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 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***[1]. 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[2])

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 $p \mid a_i$.

[1] Nach Eratosthenes von Kryene (zw. 276 und 273 v.Chr. - 194 v.Chr.), ein griechischer Gelehrter

[2] Nach Euklid von Alexandria (3. Jh. v.Chr.), ein griechischer Mathematiker

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 $\mathrm{gcd}(a, b)$).

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, $m = \mathrm{kgV}(a_1, \ldots, a_k)$.

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

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

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

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

$$
\begin{aligned}
a &= q_0 b + r_1 & r_1 &= a - q_0 b \\
0 &\leq r_1 < b & & \\
b &= q_1 r_1 + r_2 & r_2 &= b - q_1 r_1 = b - q_1(a - q_0 b) \\
0 &\leq r_2 < r_1 & &= am_2 + bn_2,\ m_2, n_2 \in \mathbb{Z} \\
r_1 &= q_2 r_2 + r_3 & r_3 &= r_1 - q_2 r_2 \\
0 &\leq r_3 < r_2 & &= am_2 + bn_3,\ m_3, n_3 \in \mathbb{Z} \\
& & &\vdots \\
r_{k-2} &= q_{k-1} r_{k-1} + r_k & r_k &= am_k + bn_k \\
0 &\leq r_k < r_{k-1} & & m_k, n_k \in \mathbb{Z} \\
r_{k-1} &= q_k r_k + 0 & &
\end{aligned}
$$

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.

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

Weiter definieren wir

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

und

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

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*

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

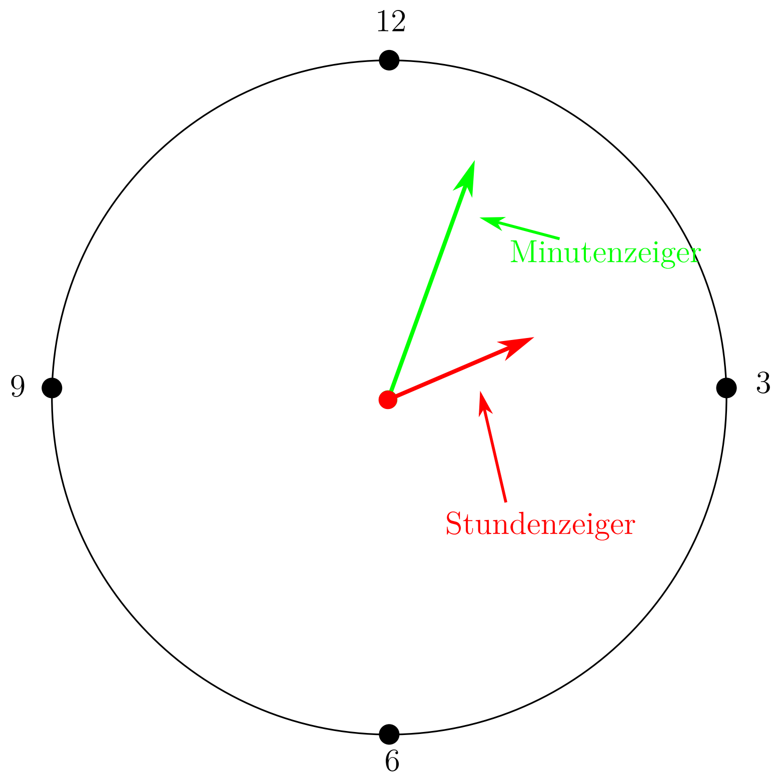
Beispiel: $d(25 \cdot 3) = d(25)d(3) = d(5^2)d(3) = 3 \cdot 2 = 6$

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 $a \equiv b \bmod M$.
Sei $r \in \mathbb{Z}$. Die Menge aller ganzen Zahlen x mit $x \equiv r \bmod M$ nennen wir die ***Kongruenzklasse von* r *modulo* M**.

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

Lemma 3.1
Sei $M > 1,\ M \in \mathbb{N},\ a_1, a_2, b_1, b_2 \in \mathbb{Z}$ mit $a_1 \equiv a_2 \bmod M$ und $b_1 \equiv b_2 \bmod M$. Dann

gilt

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

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

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

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.

3.1 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. $2x \equiv 2y \bmod 4 \overset{?}{\Longrightarrow} x \equiv y \bmod 4$
   Nein $\lightning$, z.B. $2 \cdot 3 \equiv 2 \cdot 1 \bmod 4, \; 3 \not\equiv 1 \bmod 4$

2. $2x \equiv 2y \bmod 5 \implies 5 \mid 2(x-y)$, d.h. $5 \mid x - y \implies x \equiv y \bmod 5$
   <u>oder</u> bemerke, dass $2 \cdot 3 \equiv 1 \bmod 5$ 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 $ab \equiv 1 \bmod M$. In dem Fall nennen wir die Restklasse a (modulo M) invertierbar.

