Zahlentheorie

Vorlesungsmitschrift

Prof. Dr. Damaris Schindler

LaTeX-Version von Alex Sennewald

Mathematisches Institut
Georg-August-Universität Göttingen
Sommersemester 2021

Inhaltsverzeichnis

1 Primzahlen - Bausteine der ganzen Zahlen **1**

2 Die Teilerfunktion **7**

3 Kongruenzen **11**

Definitionen **15**

Vorlesungsverzeichnis

Vorlesung 1 vom 13.04.2021 1
Vorlesung 2 vom 16.04.2021 5

Dateiverzeichnis

Datei 1 - Primzahlen & Teilbarkeit 1
Datei 2 - Der Euklidische Algorithmus 4
Datei 3 - Teilerfunktion, Kongruenzen 7
Datei 4 - Inverse Restklassen 12

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 für mich deutlich weniger umständlich ist als der Weg über Stud.IP).

glhf,
Alex

„Die Zahlentheorie ist nützlich, weil man mit ihr promovieren kann."

–Edmund Landau

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_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 1_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 1_3 *Seien $a, b, p \in \mathbb{N}$ und p eine Primzahl. Angenommen $p \mid ab$, dann gilt $p \mid a$ oder $p \mid b$.*

Korollar 1.7

Seien $a_1, \ldots, a_n \in \mathbb{N}$ und p eine Primzahl mit $p \mid a_1 \cdots a_n$. Dann $\exists\, 1 \leq i \leq n$ mit $p \mid a_i$.

Satz 1.8

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 1_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 1.9
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: Der Euklidische Algorithmus, Video 1_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: $a = 270,\ b = 192$

$$\begin{aligned} 270 &= 1 \cdot 192 + 78 \\ 192 &= 2 \cdot 78 + 36 \\ 78 &= 2 \cdot 36 + 6 \\ 36 &= 6 \cdot 6 + 0 \end{aligned}$$

$$\Longrightarrow \mathrm{ggT}(270, 192) = \ldots = \mathrm{ggT}(6, 0) = 6$$

Im Allgemeinen sieht das wie folgt aus:

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

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

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

Der erweiterte Euklidische Algorithmus

Der Euklidische Algorithmus kann noch mehr als lediglich den größten gemeinsamen Teiler zu berechnen. Sein $a, b \in \mathbb{N}$.

Vorlesung 2, 16.04.2021, Video 2_1

$$
\begin{aligned}
a &= q_0 b + r_1 & r_1 &= a - q_0 b \\
0 &\le r_1 < b & & \\
b &= q_1 r_1 + r_2 & r_2 &= b - q_1 r_1 = b - q_1(a - q_0 b) \\
0 &\le r_2 < r_1 & &= a m_2 + b n_2,\ m_2, n_2 \in \mathbb{Z} \\
r_1 &= q_2 r_2 + r_3 & r_3 &= r_1 - q_2 r_2 \\
0 &\le r_3 < r_2 & &= a m_2 + b n_3,\ m_3, n_3 \in \mathbb{Z} \\
& & \dots & \\
r_{k-2} &= q_{k-1} r_{k-1} + r_k & r_k &= a m_k + b n_k \\
0 &\le r_k < r_{k-1} & & m_k, n_k \in \mathbb{Z} \\
r_{k-1} &= q_k r_k + 0 & &
\end{aligned}
$$

Satz 1.10
Seien $a, b \in \mathbb{N}$. Dann gibt es $x, y \in \mathbb{Z}$ mit

$$ax + by = \mathrm{ggT}(a, b).$$

2 Die Teilerfunktion

Datei 3: Teilerfunktion Kongruenzen, Video 2_2

Definition (Teilerfunktion)
Sei $n \in \mathbb{N}$. Wir definieren $d(n)$ als die Zahl der positiven Teiler von n, d.h.

$$d(n) = \sum_{\substack{d|n \\ d\geq 1}} 1.$$

Weiter definieren wir

$$S(n) = \sum_{\substack{d|n \\ d\geq 1 \\ d<n}} d$$

und

$$\sigma(n) = \sum_{\substack{d|n \\ d\geq 1}} d$$

Beispiel: $d(7) = 2,\ d(6) = 4$
Sei p eine Primzahl, dann gilt $d(p) = 2$ und $d(p^k) = k + 1$ für $k \geq 0$.

Bemerkung: $\sigma(n) = S(n) + n$

Definition (perfekte Zahl)
Wir nennen eine natürliche Zahl n ***perfekt***, falls

$$S(n) = n.$$

Beispiel: $6 = 1 + 2 + 3$ ist perfekt. 28 ist perfekt.

