}\left(b+(x+k)\cdot a, p_{s+1}^{\alpha_{s+1}} \ldots p_{s+t}^{\alpha_{s+t}}\right) > 1$ für ein $k \in \{1,\ldots,c\}$, dann würde es eine Primzahl p geben, welche sowohl $b+(x+k)\cdot a$, als auch $p_{s+1}^{\alpha_{s+1}} \ldots p_{s+t}^{\alpha_{s+t}}$ teilt.
Aus

$$\begin{aligned} & p \mid (p_{s+1}^{\alpha_{s+1}} \ldots p_{s+t}^{\alpha_{s+t}}) \Rightarrow p \in \{p_{s+1},\ldots,p_{s+t}\} \\ & \Rightarrow p \nmid (b+(x+k)\cdot a) \quad \text{für} \quad 1 \leq k \leq c. \end{aligned}$$

Dies führt also zu einem Widerspruch.
Nach Proposition 5.1. gibt es ein $h \in \{1,\ldots,p_1 \ldots p_s\}$, derart dass $p_i \nmid (b+(x+h)\cdot a)$ für $1 \leq i \leq s$ gilt. Dabei ist

$$1 \leq h \leq p_1 \cdots p_s \leq p_1^{\alpha_1} \cdots p_s^{\alpha_s} \cdot p_{s+1}^{\alpha_{s+1}} \cdots p_{s+t}^{\alpha_{s+t}} = c.$$

Es folgt $\mathrm{ggT}(b+(x+h)\cdot a, p_1^{\alpha_1} \cdots p_s^{\alpha_s}) = 1$.
Wäre nämlich $\mathrm{ggT}(b+(x+h)\cdot a, p_1^{\alpha_1} \cdots p_s^{\alpha_s}) > 1$, so würde es eine Primzahl p geben für die gilt $p \mid (b+(x+h)\cdot a)$ und $p \mid p_1^{\alpha_1} \cdots p_s^{\alpha_s}$. Aus

$$p \mid p_1^{\alpha_1} \cdots p_s^{\alpha_s} \Longrightarrow \exists\, i \in \{1,\ldots,s\} : p = p_i$$

Daraus würde folgen, dass $p_i \mid (b+(x+h)\cdot a)$, und dies ist ein Widerspruch.

Es gelten also

$$\begin{aligned} \mathrm{ggT}(b+(x+h)\cdot a,\, p_{s+1}^{\alpha_{s+1}}\cdots p_{s+t}^{\alpha_{s+t}}) &= 1 \text{ und} \\ \mathrm{ggT}(b+(x+h)\cdot a,\, p_1^{\alpha_1}\ldots p_s^{\alpha_s}) &= 1. \end{aligned}$$

Daraus folgt:

$$\mathrm{ggT}(b+(x+h)\cdot a, c) = \mathrm{ggT}\left(b+(x+h)\cdot a, p_1^{\alpha_1}\ldots p_s^{\alpha_s}\cdot p_{s+1}^{\alpha_{s+1}}\cdots p_{s+t}^{\alpha_{s+t}}\right) = 1.$$

□

Bemerkung 5.3. Für alle $x \geq -1$, folgt aus Proposition 5.2.:

$$\mathrm{ggT}(a,b,c) = 1 \implies \min_{x+1\leq y\leq x+c} \mathrm{ggT}(b+ay,c) = 1.$$

Korollar 5.4. *Ist* $\mathrm{ggT}(a,b,c) = 1$ *und* $k \geq c$*, so enthalten* k *aufeinander folgende Glieder der Folge* $(b+ka)_{k\geq 0}$ *mindestens ein Glied* $b+ha$ *mit der Eigenschaft* $\mathrm{ggT}(b+ha,c) = 1$*.*

Beweis. Dies folgt unmittelbar aus Proposition 5.2. □

Bemerkung 5.5. Für alle $x \geq -1$, folgt aus Korollar 5.4.:

$$\text{Wenn } \mathrm{ggT}(a,b,c) = 1 \text{ und } k \geq c, \text{ dann } \min_{x+1\leq y\leq x+k} \mathrm{ggT}(b+ay,c) = 1$$