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

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 $a \bmod M$ invertierbar modulo M. Die Menge aller $b \in \mathbb{Z}$ mit $ba \equiv 1 \bmod M$ 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.

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

Lemma 3.3 (Satz von Wilson)
Sei p prim. Dann gilt $(p-1)! \equiv -1 \bmod p$.

3.2 Lineare Kongruenzgleichungen

Fragestellung: Seien $a, b \in \mathbb{Z},\ M \in \mathbb{N}$. Finde alle ganzzahligen Lösungen $x \in \mathbb{Z}$, sodass gilt

$$ax \equiv b \mod M.$$

Vorlesung 3, 20.04.2021, Datei 5: Lineare Kongruenzgleichungen, Video 3_1

Beispiel: i) $5x \equiv 7 \bmod 15$ hat *keine* Lösung

ii) $5x \equiv 25 \bmod 15$, d.h. $15 \mid (5x - 25) = 5(x-5) \iff 3 \mid x - 5$ oder $x \equiv 5 \bmod 3$, d.h. $x \equiv 2 \bmod 3$. Die Lösungen der Kongruenz $5x \equiv 25 \bmod 15$ sind gegeben durch alle $x \in \mathbb{Z}$ der Form $x = 2 + 3k$ mit $k \in \mathbb{Z}$.

Satz 3.4
Seien $a, b \in \mathbb{Z}$, $M \in \mathbb{Z}_{\geq 2}$ *und* $d = \mathrm{ggT}(a, M)$. *Die Gleichung*

$$ax \equiv b \mod M$$

hat genau dann eine Lösung $x \in \mathbb{Z}$, *wenn* $d \mid b$.
Wenn dies gilt, dann ist die Gleichung $ax \equiv b \bmod M$ *äquivalent zu*

$$\frac{a}{d}x \equiv \frac{b}{d} \mod \frac{M}{d}.$$

Diese Gleichung hat eine Lösung, denn

$$\mathrm{ggT}\left(\frac{a}{d}, \frac{M}{d}\right) = 1.$$

3.3 Der Chinesische Restsatz

Datei 6: Der Chinesische Restsatz, Video 3_2

Wir wollen alle $x \in \mathbb{Z}$ finden, die nach Teilen mit Rest durch 2,3,5 die Reste 1,2,3 lassen. Anders formuliert: Finde $x \in \mathbb{Z}$ mit

$$\begin{aligned} x &\equiv 1 \mod 2 \\ x &\equiv 2 \mod 3 \\ x &\equiv 3 \mod 5 \end{aligned}$$

Ist $x \in \mathbb{Z}$ eine Lösung der obigen Kongruenzen, dann auch $x + 30k$ für jedes $k \in \mathbb{Z}$. Sei nun x eine solche Lösung. Dann gilt $x \equiv 3 \bmod 5$, schreibe $x = 3 + 5u$ mit $u \in \mathbb{Z}$. Es muss außerdem gelten

$$3 + 5u \equiv 2 \mod 3,$$

d.h. $2u \equiv 2 \bmod 3 \iff u \equiv 1 \bmod 3$, also $u = 1 + 3v$ mit $v \in \mathbb{Z}$, schreibe also

$$\begin{aligned} x &= 3 + 5(1 + 3v) \\ &= 8 + 15v. \end{aligned}$$

Zuletzt betrachten wir nun

$$8 + 15v \equiv 1 \mod 2.$$

Daraus folgt, dass v ungerade ist, d.h. $v = 1 + 2w$ mit $w \in \mathbb{Z}$. Wir erhalten

$$\begin{aligned} x &= 8 + 15(1 + 2w) \\ &= 23 + 30w, \quad w \in \mathbb{Z}. \end{aligned}$$

Im Allgemeinen:

Seien $c_1, \ldots, c_n \in \mathbb{Z},\ m_1, \ldots, m_n \in \mathbb{Z}_{\geq 2}$. Finde alle $x \in \mathbb{Z}$ mit

$$\begin{aligned} x &\equiv c_1 \mod m_1 \\ x &\equiv c_2 \mod m_2 \\ x &\equiv c_n \mod m_n \end{aligned} \tag{$*$}$$

Achtung: Es ist zu beachten, dass es manchmal keine Lösung gibt, z.B. bei

$$\begin{aligned} x &\equiv 1 \mod 3 \\ x &\equiv 2 \mod 9. \end{aligned}$$

Dies rührt daher, dass wir bisher keine Annahmen über die Module getroffen haben, was wir später noch für den chinesischen Restsatz tun werden. Zunächst fassen wir unsere Vorüberlegungen, dass sich unsere Lösungsmenge durchs kleinste gemeinsame Vielfache der Module ergibt, in folgendem Lemma zusammen:

Lemma 3.5
Sei $x_0 \in \mathbb{Z}$ eine Lösung zum System $*$. Dann besteht die gesamte Lösungsmenge des Systems aus der Restklasse $x_0 \bmod M$ mit $M = \mathrm{kgV}(m_1, \ldots, m_n)$.

