4.21 Die zahlentheoretischen Bücher VII, VIII und IX der Elemente

Buch VII der Elemente behandelt auch heute noch aktuelle Begriffe wie Teiler, Vielfache, ggT, kgV und Primzahl und ihre Eigenschaften. Es beginnt mit einer Reihe von Definitionen, von denen uns die meisten bekannt erscheinen. An einigen Stellen weichen sie von den modernen Begriffen ab, was manchmal verwirrend sein kann.

1. *Einheit ist das, wonach jedes Ding eines genannt wird.*

2. *Zahl ist die aus Einheiten zusammengesetzte Menge.*

Anders als heute wird zwischen der Einheit 1 und Zahlen unterschieden, d.h. Zahlen sind die Elemente von $\{a \in \mathbb{N} \mid a \geq 2\}$.

3. *Teil einer Zahl ist eine Zahl, die kleinere von der größeren, wenn sie die größere genau misst;*

5. *Und Vielfaches die größere von der kleineren, wenn sie von der kleineren genau gemessen wird.*

Das entspricht unserer Definition:

$$a \text{ ist Teiler von } b \Leftrightarrow b \text{ ist Vielfaches von } a \Leftrightarrow \exists\, d \in \mathbb{N} : b = ad$$

Ein großer Unterschied ist, dass die Beziehung $a \mid a$ *nicht* als Teilerrelation gilt – die Beziehung $1 \mid a$ aber schon.

11. *Primzahl ist eine Zahl, die sich nur durch die Einheit messen lässt;*

Dementsprechend wird p als Primzahl bezeichnet, wenn p als einzigen Teiler 1 hat.

12. *Gegeneinander prim sind Zahlen, die sich nur durch die Einheit als gemeinsames Maß messen lassen.*

Das entspricht unserer Definition

$$a, b \text{ sind relativ prim} \quad \Leftrightarrow \quad \mathrm{ggT}(a, b) = 1.$$

13. *Zusammengesetzt ist eine Zahl, die sich durch irgendeine (andere) Zahl messen läßt.*

Modern formuliert besagt das

$$a \text{ ist zusammengesetzt} \quad \Leftrightarrow \quad \exists\, d \in \mathbb{N}, 1 < d < a : d \mid a.$$

15. *Man sagt, dass eine Zahl eine Zahl vervielfältige, wenn die zu vervielfältigende so oft zusammengesetzt wird, wieviel Einheiten jene enthält, und so eine Zahl entsteht.*

Hier wird die Multiplikation zweier natürlicher Zahlen als Abkürzung für die fortwährende Addition einer Zahl definiert, d.h.

$$m \cdot n = \underbrace{n + \cdots + n}_{m\text{-mal}}.$$

22. *Eine vollkommene Zahl ist eine solche, die ihren Teilern zusammen gleich ist.*

Also wie bereits im Abschnitt über die Pythagoreer angegeben:

$$n \text{ ist vollkommen} \quad \Leftrightarrow \quad \sum_{d|n, d<n} d = n$$

Die ersten drei Propositionen von Buch VII beschäftigen sich mit dem Bestimmen des größten gemeinsamen Teilers:

Buch VII, 1 *Nimmt man bei Vorliegen zweier ungleicher Zahlen abwechselnd immer die kleinere von der größeren weg, so müssen, wenn niemals ein Rest die vorangehende Zahl genau misst, bis die Einheit übrig bleibt, die ursprünglichen Zahlen gegeneinander prim sein.*

D.h. erhält man bei Anwendung des euklidischen Algorithmus auf a, b irgendwann den Rest 1, so ist $\mathrm{ggT}(a, b) = 1$.

Buch VII, 2 *Zu zwei gegebenen Zahlen, die nicht prim gegeneinander sind, ihr größtes gemeinsames Maß finden.*

Hier wird der euklidische Algorithmus zum Finden des größten gemeinsamen Teilers beschrieben.

Buch VII, 3 *Zu drei gegebenen Zahlen, die nicht prim gegeneinander sind, ihr größtes gemeinsames Maß zu finden.*

Hier wird $\mathrm{ggT}(a, b, c)$ mit Hilfe der Relation

$$\mathrm{ggT}(a, b, c) = \mathrm{ggT}\big(\mathrm{ggT}(a, b), c\big)$$

bestimmt.