Proposition 5.6. *Ist* $s \geq c$*, so gilt für alle* $r \geq 0$

$$\min_{r\leq y\leq r+s-1} \mathrm{ggT}(b+ay,c) = \mathrm{ggT}(a,b,c).$$

Beweis. Sei $d := \mathrm{ggT}(a,\, b,\, c)$. Setze $a' = \dfrac{a}{d}$, $b' = \dfrac{b}{d}$ und $c' = \dfrac{c}{d}$, dann ist $c' \leq c$ und $\mathrm{ggT}(a',\, b',\, c') = 1$. Aus Korollar 5.4. und mit Bemerkung 5.5. folgt $\min\limits_{r\leq y\leq r+s-1} \mathrm{ggT}(b'+\, a'y,\, c') = 1$. Und damit

$$\begin{aligned} \min_{r\leq y\leq r+s-1} \mathrm{ggT}(b+ay,\, c) &= \min_{r\leq y\leq r+s-1} \mathrm{ggT}(b'd+\, a'dy,\, c'd) = \\ &= \min_{r\leq y\leq r+s-1} \mathrm{ggT}(d(b'+\, a'y),\, dc') = \\ &= \min_{r\leq y\leq r+s-1} d\cdot \mathrm{ggT}(b'+\, a'y,\, c') = \\ &= d\cdot \min_{r\leq y\leq r+s-1} \mathrm{ggT}(b'+\, a'y,\, c') = \\ &= d\cdot 1 \\ \implies \min_{r\leq y\leq r+s-1} \mathrm{ggT}(b+ay,\, c) &= \mathrm{ggT}(a,b,c). \end{aligned}$$

□

Die nachfolgende Proposition erweist sich als nicht korrekt und ihr zugehöriger Beweis ist fehlerhaft. Aus Gründen der Vollständigkeit wird Zignanos Argumentation dennoch wiedergegeben, wobei an den entscheidenden Stellen auf den darin enthaltenen Fehler hingewiesen wird. Später folgt wird ein Gegenbeispiel angegeben, welches die Unhaltbarkeit der Behauptung eindeutig belegt.

Proposition 5.7. *Ist $k \leq a$, so ist* $\min\limits_{0\leq y\leq a-1} \max\limits_{1\leq z\leq k} \mathrm{ggT}(b+ay,\ z)$ *ein gemeinsamer Teiler von a und b.*

Beweis. *(Fehlerhafter Beweis).* Induktion nach k:
Ist $k = 1$, so ist

$$\max_{1\leq z\leq 1} \mathrm{ggT}(b+ay, z) = \mathrm{ggT}(b+ay,\ 1) = 1$$

und daher

$$\min_{0\leq y\leq a-1} \max_{1\leq z\leq k} \mathrm{ggT}(b+ay, z) = 1$$

und 1 ist gemeinsamer Teiler von a und b.
Induktionsschritt von $k-1$ auf k: Es ist

$$\max_{1\leq z\leq k} \mathrm{ggT}(b+ay, z) = \max\left\{\max_{1\leq z\leq k-1} \mathrm{ggT}(b+ay, z), \mathrm{ggT}(b+ay, k)\right\}$$

$$\Rightarrow \min_{0\leq y\leq a-1} \max_{1\leq z\leq k} \mathrm{ggT}(b+ay, z) = \min_{0\leq y\leq a-1} \max\left\{\max_{1\leq z\leq k-1} \mathrm{ggT}(b+ay, z), \mathrm{ggT}(b+ay, k)\right\}$$

Nun ist

$$\max\left\{\max_{1\leq z\leq k-1} \mathrm{ggT}(b+ay, z), \mathrm{ggT}(b+ay, k)\right\} \in \left\{\max_{1\leq z\leq k-1} \mathrm{ggT}(b+ay, z), \mathrm{ggT}(b+ay, k)\right\}$$

Hier erfolgt die fehlerhafte Schlussfolgerung am Beweis:
Der Fehler liegt im Vertauschen von Maximum und Minimum, daher wird fälschlich gefolgert:

$$\min_{0\leq y\leq a-1} \max_{1\leq z\leq k} \mathrm{ggT}(b+ay, z) = \min_{0\leq y\leq a-1} \max\left\{\max_{1\leq z\leq k-1} \mathrm{ggT}(b+ay, z), \mathrm{ggT}(b+ay, k)\right\}$$

$$\in \max\left\{\min_{0\leq y\leq a-1} \max_{1\leq z\leq k-1} \mathrm{ggT}(b+ay, z), \min_{0\leq y\leq a-1} \mathrm{ggT}(b+ay, k)\right\}$$

