Zahlentheorie

1. Die Division

Zu je zwei ganzen Zahlen *n, m* gibt es eine eindeutig bestimmte ganze Zahl *q* und – falls nicht ohnedies

$$n = q \cdot m \tag{1.1}$$

gilt – eine eindeutig bestimmte ganze Zahl $r < m$ mit

$$n = q \cdot m + r \tag{1.2}$$

Es ist klar, dass aus $n = q \cdot m + r$ die Beziehung

$$n : m = q + r : m \tag{1.3}$$

aus der Vorstellung entsteht, beide Seiten der Gleichung werden durch *m* dividiert. Schreibt man statt *r* : *m* die Reihenfolge umgekehrt, kann man wegen $r < m$ den Divisionsprozess für *m* und *r* wiederholen. Man setzt daher symbolisch:

$$n : m = q + r : m = q + \frac{1}{m : r} \tag{1.4}$$

Bei der Division *m* : *r* bestehen wieder beide Möglichkeiten $m : r = q_1$, wenn *r* Teiler von *m* ist, oder $m : r = q_1 + r_1 : r$ mit $r_1 < r$, was in der obigen Symbolik entweder

$$n : m = q + \frac{1}{q_1} \tag{1.5}$$

oder

$$n : m = q + \frac{1}{q_1 + r_1 : r} = q + \frac{1}{q_1 + \dfrac{1}{r : r_1}} \tag{1.6}$$

liefert. Diese *Kettendivision* kann so lange fortgeführt werden, bis eine Division ohne Rest ihren Abbruch herbeizwingt.

(➔ Bsp: 917:700)

$$\ldots = q + \cfrac{1}{q_1 + \cfrac{1}{\ldots + \cfrac{1}{q_k + r_k : r_{k-1}}}} = q + \cfrac{1}{q_1 + \cfrac{1}{\ldots + \cfrac{1}{q_k + \cfrac{1}{r_{k-1} : r_k}}}} = \ldots \tag{1.7}$$

Wie man, sieht werden hier der Reihe nach die folgenden Divisionen durchgeführt:

$$\begin{aligned} &n : m = q + r : m, \rightarrow r < m, \\ &m : r = q_1 + r_1 : r, \rightarrow r_1 < r, \\ &... \\ &r_{k-2} : r_{k-1} = q_k + r_k : r_{k-1}, \rightarrow r_k < r_{k-1}, \\ &r_{k-1} : r_k = q_{k+1} + r_{k+1} : r_k, \rightarrow r_{k+1} < r_k, \\ &... \end{aligned} \tag{1.8}$$

Da die Ungleichungskette

$$m > r > r_1 > ... > r_{k-1} > r_k > r_{k+1} > ... \tag{1.9}$$

in $\mathbb{Z}$ nur endlich viele Reste zwischen *m* und 1 zulässt, muss das Kettendivisionsverfahren einmal dadurch zu Ende kommen, dass der letzte Rest – er sei r_{k-1} genannt – den vorletzten Rest r_{k-2} teilt:

$$r_{k-2} : r_{k-1} = q_k \tag{1.10}$$

(bei $k = 1$ ist $r_{k-1} = r, r_{k-2} = m$). Wegen $r_{k-1} < r_{k-2}$ muss $q_k > 1$ sein und wir erhalten:

$$n : m = q + \cfrac{1}{q_1 + \cfrac{1}{... \cfrac{1}{q_k}}} \tag{1.11}$$

(➔ Bsp: Wurzel aus 2 und 40:7 in etwas anderer Schreibweise)

2. Der größte gemeinsame Teiler

Schreiben wir das Kettendivisionsverfahren in umgekehrter Reihenfolge als

$$\begin{aligned} &r_{k-2} = q_k \cdot r_{k-1}, \\ &... \\ &r_{k-1} = q_{k+1} \cdot r_k + r_{k+1}, \\ &r_{k-2} = q_k \cdot r_{k-1} + r_k, \\ &... \\ &m = q_1 \cdot r + r_1, \\ &n = q \cdot m + r \end{aligned} \tag{2.1}$$

an und gehen wir davon aus, r_{k+1} und r_k wären beide durch die natürliche Zahl *d* teilbar, dann zeigen diese Zeilen, dass *d* auch die Zahlen r_k und r_{k-1}, sowie die Zahlen r_{k-1} und r_{k-2} teilt,

was sich schrittweise schließlich auf die Teilbarkeit von *m* und *n* durch *d* überträgt. Genauso kann die Überlegung in Gegenrichtung gedacht werden: eine gemeinsamer Teiler *d* von *n* und *m* ist auch ein gemeinsamer Teiler von *m* und *r*, von *r* und r_1 und so weiter.

