Zahlentheorie

Vorlesungsmitschrift

Prof. Dr. Damaris Schindler

LaTeX-Version von Alex Sennewald

Mathematisches Institut
Georg-August-Universität Göttingen
Sommersemester 2021

Inhaltsverzeichnis

Vorlesungsverzeichnis

Dateiverzeichnis

Dieses Skript stellt keinen Ersatz für die Vorlesungsnotizen von Prof. Schindler dar und wird nicht nochmals von ihr durchgesehen. Im Grunde sind das hier nur meine persönlichen Mitschriften, ich garantiere also weder für Korrektheit noch Vollständigkeit und werde ggf. noch weitere Beispiele und Anmerkungen einfügen. Beweise werde ich in der Regel nicht übernehmen (weil das in LaTeX einfach keinen Spaß macht).

Falls Ihr Korrekturanmerkungen habt könnt Ihr mir gern bei Stud.IP schreiben oder direkt im GitHub Repository einen pull request machen (was vermutlich insgesamt weniger umständlich ist als der Weg über Stud.IP).

glhf,
Alex

1 Primzahlen - Bausteine der ganzen Zahlen

Wo ergeben sich für uns in der Zahlentheorie Unterschiede, wenn wir über $\mathbb{Z}$ anstatt über $\mathbb{Q}$ arbeiten?

Vorlesung 1, 13.04.2021, Datei 1: Primzahlen & Teilbarkeit, Video 1

Beispiel: Seien $a, b \in \mathbb{Z}$, $a \neq 0$. Dann hat die Gleichung

$$ax = b$$

nicht immer eine Lösung $x \in \mathbb{Z}$.

Definition (Teiler)
Seien $a, b \in \mathbb{Z}$. Wir sagen, dass **a *ein Teiler von* b *ist*** $(a \mid b)$, falls es eine ganze Zahl $x \in \mathbb{Z}$ gibt mit $ax = b$.

Lemma 1.1
Seien $a, b, c, d \in \mathbb{Z}$.

i) Falls $d \mid a$ und $d \mid b$, dann $d \mid a + b$.

ii) Ist $d \mid a$, dann auch $d \mid ab$.

iii) Ist $d \mid a$, dann gilt $db \mid ab$.

iv) Gilt $d \mid a$ und $a \mid b$, dann $d \mid b$.

v) Ist $a \neq 0$ und $d \mid a$, dann gilt $|d| \leq |a|$.

Bemerkung: Eine ganze Zahl $a \neq 0$ hat höchstens endlich viele Teiler.

Satz 1.2 (Teilen mit Rest)
Seien $a, b \in \mathbb{Z}, b > 0$. Dann gibt es $q, r \in \mathbb{Z}$ mit

$$a = bq + r,\ 0 \leq r < b.$$

Definition (Primzahl)

Video 2 Eine ganze Zahl $p > 1$, die genau zwei positive Teiler hat (1 und sich selbst), nenn wir ***Primzahl***.

Beispiel: $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, \ldots$

Lemma 1.3
Sei $n \in \mathbb{N}, n > 1$ und sei $p > 1$ der kleinste positive Teiler von n. Dann ist p eine Primzahl. Ist außerdem n nicht prim, dann gilt $p \leq \sqrt{n}$.

Bemerkung: Diese Eigenschaft findet Anwendung im ***Sieb von Eratosthenes***. Dies ist ein einfacher Algorithmus, um schnell alle Primzahlen bis n zu finden. Hierfür definieren wir zunächst die Menge $A = \{z \in \mathbb{Z} \mid 2 \leq z \leq n\}$. Durch Lemma 1.3 genügt es, zusätzlich lediglich die Menge $B = \{k \cdot p \mid k \in \mathbb{Z}, p \leq \sqrt{n} \text{ prim}\}$, also alle Primzahlen $p \leq \sqrt{n}$ und deren Vielfache zu betrachten. Die Differenz $A \setminus B$ beinhaltet dann nur noch alle Primzahlen $\sqrt{n} \leq p \leq n$.