Die Annahme, dass das Minimum des Maximums von zwei Werten gleich dem Maximum der Minima dieser Werte ist, ist falsch. Daher sind auch die weiteren Folgerungen im Beweis nicht korrekt, werden jedoch weiter angeführt.
Ist nun

$$\min_{0\leq y\leq a-1} \max_{1\leq z\leq k} \mathrm{ggT}(b+ay, z) = \min_{0\leq y\leq a-1} \max_{1\leq z\leq k-1} \mathrm{ggT}(b+ay, z),$$

so ist nach Induktionsvoraussetzung $\min\limits_{0\leq y\leq a-1}\max\limits_{1\leq z\leq k}\mathrm{ggT}(b+ay,z)$ ein gemeinsamer Teiler von a und b.
Im 2. Fall ist nun

$$\min_{0\leq y\leq a-1}\max_{1\leq z\leq k}\mathrm{ggT}(b+ay,z)=\min_{0\leq y\leq a-1}\mathrm{ggT}(b+ay,k)$$

Aufgrund von Proposition 5.6. folgt

$$\min_{0\leq y\leq a-1}\mathrm{ggT}(b+ay,k)=\mathrm{ggT}(a,b,k)$$

und ist daher ebenfalls ein gemeinsamer Teiler von a und b.
Wären nicht falsche Schlussfolgerungen dahinter, würde nun daraus folgen, dass

$$\min_{0\leq y\leq a-1}\max_{1\leq z\leq k}\ \mathrm{ggT}(b+ay,\ z)=\mathrm{ggT}(a,b,k),$$

was ebenfalls ein gemeinsamer Teiler von a und b ist.

□

Proposition 5.8. *Es gilt*

$$\max_{1\leq z\leq k}\ \mathrm{ggT}(u,z)=\max_{\substack{1\leq d\leq k\\ d\mid u}}d$$

Beweis. Es soll $\Big\{\,\mathrm{ggT}(u,z)\ \Big|\ 1\leq z\leq k\Big\}=\Big\{d\ \Big|\ 1\leq d\leq k,\ d\mid u\Big\}$ gezeigt werden, da dann beide Mengen dasselbe Maximum besitzen.
Zuerst wird ein größter gemeinsamer Teiler $d=\mathrm{ggT}(u,z)$ für ein $z\in\{1,2,\ldots,k\}$ betrachtet. Ist $d=\mathrm{ggT}(u,z)$, so teilt d sowohl u als auch z, das heißt

$$d\mid u\ \ \text{und}\ \ d\mid z.$$

Da $z\in\{1,2,\ldots,k\}$, gilt $d\leq z\leq k$. Daraus folgt, dass $d\in\{1,2,\ldots,k\}$ und $d\mid u$. Also

$$\Big\{\,\mathrm{ggT}(u,z)\ \Big|\ 1\leq z\leq k\Big\}\leq\Big\{d\Big|\,1\leq d\leq k,\ d\mid u\Big\}.$$

Nun wird ein Teiler d von u betrachtet, welcher ebenfalls in der Menge $\{1,2,\ldots,k\}$ liegen soll. Ist $d\in\{1,2,\ldots,k\}$ und $d\mid u$, setze $z=d$, dann gilt:

$$\mathrm{ggT}(u,z)=\mathrm{ggT}(u,d)=d$$

Da $z=d\in\{1,2,\ldots,k\}$, gilt $d\leq k$ und d ist ein Element der Menge

$\Big\{ \mathrm{ggT}(u,z) \;\Big|\; 1 \le z \le k \Big\}$. Daher gilt:

$$\Big\{ d \;\Big|\; 1 \le d \le k, d \mid u \Big\} \le \Big\{ \mathrm{ggT}(u,z) \;\Big|\; 1 \le z \le k \Big\}$$

$$\Longrightarrow \Big\{ \mathrm{ggT}(u,z) \;\Big|\; 1 \le z \le k \Big\} = \Big\{ d \;\Big|\; 1 \le d \le k,\ d \mid u \Big\}$$

$$\Longrightarrow \max_{1 \le z \le k} \mathrm{ggT}(u,z) = \max_{\substack{1 \le d \le k \\ d \mid u}} d$$

