THE TEACHING OF MATHEMATICS
2007, Vol. X, 2, pp. 63–74

ES GIBT UNENDLICH VIELE PRIMZAHLEN – DER SATZ VON EUKLID

Šefket Arslanagić und Walther Janous

Abstract. In this paper we consider famous Euclidean theorem which is mentioned in the title. Also, we consider numerous proofs of this theorem and its modifications. These modifications were given by famous mathematicians like Kummer, Stieltjes, Fermat, Sylvester, Legendre, Dirichlet, Bertrand and Euler. Proofs are various and they use number theory, analysis, algebra, combinatorics and topology. Indeed, this paper is a complete overview of all relevant fact connected with Euclidean theorem that the set of all prime numbers is infinite and his proof of this theorem.

ZDM Subject Classification: F65; *AMS Subject Classification*: 00A35.

Key words and phrases: Primes, factorization, Euclid's theorem, Fermat's numbers, Dirichlet's theorem, Euler's product, Mersenne's prime numbers, Euler's φ-function, combinatorial proof, topological proof.

Einleitung

Für manche mathematischen Aussagen gibt es "über die jahre" eine Vielzahl von Beweisen – es gehörte gewissermaßen "zum guten Ton" für bestimmte Sätze einen neuen Beweis anzugeben.

Beispiele dafür sind etwa:

- *Der pythagoreische Lehrsatz.*

Einen guten Einblick in das Umfeld und die Vielfalt seiner über 300 Beweise vermittelt das lesens- und auch für Schüller empfehlenswerte Büchlein [4]. (Als Kuriosum sei daraus erwähnt, dass der spätere [schließlich gewaltsam umgekommene] amerikanische Präsident James A. *Garfield* als Kongressabgeordneter im Jahr 1876 einen interessanten Beweis des pythagoreischen Lehrsatzes entdeckte, der im *New England Journal of Education* abgedruckt wurde. Er fand seinen Beweis als Mitglied eines Kreises von Abgeordneten, die zum Zeitvertrieb bei langweiligen Reden mathematische Aufgaben gelöst haben!)

- *Die geometrisch-aritmetische Mittelungleichung* ($\sqrt[n]{x_1 \cdot \ldots \cdot x_n} \leqslant \dfrac{x_1 + \cdots + x_n}{n}$ für nicht negative reelle Zahlen $x_1, x_2, \ldots, x_n$).

Für diese fundamentale Tatsache aus der Theorie der Potenzmittel, deren erster Beweis von *MacLaurin* im Anfangsdrittel des 18. Jahrhunderts angegeben wurde, finded sich in [5] 52 verschiedenen Beweisideen.

- *Der Fundamentalsatz der Algebra.*

Auch für ihn wurden seit *Gauß*ens erstem Beweis im Jahr 1799 – er findet sich in seiner Doktorarbeit – unüberschaubar viele weitere Beweiswege erdacht.

Auch der im Titel erwähnte Satz, den erstmals Euklid in seinen Elementen formuliert und nachgewiesen hat, zählt zu dieser Kategorie. (Selbst heute noch werden für alle diese Resultate in diversen Zeitschriften zum Teil überraschende neue Beweise veröffentlicht.)

Welche Interesse besteht eigentlich daran, eine altbekannte und elementare Tatsache immer wieder neu zu bestätigen? Wie wir beim Satz Euklid sehen werden, sind viele der Beweise das Ergebnis von weitergehenden Überlegungen, z.B. über die Verteilung der Primzahlen: Der neue Beweis ist dann die Illustration einer neuen Idee oder eines neuen Konzepts einer schwierigen allgemeineren Theorie. Beim Satz von Euklid kommen jedoch auch noch kulturelle und ästhetische Motive hinzu, wie *Ribenboim* ([13], S. 3) bemerkt: "I shall give several proofs of this theorem [...] by famous, but also forgotten, mathematicians. Some proofs suggest interesting developments; other proofs are just clever or curious." Solche Motive spielen gerade bei elementaren resultaten eine große Rolle.

Nicht zuletzt gibt es auch pädagogische Gründe, wie Benjamin F. *Finkel* (in der Ausgabe des *American Mathematical Monthlly*) schreibt: "The solution of problems is one of the lowest forms of mathematical research, ... yet its educational value cannot be overestimated. It is the ladder by which the mind ascends into higher fields of original research and investigation. Many dormant minds have been aroused into activity through the mastery of a single problem."

In dieser Arbeit sollen einige solcher Nachweise für den Satz vorgestellt werden, den bereits *Euklid* in seinen *Elementen* formuliert und bewiesen hat (und den Immanuel *Kant* in seiner *Kritik der reinen Vernunft* als ein Meisterwerk des menschlichen Geistes bezeichnete). Sie verlaufen zumeist indirekt, d.h. sie nehmen an, es gäbe nur endlich viele Primzahlen und leiten daraus einen Widerspruch her.

Die Beweise sind auch zum Großteil "elemetar" in dem Sinn, dass die *Kenntnis einfacher Aussagen* über die Teilbarkeit, über Reihen bzw. über topologische Räume zu ihrem Verständnis ausreicht. Inwieweit sie besonders elegant (in der Diktion von *Erdös.* vgl. [1]) sind, überlasse ich dem Geschmack des Lesers.

Als Hilfen bei diesem 'Rundgang' waren mir die am Ende erwähnten Bücher, Artikel und Internet-Seiten von großem Nutzen.

A) Der ursprüngliche Beweis und einige Variationen darüber

Angenommen $p_1 = 2 < p_2 = 3 < \cdots < p_n$ sind alle Primzahlen.