Satz 1.4 (Euklid)
Es gibt unendlich viele Primzahlen.

Satz 1.5 (Hauptsatz der Arithmetik, Primfaktorzerlegung)
Jede natürliche Zahl $n > 1$ kann auf eindeutige Weise als Produkt

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_r^{k_r}$$

mit $k_1, \ldots, k_r \in \mathbb{N}$ und $p_1 < p_2 < \cdots < p_r$ Primzahlen geschrieben werden.

Lemma 1.6

Video 3 *Seien $a, b, p \in \mathbb{N}$ und p eine Primzahl. Angenommen $p \mid ab$, dann gilt $p \mid a$ oder $p \mid b$.*

Satz 1.7
Seien $a, b \in \mathbb{N}$ mit Primfaktorzerlegungen

$$a = p_1^{a_1} \cdot p_2^{a_2} \cdots p_r^{a_r}, \quad b = p_1^{b_1} \cdot p_2^{b_2} \cdots p_r^{b_r}$$

mit $p_1, \ldots, r_p$ Primzahlen, $p_i \neq p_j$ für $i \neq j$ und $a_i, b_i \geq 0 \; \forall i$. Dann gilt genau dann

$b \mid a$, wenn $b_i \leq a_i \; \forall\, i$.

Der größte gemeinsame Teiler

Video 4

Definition (größter gemeinsamer Teiler)
Seien $a, b \in \mathbb{N}$. Der ***größte gemeinsame Teiler von* a *und* b** ist der größte Teiler d mit $d \mid a$ und $d \mid b$. Wir schreiben $\mathrm{ggT}(a, b) = d$ (im englischen $\gcd(a, b)$).

Bemerkung: Seien $a = p_1^{a_1} \cdot p_2^{a_2} \cdots p_r^{a_r}$, $\quad b = p_1^{b_1} \cdot p_2^{b_2} \cdots p_r^{b_r}$ mit $p_1, \ldots, r_p$ Primzahlen, $p_i \neq p_j$ für $i \neq j$ und $a_i, b_i \geq 0 \; \forall\, 1 \leq i \leq r$, und $d \in \mathbb{N}$ mit $d = p_1^{d_1} \cdot p_2^{d_2} \cdots p_r^{d_r}$, wobei $d_i \geq 0 \; \forall\, 1 \leq i \leq r$. Angenommen $d \mid a$ und $d \mid b$, dann $d_i \leq a_i, b_i \; \forall\, 1 \leq i \leq r$. Ist $d = \mathrm{ggT}(a, b)$, dann gilt $d_i = \min(a_i, b_i) \; \forall\, 1 \leq i \leq r$ und

$$\mathrm{ggT}(a, b) = p_1^{\min(a_1, b_1)} \cdot p_2^{|(a_2, b_2)} \cdots p_r^{\min(a_r, b_r)}.$$

Lemma 1.8
Seien $a, b, c, d \in \mathbb{N}$.

i) Ist $d \mid a$ und $d \mid b$, dann $d \mid \mathrm{ggT}(a, b)$.

ii) Angenommen $b \mid ac$ und $\mathrm{ggT}(a, b) = 1$. Dann gilt $b \mid c$.

iii) Sei $a \mid c$, $\; b \mid c$ und $\mathrm{ggT}(a, b) = 1$. Dann $ab \mid c$.

iv) Sei $d = \mathrm{ggT}(a, b)$. Dann gilt $\mathrm{ggT}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Das kleinste gemeinsame Vielfache

Definition (kleinstes gemeinsames Vielfaches)
Seien $a, b \in \mathbb{N}$. Die kleinste natürliche Zahl m mit $a \mid m$ und $b \mid m$ nennen wir das ***kleinste gemeinsame Vielfache von* a *und* b**. Wir schreiben $\mathrm{kgV}(a, b) = m$ (im englischen $\mathrm{lcm}(a, b)$).