Lemma 2.1
Seien $m, n \in \mathbb{N}$ *mit* $\mathrm{ggT}(m, n) = 1$. *Dann gilt*

$$d(mn) = d(m)d(n)$$

und

$$\sigma(mn) = \sigma(m)\sigma(n).$$

Bemerkung: $d(n)$ und $\sigma(n)$ sind sogenannte *multiplikative Funktionen.*

Kennt man die Primfaktorzerlegung von n, so lassen sich diese Funktionen sehr einfach berechnen. Wir wollen nun eine allgemeine Formel für $d(n)$ aufstellen.

Sei $n = p_1^{k_1} \cdots p_r^{k_r}$ mit $p_1 < \cdots < p_3$ Primzahlen, $k_1, \cdots, k_r \geq 0$. Dann gilt nach Lemma 2.1

$$\begin{aligned} d(n) &= d\left(p_1^{k_1} \cdots p_r^{k_r}\right) \\ &= d\left(p_1^{k_1}\right) \cdots d\left(p_r^{k_r}\right) \end{aligned}$$

Es gilt

$$d(p^k) = k + 1,$$

also

$$d(n) = (k_1 + 1)(k_2 + 1) \cdots (k_r + 1).$$

Weiterhin berechnen wir

$$\begin{aligned} \sigma(n) &= \sigma\left(p_1^{k_1}\right) \cdots \sigma\left(p_r^{k_r}\right) \\ \sigma\left(p^k\right) &= 1 + p + p^2 + \cdots + p^k \\ &= \frac{p^{k+1} - 1}{p - 1} \end{aligned}$$

Wir erhalten

$$\sigma(n) = \frac{p_1^{k_1+1} - 1}{p_1 - 1} \cdots \frac{p_r^{k_r+1} - 1}{p_r - 1}$$

Satz 2.2
Sei $n = p_1^{k_1} \cdots p_r^{k_r}$ mit $p_1 < \cdots < p_3$ Primzahlen, $k_1, \cdots, k_r \geq 0$. Dann gilt

$$\begin{aligned} d(n) &= \prod_{i=1}^{r} (k_i + 1) \\ \sigma(n) &= \prod_{i=1}^{r} \frac{p_i^{k_i+1} - 1}{p_i - 1}. \end{aligned}$$

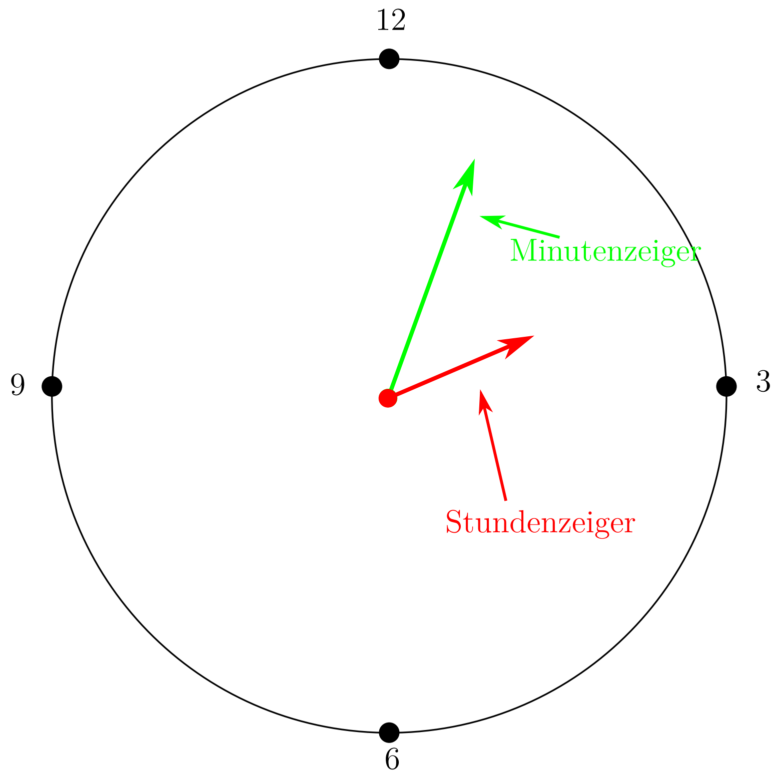
Beispiel: $d(25 \cdot 3) = d(25)d(3) = d(5^2)d(3) = 3 \cdot 2 = 6$

Bemerkung: $S(n)$ ist keine multiplikative Funktion:
$1 = S(2)S(3) \neq S(6) = 6$

3 Kongruenzen

Video 2_3

Beispiel: Die Uhr



Der Minutenzeiger weiß nur, wie viele Minuten es nach einer vollen Stunde ist

Definition (Kongruenz, Kongruenzklasse)
Sei $M \in \mathbb{N},\ M > 1,\ a, b \in \mathbb{Z}$. Wir sagen, dass **a *kongruent zu* b *ist modulo* M**, falls $M \mid (a - b)$, schreibe $a \equiv b \mod M$.
Sei $r \in \mathbb{Z}$. Die Menge aller ganzen Zahlen x mit $x \equiv r \mod M$ nennen wir die ***Kongruenzklasse von* r *modulo* M**.