□

Proposition 5.9. *Es gilt*

$$\min_{0 \le y \le a-1} \max_{1 \le z \le a} \mathrm{ggT}(b+ay, z) = \mathrm{ggT}(a,b)$$

Beweis. Aus vorheriger Proposition 5.8. folgt

$$\max_{1 \le z \le a} \mathrm{ggT}(b+ay, z) = \max \Big\{ d \;\Big|\; 1 \le d \le a,\ d \mid (b+ay) \Big\}$$

Da $\mathrm{ggT}(a,b) \mid a$, folgt $\mathrm{ggT}(a,b) \le a$ und da $\mathrm{ggT}(a,b)$ sowohl a als auch b teilt, gilt auch

$$\mathrm{ggT}(a,b) \;\Big|\; (b+ay)$$

für $y \in \{0, 1, \ldots, a-1\}$. Daraus folgt:

$$\mathrm{ggT}(a,b) \le \max \Big\{ d \mid 1 \le d \le a,\ d \mid (b+ay) \Big\} = \max_{1 \le z \le a} \mathrm{ggT}(b+ay, z).$$

Da dies für jedes $y \in \{0, 1, \ldots, a-1\}$ gilt, folgt

$$\mathrm{ggT}(a,b) \le \min_{0 \le y \le a-1} \max_{1 \le z \le a} \mathrm{ggT}(b+ay, z)$$

Nach Proposition 5.7., dem fehlerhaften Beweis, wäre $\min\limits_{0 \le y \le a-1} \max\limits_{1 \le z \le a} \mathrm{ggT}(b+ay, z)$ ein gemeinsamer Teiler von a und b und daher

$$\min_{0 \le y \le a-1} \max_{1 \le z \le a} \mathrm{ggT}(b+ay, z) \le \mathrm{ggT}(a,b).$$

Daraus folgt nun fälschlicherweise:

$$\min_{0 \le y \le a-1} \max_{1 \le z \le a} \mathrm{ggT}(b+ay, z) = \mathrm{ggT}(a,b).$$

□

Proposition 5.10. *Sind* $1 < b \leq a$ *und* $\mathrm{ggT}(a,b) = 1$*, so ist eine der Zahlen in der Folge*

$$b, b+a, b+2a, \ldots, b+(a-1)a = (b+ka)_{0\,\leq\, k\,\leq\, a-1}$$

eine Primzahl.

Beweis. Es ist $\mathrm{ggT}(a,b) = 1$, nach den vorherigen Propositionen gilt:

$$\begin{aligned} \mathrm{ggT}(a,b) &\overset{\text{Prop 5.9.}}{=} \min_{1\leq y\leq a-1} \max_{1\leq z\leq a} \mathrm{ggT}(b+ay, z) \\ &\overset{\text{Prop 5.8.}}{=} \min_{1\leq y\leq a-1} \max_{1\leq \substack{d\\ d\mid(b+ay)}\leq a} d \;=\; 1. \end{aligned}$$

Da das Minimum dieser Maxima gleich 1 ist, existiert eine Zahl $y' \in \{1, \ldots, a-1\}$, für die gilt, dass

$$1 \leq \max_{\substack{d\\ d\mid(b+ay')}} \leq a \; d = 1.$$

Das heißt, außer für $d = 1$, gilt weiters:

$$d \mid (b+ay') \Rightarrow d > a.$$

Es ist

$$1 < b+ay' \leq b+(a-1)a \;\leq a+(a-1)a = a^2$$

Angenommen

$$b+ay' = k \cdot l$$

für $1 < k,\ l < b+ay'$, so muss $k \leq a$ oder $l \leq a$ sein.

Sonst wäre $k, l > a$ und daher

$$b+ay' = kl > a^2.$$

Dies führt zu einem Widerspruch, also ist $k = 1$ oder $l = 1$ und $b+ay'$ somit eine Primzahl.

□

Proposition 5.11. *Ist* $\mathrm{ggT}(a,b) = 1$*, so enthält die Folge*

$$b, b+a, b+2a, b+3a, \cdots = (b+ka)_{k\geq 0}$$

eine Primzahl.