Bemerkung: Seien a, b mit den gleichen Primfaktorzerlegungen wie oben. Dann

$$\mathrm{kgV}(a, b) = p_1^{\max(a_1, b_1)} \cdot p_2^{\max(a_2, b_2)} \cdots p_r^{\max(a_r, b_r)}.$$

Bemerke: $\max(a_i, b_i) + \min(a_i, b_i) = a_i + b_i$. Also $ab = \mathrm{ggT}(a, b) \cdot \mathrm{kgV}(a, b)$.

Definition

Seien $a_1, \ldots, a_k \in \mathbb{Z}$, nicht alle gleich null. Der größte gemeinsame Teiler von $a_1, \ldots, a_k$ ist die größte natürliche Zahl d, die jedes der a_i teilt. Wir schreiben $d = \mathrm{ggT}(a_1, \ldots, a_k)$. Analog dazu können wir das kleinste gemeinsame Vielfache von $a_1, \ldots, a_k$ als die kleinste positive ganze Zahl m definieren, die durch jedes der a_i teilbar ist, $m = \mathrm{kgV}(a_1, \ldots, a_k)$.

Der Euklidische Algorithmus

Datei 2, Video 5

Motivation: Seien $a, b \in \mathbb{N}$. Wie können wir $\mathrm{ggT}(a, b)$ schnell berechnen?

Bemerkung: Für $a, b \in \mathbb{N}$ schreibe $a = qb + r$ mit $0 \leq r < b$.

i) Ist $d \in \mathbb{N}$ mit da und $d \mid b$, dann gilt auch $d \mid r$.

ii) Ist $d \mid b$ und $d \mid r$, dann $d \mid a$.

Es folgt: $\mathrm{ggT}(a, b) = \mathrm{ggT}(b, r)$.

Beispiel: $a = 270,\ b = 192$

$$\begin{aligned} 270 &= 1 \cdot 192 + 78 \\ 192 &= 2 \cdot 78 + 36 \\ 78 &= 2 \cdot 36 + 6 \\ 36 &= 6 \cdot 6 + 0 \\ \Longrightarrow \mathrm{ggT}(270, 192) &= \ldots = \mathrm{ggT}(6, 0) = 6 \end{aligned}$$

Im Allgemeinen sieht das wie folgt aus:

$$\begin{aligned} a &= q_0 b + r_1 \\ b &= q_1 r_1 + r_2 \\ r_1 &= q_2 r_2 + r_3 \\ &\ldots \\ r_{k-2} &= q_{k-1} r_{k-1} + r_k \\ r_{k-1} &= q_k r_k + 0 \\ \Longrightarrow \mathrm{ggT}(a, b) &= r_k \end{aligned}$$

Warum endet der Euklidische Algorithmus nach endlich vielen Schritten? In jedem Schritt gilt $0 \leq r_{j+1} < r_j \; \forall \, j$. Da wir mit einer endlichen Zahl b angefangen haben ist auch unser r_1 endlich, und da sich der Rest in jedem Schritt um mindestens 1 verkleinert sind wir nach maximal $|b|$ Schritten fertig.

Der Euklidische Algorithmus ist schnell. Sei $a > b$, dann ist $r_1 < \frac{a}{2}$. Wenn wir dies fortsetzen erhalten wir

$$\begin{aligned} r_2 &< r_1 < \frac{a}{2} \\ r_3 &< \frac{r_1}{2} < \frac{a}{4} \\ r_4 &< \frac{r_2}{2} < \frac{a}{4} \\ &\dots \end{aligned}$$

Nach Vollständiger Induktion folgt

$$r_m < \frac{a}{2^{\frac{m}{2}}} \qquad \forall \, m > 0.$$

Daher $1 \leq r_k < \frac{a}{2^{\frac{k}{2}}}$, also $2^{\frac{k}{2}} < a$ und somit

$$k < 2\frac{\log a}{\log 2}$$

Definitionen