Einfürung in die Algebra Hausaufgabenblatt Nr. 1

Jun Wei Tan*

Julius-Maximilians-Universität Würzburg

(Dated: October 26, 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 $M = \varnothing$, 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 Berechung des größten gemeinsamen Teilers vor. Seien hierzu zwei natürliche Zahlen $a, b \in \mathbb{N}$ mit $b \neq 0$ vorgelegt. Wir setzen $r_0 := a, r1 := b$ 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 $i \in \{1, 2, 3, \ldots, n\}$ 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 Euklidschen Algorithmus.

Proof. (a)

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

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)

$$
\begin{aligned}
210 &= 4 \times 45 + 30 \\
45 &= 1 \times 30 + 15 \\
30 &= 2 \times 15 + 0 \\
15 & \\
0 &
\end{aligned}
$$

$$ggT(210, 45) = 15.$$

□

Problem 3. (Bonus Problem) Wir wissen von dem Lemma von Bezout, dass für jeder $x, y, \in \mathbb{N}$ es $a, b \in \mathbb{Z}$ gibt, so dass

$$ax + by = ggT(x, y).$$

Zum Beispiel ist $-210 + 5 \times 45 = 15$. Kann man von das Euklidische Algorithmus die Zahlen a, b rechnen?

Proof. Wir berechnen zuerst eine andere Beispiel

$$
\begin{aligned}
427 =& 1 \times 264 + 163 \\
264 =& 1 \times 163 + 101 \\
163 =& 1 \times 101 + 62 \\
101 =& 1 \times 62 + 39 \\
62 =& 1 \times 39 + 23 \\
39 =& 1 \times 23 + 16 \\
23 =& 1 \times 16 + 7 \\
16 =& 2 \times 7 + 2 \\
7 =& 3 \times 2 + 1 \\
2 =& 1 \times 2 + 0
\end{aligned}
$$

Wir kehren zurück:

$$\begin{aligned}
7-1 =& 3\times 2\\
3\times 16 =& 6\times 7 + 3\times 2\\
=& 6\times 7 + (7-1)\\
=& 7\times 7 - 1\\
6\times 16 =& 14\times 7 - 1\\
6\times 16 + 1 =& 14\times 7\\
14\times 23 =& 14\times 16 + 14\times 7\\
=& 14\times 16 + (6\times 16 + 1)\\
=& 20\times 16 + 1
\end{aligned}$$

In der letzte Gleichung bleibt $ggT(427, 264)$ (1). Wir setzen immer wieder ein, bis zu wir eine Gleichung des Forms $427a + 264b = 1$ haben □

Problem 4. Sei $k \in \mathbb{N}$ gegeben. Für welche Zahlen $\mathbb{N} \ni a, b < k$ braucht das Euklidische Algorithismus die meiste Schritte?

Proof. Wir möchten, dass die Folge $r_n \to 0$ nicht so schnell.

$$\begin{aligned}
13 &= 1\times 8 + 5\\
8 &= 1\times 5 + 3\\
5 &= 1\times 3 + 2\\
3 &= 1\times 2 + 1\\
2 &= 1\times 2 + 0\\
1 &\\
0 &
\end{aligned}$$

ist die Fibonacci Folge. □

Problem 5. 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

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

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 6. 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 $ggT(a, n) = 1$ gilt.

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

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