Beweis. Falls $b = 1$: Es ist a und b teilerfremd und $\mathrm{ggT}(a, b) = \mathrm{ggT}(a, 1) = 1$, daher wird b durch $b + a > b = 1$ ersetzt, wobei beachtet wird, dass

$$\mathrm{ggT}(a + b, a) = \mathrm{ggT}(a + 1, a).$$

Man kann zeigen, dass

$$(b + a + ka)_{k\geq 0} = (b + (k + 1)a)_{k\geq 0} = (b + ka)_{k\geq 1}$$

eine Primzahl enhält, und daher $(b + ka)_{k\geq 0}$ erst recht eine Primzahl enthält. Daher kann ab jetzt o.B.d.A für $b > 1$ vorrausgesetzt werden.
Falls $b \leq a$, so folgt die Behauptung aus Proposition 5.10.
Daher sei $b > a$.
Es wird ein $c > b$ gewählt, sodass $\mathrm{ggT}(b, c) = 1$, z.B. $c = b + 1$. Dann gilt

$$\mathrm{ggT}(ac, b) = \mathrm{ggT}(a, b) = 1$$

und außerdem

$$ac \geq c > b.$$

Nach Proposition 5.10. enthält die Folge $(b + kac)_{k\geq 0}$ eine Primzahl der Gestalt

$$b + k(ac) = b + (kc)a.$$

Diese ist damit auch ein Element der ursprünglichen Folge $(b + ka)_{k\geq 0}$, welche somit ebenfalls eine Primzahl enthält.

□

Proposition 5.12. *Ist* $\mathrm{ggT}(a, b) = 1$*, so enthält die Folge*

$$b, b + a, b + 2a, b + 3a, \cdots = (b + ka)_{k\geq 0}$$

unendlich viele Primzahlen.

Beweis. Nach Proposition 5.11. gibt es ein $y_1 \geq 0$, sodass

$$p_1 := b + y_1 a$$

eine Primzahl ist.
Angenommen, es wurden bereits alle $0 \leq y_1 < y_2 < \cdots < y_n$ gefunden, welche die Eigenschaft besitzen, dass $p_i = b + y_i a$ prim ist, wobei $1 \leq i \leq n$.

Es gilt nun

$$\text{ggT}(a, b + (y_n + 1)a) = 1.$$

Wäre $\text{ggT}(a, b + (y_n + 1)a) > 1$, so würde es eine Primzahl p geben, sodass gilt

$$p \mid a \text{ und } p \mid (b + (y_n + 1)a) .$$

Angenommen, es gibt eine Primzahl p mit soeben genannten Eigenschaften, dann würde p auch die Differenz $(b + (y_n + 1)a) - (y_n + 1)a$ teilen.
Da

$$\begin{aligned} & p \mid \Big((b + (y_n + 1)a) - (y_n + 1)a\Big) \\ \implies & p \mid b \end{aligned}$$

So wäre p ein Teiler von a und b

$$\implies \text{ggT}(a, b) > 1.$$

Dies führt zu einem Widerspruch zur Annahme $\text{ggT}(a, b) = 1$.
Es soll gezeigt werden, dass es eine weitere Zahl y_{n+1} gibt, für die $b + (y_{n+1})a$ ebenfalls eine Primzahl ist.
Erneut nach Proposition 5.11. enthält die Folge $(b + (y_n + 1)a + ka)_{k\geq 0}$ eine Primzahl, das heißt, es existiert ein $k \geq 0$, sodass

$$b + (y_n + 1)a + ka = b + (y_n + k + 1)a$$

eine Primzahl ist.
Um $y_1, y_2, \ldots y_n$ fortzusetzen, setzt man

$$y_{n+1} = y_n + k + 1.$$

Dann ist $y_{n+1} > y_n$ und $b + (y_{n+1})a$ bildet somit die nächste Primzahl in der Folge.
Daher enthält die Folge $(b + ka)_{k\geq 0}$ unendlich viele Primzahlen.

□

In Proposition 5.12. wurde gezeigt, dass die Folge $(b + ka)_{k\geq 0}$ unendlich viele Primzahlen enthält. Dieser Beweis stützt sich jedoch auf die fehlerhaften Aussagen der Propositionen 5.7., 5.9., 5.10. und 5.11.. Da diese nicht korrekt sind, erweist sich auch der Schluss in Proposition 5.12. als ungültig.

