Zusammenfassung In diesem Artikel stellen wir Euklids Fundamentalsatz der Zahlentheorie vor und bringen Belege für die Behauptung, dass dieser heute weitgehend unbekannte Satz den Zahlentheoretikern vor Gauß so vertraut war wie uns die Gaußsche Version des Fundamentalsatzes.

In einem zweiten Teil werden wir die Bedeutung von Euklids Fundamentalsatz für die heutige Algebra erläutern. Dabei gehen wir aus von Ringen, in denen das Gaußsche Lemma gilt, und stoßen dabei Begriffe wie den der ganzen Abgeschlossenheit und Dedekinds Prager Satz.

Noname manuscript No.
2(will be inserted by the editor)

Zur Zahlentheorie der Griechen

Franz Lemmermeyer

Received: date / Accepted: date

Teil I. Euklids Fundamentalsatz der Arithmetik

Der Fundamentalsatz der Arithmetik, die Eindeutigkeit der Primfaktorzerlegung in den natürlichen Zahlen $\mathbb{N}$, wurde erstmals von Gauß in seinen Disquisitiones Arithmeticae [14] explizit formuliert und bewiesen. Bisweilen liest man, dieser Satz gehe auf Euklid zurück. Ganz falsch ist das sicher nicht, besser allerdings wäre es, die Frage etwas anders zu stellen: es geht ja in erster Linie nicht darum, ob Euklid wusste, dass sich jede Zahl eindeutig in ihre Primfaktoren zerlegen lässt: den meisten Autoren, die sich z.B. mit der Konstruktion vollkommener und befreundeter Zahlen befassten, waren zumindest Spezialfälle dieses Resultats geläufig, und manche (nach Euklid insbesondere al Farisi (sh. [1]) und Prestet (sh. [15]).) gaben dafür auch Beweise à la Euklid. Aber erst Gauß machte die eindeutige Primzerlegung zu einem Fundamentalsatz.

Interessant ist daher vielmehr, ob Euklid dieses Ergebnis so verstanden hat wie wir, d.h. ob er dessen fundamentalen Charakter erkannt hat. Letzteres war nun zweifellos nicht der Fall. Dies wirft dann die Frage auf, was denn die Grundlage der Euklidischen Zahlentheorie war, und die Antwort darauf wird meist durch den Hinweis auf den fundamentalen Charakter des euklidischen Algorithmus erledigt. Die Hauptergebnisse der euklidischen Zahlentheorie, insbesondere das Euklidische Lemma, wonach irreduzible Elemente prim sind, werden bei Euklid aber alle mit Hilfe der Proposition VII.19 bewiesen. Wir wollen im Folgenden zeigen, dass diese nur wenig bekannte Proposition nicht nur für Euklid fundamental war, sondern von Euler und anderen Zahlentheoretikern als "Ersatz" für die eindeutige Primzerlegung benutzt wurde und selbst heute noch, wenn auch unter anderem Namen, eine gewisse Rolle in der modernen Algebra spielt.

F. Lemmermeyer
Mörikeweg 1, 73489 Jagstzell
E-mail: hb3@ix.urz.uni-heidelberg.de

1 Eindeutige Primzerlegung?

Wenn man liest, dass Euklid die eindeutige Primzerlegung gekannt und bewiesen habe, bezieht sich diese Aussage auf Euklids (vgl. die Euklidausgaben von Thaer [30] und Heath [16]):

> Proposition IX.14. Ist eine Zahl die kleinste, welche von gegebenen Primzahlen geteilt wird, dann wird sie von keinen anderen Primzahlen geteilt außer den ursprünglichen.

Mit anderen Worten: ist $n = \mathrm{kgV}(p_1, \ldots, p_t)$ das kleinste gemeinsame Vielfache[1] der p_j, so sind $p_1, \ldots, p_t$ die einzigen Primfaktoren von n. Anscheinend war es Heath [16, vol. II, p. 402], der darin die eindeutige Primzerlegung gesehen hat: in seinen Kommentaren zu IX.14 schreibt er:

> In other words, a number can be resolved into prime factors in only one way.[2]

Dass Euklid nicht das Produkt, sondern die kleinste durch $p_1, \ldots, p_t$ teilbare Zahl benutzt, liegt daran, dass Euklids geometrische Sprache ihm nur erlaubt hat, von Produkten von zwei (ebene Zahlen) oder drei Zahlen (solide Zahlen) zu sprechen.

Dass er den Beweis exemplarisch an einer Zahl, die durch drei verschiedene Primzahlen teilbar ist, durchführt, entspricht den Gepflogenheiten in der griechischen Mathematik und ist eine Konsequenz der Tatsache, dass den Griechen die Technik der vollständigen Induktion fehlte.

Die wesentliche Schwäche von IX.14 im Vergleich zum Satz von der eindeutigen Primzerlegung ist die Tatsache, dass IX.14 die eindeutige Primzerlegung nur für Produkte verschiedener Primzahlen liefert, also für quadratfreie Zahlen; letztendlich besagt IX.14 von einem Produkt $n = p_1^{a_1} p_2^{a_2} p_3^{a_3}$ nur, dass p_1, p_2 und p_3 die einzigen Primfaktoren von n sind[3].

Trotz dieses Mangels wird Euklids IX.14 ebenso wie heute der Satz von der Eindeutigkeit der Primzerlegung mit "Euklids Lemma" (Prop. VII.30) bewiesen, wonach aus $p \mid ab$ für prime[4] p immer $p \mid a$ oder $p \mid b$ folgt. Was Euklid also von einer vollständigen Formulierung nebst Beweis des Fundamentalsatzes der Arithmetik abgehalten hat, war zum einen sicherlich die mangelhafte Sprache, derer er sich bedienen musste, zum andern aber auch die Tatsache, dass IX.14 für Euklid alles andere als fundamental war und nicht viel mehr als ein kleines Lemma, das er beiläufig erwähnt. Euklid benutzt seine Proposition IX.14 in der Folge an keiner Stelle, und diese Beobachtung allein verbietet es, in diesem Zusammenhang von einem Fundamentalsatz zu sprechen.

Das Fundament der euklidischen Zahlentheorie ist die Existenz des euklidischen Algorithmus, und der Fundamentalsatz, aus dem die zentralen Sätze gewonnen werden, ist Euklids Proposition VII.19, welcher wir uns nun zuwenden wollen.

---

[1] Dass das kgV teilerfremder Zahlen gleich ihrem Produkt ist, folgt aus Euklids Proposition VII.34.

[2] Mit anderen Worten: eine Zahl kann auf nur eine Art und Weise in Primfaktoren zerlegt werden.

[3] Es sei aber hinzugefügt, dass Euklid an anderen Stellen Sätze beweist, mit denen sich IX.14 präzisieren ließe: so wird in Buch VIII u.A. bewiesen, dass die einzigen Teiler einer Primzahlpotenz p^n die Zahlen $1, p, p^2, \ldots, p^{n-1}$ sind (für Euklid teilt keine Zahl sich selbst). Schließlich hat Euklid auch bewiesen, dass die einzigen Teiler der Zahl $2^{p-1}q$ für prime $q = 2^p - 1$ durch $1, 2, 4, \ldots, 2^{p-1}, q, 2q, 4q, \ldots, 2^{p-2}q$ gegeben sind.