(1) [*Euklid*] Man betrachte nun die Zahl $P_n = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$. Jeder Primteiler p von P_n muss aber von $p_1, \ldots, p_n$ vershieden sein. (Sonst müsste p die Zahle 1 teilen!) Damit ergibt sich aber, dass es eine weiter Primzahl geben muss.

Auch diese Beweis erhält man induktiv auch eine (sehr ungenaue) Abschätzung für die n-te Primzahl, nämlich: Es gilt: $p_n \leqslant 2^{(2^{n-1})}$.

(2) [*Kummer*] In diesen Beweis wird die (kleinere) Zahl $Q_n = p_1 \cdot p_2 \cdot \ldots \cdot p_n - 1$ an Stelle von P_n verwendet.

(3) [*Stieltjes*] Man denke sich das Produkt $N_n = p_1 \cdot p_2 \cdot \ldots \cdot p_n$ in zwei Faktoren a und b zelegt, also $N_n = a \cdot b$. Da keine Primzahl beide Faktoren teilt, ist die Summe $a + b$ durch keine der vorhandenen Primzahlen teilbar.

Die Beweise von Euklid und Kummer führen auf verschiedenne Fragestellungen, von deren Lösungen man momentan noch weit entfernt ist. Dazu definieren wir vier Folgen, nämlich:

a) Es sei $a_1 = 2$, Für $n \geqslant 1$ betrachte man die Zahl $A_n = a_1 \cdot a_2 \cdot \ldots \cdot a_n + 1$ und wähle als a_{n+1}

i) den kleinsten bzw.

ii) den größten Primteiler von A_n.

b) Ausgehend von $b_1 = 3$ betrachte man die analogen, sich nun aber über $B_n = b_1 \cdot b_2 \cdot \ldots \cdot b_n - 1$ ergebenden beiden unendlichen Folgen von Primzahlen.

Vermutlich enthalten in beiden Fällen die Folgen **i)** *alle Primzahlen.*

Über die Folgen **ii)** vermutet man, dass es für **a)** *unendlich viele Primzahlen* gibt, die in ihr *nicht vorkommen*, während die Folge **b)** noch ziemlich "im Dunkeln" ligt. (Man weiß aber, dass in ihr die Primzahlen 7, 11, 13, 17 und 19 *nicht* auftreten.)

B) Von teilerfremden Zahlen zu Primzahlen

Die nun folgenden Beweise beruhen auf dem einfachen (in dieser Form wohl ertsmals von *Hurwitz* formulierten)

Hilfssatz. Aus der Existenz einer unendlichen Folge natürlicher Zahlen, die alle größer als 1 sind und deren Glieder paarweise teilerfremd sind, ergibt sich die Unendlichkeit der Menge $\mathcal{P}$ aller Primzahlen.

(Denn man ordne jeder natürlichen Zahl einen Primteiler des entsprechenden Folgengliedes zu.)

Man baachte, dass der größte gemeinsame Teiler mit Hilfe des Euklid'schen Algorithmus bestimmt werden kann. Deshalb ist die Kenntnis der Primfaktorzerlegung der einzelnen Folgenglieder nötig.

(1) [*Goldbach*] Die Fermat'schen Zahlen $F_n = 2^{(2^n)} + 1$, $n \geqslant 0$, erfüllen die Bedingung des Hilfssatzes.

(Denn: Mit vollständiger Induktion weist man unschwer nach, dass $F_n = F_0 \cdot F_1 \cdot \ldots \cdot F_{n-1} + 2$, $n \geqslant 1$, gilt. Deshalb ist für $0 \leqslant k < n$ die Zahl F_k ein Teiler von $F_n - 2$. Wäre $d > 1$ ein gemeinsamer Teiler von F_k und F_n, so müsste d also auch 2 teilen. Dies ist aber ein Widerspruch, weil alle Fermat'schen Zahlen ungerade sind.)

(2) [*Sylvester*] Die durch $x_1 = 2$, $x_{n+1} = x_n^2 - x_n + 1$, $n \geqslant 1$, rekursiv definierte Folge erfüllt die Bedingungen des Hilfssatzes.

(Denn nun beweist man mit vollständiger Induktion, dass $x_{n+1} = x_1 \cdot x_2 \cdot \ldots \cdot x_n + 1$, $n \geqslant 1$, gilt.)

(3) Naheliegend ist nun die Frage, ob man die Ideen hinter diesen beiden Beweisen erweitern kann. Und es gilt in der Tat der folgende allgemeine.

Satz. Für die teilerfremden natürlichen Zahlen a und b erfüllen alle Folgen $x_1 = a$ und $x_{n+1} = x_1 \cdot x_2 \cdot \ldots \cdot x_n + b$, $n \geqslant 1$, die bedingungen des Hilfssatzes.

(Der Beweis kann induktiv geführt werden und bleibe dem Leser als Übungsaufgabe.)

Als weiteren Weg der Verallgemeinerung könnte man auch Folgen des Typs $x_1 \geqslant 2$ und $x_{n+1} = x_n(x_n - 1)y_n + 1$, $n \geqslant 1$, konstruieren, die den Bedingungen des Hilfssatzes genünigen. Ein Beispiel dafür ist $y_n = x_n$, also die Rekursion $x_{n+1} = x_n^2(x_n - 1) + 1$.

Eine sich von den vorangehenden Beweisen etwas unterscheidende Variante ist.

(4) [*Schorn*] Für eine natürliche Zahl $n \geqslant 2$ sind die Zahlen $n! \cdot i + 1$ und $n! \cdot j + 1$, $1 \leqslant i < j \leqslant n$, paarweise teilfremd.