Beispiel: $7 \equiv 27 \mod 10,\ 4 \equiv 1 \mod 3$

Lemma 3.1

Sei $M > 1$, $M \in \mathbb{N}$, $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ *mit* $a_1 \equiv a_2 \mod M$ *und* $b_1 \equiv b_2 \mod M$. *Dann gilt*

i) $a_1 + b_1 \equiv a_2 + b_2 \mod M$

ii) $a_1 - b_1 \equiv a_2 - b_2 \mod M$

iii) $a_1 b_1 \equiv a_2 b_2 \mod M$

Notation: Schreibe $\mathbb{Z}/M\mathbb{Z}$ für die Menge aller Restklassen modulo M.

Eine Anwendung: Eine natürliche Zahl n ist durch 9 teilbar genau denn, wenn die Summe ihrer Ziffern in der Dezimaldarstellung (also ihre Quersumme) durch 9 teilbar ist.

Beispiel: 43227 ist durch 9 teilbar.

Inverse Restklassen

Datei 4: Inverse Restklassen, Video 2_4

Seien $x, y \in \mathbb{Z}$ mit $2x = 2y$. Die echten Detektive unter uns erkennen, dass man dies einfach zu $x = y$ kürzen kann. Nun ist die Frage, ob das auch funktioniert, wenn wir statt über $\mathbb{Z}$ über dem Restklassenring arbeiten, also ob wir auch bei Kongruenzen kürzen können.

Beispiel:

1. $2x \equiv 2y \mod 4 \overset{?}{\Longrightarrow} x \equiv y \mod 4$
   Nein $\lightning$, z.B. $2 \cdot 3 \equiv 2 \cdot 1 \mod 4,\ 3 \not\equiv 1 \mod 4$

2. $2x \equiv 2y \mod 5 \implies 5 \mid (2x - y)$, d.h. $5 \mid x - y \implies x \equiv y \mod 5$
   oder bemerke, dass $2 \cdot 3 \equiv 1 \mod 5$ und multipliziere die obige Kongruenz mit 3.

Definition (Invertierbare Restklasse)
Sei $M \in \mathbb{N}$, $M > 1$. Wir nennen $a \in \mathbb{Z}$ ***invertierbar modulo* M**, falls es $\exists\, b \in \mathbb{Z}$ gibt mit $ab \equiv 1 \mod M$. In dem Fall nennen wir die Restklasse a (modulo M) invertierbar.

Beispiel: 2 ist invertierbar modulo 25, denn $2 \cdot 13 \equiv 1 \mod 25$.

Satz 3.2
Sei $M \in \mathbb{N},\ M > 1,\ a \in \mathbb{Z}$. Dann ist a invertierbar modulo M genau dann, wenn $\mathrm{ggT}(a, M) = 1$.

Bemerkung: Ist $a \in \mathbb{Z}$ invertierbar modulo M, dann ist jedes Element in der Restklasse $a \mod M$ invertierbar modulo M. Die Menge aller $b \in \mathbb{Z}$ mit $ba \equiv 1 \mod M$ ist eine Restklasse modulo M, schreibe a^{-1} (modulo M) für diese Restklasse. Video 2_5

Sei $a \in \mathbb{Z},\ M \in \mathbb{N},\ M > 1$ mit $\mathrm{ggT}(a, M) = 1$. Wie können wir die inverse Restklasse a^{-1} berechnen?
$\Longrightarrow$ wir verwenden den erweiterten Euklidischen Algorithmus um $x, y \in \mathbb{Z}$ zu finden mit $ax + My = 1$.

Notation: Ist $M > 1$, so schreiben wir $(\mathbb{Z}/M\mathbb{Z})^*$ für die Menge der invertierbaren Restklassen modulo M.

Beispiel:

1. $(\mathbb{Z}/6\mathbb{Z})^* = \left\{\bar{1}, \bar{5}\right\}$, also $|(\mathbb{Z}/6\mathbb{Z})^*| = 2$
2. Sei p prim.

$$(\mathbb{Z}/p\mathbb{Z})^* = \{1, 2, \dots, p-1\} \implies |(\mathbb{Z}/p\mathbb{Z})^*| = p - 1$$

Lemma 3.3
Sei p prim. Dann gilt $(p-1)! \equiv -1 \mod p$.

Definitionen

größter gemeinsamer Teiler, 3

kleinstes gemeinsames Vielfaches, 3
Kongruenzklasse, 11
    Invertierbare Restklasse, 12

perfekte Zahl, 7
Primzahl, 2

Teiler, 1
Teilerfunktion, 7