[4] Der Begriff der Primzahl bei Euklid stimmt mit dem überein, was man in der heutigen Algebra irreduzibel nennt. Die Eigenschaft aus Euklids Lemma benutzt man dann zur Definition von Primzahlen.

2 Euklids Proposition VII.19

Um Euklids Proposition VII.19 verstehen zu können, benötigen wir seine Definition VII.20:

> Zahlen sind proportional, wenn die erste Zahl dasselbe Vielfache, oder derselbe Teil, oder dieselben Teile, der zweiten ist wie die dritte der vierten.

Dass die erste Zahl dasselbe Vielfache der zweiten ist wie die dritte der vierten bedeutet, dass es eine natürliche Zahl m gibt mit $a = mb$ und $c = md$. Entsprechend bedeutet "derselbe Teil", dass es einen Teiler n von b und d gibt mit $a = \frac{1}{n}b$ und $c = \frac{1}{n}d$; mit $b = nx$ und $d = ny$ liefert dies $a = x$, $b = nx$, $c = y$, $d = ny$. Endlich bedeutet "dieselben Teile" $a = \frac{m}{n}b$ und $c = \frac{m}{n}d$ für natürliche Zahlen m, n mit $n \mid b$ und $n \mid d$.[5] Übersetzt bedeutet dies also:

Definition. Für natürliche Zahlen $a, b, c, d \in \mathbb{N}$ sind die Verhältnisse $a : b$ und $c : d$ proportional (d.h. es gilt $a : b = c : d$) genau dann, wenn es $m, n, x, y \in \mathbb{N}$ gibt mit

$$a = mx, \quad b = nx, \quad c = my, \quad d = ny. \tag{1}$$

So ist z.B. $6 : 2 = 9 : 3$ via $m = 3$, $n = 1$, $x = 2$, und $y = 3$. Damit lautet

> Proposition VII.19. Sind vier Zahlen proportional, dann ist das Produkt der ersten und der vierten gleich dem Produkt der zweiten und der dritten Zahl. Ist das Produkt der ersten und der vierten gleich dem Produkt der zweiten und der dritten Zahl, dann sind die vier Zahlen proportional.

Euklid behauptet also, dass genau dann $a : b = c : d$ ist, wenn $ad = bc$ gilt. In der darauf folgenden Proposition VII.20 zeigt Euklid, dass die minimalen Zahlen a, b mit Verhältnis $c : d$ diese Zahlen c und d teilen, und zwar so, dass $c = am$ und $d = bm$ gilt. In VII.21 und VII.22 schließlich wird gezeigt, dass a und b genau dann die minimalen Zahlen mit $a : b = c : d$ sind, wenn a und b teilerfremd sind.

Wir neigen dazu, Euklids Proportionen von Zahlen mit den modernen Brüchen zu identifizieren (für Euklid waren Proportionen keine Zahlen, und er erklärt auch nicht, wie man Proportionen addiert); in dieser Sprache geht es in den Propositionen VII.19 ff darum zu zeigen, dass sich jeder Bruch eindeutig in maximal gekürzter Form darstellen lässt.

Von Zahlen und Größen

Neben Proportionen von Zahlen behandelt Euklid in Buch V auch Proportionen von Größen; darunter fallen Winkel, Längen, Flächen und Volumina, also Objekte, die sich kontinuierlich ändern können. Alle gleichartigen Größen bei Euklid haben folgende Eigenschaften: man kann sie addieren, und sie verhalten sich archimedisch in folgendem Sinne: sind A und B Größen derselben Art (solche lassen sich in bezug auf ihre Größe vergleichen), so gibt es immer ein $n \in \mathbb{N}$ derart, dass $nB > A$ ist.

[5] Die ersten beiden Fälle würden wir als die Spezialfälle $n = 1$, bzw. $m = 1$ der letzten Definition ansehen; Euklids Zahlbegriff unterscheidet sich aber von unserem: für ihn waren Zahlen echte Vielfache der Einheit 1, und die Einheit keine Zahl.

Für Verhältnisse $A : B$ und $C : D$ von Größen[6] gilt nach einer Eudoxos zugeschriebenen Definition $A : B = C : D$ genau dann, wenn gilt: für jede natürliche Zahl n ist $nA < nB$ ($nA = nB$; $nA > nB$) genau dann, wenn $nC < nD$ ($nC = nD$; $nC > nD$).

Damit lässt sich dann z.B. zeigen, dass sich einem Kreis einbeschriebene ähnliche Polygone zueinander verhalten wie die Quadrate ihrer Seitenlängen (Prop. XII.1), oder dass sich Kreise zueinander verhalten wie die Quadrate ihrer Durchmesser (Prop. XII.2).

Um die Unterschiede der Definition der Proportionalität von Zahlen und Größen deutlich zu machen, stellen wir folgendes fest:

- Euklids Definition der Proportionalität von Zahlen ist nicht nur in $\mathbb{N}$, sondern in beliebigen multiplikativ geschriebenen Monoiden sinnvoll.
- Die Definition der Proportionalität von Größen ist für alle additiv geschriebenen und im obigen Sinne "archimedischen" Monoide sinnvoll.

Prinzipiell ließen sich Zahlen auch als Größen auffassen[7]; Euklid macht das aber nicht. Die manchmal anzutreffende Behauptung, Euklid habe Aussagen über Proportionen von Größen bewusst oder unbewusst auf Zahlen angewandt, scheint mir weitgehend unbegründet zu sein, und passt auch nicht recht zur Tatsache, dass die Lehre der Proportionen von Zahlen deutlich älter[8] ist als diejenige von Größen.

3 Folgerungen aus Euklids VII.19

Euklids VII.19 ist ein auf den ersten Blick unscheinbares Resultat; tatsächlich handelt es sich dabei aber um ein ganz außerordentliches Ergebnis. Im Folgenden wollen wir kurz auf einige bekannte Folgerungen aus VII.19 eingehen. Den Anfang macht

Proposition 1 *Aus VII.19 folgt Euklids Lemma: alle irreduziblen Elemente sind prim.*

Beweis. Sei p irreduzibel und $p \mid bc$, also $pd = bc$. Nach VII.19 gibt es m, n, x, y mit $p = mx$, $b = nx$, $c = my$, und $d = ny$. Da p irreduzibel ist, ist m oder x eine Einheit, und dies impliziert $p \mid b$ im ersten und $p \mid c$ im zweiten Fall.

VII.19 genügt auch zum Beweis der folgenden Verallgemeinerung von Euklids Lemma:

Proposition 2 *Euklids Proposition VII.19 für natürliche Zahlen ist äquivalent mit dem folgenden Resultat: ist $a \mid bc$ und $\mathrm{ggT}(a, b) = 1$, dann gilt $a \mid c$.*

Beweis. Es gelte VII.19. Ist dann $a \mid bc$, also $ad = bc$ für ein $d \in \mathbb{N}$, so gibt es $m, n, x, y \in \mathbb{N}$ mit $a = mx$, $b = nx$, $c = my$, und $d = ny$. Wegen $\mathrm{ggT}(a, b) = 1$ muss daher $x = 1$ sein, folglich ist $a = m$ ein Teiler von $c = my$.