(Denn mit $j = i + k$, $1 \leqslant k < n$ ist $n! \cdot j + 1 = (n! \cdot i + 1) + n! \cdot k$. Dies zeigt, dass es (für jedes n) mindestens n Primzahlen geben muss.)

Die Bedeutung der *Fermat'schen Primzahlen* (die Frage, ob es unendlich viele gibt, ist offen) für die Konstruierbarkeit regelmäßiger Vielecke ist seit Gauß bekannt. Die Entscheidung, ob eine spezielle Zahl F_n faktorisierbar ist, gehört zu den "Härtetests für Supercomputer" (und ist für Verschlüsselungsfragen bedeutsam).

C) "Ungewöhnliche" größte gemeinsame Teiler und unendlich viele Primzahlen

Diesen Abschnitt beginnen wir mit zwei zahlentheoretischen Aussagen, die auch für sich von Interesse sind. Dabei sind $a \geqslant 2$, $m, n \geqslant 1$ natürliche Zahlen und f_n die n-te *Fibonacci*-Zahl. Den größte gemeinsamen Teiler der Zahlen u and v ist bezeichen wir mit (u, v). Dann gelten:

i) $(a^m - 1, a^n - 1) = a^{(m,n)} - 1$ und

ii) $(f_m, f_n) = f_{(m,n)}$.

Beide Aussagen beweist man mit dem Euklid'schen Algorithmus. (Die Hauptgedanken sind

Für **i)**: Wenn $n = mq + r$ mit $q \geqslant 0$ und $0 \leqslant r < m$ ist, so gilt $a^n - 1 = a^r(a^{mq} - 1) + (a^r - 1)$, womit sich $(a^m - 1, a^n - 1) = (a^n - 1, a^r - 1)$ ergibt.

Für **ii)**: Benachbarte Fibonacci-Zahlen sind teilfremd und es gilt $f_{m+n} = f_{m-1}f_n + f_m f_{n+1}$, $m, n \geqslant 1$, woraus sich $f_{(k+1)m} = f_{km-1}f_m + f_{km}f_{m+1}$ für $m, k \geqslant 1$ ergibt.)

(1) Angenommen, die $n - 1$ Zahlen $p_2 = 3 < \cdots < p_n$ seien alle ungeraden Primzahlen. (Hinzu kommt $p_1 = 2$.) Dann sind die n *Mersenne*'schen Zahlen $2^{p_1} - 1, \ldots, 2^{p_n} - 1$ paarweise teilerfremd (man wählt $a = 2$ in **i)** und es gibt mindestens n ungerade Primzahlen (vgl. Hilssatz).

(2) Mit den Zahlen $f_{p_1}, \ldots, f_{p_n}$ kommt man analog (mit **(ii)**) zu einem Widerspruch.

Die Bedeutung der *Mersenne'schen Primzahlen* $M_p = 2^p - 1$ zur Charakterisierung der geraden vollkommenen Zahlen ist seit *Euler* bekannt. (Die Frage, ob es unendlich viele derattige Primzahlen gibt, ist ungeklärt.)

D) Zahlen mit "ausreichend" vielen Primteilern

Man kann den Satz von Euklid auch dadurch beweisen, dass man Folgen natürlicher Zahlen angibt, deren Glieder eine streng monoton steigende Zahl Primteilern haben.

(1) Die Folge $x_n = 2^{(2^n)} + 2^{(2^{n-1})} + 1$, $n \geqslant 1$, ist von der angegebenen Art.

(Denn mit Hilfe der Identität $a^4 + a^2 + 1 = (a^2 - a + 1)(a^2 + a + 1)$ folgt für $a = 2^{(2^n-1)}$: $x_{n+1} = (2^{(2^n)} - 2^{(2^{n-1})} + 1)x_n$, $n \geqslant 1$. Weil die beiden Faktoren größer als 1 und teilfremd sind, ergbit sich mit $x_1 = 7$, dass jedes Folgenglied x_n wenigstens n Primteiler besitzt.)

(2) Nun betrachten wir die Primfaktorzerlegung von $n! = 1 \cdot 2 \cdot \ldots \cdot n$, $n \geqslant 2$, also $n! = \prod_{p \leqslant n} p^{e_n(p)}$. (Dabei erstreckt sich die Produkt über alle Primzahlen aus dem Intervall $[2, n]$.) Wir zeigen die Ungleichung $\prod\limits_{p \leqslant n} \sqrt[p-1]{p} > \dfrac{n}{e}$ und damit die Unendlichkeit der Menge $\mathcal{P}$ aller Primzahlen. Seit *Legendre* kennt man eine "kompakte" Formel zur Bestimmung der Exponenten $e_n(p)$, nämlich $e_n(p) = \sum\limits_{j \geqslant 1} \left\lfloor \dfrac{n}{p^j} \right\rfloor$. (Dafür beachte man: Genau $\lfloor n/p \rfloor$ der Faktoren von $n!$ sind durch p teilbar, genau $\lfloor n/p^2 \rfloor$ davon sind ein weiteres Mal durch p, also durch p^2 teilbar, usw.) Deshalb gilt $e_n(p) \leqslant \sum\limits_{j \geqslant 1} \dfrac{n}{p_j} = \dfrac{n}{p-1}$, woraus $\sqrt[n]{n!} \leqslant \prod\limits_{p \leqslant n} \sqrt[p-1]{p}$ folgt.