Bemerkung. Um den Fehler in Proposition 5.7. zu veranschaulichen, folgt ein konkretes Gegenbeispiel:
Falls $\mathrm{ggT}(a,b) = 1$ müsste gelten, dass

$$\min_{0 \leq y \leq a-1} \max_{1 \leq z \leq a} \mathrm{ggT}(b+ay, z) = 1.$$

Setze $a = 13$ und $b = 672$, tatsächlich ist $\mathrm{ggT}(13, 672) = 1$. Die Behauptung nach Proposition 5.7. wäre, dass

$$\min_{0 \leq y \leq 12} \max_{1 \leq z \leq 13} \mathrm{ggT}(672 + 13y, z) = 1.$$

Es wird für jedes $y \in \{0, \ldots, 12\}$ zunächst die Zahl $672 + 13y$ ermittelt, dann der Wert von $\mathrm{ggT}(672 + 13y, z)$ für alle $z \in \{1, \cdots, 13\}$ berechnet und daraus das Maximum angegeben. Anschließend wird über alle y das Minimum dieser Maxima gebildet.

Es wird das Beispiel für $y = 0$ genauer betrachtet, für $y = 2$ bis $y = 12$ wird das Beispiel danach kürzer angeschrieben.

Für $y = 0$ ist

$$\mathrm{ggT}(b + ay, z) = \mathrm{ggT}(672 + 0, z) = \mathrm{ggT}(672, z)$$

Es wird die Primfaktorzerlegung von $b + ay = 672 + 0 = 672$ durchgeführt

$$672 = 2^5 \cdot 3 \cdot 7$$

Nun wird jeder $\mathrm{ggT}(2^5 \cdot 3 \cdot 7, z)$ für $1 \leq z \leq 13$ gebildet.

$\mathrm{ggT}(2^5 \cdot 3 \cdot 7, 1) = 1$ $\quad$ $\mathrm{ggT}(2^5 \cdot 3 \cdot 7, 6) = 6$ $\quad$ $\mathrm{ggT}(2^5 \cdot 3 \cdot 7, 10) = 2$

$\mathrm{ggT}(2^5 \cdot 3 \cdot 7, 2) = 2$ $\quad$ $\mathrm{ggT}(2^5 \cdot 3 \cdot 7, 7) = 1$ $\quad$ $\mathrm{ggT}(2^5 \cdot 3 \cdot 7, 11) = 1$

$\mathrm{ggT}(2^5 \cdot 3 \cdot 7, 3) = 3$ $\quad$ $\mathrm{ggT}(2^5 \cdot 3 \cdot 7, 8) = 8$ $\quad$ $\mathrm{ggT}(2^5 \cdot 3 \cdot 7, 12) = 12$

$\mathrm{ggT}(2^5 \cdot 3 \cdot 7, 4) = 4$ $\quad$ $\mathrm{ggT}(2^5 \cdot 3 \cdot 7, 9) = 3$ $\quad$ $\mathrm{ggT}(2^5 \cdot 3 \cdot 7, 13) = 1$

$\mathrm{ggT}(2^5 \cdot 3 \cdot 7, 5) = 1$

Anschließend wird das Maximum angegeben:

$$y = 0 : \max_{1 \leq z \leq 13} \mathrm{ggT}(672, z) = \max_{1 \leq z \leq 13} \mathrm{ggT}(2^5 \cdot 3 \cdot 7, z) = 12$$

In dieser gekürzten Form werden nun auch die restlichen Berechnungen für $y \in \{1, \ldots, 12\}$ angegeben:

$$y = 1 : \max_{1 \leq z \leq 13} \text{ggT}(685, z) = \max_{1 \leq z \leq 13} \text{ggT}(5 \cdot 137, z) = 5$$

$$y = 2 : \max_{1 \leq z \leq 13} \text{ggT}(698, z) = \max_{1 \leq z \leq 13} \text{ggT}(2 \cdot 349, z) = 2$$

$$y = 3 : \max_{1 \leq z \leq 13} \text{ggT}(711, z) = \max_{1 \leq z \leq 13} \text{ggT}(3^2 \cdot 79, z) = 9$$

$$y = 4 : \max_{1 \leq z \leq 13} \text{ggT}(724, z) = \max_{1 \leq z \leq 13} \text{ggT}(2^2 \cdot 181, z) = 4$$