Sei nun $ad = bc$, und setze $m = \mathrm{ggT}(a, b)$. Dann gibt es $x, y \in \mathbb{N}$ mit $a = mx$ und $b = my$. Daher ist $xd = yc$ und $\mathrm{ggT}(x, y) = 1$; dies impliziert $x \mid c$, also $c = nx$ für ein $n \in \mathbb{N}$. Damit ist aber $d = \frac{yc}{x} = ny$.

[6] Hier müssen natürlich A und B, bzw. C und D gleichartige Größen sein.

[7] Denn $\mathbb{N}$ ist ja auch ein additives archimedisches Monoid.

[8] Van der Waerden schreibt in [31] praktisch das komplette Buch VII den Pythagoreern zu; wie wir weiter unten erläutern werden, drängt sich die Definition der Proportionalität von Zahlen fast auf, wenn man sich wie die Pythagoreer mit Harmonielehre und ganzen Zahlen beschäftigt. Dagegen wird die Definition der Proportionalität von Größen allgemein Eudoxos zugeschrieben.

Es ist heutzutage natürlich kein Problem, die Eindeutigkeit der Primfaktorzerlegung mit Hilfe von Prop. 2 (oder dem Euklidschen Lemma) zu beweisen. Unter Zuhilfenahme einer Idee von Zermelo [33] kann man das aber direkt aus Euklids VII.19 herleiten:

Proposition 3 *Die Eindeutigkeit der Zerlegung in irreduzible Elemente folgt aus Euklids VII.19.*

Beweis. Wäre die Eindeutigkeit falsch, so gäbe es eine kleinste natürliche Zahl N mit zwei verschiedenen Faktorisierungen. Sei p ein irreduzibler Faktor von N, und schreibe $N = ph$; entsprechend sei q ein irreduzibler Faktor der zweiten Faktorisierung, und $N = qk$. Aus $ph = qk$ folgt mit VII.19 die Existenz von $m, n, x, y \in \mathbb{N}$ mit $p = mx$, $q = nx$, $k = my$, und $h = ny$. Da p irreduzibel ist, muss $m = 1$ oder $x = 1$ sein. Dann folgt aber $p \mid q$ (und damit $p = q$) im ersten und $p \mid k$ im zweiten Fall. Damit kommt p auch in der zweiten Faktorisierung vor, und Kürzen von p liefert eine natürliche Zahl $M = \frac{N}{p}$ mit zwei verschiedenen Faktorisierungen in irreduzible Elemente: dieser Widerspruch zur Annahme der Minimalität von N beweist den Satz.

Kalmár [19] (vgl. Suranyi [27,28]) nennt Euklids VII.19 den Vierzahlensatz und schreibt ihn Euler zu. Die Verallgemeinerung auf mehr Zahlen (ausgehend von einer Faktorisierung $a_1 \dots a_i = b_1 \cdots b_j$) hat Euler ebenfalls schon gekannt und folgt durch Induktion über die Anzahl der Faktoren aus dem einfachen Vierzahlensatz. Kalmár hat dann bemerkt, dass aus dieser Verallgemeinerung die Eindeutigkeit der Primzerlegung folgt (sh. auch Bell [4,5], Rosenthall [26] und Erdös & Suranyi [9]), und Suranyi [28, S. 44 ff.] gab für den Vierzahlensatz einen geometrischen Beweis. Es scheint bisher niemandem aufgefallen sein, dass der Vierzahlensatz euklidischen Ursprungs ist[9].

Es ist eine leichte Übung, z.B. mit Hilfe des Satzes von der eindeutigen Primzerlegung das folgende Resultat zu beweisen, das in vielen elementaren Untersuchungen über diophantische Gleichungen benutzt wird:

Proposition 4 *Sind $a, b \in \mathbb{N}$ teilerfremd und ist ab ein Quadrat, so sind auch a und b Quadrate.*

Auch diese Proposition ist eine einfache Folgerung aus dem Euklidischen VII.19, wie man leicht nachrechnet (wir werden auf den Beweis in Prop. 9 noch einmal zurückkommen). Gauß hat in den Disquisitiones [14] als erster darauf hingewiesen, dass dieses Ergebnis (bzw. die Verallgemeinerung auf n-te Potenzen) aus der eindeutigen Primzerlegung in $\mathbb{Z}$ folgt. Der Umkehrschluss, dass sich Prop. 4 nur mit Hilfe des Fundamentalsatzes der Arithmetik beweisen lässt, ist oft anzutreffen, aber falsch.

Euler, dem ja oft nachgesagt wird, er hätte die eindeutige Primzerlegung in seinen Arbeiten unbewusst benutzt oder als selbstverständlich angesehen, hat Prop. 4 in seiner ersten Arbeit [10] über diophantische Fragen erwähnt:

> Factum ex duobus pluribusque numeris inter se primis nec quadratum nec cubus nec ulla alia potestas esse potest, nisi singuli factores sint quadrata vel cubi vel eiusmodi aliae potestates.[10]

[9] Wer sich näher mit den Elementen befasst hat, hätte das natürlich auf Anhieb sagen können, aber scheinbar gibt es recht wenige Mathematiker, welche sowohl mit den Elementen, als auch mit der modernen Algebra hinreichend vertraut sind. Selbst Suranyi, der sich in [28] ganz explizit mit griechischer Mathematik befasst, hat den Zusammenhang zwischen Euklids VII.19 und dem Vierzahlensatz übersehen.

[10] Eine Zahl, die aus zwei oder mehr paarweise teilerfremden Faktoren besteht, kann kein Quadrat oder eine Kubikzahl oder eine höhere Potenz sein außer wenn die einzelnen Faktoren Quadrate, Kubikzahlen, oder entsprechende höhere Potenzen sind.

Anstatt einen Beweis zu geben bemerkt er dann:

> Demonstratio huius Lemmatis facilis est atque ab Euclide iam est tradita, ita ut superfluum foret eam hic exponere.[11]

Es ist mir nicht bekannt, auf welches Ergebnis von Euklid sich Euler hier bezieht. Für Quadrate folgt die Behauptung relativ einfach aus Euklids Theorie der ähnlichen ebenen Zahlen (ähnliche ebene Zahlen sind in heutiger Sprechweise Zahlen, deren Produkt ein Quadrat ist), und für höhere Potenzen mit etwas mehr Mühe aus vielen seiner Propositionen im Buch VIII.

Wo wir uns also auf die eindeutige Primzerlegung, d.h. eine einführende Vorlesung in die Zahlentheorie oder die Gaußschen Disquisitiones [14], berufen würden, erledigt Euler das mit einem Verweis auf Euklid. Es scheint mir recht plausibel, dass Euler auch an anderen Stellen, an denen wir eine Lücke sehen, die durch eindeutige Primzerlegung geschlossen werden kann, etwaige Einwände mit einem Hinweis auf Euklid abgetan hätte.