Die behaupte Ungleichung ergibt sich jetzt der folgenden Abschätzung vom "*Stirling*-Typ", nämlich $\sqrt[n]{n!} > \dfrac{n}{e}$, d.h. in logarithmierter Form $\dfrac{1}{n}(\ln 2 + \cdots + \ln n) > \ln n - 1$.

(Weil die Funktion $y = \ln x$, $x > 0$, streng monoton steigt, gilt für $j = 2, \ldots, n$ dass $\ln j = (\ln j) \cdot 1 > \int_{j-1}^{j} \ln x \, dx$. Deshalb ist schließlich

$$\ln 2 + \cdots + \ln n > \int_1^n \ln x \, dx = (x \ln x - x)|_1^n = n \ln n - n + 1 > n(\ln n - 1).)$$

(3) Es sei $f(x)$ ein nicht konstantes Polynom mit ganzzahligen Koeffizienten. Dann ergibt die Menge $\{f(1), f(2), \ldots\}$ unendlich viele Primteiler, d.h. Primzahlen p, sodass für eine passende natürliche Zahl N der Polynomwert $f(N)$ durch p teilbar ist.

Es ist $f(x) = a_n x^n + \cdots + a_1 x + a_0$, $n \geqslant 1$ und $a_n \neq 0$. Es soll $a_0 \neq 0$ sein. (Die Aussage für $a_0 = 0$ folgt dann mit Euklid: Man setze $N = p$.) Wir nehmen an, die Menge $\{f(1), f(2), \ldots\}$ würde nur endliche viele Primteiler $p_1, \ldots, p_r$ ergeben und betrachten die unendliche Zahlenfolge $N_m = 2^m \cdot p_1 \cdot \ldots \cdot p_r \cdot a_0^2$, $m = 1, 2, \ldots$, für die (mit der Abkürzung $q = 2^m \cdot p_1 \cdot \ldots \cdot p_r$) gilt, dass $f(N_m) =$

$a_0(a_n a_0^{2n-1} q^n + \cdots + a_1 a_0 q + 1)$. Wegen $|f(x)| \to \infty$ für $x \to \infty$ ist der Absolutwert der Klammer für hinreichend großes m größer als 1 und besitzt demmach wenigstens einen Primteiler, der aber von p_1 bis p_r vershieden sein muss.

E) Jenseits des euklidischen Horizonts

Die obigen elementaren Ideen können sehr rasch zu sehr schwierigen Fragen führen. Deren Lösungen sind dann tief liegende Theoreme, aus denen sich der Satz von Euklid als einfache Folgerung ergibt (weswegen wir hier selbsrendend nicht mehr von "alternativen Beweisen" sprechen können). Nicht vorbeigehen können wir dabei an folgenden zwei Resultaten:

(1) [*Dirichlet*] Einen interessanten Spezialfall von **(3)** aus Abschnitt **D)** bilden die linearen Funktionen $f(x) = dx + a$ ($a, d \in \mathbf{Z}$, $d \neq 0$), deren Funktionswerte $f(1)$, $f(20, \ldots$ unendlich viele Primteiler ergeben. Hier gilt allerdings ein viel wichtigeres Resultat, nämlich der

Satz von Dirichlet. Es sei $q_n = dn + a$, $n = 0, 1, 2, \ldots$, eine streng monoton steigende (aritmetische) Folge ganzer Zahlen, wobei die Zahlen a und d teilfremd sind. Dann enthält diese Folge unendlich viele Primzahlen (Es gilt sogar genauer: Jede Restklasse in $\mathbf{Z}_d^*$ enthält grob gesprochen "den $\varphi(d)$-ten Teil aller Primzahlen".)

Wir beweisen nun *exemplarisch zwei Spezialfälle des Dirichlet'schen Satzes*, nämlich:

(a) Es gibt unendlich viele Primzahlen der Form $p = 3n + 2$.

Angenommen, es gäbe nur endlich viele deratige Primzahlen, also $p_1 = 2$, $p_2 = 5$, $p_3 = 11$, $\ldots$, p_N. Dann ist die Zahl $z = 3p_1 \cdot \ldots \cdot p_N - 1$ teilerfremd zu $p_1, \ldots, p_N$ und erfült $z \equiv 2 \pmod 3$. z kann deshalb nicht lauter Primteiler q mit $q \equiv 1 \pmod 3$ haben!

(Weil n ungerade sein muss, haben wir auch bewiesen, dass es unendlich viele Primzahlen des Typs $p = 6m + 5$ gibt.)

(b) Wesentlich schwieriger ist der Nachweis, dass es auch unendlich viele Primzahlen der Art $p = 6n + 1$ gibt.

Ihm wird folgende für sich selbst interessante Aussage vorausgeschickt:

($*$) Alle Primteiler $p > 3$ des Trinoms $x^2 + x + 1$, $x \in \mathbf{N}$, erfüllen $p \equiv 1 \pmod 6$.

(Denn, angenommen, $p = 3m + 2$ wäre ein Teiler von $x^2 + x + 1$. Nun ist aber p kein Teiler von x ist und es gilt $(x - 1)(x^2 + x + 1) \equiv 0 \pmod p$, d.h. $x^3 \equiv 1 \pmod p$. Deshalb ergibt sich $x^{p-2} \equiv 1 \pmod p$, also $x^{p-1} \equiv x \pmod p$. Nach dem 'kleinen Satz' von *Fermat* ist aber $x^{p-1} \equiv 1 \pmod p$. Deshalb ist $x \equiv 1 \pmod p$, woraus aber wegen $x^2 + x + 1 \equiv 3 \pmod p$ der Widerspruch $3 \equiv 0 \pmod p$ folgt. Somit muss $p \equiv 1 \pmod 3$, also auch $p \equiv 1 \pmod 6$ gelten.)