$$y = 5 : \max_{1 \leq z \leq 13} \text{ggT}(737, z) = \max_{1 \leq z \leq 13} \text{ggT}(11 \cdot 67, z) = 11$$

$$y = 6 : \max_{1 \leq z \leq 13} \text{ggT}(750, z) = \max_{1 \leq z \leq 13} \text{ggT}(2 \cdot 3 \cdot 5^3, z) = 10$$

$$y = 7 : \max_{1 \leq z \leq 13} \text{ggT}(763, z) = \max_{1 \leq z \leq 13} \text{ggT}(7 \cdot 109, z) = 7$$

$$y = 8 : \max_{1 \leq z \leq 13} \text{ggT}(776, z) = \max_{1 \leq z \leq 13} \text{ggT}(2^3 \cdot 97, z) = 8$$

$$y = 9 : \max_{1 \leq z \leq 13} \text{ggT}(789, z) = \max_{1 \leq z \leq 13} \text{ggT}(3 \cdot 263, z) = 3$$

$$y = 10 : \max_{1 \leq z \leq 13} \text{ggT}(802, z) = \max_{1 \leq z \leq 13} \text{ggT}(2 \cdot 401, z) = 2$$

$$y = 11 : \max_{1 \leq z \leq 13} \text{ggT}(815, z) = \max_{1 \leq z \leq 13} \text{ggT}(5 \cdot 163, z) = 5$$

$$y = 12 : \max_{1 \leq z \leq 13} \text{ggT}(828, z) = \max_{1 \leq z \leq 13} \text{ggT}(2^2 \cdot 3^3 \cdot 23, z) = 12$$

Aus diesen Maximalwerten wird nun das Minimum angegeben:

$$\min_{0 \leq y \leq 12} \max_{1 \leq z \leq 13} \text{ggT}(672 + 13y, z) = 2$$

$$\Longrightarrow \min_{0 \leq y \leq 12} \max_{1 \leq z \leq 13} \text{ggT}(672 + 13y, z) = 2 \neq 1 = \text{ggT}(a, b)$$

Daher ist die Aussage von Proposition 5.7. mit diesem Gegenbeispiel widerlegt worden.

6 Resümee

Es lässt sich festhalten, dass diese Arbeit einen breiten Überblick über die verschiedenen elementaren und analytischen Beweisansätze zur Unendlichkeit der Primzahlen bietet. Der älteste Beweis für die Unendlichkeit von Primzahlen stammt von Euklid und gilt als einer der schönsten Beweise der Zahlentheorie. Im Laufe der Jahrhunderte haben sich weitere Mathematiker mit der Frage nach der Unendlichkeit der Primzahlen beschäftigt und dabei unterschiedliche, kreative Beweisstrategien genutzt.
Goldbachs Beweisidee beruht auf den Fermat-Zahlen, Euler nutzte die Eindeutigkeit der Primfaktorzerlegung, die Divergenz der Reihe $\sum_{i=1}^{n} \frac{1}{i}$, sowie den natürlichen Logarithmus. Erdös betrachtet in seinem Beweis die Reihe der Inversen Primzahlen und beweist neben der Unendlichkeit der Primzahlen auch die Divergenz der Reihe $\sum \frac{1}{p}$ und Furstenbergs Beweis basiert auf topologischen Überlegungen und verbindet abstrakte mathematische Konzepte mit der Zahlentheorie.
Dirichlet betrachtet Primzahlen in arithmetischen Progressionen und trägt mit seinem Dirichletschen Primzahlsatz auch zum Verständnis der Verteilung von Primzahlen bei. Es gibt verschiedene Beweise für die Unendlichkeit der Primzahlen in sogenannten Spezialfällen arithmetischer Progressionen. Neben den elementaren Beweisen für die Unendlichkeit der Primzahlen der Gestalt $4k + 1$ bzw. $4k - 1$, werden auch Beweise mit der Verwendung von Kongruenzen, Produktzerlegungen, den Fermat-Zahlen, dem Legendre-Symbol und den Eigenschaften des Reziprozitätsgesetzes beschrieben.
Italo Zignano versuchte den Dirichletschen Primzahlsatz für arithmetische Progressionen mit rein elementaren Mitteln zu beweisen. Der Kernfehler seines Beweises liegt im unrechtmäßigen Vertauschen von Minimum und Maximum. Ein numerisches Gegenbeispiel kann die fehlerhafte Aussage aufzeigen, die darauffolgenden Propositionen erweisen sich daher als ungültig und somit auch die eigentlich zu beweisende Aussage für die Unendlichkeit von Primzahlen in arithmetischen Progressionen.
Der Beweis zeigt exemplarisch, wie kritisch Beweise, deren Lemmata und Aussagen betrachtet werden sollten, denn bereits kleine Unachtsamkeiten können den gesamten Beweis ins Wanken bringen. Weiters wird klar, dass der Dirichletsche Primzahlsatz nicht ohne analytische Methoden bewiesen werden kann.
Die Arbeit zeigt, wie wertvoll die Erkenntnisse der unterschiedlichen Beweise in der Zahlentheorie sind und wie vielfältig und kreativ Mathematiker an das Problem der Unendlichkeit der Primzahlen herangegangen sind.