In [11] zum Beispiel führt er zum Studium befreundeter Zahlen die Funktion $\sigma(n)$ aller Teiler von $n \in \mathbb{N}$ ein und zeigt in Lemma 1, dass σ multiplikativ ist, also $\sigma(mn) = \sigma(m)\sigma(n)$ für teilerfremde Zahlen m, n gilt. Hier ist sein Beweis: "Denn das Produkt mn hat erstens die einzelnen Teiler beider Faktoren m und n, und ist dann noch teilbar durch die Produkte der Teiler von m und derjenigen von n. Deshalb ist die Summe aller Teiler von mn gleich dem Produkt von $\sigma(m)$ und $\sigma(n)$." Euler benutzt also das folgende Lemma ohne Beweis:

Lemma 5 *Seien m und n teilerfremd. Dann lässt sich jeder Teiler a von mn eindeutig in der Form $a = rs$ schreiben, wo $r \mid m$ und $s \mid n$ gilt.*

Wir würden dieses Lemma heute ohne zu zögern aus dem Fundamentalsatz der Arithmetik herleiten; Euler hätte dagegen vermutlich auf Euklid verwiesen: Die Existenz von r und s folgt so: $a \mid mn$ bedeutet $ab = mn$ für ein $b \in \mathbb{N}$; Euklids VII.19 liefert die Existenz von $r, s, t, u \in \mathbb{N}$ mit $a = rs$, $b = tu$, $m = rt$ und $n = su$, und die Behauptung folgt. Die Eindeutigkeit ist aber klar: ist $a = rs = r's'$, so ist $r \mid r's'$ und $\mathrm{ggT}(r, s') \mid \mathrm{ggT}(m, n) = 1$, also $r \mid r'$. Ebenso folgt $r' \mid r$.

4 Die Lücke

Die Gültigkeit von Euklids VII.19 ist, wie wir gesehen haben, für die Eindeutigkeit der Zerlegung in irreduzible Elemente in $\mathbb{N}$ verantwortlich. Eine einfache Struktur, in welcher VII.19 nicht mehr richtig ist, ist das Monoid $M = \{1, 5, 9, 13, \ldots\}$ aller natürlichen Zahlen $\equiv 1 \bmod 4$ (Hilbert hat in seiner Vorlesung [18] das Monoid aller natürlichen Zahlen $\equiv 1 \bmod 5$ benutzt, um die Einführung von Idealen zu motivieren). In M gilt offenbar $21 \cdot 21 = 9 \cdot 49$ (diese Gleichung zeigt auch sofort, dass das Analogon von Prop. 4 in M nicht gilt), aber $49 : 21 \neq 21 : 9$; denn aus (1) folgt die Existenz von m, n, x, y mit $49 = mx$, $21 = nx = my$, und $9 = ny$. Da 9 in M irreduzibel ist, muss $n = 1$ (und damit $y = 9$, also $9 \mid my = 21$) oder $y = 1$ (und damit $n = 9$ und ebenfalls $9 \mid nx = 21$).

[11] Der Beweis dieses Lemmas ist leicht und wurde bereits von Euklid her überliefert; es ist daher überflüssig, ihn hier zu geben.

Dagegen zeigt man leicht, dass für $a, b, f \in M$ immer $a : b = af : bf$ gilt. Also ist

$$49 : 21 = 49 \cdot 9 : 21 \cdot 9 = 21 \cdot 21 : 21 \cdot 9 = 21 : 9,$$

wobei wir zweimal die Beobachtung $a : b = af : bf$ angewendet haben. Wie wir aber schon gesehen haben, ist die Gleichung $49 : 21 = 21 : 9$ falsch. An welcher Stelle haben wir den Fehler gemacht? Die Gleichungen $49 : 21 = 21 \cdot 21 : 21 \cdot 9$ und $21 \cdot 21 : 21 \cdot 9 = 21 : 9$ sind, wie man leicht auch direkt nachprüft, zweifellos richtig. Der Fehler in der obigen Argumentation liegt in der Annahme, dass die Gleichheit von Proportionen[12] transitiv ist: aus $a : b = c : d$ und $c : d = e : f$ folgt im allgemeinen nicht, dass auch $a : b = e : f$ ist.

Taisbak hat in [29] herausgefunden, dass Euklid im Beweis seines Fundamentalsatzes VII.19 genau diese Lücke gelassen hat: er hat die Transitivität der Gleichheit benutzt, aber nicht bewiesen. Wie diese Lücke zu schließen ist, kann man bei Taisbak [29] wie auch bei Pengelley & Richman [22] nachlesen. Das einfache Argument beruht darauf zu zeigen, dass man einige der Zahlen im Vierzahlensatz mehr oder weniger "kanonisch" als größte gemeinsame Teiler wählen kann:

Lemma 6 *Sei $a : b = c : d$. Dann gibt es $p, q, r, s \in \mathbb{N}$ mit $a = pr$, $b = qr$, $c = ps$ und $d = qs$, wobei wir $r = \mathrm{ggT}(a, b)$ und $s = \mathrm{ggT}(c, d)$ wählen können.*

Beweis. Aus $a : b = c : d$ folgt die Existenz von Zahlen $m, n, x, y \in \mathbb{N}$ mit (1). Also ist $x \mid \mathrm{ggT}(a, b)$ und $y \mid \mathrm{ggT}(c, d)$, folglich gibt es $i, j \in \mathbb{N}$ mit $\mathrm{ggT}(a, b) = ix$ und $\mathrm{ggT}(c, d) = jy$.

Jetzt behaupten wir $i \mid j$. Aus Symmetriegründen ist dann $j \mid i$, also $i = j$. Aber dann bekommen wir wie gewünscht $c = piy = pjy = p \cdot \mathrm{ggT}(c, d)$ und $d = qiy = qjy = q \cdot \mathrm{ggT}(c, d)$.

Es bleibt $i \mid j$ zu zeigen. Aus $ix \mid a = mx$ erhalten wir $i \mid m$ und $iy \mid my = c$; ähnlich sehen wir $iy \mid ny = d$. Also ist $iy \mid \mathrm{ggT}(c, d) = jy$, und damit $i \mid j$ wie behauptet.

Damit können wir die Transitivität der Gleichheit so zeigen: sei $a : b = c : d$ und $c : d = e : f$. Dann gilt (1) mit $x = \mathrm{ggT}(a, b)$ und $y = \mathrm{ggT}(c, d)$. Lemma 6 zeigt $c = m \cdot \mathrm{ggT}(c, d)$ und $d = n \cdot \mathrm{ggT}(c, d)$. Wenden wir dieses Lemma ein zweites Mal an, so finden wir $e = m \cdot \mathrm{ggT}(e, f)$ und $f = n \cdot \mathrm{ggT}(e, f)$. Aber dann ist sicherlich $a : b = e : f$.

Man beachte, dass Lemma 6 in dem oben angeführten Hilbertschen Monoid M nicht gilt, da in M zwei Zahlen keinen ggT zu haben brauchen. So sind die gemeinsamen Teiler von $3^2 \cdot 7 \cdot 11$ und $3^2 \cdot 7 \cdot 19$ gegeben durch 1, 3^2 und $3 \cdot 7$, aber es gibt keinen größten gemeinsamen Teiler bezüglich der Teilbarkeit, also keinen gemeinsamen Teiler, der durch alle gemeinsamen Teiler teilbar ist.