Wir nehmen wieder an, $p_1 = 7$, $p_2 = 13$, $\ldots$, p_N wären alle Primzahlen des Typs $p \equiv 1 \pmod 6$ und betrachten nun die Zahl $z = w^2 + w + 1$, wobei $w = p_1 \cdot \ldots \cdot p_N$ ist. Aus $w = 6k + 1$ ergibt sich $z = 36k^2 + 18k + 3$, d.h. $z \equiv 3 \pmod 9$. Deshalb ist die ungerade Zahl z keine vollständige Potenz von 3 und z

muss eienen Primteiler $q > 3$ besitzen, füt den wegen $(*)$ aber $q \equiv 1 \pmod 6$ erfüllt sein muss. q ist aber im Widerspruch zur Annahme von $p_1, \ldots p_N$ verschieden.

Wir bemerken noch, dass sich die Aussage $(*)$ folgendermaßen verallgemeinern lässt: Es sein p und q zwei Primzahlen, $p \neq q$. Wenn p ein Teiler des Polynoms $x^{q-1} + x^{q-2} + \cdots + x + 1$ ist, wobei $x \in \mathbf{N}$, dann gilt $p \equiv 1 \pmod q$.

(Damit lassen sich *unendlich viele weitere Spezialfälle des Satzes von Dirichlet* bestätigen, nämlich, dass es unendlich viele Primzahlen des Typs $p = qn + 1$ gibt, wobei q prim ist.)

Für allgemeine Problemstellungen, die den Dirichlet'schen Satz nach vielen Seiten erweitern, möchte ich auf die einschlägige Literatur verweisen, darunter besonders [13], Chapt. 3, 4 und 6, und [15], Kap. III und IV.

Dabei geht es u.a. um die Frage der polynomialen "Primzahlerzeugung" (d.h. ob ein Polynom mit *ganzzahlingen* Koeffizienten über der Menge $\mathbf{N}$ bzw. $\mathbf{N}^n$ unendlich viele oder sogar alle Primzahlen als Werte annimmt), und zwar

(i) durch Polynome $P(x)$ in einer Unabhängigen und Grad wenigstens 2.

(Bereits das 'unschuldig' wirkende Polynom $P(x) = x^2 + 1$ führt auf schwierigste Fragen im Zusammenhang mit Klassenzahlen $h(p)$ der quadratischen Körper $\mathbf{Q}(\sqrt{p})$, p prim.)

Bis heute ist kein Polynom P bekannt, für das $P(\mathbf{N})$ unendlich viele Primzahlen enthält, man weiß aber, dass sich bei nichtkonstanten Polynomen unter den Zahlen $|P(n)|$, $n \in \mathbf{N}$, unendlich viele zusammengesetzte befinden.

(ii) durch Polynome $P(x_1, \ldots, x_n)$, die von endlich vielen Variablen abhängen $(n \geqslant 2)$. Für derartige Polynome wurden viele tiefliegende Ergebnisse bewiesen, von denen ich einige anführen möchte.

• *Euler* hat gefunden, dass es gewisse Koeffizienten $d \in \mathbf{N}$ gibt (er nannte sie 'taugliche' Zahlen [= numeri idonei]), für die gilt: Eine ungerade Zahl z ist genau dann eine Primzahl, wenn eine eindeutige Darstellung der Form $z = x^2 + dy^2$ mit $x, y \geqslant 0$ und $\mathrm{ggT}(x, dy) = 1$ besitzt. (Heute weiß man, dass es nur endlich viele derartige Zahlen gibt.)

• Allgemeiner gilt sogar: Sogenennte primitive quadratische Formen $ax^2 + bxy + cy^2$ stellen unendlich viele Primzahlen dar, wenn a, b und c teilerfremd sind.

• Wenn die Absolutwerde (sogar) eines Polynoms $P \in \mathbf{C}[x_1, \ldots, x_n]$ über der Menge $\mathbf{N}^n$ $(n \geqslant 1)$ lauter Primzahlen sind, so ist P konstant.

• Im Zusammenhang mit der Lösung des *zehnten Hilbert'schen Problems*, das die Berechenbarkeit der Lösungen von polynomialen diophantischen Gleichungen zum Thema hat, wurde eine überraschende Einsicht gewonnen (*Matijasevič, Putnam, Davis* und *Robinson*):

Es gibt ein Polynom $P(x_1, \ldots, x_n)$, sodass die *Menge seiner positiven Funktionswerte* über der Menge $\mathbf{N}^n$ *mit der menge* $\mathcal{P}$ *aller Primzahlen zusammenfällt.* (Derartige Polynome wurden auch explizit angegeben. Dabei ist etwa für $n = 26$ der Polynomgrad $d = 25$. Man weiß auch, dass die Größen von n und p 'in indirektem Verhältnis' zueinander stehen.)

(Übrigens wurde in diesem Umfeld von *Jones* im Jahr 1982 ein bemerkenswerter (Meta-) Satz über axiomatisierbare Theorien **T** bewiesen, nämlich: Wenn eine Proposition P in **T** beweisbar ist, dann hat P außerhalb von **T** einen 'Beweis', der aus 100 Additionen und Multiplikationen ganzer Zahlen besteht.)