Die erste Zeile zeigt offenkundig, dass $d = r_{k-1}$ der *größte gemeinsame Teiler* von r_{k-2} und r_{k-1} ist; darum erweist sich diese Zahl zugleich als der größte gemeinsame Teiler von *n* und *m*, in Symbolen:

$$r_{k-1} = \mathrm{ggT}(n,m) \,. \tag{2.2}$$

Im Falle $d = 1$ nennen wir die natürlichen Zahlen *n* und *m relativ prim.*

3. Eine Folgerung der Kettendivision

Sind *n* und *m* mit $n > m > 1$ zueinander relativ prime natürliche Zahlen und definiert man bei

$$n : m = q + \cfrac{1}{q_1 + \cfrac{1}{\ldots + \cfrac{1}{q_{k-1} + \cfrac{1}{q_k}}}} \tag{3.1}$$

die zueinander relativ primen natürlichen Zahlen *s* und *r* gemäß

$$q + \cfrac{1}{q_1 + \cfrac{1}{\ldots \cfrac{1}{q_{k-1}}}} = s : r \tag{3.2}$$

(bei $s : r$ fehlt der letzte Teilnenner), dann gilt für ungerade *k*

$$n \cdot r - m \cdot s = 1 \tag{3.3}$$

und für gerade *k*

$$m \cdot s - n \cdot r = 1 \tag{3.4}$$

Euklid folgert hieraus:

Zu je zwei zueinander relativ primen natürlichen Zahlen *n* und *m* kann man natürliche Zahlen *x* und *y* mit

$$n \cdot x - m \cdot y = 1 \tag{3.5}$$

bestimmen.

(➔ Bsp: $100 \cdot x - 131 \cdot y = 1$)

4. Kongruenzen

Zweitausend Jahre nach Euklid entdeckte Gauß bereits als junger Mann, dass eine bemerkenswerte Struktur der natürlichen Zahlen mit diesen Gleichungen verbunden ist. Gauß betrachtete neben der gewöhnlichen Gleichheit zwischen natürlichen Zahlen einen neue Gleichheitsrelation, die er *Kongruenzen* nannte: Ist m eine vorgegebene natürliche Zahl, wird die nicht durch m teilbare natürliche Zahl $n > m$ mit dem Rest r identifiziert, den die Division von n und m ergibt:

$$n \equiv r \pmod{m} \tag{4.1}$$

gelesen als n ist zu r *modulo* m *kongruent*, bedeutet

$$n = q \cdot m + r \tag{4.2}$$

Ist n durch m restlos teilbar, schreibt Gauß

$$n \equiv 0 \pmod{m} \tag{4.3}$$

Allgemein heißen zwei beliebige natürliche Zahle n und r modulo der natürlichen Zahl m, des sogenannten *Moduls*, wenn entweder $n = r$ ist oder $n < r$ die Differenz $r - n$ bzw. bei $n > r$ die Differenz $n - r$ durch m teilbar ist. Es ist klar, dass mit

$$n \equiv r \pmod{m} \text{ und } p \equiv r \pmod{m}$$

auch

$$n \equiv p \pmod{m} \tag{4.4}$$

stimmt und man kann ohne weiteres bestätigen, dass aus

$$n \equiv r \pmod{m} \text{ und } p \equiv s \pmod{m}$$

die Beziehung

$$n + p \equiv r + s \pmod{m} \tag{4.5}$$

und

$$n \cdot p \equiv r \cdot s \pmod{m} \tag{4.6}$$

folgen.

(➔Bsp: Kurzbeweis)

Fasst man mit Gauß die Kongruenzen nach dem Modul m als Gleichheitsbeziehung auf, nennt man die natürlichen Zahlen *Restklassen* modulo m. Es gibt genau m Restklassen modulo m von jeweils einander kongruenten Zahlen: die *Nullklasse* 0, welche zu allen durch m teilbaren Zahlen kongruent ist (und für $m = 1$ die einzige Restklasse ist – in diesem [trivialen] Fall sind alle natürlichen Zahlen zueinander kongruent), für $m > 1$ die *Einsklasse* 1, die zu allen Zahlen natürlichen Zahlen kongruent ist, die bei Division durch m den Rest 1 lassen, und so weiter bis zur $(m - 1)$ – Klasse $m - 1$, zu der eine natürliche Zahl dann kongruent ist, wenn bei ihrer Division durch m der maximale Rest $m - 1$ verbeibt.