Es folgen einige Rechenregeln für Teiler und eine Theorie der Proportionen (jetzt für Zahlen), die viele Ähnlichkeiten mit der aus Buch V für Grössen hat.

Buch VII, 16 *Wenn irgendwelche Zahlen entstehen, indem zwei Zahlen einander vervielfältigen, dann müssen die Ergebnisse einander gleich sein.*

Hier wird die Kommutativität der Multiplikation von Zahlen bewiesen, d.h. $ab = ba$.

Buch VII, 19 *Stehen vier Zahlen in Proportion, dann muss das Produkt aus der ersten und vierten dem Produkt aus der zweiten und dritten gleich sein; und wenn das Produkt aus der ersten und vierten Zahl dem aus der zweiten und dritten gleich ist, dann müssen die vier Zahlen in Proportion stehen.*

Das besagt

$$a : b = c : d \quad \Leftrightarrow \quad ad = bc$$

und erscheint uns wie ein Kriterium für die Gleichheit von zwei Elementen von $\mathbb{Q}^+$.

Buch VII, 23 Aus $\operatorname{ggT}(a, b) = 1$ und $c \mid a$ folgt $\operatorname{ggT}(c, b) = 1$.

Buch VII, 24 Aus $\operatorname{ggT}(a, c) = \operatorname{ggT}(b, c) = 1$ folgt $\operatorname{ggT}(ab, c) = 1$.

Buch VII, 25 Aus $\operatorname{ggT}(a, b) = 1$ folgt $\operatorname{ggT}(a^2, b) = 1$.

Buch VII, 26 Aus

$$\operatorname{ggT}(a, c) = \operatorname{ggT}(b, c) = \operatorname{ggT}(a, d) = \operatorname{ggT}(b, d) = 1$$

folgt $\operatorname{ggT}(ab, cd) = 1$.

Buch VII, 27 Aus $\operatorname{ggT}(a, b) = 1$ folgt

$$\operatorname{ggT}(a^2, b^2) = \operatorname{ggT}(a^3, b^3) = 1.$$

Buch VII, 28

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

Buch VII, 29 Ist p eine Primzahl und $p \nmid a$, so $\mathrm{ggT}(p,a)=1$.

Buch VII, 30 Ist p eine Primzahl und $p \mid (ab)$, so $p \mid a$ oder $p \mid b$.

Buch VII, 32 Eine Zahl a ist entweder eine Primzahl oder es gibt eine Primzahl p, derart dass $p \mid a$.

Buch VII, 34 Bestimme das $\mathrm{kgV}(a,b)$ zweier Zahlen a, b.

Buch VII, 35 Aus $a \mid c$ und $b \mid c$ folgt $\mathrm{kgV}(a,b) \mid c$.

Buch VII, 36 Bestimme das $\mathrm{kgV}(a,b,c)$ dreier Zahlen a, b, c.

In Buch VIII und am Beginn von Buch IX werden ausführlich geometrische Folgen und ihre Eigenschaften behandelt, d.h. Folgen $a_1, a_2, \ldots, a_n$ von Zahlen mit der Eigenschaft

$$a_1 : a_2 = a_2 : a_3 = \cdots = a_{n-1} : a_n$$

Buch IX, 20 *Es gibt mehr Primzahlen als jede vorgelegte Anzahl von Primzahlen.*

Hier wird bewiesen, dass es unendlich viele Primzahlen gibt. Der Beweis ist praktisch derselbe, der auch heute (meistens) verwendet wird. D.h. sind $p_1, \ldots, p_n$ paarweise verschiedene Primzahlen und ist p eine Primzahl mit der Eigenschaft

$$p \mid (p_1 \cdots p_n + 1)$$

so ist p eine Primzahl, die von jeder der Primzahlen $p_1, \ldots, p_n$ verschieden ist.

Ein großer Teil von Buch IX beschäftigt sich mit den Eigenschaften gerader und ungerader Zahlen.

Viele der Propositionen würden wir knapp als Rechnungen im Restklassenring modulo 2 beschreiben.

Buch IX, 21 Sind $a_1, \ldots, a_k$ gerade, so ist $a_1 + \cdots + a_k$ gerade.

Buch IX, 22 Ist k gerade und sind $a_1, \ldots, a_k$ ungerade, so ist $a_1 + \cdots + a_k$ gerade.

Buch IX, 23 Ist k ungerade und sind $a_1, \ldots, a_k$ ungerade, so ist $a_1 + \cdots + a_k$ ungerade.