Bevor wir ins noch weiteren Beweisen des Euklid'schen Satzes zuwenden, sei noch erwähnt, dass das berühmte Polynom $P_{41}(x) = x^2 - x + 41$, das für $x = 0, 1, \ldots, 40$ lauter Primzahlen ergibt, samt seiner entsprechenden Verallgemeinerung $P_q(x) = x^2 - x + q$ mit einem interesanten Faktorisierungsproblem zusammenhängt: Es gibt genau *neun* ganze Zahlen d (sog. *Heegner*-Zahlen), nämlich $d = 1, 2, 3, 7, 11, 19, 43, 67$ und 163, für die die 'ganzen' Zahlen der Form $a + b\sqrt{-d}$ eindeutige Primfaktorzerlegungen zulassen. (Dabei ist sind für $d = 1, 2$ die Zahlen a und b ganze Zahlen, in den sieben übrigen Fällen muss man für a und b auch Hälften von ganzen Zahlen zulassen – vgl. [6], p. 251 ff.) Und genau für die sechs sinnvollen ganzzahligen Werte $q = \frac{1+d}{4}$, d.h. $q = 2, 3, 5, 11, 17$ und 41 erhält man die schon von *Euler* und *Gauß* als einzig möglich vermuteten Polynome $P_q(x)$.

(2) [*Bertrand*] Es zählt zu den schwierigsten Fragen der Zahlentheorie, "gute" Funktionen $f\colon \mathbf{N} \to \mathbf{R}^+$ zu finden, die garantieren, dass im Intervall $(n, n + f(n)]$ 'immer' eine Primzahl liegt (und zwar entweder für alle $n \geqslant 1$ oder auch nur für fast alle $n \in \mathbf{N}$, d.h. für alle $n \geqslant N_f$, wobei die Schranke N_f von f abhängt – dabei ist zwar ihre Existenz gesichert, in den meisten Fällen ist aber N_f nicht effektiv berechenbar.) Das folgende Postulat (dafür wurde von *Erdös* im Alter von 19 Jahren ein besonders schöner Beweis gefunden, vgl. [1], Chapt. 2) zeigt, dass $f(n) = n$ eine solche Funtion ist.

Satz von Bertrand. Für jede natürliche Zahl $n \geqslant 1$ befindet sich unter den Zahlen $n + 1$, $n + 2$, ... , $2n$ eine Primzahl.

Daraus ergibt sich der Satz von Euklid wie folgt: Setzt man für n der reihe nach 1, 2, 2^2, ... , 2^N, ... ein, so ist zwischen jeder dieser Zahlen eine Primzahl und $\mathcal{P}$ daher unendlich. Außerdem erhält man so die noch immer nicht sehr genaue Abschätzung $p_n \leqslant 2^n$.

(Die momentan besten Abschätzungen für die n-te Pimzahl p_n gehen auf *Rosser, Schoenfeld* und *Robin* zurück und lauten $n(\log n + \log\log n - \alpha) < p_n < n(\log n + \log\log n - \beta)$, wobei die erste Ungleichung mit $\alpha = 1.0072629$ für alle $n \geqslant 2$, die zweite dagegen für alle $n \geqslant 20$ zutrifft, wenn $\beta = 0.5$. Man kann auf der rechten Seite sogar $\beta = 0.9385$ wählen, wenn man sich auf $n \geqslant 7022$ beschränkt.)

Über die zuerst genannten Funtionen f weiß man einerseits, dass die momentan beste Potenzfunktion durch $f(n) = n^{0.535+\varepsilon}$ gegeben ist. (Dabei ist $\varepsilon > 0$ beliebig.) Sie liefert für fast alle n Intervalle der gesuchten Art. Andrerseits konnte auch gezeigt werden, dass es eine Teilmenge $M \subset \mathbf{N}$ der Dichte 1 gibt, sodass sogar alle Intervalle $[n, n + n^{1/6+\varepsilon}]$, $\varepsilon > 0$, für alle $n \in M$ eine Primzahl enthalten.

(Weil für $N \geqslant 1$ alle der N aufeinanderfolgenden Zahlen $(N+1)!+2$, $(N+1)!+3$, ... , $(N+1)! + (N+1)$ zusammengesetzt sind, ist unmittelbar einsichtig, dass die oben angesprochenen Funktionen f unbeschränkt sein müssen.)

Man *vermutet* auch, dass zwischen aufeinanderfolgenden Qudratzahlen immer

zwei Primzahlen liegen, während es zwischen aufeinanderfolgenden Kubikzahlen deren vier sind.

Mitunter können die Intervalle auch sehr kurz sein, nämlich bei *Primzahlzwillingen* p und $p+2$, etwa 5 und 7 oder 41 und 43. Man weiß zwar noch nicht, ob es unendlich viele davon gibt, aber es wurde von *Brun* ein verblüffendes resultat bewiesen:

Die Summe $B = \sum_{(p,p+2)\in\mathcal{P}^2} \left(\frac{1}{p} + \frac{1}{p+2}\right)$ aller Kehrwerte (sie wird als "*Brun'sche Konstante*" bezeicnet) der zwillingsweise auftretenden Primzahlen konvergiert. Später wurde mit komplizierten Methoden der analytischen Zahlentheorie sogar der Wert von B bestimmt! (Vgl. zu all dem etwa [9], Chapt. VII–IX, und [13], Chapt. 4.)

F) Der Beweis von Euler und eine Variante davon

Auf *Euler* geht ein einfaches, aber folgenreiches analytisches Argument zurück: Wieder werde angenommen, es gäbe nur die n Primzahlen $p_1, \ldots, p_n$.