5 Euklid oder Pythagoras?

Zahlreiche Mathematikhistoriker schreiben Euklids Zugang zur Zahlentheorie den Pythagoreern zu. Diese sind, wie man annimmt, auf dem Weg über die Musik zu ihren

[12] Man könnte versucht sein, das darauf zurückzuführen, dass die Transitivität der Gleichheit bei Euklid ein Axiom ist ("Was demselben gleich ist, ist einander gleich"); allerdings ist das, was wir Gleichheit von Proportionen nennen, keine Gleichheit im Euklidischen Sinne: Euklid definiert nicht die Gleichheit zweier Proportionen $a : b$ und $c : d$, sondern sagt, vier Zahlen seien proportional, wenn es Zahlen wie in (1) gibt. Aus diesem Grund schreiben viele Kommentatoren Euklids nicht $a : b = c : d$, sondern genauer $a : b :: c : d$.

Proportionen gekommen: sie hatten beobachtet, dass die Längen schwingender Saiten in einfachen Verhältnissen zueinander stehen, wenn die entsprechenden Töne harmonisch klingen. So entsprechen die Verhältnisse $1 : 2$ bzw. $2 : 3$ der Oktave bzw. der Quinte.

Eine der ersten Beobachtungen dürfte dann gewesen sein, dass sich gewisse Proportionen vereinfachen lassen: so ist ja $2 : 4 = 1 : 2$. Letztlich führt diese Fragestellung zwangsläufig auf das Ergebnis, dass sich Proportionen eindeutig kürzen lassen: sind m und n minimal mit $a : b = m : n$, so gilt $m \mid a$ und $n \mid b$; genauer: es gibt ein $x \in \mathbb{N}$ mit $a = mx$ und $b = nx$. Das ist aber der Inhalt von Euklids Prop. VII.20. Danach wird in VII.21 gezeigt, dass die minimalen m und n teilerfremd sind.

Hat man VII.20 einmal empirisch entdeckt, und ist $a : b = c : d$, so folgt einerseits $a = mx$ und $b = nx$, andererseits $c = my$ und $d = ny$. Das ist aber gerade die Euklidische Definition der Proportionalität von Zahlen, die sich damit ganz natürlich aus der Beschäftigung mit elementarsten Eigenschaften von Proportionen ergibt.

Nach Meinung von van der Waerden [31] machten die Pythagoreer diesen Vierzahlensatz zur Grundlage ihrer Zahlentheorie, welche Euklid dann später samt Aufbau im wesentlichen unverändert übernahm. Ebenso wie andere Kommentatoren vor und nach ihm hat van der Waerden Euklids Definition der Proportionalität von Zahlen eher als Fehltritt[13] denn als Geniestreich betrachtet. Allerdings zeigen die obigen Betrachtungen und z.B. der Beweis von Lemma 5, dass die Definition einerseits recht natürlich und der Vierzahlensatz zum Beweis fundamentaler Ergebnisse der diophantischen Analysis durchaus geeignet ist.

Außer den von van der Waerden angeführten Argumenten für die Behauptung, Euklids Buch VII gehe auf die Pythagoreer zurück, kann man auch das Fehlen des Beweises der Transitivität der Gleichheit für Proportionen von Zahlen als Beleg dafür auffassen: bei Zugrundelegung der von Eudoxos gegebenen Definition der Gleichheit von Proportionen wird der Beweis der Transitivität der Gleichheit fast trivial. Dennoch hat ihn Euklid in V.11 ausgeführt. Dies mag daran liegen, dass die Lehre der Proportionen von Größen auf Eudoxos zurückgeht, und dass zu dessen Zeit die Einsicht, dass derartige Schritte bewiesen werden müssen, unter den Mathematikern bereits verbreitet war. Es ist meiner Ansicht nach durchaus denkbar, dass die Pythagoreer schlicht übersehen haben, dass die Transitivität der Gleichheit von Proportionen von Zahlen überhaupt nicht trivial ist. Dass auch Euklid das nicht gesehen hat, obwohl er natürlich V.11 kannte, verwundert schon eher, ließe sich aber dadurch erklären, dass er die Zahlentheorie der Pythagoreer ohne große Änderungen in sein Buch VII übernommen hat.

6 Der Vierzahlensatz

Um uns über die Bedeutung des Euklidischen Vierzahlensatzes Klarheit zu verschaffen, nennen wir Integritätsringe, in denen dieser Satz gilt, Rieszsche[14] Ringe. In einem

[13] D. Fowler schreibt z.B. in [12]:

> Commentators rarely point out the unsatisfactory nature of this definition: it is a vivid, though incomplete, description of four numbers in proportion, and not the mathematical criterion needed for the foundation of a theory.

[14] Zafrullah [32] hat diese Ringe prä-Schreiersch genannt; weiter unten werden wir aber sehen, dass die Divisionsgruppe Rieszscher Ringe “Rieszsche Gruppen” im Sinne der Gruppentheorie sind.

Rieszschen Ring R folgt also aus $ad = bc$ mit $a, b, c, d \in R$ die Existenz von $m, n, x, y \in R$ mit $a = mx$, $b = nx$, $c = my$, und $d = ny$.

Ein Element $a \in R$ heißt primal[15], wenn aus $a \mid bc$ für beliebige $b, c \in R$ die Existenz von $r, s \in R$ folgt mit $a = rs$, $r \mid b$, und $s \mid c$. Man beachte, dass 0 und die Einheiten immer primal sind.

Ein Integritätsring ist offenbar genau dann Rieszsch, wenn jedes Element von R primal ist. Das folgende Lemma zeigt, dass in Rieszschen Ringen alle irreduziblen Elemente prim sind:

Proposition 7 *Irreduzible Elemente sind genau dann primal, wenn sie prim sind.*

Beweis. Sei a prim und $a \mid cd$; dann ist oBdA $a \mid c$. Mit $r = a$ und $s = 1$ gilt dann $a = rs$, $r \mid c$ und $s \mid d$, d.h. a ist primal.

Sei nun a irreduzibel und primal. Ist $a \mid cd$, so gibt es r, s mit $a = rs$, $r \mid c$ und $s \mid d$. Da a irreduzibel ist, muss r oder s – sagen wir r – eine Einheit sein. Aus $s \mid d$ folgt dann aber $a \mid d$, und damit ist a prim.

Euklid hat in Prop. VII.19 gezeigt, dass $\mathbb{N}$ Rieszsch ist; sein Beweis, dass irreduzible Elemente in $\mathbb{N}$ prim sind, ist im wesentlichen eine Hälfte des obigen Beweises.

Sieht man sich den Euklidischen Beweis von VII.19 (bzw. dessen Ergänzung durch Taisbak) genauer an, so stellt man fest, dass der Vierzahlensatz in allen GGT-Ringen (dies sind Integritätsringe, in denen je zwei Elemente einen größten gemeinsamen Teiler besitzen) gilt, dass also jeder GGT-Ring Rieszsch ist.