Abbildungsverzeichnis

Literatur

[1] Aigner, Martin: *Zahlentheorie: Eine Einführung mit Übungen, Hinweisen und Lösungen*, Vieweg+Teubner Verlag, 2011.

[2] Aigner, Martin/Günter M. Ziegler: *Das BUCH der Beweise*, 3. Aufl., Berlin, Heidelberg: Springer-Verlag, 2010.

[3] Baxa, Christoph: *Zahlentheorie*, Vorlesung der Universität Wien, 2017.

[4] Bundschuh, Peter: *Einführung in die Zahlentheorie*, 6.Aufl., Berlin, Heidelberg: Springer, 2008

[5] Böhm, Janko: *Grundlagen der Algebra und Zahlentheorie*, Berlin, Heidelberg: Springer Spektrum, 2016.

[6] Conrad, Keith: *THE "TOPOLOGICAL" PROOF OF THE INFINITUDE OF PRIMES*, in: Amer. Math. Monthly, Bd. 62, 1955, [online] https://kconrad.math.uconn.edu/blurbs/ugradnumthy/primestopology.pdf.

[7] Estermann, T.: *Note on a paper of A. Rotkiewicz*, in: Acta Arithmetica, Bd. 8, Nr. 4, 1963, S. 465–467.

[8] Fulmek, Markus: *Vorlesungsskript der VO Zahlentheorie*, Universität Wien, 2019, [online] https://www.mat.univie.ac.at/mfulmek/scripts/ZT/skriptum.pdf

[9] Fürstenberg, H.: *On the infinitude of primes*, in: The American Mathematical Monthly, 62, 1955, S. 353.

[10] Lucas, Édouard: *Théorie des nombres*, Paris: Gauthier-Villars et Fils, tume 1, 1891.

[11] Reiss, Kristina/ Gerald Schmieder: *Basiswissen Zahlentheorie: Eine Einführung in Zahlen und Zahlbereiche*, 3. Aufl., Berlin, Heidelberg: Springer Spektrum, 2014.

[12] Ribenboim, Paulo: *The Book of Prime Number Records*, Springer-Verlag, 1988.

[13] Ribenboim, Paulo: *Meine Zahlen, meine Freunde: Glanzlichter der Zahlentheorie*, Berlin, Heidelberg: Springer-Verlag, 2009.

[14] Ribenboim, Paulo: *Die Welt der Primzahlen: Geheimnisse und Rekorde*, 2. Aufl., Berlin, Heidelberg: Springer-Verlag, 2011.

[15] Robbins, Neville: *ON FIBONACCI NUMBERS AND PRIMES OF THE FORM* $4k + 1$, in: Reviews in Number Theory, 1984-96: As Printed in Mathematical Reviews, Band 5, Teil 2, 1994, [online] https://www.mathstat.dal.ca/FQ/Scanned/32-1/robbins.pdf, S. 15–16.

[16] Serret, J.-A.: *Note sur un théorème de la théorie des nobres*, in: Journal De Mathématiques Pures Et Appliquées 1 Série, tome 12, 1852, p 186–189.

[17] Sierpiński, W./ A. Schinzel: *Elementary Theory of Numbers*, Polish Scientific Publishers, 1988.

[18] Zignago, Italo: *Intorno ad un teorema di aritmetica*, in: Annali Di Matematica Pura Ed Applicata (1923 -), Bd. 21, Nr. 1, 1893, [online] doi:10.1007/bf02420437, S. 47–55.