(1) [*Euler*] Weil jede Primzahl p der Ungleichung $1/p < 1$ genügt, konvergiert die unendliche geometrische Reihe $1 + \frac{1}{p} + \frac{1}{p^2} + \cdots$ (und hat den Summenwert $\frac{p}{p-1}$). Dammit folgt aber

$$\left(1 + \frac{1}{p_1} + \frac{1}{p_1^2} + \cdots\right) \cdot \ldots \cdot \left(1 + \frac{1}{p_n} + \frac{1}{p_n^2} + \cdots\right) < \infty.$$

Nach dem Fundamentalsatz der Arithmetik hat jede natürliche Zahl z die eindeutige Darstellung $z = p_1^{e_1} \cdot \ldots \cdot p_n^{e_n}$. Deshalb ergibt sich durch Ausmultiplizieren auch, dass das angegebene Produkt der n geometrischen Reihen den endlichen Wert $1 + \frac{1}{2} + \frac{1}{3} + \cdots$ haben muss. (Dies ist jedoch nicht möglich, weil die harmonische Reihe divergiert.)

(2) [*Legendre*] Einen analogen Beweis erhält man, wenn man die n geometrische Reihen $1 + \frac{1}{p_j^2} + \frac{1}{p_j^4} + \cdots = \frac{p_j^2}{p_j^2 - 1}$ betrachtet ($j = 1, 2, \ldots, n$). Mit ihnen erhielte man nun, dass die Summe $\zeta(2) = 1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots$ einen rationalen Wert hätte. (Dies ist aber wegen $\zeta(2) = \pi^2/6$ ein Widerspruch.)

G) Kombinatorische Beweise

Aus der Annahme, dass es nur endlich viele Primzahlen gibt, werden widersprüchliche Abschätzungen zahlentheoretischer Größen abgeleitet. Besonders schön ist folgender Beweis mit der *Euler'schen φ-Funktion*, die für jede natürliche Zahl z die Anzahl der zu z teilfremden $k \in \{1, 2, \ldots, z-1\}$ zählt. Es werde wieder vorausgesetzt, dass $p_1 = 2$, $p_2 = 3$, $\ldots$, p_r alle Primzahlen seien.

(1) Für ihr Produkt $P = p_1 \cdot \ldots \cdot p_r$ müsste dann aber $\varphi(P) = 1$ gelten, was ein Widerspruch zur bakannten Formel $\varphi(P) = (p_1 - 1) \cdot \ldots \cdot (p_r - 1) > 1$ ist.

(2) Jede natürliche Zahl z lässt sich in der Form $z = z_1^2 \cdot k$ schreiben, wobei k quadratfrei ist, d.h. die Gestalt $k = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$ mit Exponenten $e_j \in \{0, 1\}$ hat $(j = 1, \ldots, r)$. Nun ist aber $z_1 \leqslant \sqrt{z}$ und für k gibt es höchsten 2^r Möglichkeiten. Deshalb besteht für die Anzahl z der Elemente in $\{1, 2, \ldots, z\}$ die Ungleichung $z \leqslant \sqrt{z} \cdot 2^r$, die aber für $z \to \infty$ falsch ist.

(Mann kann sogar zeigen, dass der Anteil α_n der quadratfrein Zahlen, die unter den Zahlen 1, 2, ... , n auftreten, der Beziehung $\alpha_n \to 6/\pi^2 = 0.6079\ldots$ $(n \to \infty)$ genügt, es gilt sogar genauer $\alpha_n = \dfrac{6}{\pi^2} + o\Big(\dfrac{1}{\sqrt{n}}\Big)$, wenn $n \to \infty$.)

(3) [*Thue*] Es sein $n, k \geqslant 1$ ganze Zahlen, für die $(1 + n)^k < 2^n$ gelten soll. Wir überlegen, dass es unter den Zahlen $1, 2, 3, \ldots, 2^n$ wenigstens $k+1$ Primzahlen gibt.

Angenommen, es gäbe nur r Primzahlen, wobei $r \leqslant k$ ist. Jede natürliche Zahl z, $1 \leqslant z \leqslant 2^n$, hat eine eindeutige darstellung $z = 2^{e_1} \cdot 3^{e_2} \cdot \ldots \cdot p_r^{e_r}$, wobei entweder $e_1 = n$ und $e_j = 0$ sonst oder $0 \leqslant e_1 < n$, $0 \leqslant e_2 < n$, ... , $0 \leqslant e_r < n$ sind. Daraus erhält man aber für die Anzahl aller betrachteten Zahlen z, dass $2^n \leqslant 1 + n^r < (n + 1)^r \leqslant (n + 1)^k < 2^n$ gelten müsste, also einen Widerspruch. (Für $n = 2k^2$ folgt wegen $1 + 2k^2 < 2^{2k}$, $k \geqslant 1$, dass es wenigstens $k+1$ Primzahlen gibt, die kleiner als $4^{(k^2)}$ sind. Daher gilt die grobe Abschätzung $p_{k+1} < 4^{(k^2)}$.)

H) Fürstenbergs topologische Beweis

Der Menge $\mathbf{Z}$ aller ganzen Zahlen soll in folgender bemerkenswerten Weise eine Topologie aufgeprägt sein:

Für $a, b \in \mathbf{Z}$, $b > 0$, sei $N_{a,b} = \{\, a + bn : n \in \mathbf{Z} \,\}$ (d.h. $N_{a,b}$ ist eine 'zweiseitig unendliche' arithmetische Folge). Eine Menge $O \subset \mathbf{Z}$ heißt offen, wenn entweder $O = \varnothing$ oder es für jedes $a \in O$ ein $b > 0$ gibt, sodass $N_{a,b} \subset O$ erfüllt ist.