Buch IX, 24 Ist a gerade und b gerade, so ist $a - b$ gerade.

Buch IX, 25 Ist a gerade und b ungerade, so ist $a - b$ ungerade.

Buch IX, 26 Ist a ungerade und b ungerade, so ist $a - b$ gerade.

Buch IX, 27 Ist a ungerade und b gerade, so ist $a - b$ ungerade.

Buch IX, 28 Ist a ungerade und b gerade, so ist ab gerade.

Buch IX, 29 Ist a ungerade und b ungerade, so ist ab ungerade.

Buch IX, 30 Ist a ungerade, b gerade und $a \mid b$, so gilt $a \mid \frac{b}{2}$.

Buch IX, 31 Ist a ungerade und $\mathrm{ggT}(a, b) = 1$, so ist $\mathrm{ggT}(a, 2b) = 1$.

Buch IX, 35 *Hat man beliebig viele Zahlen in geometrischer Reihe und nimmt man sowohl von der zweiten als auch von der letzten der ersten gleiche weg, dann muss sich, wie der Überschuss der zweiten zur ersten, so der Überschuss der letzten zur Summe der ihr vorangegangenen verhalten.*

Es handelt sich hier – für uns nicht auf den ersten Blick erkennbar – um die Summenformel für die (endliche) geometrische Reihe.

Bezeichnen $a_1, \ldots, a_{n+1}$ die Zahlen in geometrischer Folge (die Bezeichnung *Reihe* in der Übersetzung ist verwirrend, da sie nicht unserem modernen Begriff entspricht), so ist die Behauptung

$$(a_{n+1} - a_1) : (a_1 + \cdots + a_n) = (a_2 - a_1) : a_1$$

oder

$$a_1 + \cdots + a_n = a_1 \frac{a_{n+1} - a_1}{a_2 - a_1}.$$

Da $a_1, \ldots, a_{n+1}$ eine geometrische Folge ist, gilt

$$a_2 : a_1 = a_3 : a_2 = \cdots = a_{n+1} : a_n,$$

d.h. es gibt ein $q \in \mathbb{Q}^+$ mit der Eigenschaft

$$q = \frac{a_2}{a_1} = \frac{a_3}{a_2} = \cdots = \frac{a_{n+1}}{a_n}.$$

Daher ist $a_k = a_1 \cdot q^{k-1}$ für $1 \leq k \leq n+1$ und somit

$$a_1 + \cdots + a_n = a_1(1 + q + q^2 + \cdots + q^{n-1})$$

$$= a_1 \frac{q^n - 1}{q - 1} = a_1 \frac{a_1 q^n - a_1}{a_1 q - a_1} = a_1 \frac{a_{n+1} - a_1}{a_2 - a_1}.$$

Euklid gibt den folgenden eleganten Beweis an: Aus

$$a_2 : a_1 = a_3 : a_2 = \cdots = a_{n+1} : a_n$$

folgt mit Trennung

$$(a_2 - a_1) : a_1 = (a_3 - a_2) : a_2 = \cdots = (a_{n+1} - a_n) : a_n.$$

Daraus erhält man (mittels des Analogons zu Buch V, 12 für Zahlen)

$$\begin{aligned} \big((a_2 - a_1) + (a_3 - a_2) + \cdots + (a_{n+1} - a_n)\big) : (a_1 + \cdots + a_n) \\ = (a_2 - a_1) : a_1, \end{aligned}$$

und nach Kürzen in der Teleskopsumme gerade

$$(a_{n+1} - a_1) : (a_1 + \cdots + a_n) = (a_2 - a_1) : a_1.$$

Buch IX, 36 *Verschafft man sich beliebig viele Zahlen, von der Einheit aus in Reihe nach dem Verhältnis 1:2, bis die Summe aus allem eine Primzahl wird, und bildet die Summe, mit dem letzten Glied vervielfältigt, eine Zahl, so muss das Produkt eine vollkommene Zahl sein.*

D.h. ist

$$1 + 2 + 2^2 + \cdots + 2^{n-1} = 2^n - 1$$

eine Primzahl, so ist

$$2^{n-1}(1 + 2 + \cdots + 2^{n-1}) = 2^{n-1}(2^n - 1)$$

eine vollkommene Zahl. (Wir haben diese Aussage bereits im Abschnitt *Zahlentheorie bei den Pythagoreern* in Teil 4.11 bewiesen.)