Es sei an dieser Stelle darauf hingewiesen, dass primale Elemente auf der einen und irreduzible bzw. prime Elemente auf der andern Seite von ganz unterschiedlicher Natur sind: so sind Produkte von irreduziblen (bzw. primen) Elementen nicht mehr irreduzibel (bzw. prim), ausgeschlossen den trivialen Fall eines Faktors. Für primale Elemente dagegen gilt:

Lemma 8 *Produkte primaler Elemente sind primal.*

Beweis. Seien $a, b \in R$ primal und $ab \mid c_1c_2$, also $c_1c_2 = abd$. Da a primal ist, gibt es eine Faktorisierung $a = a_1a_2$ mit $a_i \mid c_i$. Schreiben wir $c_i = a_id_i$, so folgt $abd = c_1c_2 = a_1a_2d_1d_2 = ad_1d_2$, also $bd = d_1d_2$. Da b primal ist, gilt $b = b_1b_2$ mit $b_i \mid d_i$.

Damit ist $ab = a_1b_1a_2b_2$ mit $a_ib_i \mid a_id_i = c_i$, und folglich ist ab primal. Mit Induktion folgt dann, dass beliebige Produkte primaler Elemente primal sind.

Jetzt zeigen wir folgende Verallgemeinerung von Prop. 4:

Proposition 9 *Sei R Rieszsch. Gilt dann $ab = c^2$ für $a, b, c \in R$ und sind a und b teilerfremd, dann gibt es eine Einheit $e \in R^\times$ derart, dass ae und be Quadrate in R sind.*

Bemerkung. Obwohl der Begriff eines größten gemeinsamen Teilers zweier beliebiger Ringelemente nur in GGT-Ringen Sinn macht, darf man in beliebigen Integritätsringen von "teilerfremden" Elementen reden: dies sind per definitionem solche, deren gemeinsame Teiler allesamt Einheiten sind. So sind z.B. 2 und 3 teilerfremd in $R = \mathbb{Z}[\sqrt{-5}\,]$, während 6 und $2 + 2\sqrt{-5}$ in R keinen ggT besitzen.

[15] Dieser Begriff geht auf Cohn [7] zurück.

Beweis. (Beweis von Prop. 9) Nach dem Vierzahlensatz gibt es $m, n, x, y \in R$ mit $a = mx$, $b = ny$, und $c = my = nx$. Wendet man den Vierzahlensatz auf die Gleichung $my = nx$ an, so folgt die Existenz von $r, s, t, u \in R$ mit $m = rs$, $y = tu$, $n = rt$, und $x = su$. Mit a und b sind natürlich auch m und n, bzw. x und y teilerfremd, folglich sind r und u Einheiten in R. Mit $e = 1/ru$ ist dann $ae = mxe = rs^2ue = s^2$ und $be = nye = rt^2ue = t^2$.

Auch wenn sich einige von Euler ohne Beweis verwendete Tatsachen mit Euklids Vierzahlensatz schließen lassen, sind Rieszsche Ringe doch nur "fast" faktorielle Ringe. Betrachten wir zwei Faktorisierungen $a_1 \cdots a_m = b_1 \cdots b_n$, so folgt in Rieszschen Ringen nur, dass beide Faktorisierungen eine gemeinsame Verfeinerung besitzen: es existieren Elemente $c_{ij} \in R$ $(1 \le i \le m,\ 1 \le j \le n)$ mit $a_i = c_{i1} \cdots c_{in}$ und $b_j = c_{1j} \cdots c_{mj}$. Für $m = n = 2$ ist dies gerade der Vierzahlensatz, der allgemeine Fall (der durch Induktion aus dem Vierzahlensatz folgt) heißt die "Schreiersche Verfeinerungseigenschaft". Beispielsweise hat der Ring aller ganzen algebraischen Zahlen diese Verfeinerungseigenschaft, ist aber kein faktorieller Ring mangels irreduzibler Elemente.

Integritätsringe, in denen sich jedes von 0 verschiedene Element als Produkt einer Einheit und irreduzibler Elemente schreiben lässt, nennt man atomar. Damit gilt der folgende

Satz 10 *Ein Integritätsring R ist genau dann faktoriell, wenn R Rieszsch und atomar ist.*

Beweis. In Rieszschen Ringen sind irreduzible Elemente prim nach Prop. 7; damit sind Faktorisierungen in irreduzible Elemente bekanntlich eindeutig. Ist umgekehrt R faktoriell, so ist R ein GGT-Ring und damit Rieszsch, und zweitens hat jedes Element $\neq 0$ eine Faktorisierung in irreduzible (sogar prime) Elemente.

Diese Aussage ist (wegen Prop. 7) etwas schwächer als der bekannte Satz, wonach Integritätsringe genau dann faktoriell sind, wenn sie atomar sind und jedes irreduzible Element prim ist.

Der Euklidische Aufbau der Zahlentheorie kann wie folgt schematisiert werden:

$$\text{Euklid} \longrightarrow \text{GGT} \longrightarrow \text{Riesz} \longrightarrow \text{AP},$$

wobei AP für die Gültigkeit des Euklidischen Lemmas steht, also für die Eigenschaft, dass irreduzible Elemente (Atome) prim sind. Allgemeiner kann man folgende Inklusionen zeigen:

$$\begin{array}{ccccccccc} \text{Euklid} & \subset & \text{HI} & \subset & \text{Bezout} & & & & \\ & & \cap & & \cap & & & & \\ & & \text{ZPE} & \subset & \text{GGT} & \subset & \text{Riesz} & \subset & \text{AP} \\ & & \cap & & & & & & \\ & & \text{atomar} & & & & & & \end{array}$$

Hierbei bezeichnen HI Hauptidealringe, ZPE faktorielle Ringe (also solche mit eindeutiger Zerlegung in Prim-Elemente), und AP Ringe, in denen alle Atome (also alle irreduziblen Elemente) prim sind. Bezoutringe sind solche, in denen je zwei Elemente a, b einen ggT besitzen und sich dieser als R-Linearkombination von a und b schreiben

lässt; gleichbedeutend damit ist, dass der Durchschnitt zweier Hauptideale wieder ein Hauptideal ist.

Während Hilbert die euklidische Geometrie auf eine moderne algebraische Grundlage gestellt hat, ist eine entsprechende Untersuchung der euklidischen Zahlentheorie meines Wissens bisher nicht durchgeführt worden. Man kann sich beispielsweise fragen, in welchen Ringen folgendes gilt: sind a und b teilerfremd (also jeder gemeinsame Teiler eine Einheit) und ist $a \mid bc$, dann gilt $a \mid c$. Der erste Teil des Beweises von Prop. 2 zeigt, dass dies in Rieszschen Ringen gilt; der zweite Teil des Beweises benutzt aber die Existenz des ggT, sodass wir nicht schließen können, dass solche Ringe auch Rieszsch sind. Andererseits sind Ringe mit dieser Eigenschaft AP. Man kann nun allgemein die Frage stellen, in welchen Integritätsringen die Propositionen aus Euklids Zahlentheorie gelten ,d.h. welche Axiome man zu ihrem Beweis benötigt.

7 Rieszsche Gruppen

In diesem Abschnitt wollen wir auf einige Verallgemeinerungen des Vierzahlensatzes eingehen. Dazu werden wir etwas allgemeiner Rieszsche Gruppen untersuchen.