Aus dieser Definition erkennt man unmittelbar, dass die Vereiningungsmenge von zwei (bzw. endlich vielen) offenen Mengen O_1 und O_2 wieder offen ist. Sei $a \in O_1 \cap O_2$. Dann gibt es $b_1, b_2 > 0$ mit $N_{a_1,b_1} \subset O_1$ und $N_{a_2,b_2} \subset O_2$. Folglich ist $a \in N_{a,b_1b_2} \subset O_1 \cap O_2$ und die bahaupteten Topologie-Eigenschaften sind nachgewisen. Aus ihnen ergeben sich:

(a) Jede nichtleere offene Menge ist unendlich.

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

Wir müssen nur **(b)** überlegen. Wegen $N_{a,b} = \mathbf{Z} \setminus \bigcup_{k=1}^{b-1} N_{a+k,b}$ ist aber $N_{a,b}$ das Komplement einer offenen Menge.

Angenommen, die Menge $\mathcal{P}$ aller Primzahlen wäre endlich. Weil jede Zahl $z \neq \pm 1$ einen Primteiler p besitzt, also in $N_{0,p}$ enthalten ist, folgt $\mathbf{Z} \setminus \{-1, 1\} = \bigcup_{p \in \mathcal{P}} N_{0,p}$. Nach **(b)** ist deshalb $\mathbf{Z} \setminus \{-1, 1\}$ abgeschlossen. Folglich ist aber $\{-1, 1\}$ im Widerspruch zu **(a)** eine offene Menge.

Abschluss

Zum Abschluss kehren wir noch einmal in die Zahlentheorie zurück.

In der Hoffnung mit diesem Bericht über einen Bruchteil aus der Theorie der Primzahlen beim Leser das Interesse für die eingehendere Beschäftigung mit den "einfachen Zahlen" wachgerufen zu haben, möchte ich abschließend bemerken, dass *Erdös* einen in seiner Einfachheit genialen Beweis der Unendlichkeit von $\mathcal{P}$ gegeben hat, aus dem sich sofort ein weiterer Satz von *Euler* ergibt, nämlich die Divergenz der Summe $\sum_{p\in\mathcal{P}} \frac{1}{p}$. (Vgl. [1], Chapt. 1.)

Zum Ausklang möchte ich folgende **Aufgabe** anbieten (um der eingangs zitierten Ansicht *Finkels* folgend den Leser einzuladen, die "Leiter in die Zahlentheorie" zu erklimmen):

Die Folge aller Zahlen der Form $2^n - 3$, $n = 2, 3, \ldots$ enthält eine unendliche Teilfolge mit paarweise teilerfremden Gliedern. (Vgl. auch [2], S. 98–99.)

REFERENCES

1. M. Aigner and G. M. Ziegler, *Proofs from THE BOOK*, Springer-Verlag, Berlin-Heidelberg, 1998.
2. Š. Arslanagić, *Matematička indukcija*, Otisak, Sarajevo, 2001.
3. P. Basieux, *Die Top Ten der schönsten mathematischen Sätze*, Rowohlt Taschenbuch Verlag, Reinbeck bei Hamburg, 2000.
4. P. Baptist, *Pythagoras – und kein Ende?*, Ernst-Klett-Verlag, Leipzig-Stuttgart-Düsseldorf, 1997.
5. P. S. Bullen, D. S. Mitrinović and P. M. Vasić, *Means and Their Inequalities*, Reidel Publ., Dordrecht, 1988.
6. J. H. Conway and R.K. Guy, *Zahlenzauber*, Birkhäuser Verlag, Basel-Boston-Berlin, 1997.
7. А. Эвнин, *Девятнадцать доказательств теоремы Евклида*, Квант **32** (2001), 1, 35–38.
8. R. L. Graham, D. E. Knuth and O. Patashnik, *Concrete Mathematics*, Addison-Wesley Publ., Reading, Ma.-New York, 1989.
9. D. S. Mitrinović, J. Sándor and B. Crstici, *Handbook of Number Theory*, Kluwer Acad. Publ., Dordrecht-Boston-London, 1996.
10. L. J. Mordell, *Diophantine Equations*, Academic Press, London-New York, 1969.
11. I. Niven and H. S. Zuckermann, *Einführung in die Zahlentheorie*, Bd. I, Bibliograph. Inst., Mannheim-Wien-Zürich, 1976.
12. G. Pólya und G. Szegö, *Aufgaben und Lehrsätze aus der Analysis*, Bd. II, Springer-Verlag, Berlin-Heidelberg-New York, 1971.
13. P. Ribenboim, *The New Book of Prime Number Records*, Springer-Verlag, New York-Berlin-Heidelberg, 1971.
14. W. Schwarz, *Einführung in Methoden und Ergebnisse der Primzahlentheorie*, Bibliograph. Inst., Mannheim-Wien-Zürich, 1969.
15. E. Trost, *Primzahlen*, Birkhäuser Verlag, Basel-Stuttgart, 1968.
16. N. N. Worobjow, *Die Fibonnaccischen Zahlen*, Deutscher Verlag der Wissenschaften, Berlin, 1971.
17. E. W. Wiesstein, *CRC Concise Encyclopedia of Mathematics*, Chapman & Hall/CRC Boca Raton-London-New York-Washington D.C., 1999.
18. `http://www.mathworld.wolfram.com`

19. http://www.utm.edu.research.primes

Š. Arslanagić, University of Sarajevo, Faculty of Science and Mathematics, Department of Mathematics, Zmaja od Bosne 35, 71000 Sarajevo, Bosnia and Herzegovina

E-mail: asefket@pmf.unsa.ba

W. Janous, Ursulinengymnasium, Fürstenweg 86, A-6010 Innsbruck, Österreich

E-mail: walther.janous@tirol.com