

# Einführung in die Algebra Hausaufgabenblatt Nr. 1

Jun Wei Tan\*

*Julius-Maximilians-Universität Würzburg*

(Dated: October 22, 2023)

**Problem 1.** Sei  $G := 2\mathbb{N}^* := \{2n | n \in \mathbb{N}^*\}$  die Menge der positiven geraden Zahlen. Wir nennen  $a \in G$  *zerlegbar*, falls sich  $a$  als Produkt zweier Elemente aus  $G$  schreiben lässt. Ansonsten nennen wir  $a$  *unzerlegbar*. Beispielsweise sind 4 zerlegbar und 6 unzerlegbar. Zeigen Sie:

- (a)  $G$  ist multiplikativ abgeschlossen.
- (b) Jedes  $a \in G$  lässt sich als Produkt unzerlegbarer Elemente aus  $G$  schreiben.
- (c) Selbst wenn man die Reihenfolge der Faktoren nicht berücksichtigt, so ist die Zerlegung nach (b) im Allgemeinen nicht eindeutig.

*Proof.* (a)  $2n \times 2n' = 4nn' = 2(nn')$

- (b) Wir beweisen es per Induktion. Nehme an, dass jede Elemente  $2n, n < k$  entweder unzerlegbar ist, oder als Produkt unzerlegbare Elemente aus  $G$  geschrieben werden kann. Für  $2(1) = 2$  ist es klar - 2 ist unzerlegbar.

Sei  $M_k \subseteq G = \{m \in G | \exists n \in G, mn = 2k\}$

Entweder ist  $M = \emptyset$ , also  $k$  ist unzerlegbar, oder es existiert  $m, n \in G, mn = 2k$ . Weil  $m$  und  $n$  ein Produkt unzerlegbarer Elemente aus  $G$  sind, ist  $2k$  auch ein Produkt unzerlegbarer Elemente.

- (c) Gegenbeispiel:

$$G \ni 1020 = 30 \times 34 = 102 \times 10.$$

□

---

\* jun-wei.tan@stud-mail.uni-wuerzburg.de

**Problem 2.** In dieser Aufgabe stellen wir den Euklidischen Algorithmus zur Berechnung des größten gemeinsamen Teilers vor. Seien hierzu zwei natürliche Zahlen  $a, b \in \mathbb{N}$  mit  $b \neq 0$  vorgelegt. Wir setzen  $r_0 := a, r_1 := b$  und rekursiv für alle  $i \in \mathbb{N}^*$  mit  $r_i \neq 0$ .

$$r_{i+1} := \text{Rest von } r_{i-1} \text{ bei der Division durch } r_i$$

(a) Zeigen Sie, dass es ein  $n \geq 2$  mit  $r_n = 0$  gibt.

Da die Rekursionsformel für  $i = n$  nicht mehr anwendbar ist, bricht die Folge  $(r_i)$  der Reste beim Index  $n$  ab. Daher gibt es nur genau einen Index  $n \geq 2$  mit  $r_n = 0$ . Beweisen Sie nun:

(b) Für alle  $i \in \{1, 2, 3, \dots, n\}$  gilt  $ggT(a, b) = ggT(r_{i-1}, r_i)$ .

(c) Es ist  $ggT(a, b) = r_{n-1}$ .

(d) Berechnen Sie  $ggT(210, 45)$  mit Hilfe des Euklidischen Algorithmus.

*Proof.* (a)

$$r_{i-1} = qr_i + r_{i+1} \quad 0 \leq r_{i+1} < r_i$$

per Definition. Weil  $r_{i-1} < r_i$ , ist die Folge monoton fallend. Da es endlich viele natürliche Zahlen  $k < b$  gibt, muss  $r_n = 0$ .

(b) Wir beweisen:

$$ggT(r_{i-1}, r_i) = ggT(r_i, r_{i+1}).$$

Die gewünschte Ergebnisse folgt daraus per Induktion.

Es gilt  $r_{i-1} - qr_i = r_{i+1}$ . Dann folgt:  $ggT(r_{i-1}, r_i)$  teilt  $r_{i-1}$  und  $r_i$  und daher auch  $r_{i-1} - qr_i$ . Deshalb ist  $ggT(r_{i-1}, r_i)$  auch einen Teiler von  $r_{i+1} \implies ggT(r_{i-1}, r_i) \leq ggT(r_i, r_{i+1})$ .

Weil  $r_{i-1} = qr_i + r_{i+1}$ , ist  $ggT(r_i, r_{i+1})$  einen Teiler von  $r_i$  und  $r_{i+1}$  und daher auch von  $qr_i + r_{i+1}$ . Deshalb ist es auch einen Teiler von  $r_{i-1}$ , und  $ggT(r_i, r_{i+1}) \leq ggT(r_{i-1}, r_i)$

(c) Es gilt

$$r_{n-2} = qr_{n-1} + \cancel{r_n},$$

also  $r_{n-1}$  teilt  $r_{n-2}$ . Daraus folgt

$$ggT(r_{n-1}, r_{n-2}) = r_{n-1} = ggT(a, b).$$

(d)

$$210 = 4 \times 45 + 30$$

$$45 = 1 \times 30 + 15$$

$$30 = 2 \times 15 + 0$$

$$15$$

$$0$$

$$\text{ggT}(210, 45) = 15.$$

□

**Problem 3.** Seien  $p$  und  $q$  zwei ungerade und aufeinanderfolgende Primzahlen, so dass also zwischen  $p$  und  $q$  keine weiteren Primzahlen existieren. Zeigen Sie, dass  $p + q$  ein Produkt von mindestens drei (nicht notwendig verschiedenen) Primzahlen ist.

*Proof.* Sei obdA  $p < q$ . Weil  $p$  und  $q$  ungerade sind, ist  $p + q$  gerade, also  $p + q = 2k, k \in \mathbb{N}$ . Nehme an, dass  $p + q$  ein Produkt von zwei Primzahlen ist, also  $k \in \mathbb{P}$ . Dann gilt

$$p < k < q, \quad k \in \mathbb{P},$$

ein Widerspruch. Deshalb ist  $k \notin \mathbb{P}$  und  $k$  ist ein Produkt von mindestens zwei Primzahlen, also  $p + q$  ist ein Produkt von mindestens drei Primzahlen. □

**Problem 4.** Seien  $n \in \mathbb{N}^*$  und  $a \in \mathbb{Z}$ . Zeigen Sie, dass es genau dann ein  $x \in \mathbb{Z}$  mit  $ax \equiv 1 \pmod{n}$  gibt, wenn  $\text{ggT}(a, n) = 1$  gilt.

*Proof.*  $ax \equiv 1 \pmod{n} \iff ax - 1 = kn, k \in \mathbb{Z}$ , also  $ax - kn = 1$ .

Weil  $\text{ggT}(a, n) = 1$ , gibt es so zwei Zahlen  $a, -k$ , so dass  $ax - kn = 1$  (Lemma von Bezout) □