Sei R ein Integritätsring mit Quotientenkörper K. Wir erinnern daran, dass $a \mid c$ für $a, c \in K^\times$ bedeutet, dass es ein $b \in R$ gibt mit $ab = c$. Für die Untersuchung von Teilbarkeitseigenschaften sind Einheiten irrelevant; es macht daher Sinn, statt $K^\times$ die Faktorgruppe $G(R) = K^\times / R^\times$ zu betrachten, die wir auch als Gruppe der von (0) verschiedenen gebrochenen Hauptideale auffassen können; die Elemente von $G(R)$ bezeichnen wir vorläufig mit $aR^\times = (a)$. Die Gruppe $G(R)$ ist halbgeordnet durch $(a) \leq (b)$ genau dann, wenn $a \mid b$, d.h. wenn $\frac{b}{a} \in R$ ist. Weiter ist $(a) \leq (b)$ äquivalent mit $(ac) \leq (bc)$ für ein beliebiges $(c) \in G(R)$. Die Menge $G(R)^+ = \{(g) \in G(R) : (g) \geq (1)\}$ aller "positiven" Elemente besteht also aus allen ganzen Hauptidealen $\neq (0)$ und ist offenbar ein Monoid, das aus $R^* = R \setminus \{0\}$ durch Übergang zu Idealen, also durch Identifizieren aller Einheiten entsteht.

Wir wollen nun den Euklidischen Vierzahlensatz für R in diese Sprache übersetzen. Ist $ad = bc$, so gilt $a \mid bc$, folglich $(a) \leq (b)(c)$ für die entsprechenden Hauptideale in $G(R)$. Nach dem Vierzahlensatz existieren $r, s \in R$ mit $a = rs$, $b = ru$, $c = ts$ und $d = tu$. Also gilt $r \mid b$ und $s \mid c$, und damit $(r) \leq (b)$, sowie $(s) \leq (c)$. Daher gilt

Proposition 11 *Sei R ein Integritätsring. Dann gilt der Vierzahlensatz in R genau dann, wenn $G(R)$ die folgende "Fuchssche Interpolationseigenschaft" F_2 besitzt*[16]*: Sind $a, b, c \in G(R)$ und ist $a \leq bc$, dann gibt es eine Faktorisierung $a = rs$ mit $r, s \in G(R)$ derart, dass $r \leq b$ und $s \leq c$ ist.*

Wir werden nun eine Reihe allgemeiner Interpolations- und Verfeinerungseigenschaften von halbgeordneten Gruppen G definieren:

- Die "Fuchssche Interpolationseigenschaft" F_n: Sind a, b_1, …, $b_n \in G^+$, und ist $a \leq b_1 \cdots b_n$, so gibt es $a_i \in G^+$ mit $a = a_1 \ldots a_n$ und $a_i \leq b_i$ für $1 \leq i \leq n$.
- Die "Rieszsche Interpolationseigenschaft" $R_{m,n}$: Sind $a_1, \ldots, a_m$, $b_1, \ldots, b_n \in G$ gegeben mit $a_i \leq b_j$ für alle $1 \leq i \leq m$ und $1 \leq j \leq n$, dann gibt es ein $c \in R$ mit $a_i \leq c \leq b_j$.

[16] Ab jetzt bezeichnen wir die Elemente von $G(R)$ statt (a) einfach mit a.

- Die "Schreiersche Verfeinerungseigenschaft" $S_{m,n}$: Sind $a_1, \ldots, a_m,\ b_1, \ldots, b_n \in G^+$ gegeben mit $a_1 \cdots a_m = b_1 \cdots b_n$, so gibt es Elemente $c_{ij} \in G^+$ $(1 \leq i \leq m,\ 1 \leq j \leq n)$ mit $a_i = c_{i1} \cdots c_{in}$ und $b_j = c_{1j} \cdots c_{mj}$.
- Die "Euklidische Verfeinerungseigenschaft" $E_{m,n}$: Sind $a, b_i, c_j \in G^+$ und $a \leq b_i c_j$ für $i = 1, \ldots, m$ und $j = 1, \ldots, n$, dann gibt es eine Faktorisierung $a = rs$ für $r, s \in G^+$ mit $r \leq b_i$ und $s \leq c_j$ für alle $1 \leq i \leq m$ und $1 \leq j \leq n$.

Die Eigenschaften $R_{2,0}$ und $R_{0,2}$ kann man so auffassen: zu a_1, a_2 gibt es $b, c \in G$ mit $b \leq a_1$ und $a_2 \leq c$; halbgeordnete Gruppen mit dieser Eigenschaft nennt man gerichtet[17]. Die Teilbarkeitsgruppen $G(R)$ von Integritätsringen sind automatisch gerichtet: zu $a_1, a_2 \in K^\times$ gibt es, wie man sofort sieht, immer ein $c \in K^\times$ mit $a_1 \mid c$, $a_2 \mid c$ (man wähle c als das Produkt der (beliebig gewählten) Zähler von a_1 und a_2). Analog findet man immer ein $b \in K^\times$ mit $b \mid a_1$ und $b \mid a_2$.

Jetzt behaupten wir

Satz 12 *Für eine halbgeordnete gerichtete abelsche Gruppe G sind folgende Eigenschaften gleichbedeutend:*

1. *In G gilt $R_{2,2}$;*
2. *In G gilt $R_{m,n}$ für alle $m, n \geq 0$;*
3. *In G gilt F_2;*
4. *In G gilt F_n für alle $n \geq 1$;*
5. *In G gilt $S_{2,2}$;*
6. *In G gilt $S_{m,n}$ für alle $m, n \geq 1$;*
7. *In G gilt $E_{1,1}$;*
8. *In G gilt $E_{m,n}$ für alle $m, n \geq 1$;*
9. *In G gilt $[1, a] \cdot [1, b] = [1, ab]$ (hier ist $[a, b] = \{r \in G : a \leq r \leq b\}$).*

Die Voraussetzung, dass G gerichtet ist, braucht man nur, um von $R_{2,2}$ auf $R_{m,n}$ schließen zu können. Die Beweise sind alle elementar (im wesentlichen vollständige Induktion) und brauchen hier nicht vorgeführt zu werden.

Halbgeordnete abelsche Gruppen, welche die in Satz 12 angeführten Eigenschaften haben, nennt man nach L. Fuchs [13] Rieszsche Gruppen[18]. Diese wurden erstmals von F. Riesz [25] 1940 untersucht, danach von H. Bauer [3] und Birkhoff [6]. In diesen Arbeiten findet man auch Teile des Beweises von Satz 12 und weitere zu 1 – 9 äquivalente Eigenschaften. Die Schreiersche Verfeinerungseigenschaft $S_{m,n}$ ist die Verallgemeinerung des Vierzahlensatzes, welche Kalmár zum Beweis des Fundamentalsatzes der Arithmetik benutzt hat. Im zweiten Teil werden wir schließlich die Euklidische Verfeinerungseigenschaft benötigen.

Abschließende Bemerkungen

Wer sich näher mit der Zahlentheorie Euklids befasst, stößt schnell auf die zentrale Rolle seiner Proposition VII.19, des Vierzahlensatzes. Aber auch wer sich nur für die Geschichte der Zahlentheorie vor Gauß interessiert, muss Euklids zahlentheoretische Bücher, und insbesondere das zentrale Ergebnis VII.19, kennen: der oft formulierte

[17] Da $a \leq b$ zu $b^{-1} \leq a^{-1}$ äquivalent ist, ist eine halbgeordnete Gruppe bereits gerichtet, wenn z.B. $R_{2,0}$ erfüllt ist.

[18] Genauer wird bei Rieszschen Gruppen auf die Forderung der Kommutativität verzichtet; in diesem Fall sind nicht mehr alle Eigenschaften aus Satz 12 gleichbedeutend.

Vorwurf, Euler hätte an manchen Stellen implizit ein Ergebnis von Gauß, nämlich die eindeutige Primzerlegung, verwendet, ist in dieser Form erstens ohnehin etwas anachronistisch, und vor dem Hintergrund von Euklids VII.19 wohl auch nicht haltbar[19]. Mit diesen Bemerkungen soll Euler nicht von jeglicher "Schuld" reingewaschen werden: eine erkleckliche Anzahl seiner Beweise sind nach heutigem Verständnis nicht rigoros, und nicht alle Lücken lassen sich mit Euklid füllen. Der Pauschalvorwurf aber, Euler hätte oft stillschweigend die eindeutige Primzerlegung benutzt, sollte vielleicht doch überdacht werden.

Literatur

1. A.G. Agargün, C.R. Fletcher, *Al-Farisi and the fundamental theorem of arithmetic*, Hist. Math. **21** (1994), 162–173
2. P. Barlow, *An elementary investigation of the theory of numbers, with its application to the indeterminate and Diophantine analysis, the analytical and geometrical division of the circle, and several other curious algebraical and arithmetical problems*, London, J. Johnson and Co, 1811; online zugänglich unter `http://dlxs2.library.cornell.edu/m/math/`
3. H. Bauer, *Geordnete Gruppen mit Zerlegungseigenschaft*, S.-B. Bayer. Akad. Wiss. 1958, 25–36 (1959)
4. E.T. Bell, *Polynomial diophantine systems*, Trans. Amer. Math. Soc. **35** (1933), 903–914
5. E.T. Bell, *Reciprocal arrays and diophantine analysis*, Amer. J. Math. **55** (1933), 50–66
6. G. Birkhoff, *Lattice-ordered groups*, Ann. Math. **43** (1942), 298–331
7. P.M. Cohn, *Bezout rings and their subrings*, Proc. Cambridge Philos. Soc. **65** (1968) 251–264
8. M.J. Collison, *The unique factorization theorem: from Euclid to Gauss*, Math. Mag. **53** (1980), 96–100
9. P. Erdös, J. Suranyi, *Topics in the theory of numbers*, Translated from the Hungarian by Barry Guiduli, New York, Springer, 2003. Originalveröffentlichung 1960
10. L. Euler, *Theorematum quorumdam arithmeticorum demonstrationes*, Comm. Acad. Sci. Petrop. **10** (1738), 1747, pp. 125-146. Opera Omnia I.2, pp. 38–58; online zugänglich unter `EulerArchive.org`.
11. L. Euler, *De numeris amicabilibus*, Opuscula varii argumenti **2** (1750),23–107; Opera Omnia I-2, 86–162; Commentat. Arithm. **1** (1849), 102–145
12. D. Fowler, *Ratio in early Greek mathematics*, Bull. Am. Math. Soc. **1** (1979), 807–846
13. L. Fuchs, *Riesz groups*, Ann. Sc. Norm. Super. Pisa, III. Ser. **19** (1965), 1–34
14. C.F. Gauß, *Disquisitiones Arithmeticae*, G. Fleischer, Leipzig 1801; deutsche Übers. durch H. Maser (1889)
15. C. Goldstein, *On a seventeenth century version of the "fundamental theorem of arithmetic"*, Hist. Math. **19** (1992), 177–187
16. Th. L. Heath (ed.), *The thirteen books of Euclid's Elements*, Translated from the Text of Heiberg with Introduction and Commentary. Cambridge Univ. Press 1908; 2nd ed. Dover 1926
17. M.D. Hendy, *Euclid and the fundamental theorem of arithmetic*, Hist. Math. **2** (1975), 189–191
18. D. Hilbert, *Zahlentheorie*, Vorlesungen 1897–1898, (E. Maus, ed.), Univ. Göttingen (E. Maus, Hrsg.), 1990
19. L. Kalmár, *Über den Fundamentalsatz der Zahlentheorie* (Ungarisch; deutsche Zusammenfassung), Mat. Fiz. Lapok **43** (1936), 27–45
20. A.E. Kramer, *De quibusdam aequationibus indeterminatis quarti gradus*, Diss. 1839
21. F. Lemmermeyer, *Unique Factorization. The Fundamental Theorem of Arithmetic*, Buch in Vorbereitung.
22. D. Pengelley, F. Richman, *Did Euclid need the Euclidean algorithm to prove unique factorization?*, Amer. Math. Monthly, 113 (2006), 196–205

[19] Auch andere Autoren (sogar noch nach Gauß) haben den Vierzahlensatz benutzt, und zwar ohne auf Euler oder Euklid zu verweisen: sh. Barlow [2, p. 401], Kramer [20], oder auch Pépin [23, p. 24], [24, p. 413].

23. Th. Pépin, *Sur un théorème de Legendre*, J. Math. Pures Appl. (3) **5** (1879), 21–31
24. Th. Pépin, *Sur l'équation* $7x^4 - 5y^4 = 2z^2$, J. Math. Pures Appl. (3) **5** (1879), 405–425
25. F. Riesz, *Sur quelques notions fondamentales dans la théorie générale opérations linéaires*, Ann. Math. **41** (1940), 174–206
26. E. Rosenthall, *On some cubic diophantine equations*, Amer. J. Math. **65** (1943), 663–672
27. J. Suranyi, *On the proofs of the fundamental theorem of number theory*, Studies in mathematical analysis and related topics pp. 388–391 Stanford Univ. Press, Stanford, Calif. 1962
28. J. Suranyi, *Schon die alten Griechen haben das gewusst*, in *Grosse Augenblicke aus der Geschichte der Mathematik*, BI Mannheim 1991
29. C.M. Taisbak, *Division and Logos. A theory of equivalent couples and sets of integers*, Acta Historica Scientiarum Naturalium et Medicinalium **25** (1971). Odense University Press, Odense 1971
30. C. Thaer (Hrsg.), *Euklid "Die Elemente"*. Nach Heibergs Text aus dem Griechischen übersetzt und herausgegeben von Clemens Thaer; Darmstadt, Wiss. Buchges. 1980
31. B. van der Waerden, *Die Arithmetik der Pythagoreer I., II.* Math. Ann. **120** (1948), 127–153; ibid. (1949), 676–700
32. M. Zafrullah, *On a property of pre-Schreier domains*, Comm. Algebra **15** (1987), 1895–1920
33. E. Zermelo, *Elementare Betrachtungen zur Theorie der Primzahlen*, Gött. Nachr. (2) **1** (1934), 43–46