Satz 3.6 (Chinesischer Restsatz)
Wir benutzen die gleiche Notation wie im System $*$. Angenommen, $\mathrm{ggT}(m_i, m_j) = 1$ für $i \neq j$, dann hat das System $*$ genau eine Restklasse modulo $m_1 \cdots m_n$ als Lösung. Video 3_3

4 Die Eulersche φ-Funktion

[1]

Datei 7: Eulersche φ-Funktion, Video 3_4

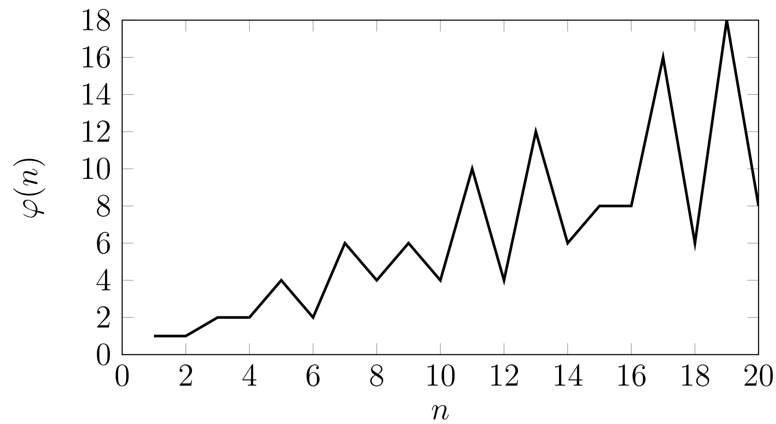
Ordnungen und Primitivwurzeln

Fragestellung: Sei $M \geq 2$. Wie viele invertierbaren Restklassen gibt es modulo M?

Notation: Wir schreiben

$$\varphi(M) = |(\mathbb{Z}/M\mathbb{Z})^*| = |\{0 < a \leq M \mid \mathrm{ggT}(a, M) = 1\}|.$$

Beispiel: i) $\varphi(2) = 1, \varphi(3) = 2, \varphi(4) = 2, \varphi(5) = 4, \varphi(6) = 2$



ii) Sei p eine Primzahl. Dann ist $\varphi(p) = p - 1$.

iii) Sei $k \geq 1$ und p prim. Dann gilt

$$\begin{aligned}\varphi(p^k) &= p^k - \left|\left\{0 < a \leq p^k \mid \mathrm{ggT}\left(a, p^k\right) > 1\right\}\right| \\ &= p^k - p^{k-1}\end{aligned}$$

[1] Nach Leonhard Euler (1707-1783), ein Schweizer Mathematiker, Physiker, Astronom, Geograph, Logiker und Ingenieur

Eine Beobachtung:

$$\begin{aligned}\varphi(1)+\varphi(p)+\varphi(p^2)+\cdots+\varphi(p^k) &= 1+(p-1)+(p^2-p)+\cdots+(p^k-k^{k-1})\\ &= p^k\end{aligned}$$

Satz 4.1
Sei $n \in \mathbb{Z}$. Dann gilt

$$\sum_{d|n} \varphi(d) = n.$$

Nun wollen wir uns mit der Berechnung der Eulerschen φ-Funktion beschäftigen. Für Primzahlpotenzen haben wir das schon getan und wollen dies jetzt auf allgemeine natürliche Zahlen anhand ihrer Primfaktorzerlegung fortsetzen.

Satz 4.2
Video 3_5 *φ ist eine multiplikative Funktion, d.h. für $m, n \in \mathbb{N}$ mit $\operatorname{ggT}(m,n)=1$ gilt*

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

Korollar 4.3
Sei $m = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ mit $p_1 < p_1 < \cdots < p_r$ Primzahlen und $k_i \geq 0$ für $1 \leq i \leq r$. Dann gilt

$$\varphi(m) = \prod_{i=1}^{r} \left(p_i^{k_1} - p_i^{k_i-1}\right)$$

oder

$$\varphi(m) = m \cdot \prod_{\substack{p|m \\ p \text{ prim}}} \left(1 - \frac{1}{p}\right).$$

Vorlesung 4, 23.04.2021, Datei 8: Kleiner Satz von Fermat, Video 4_1

Satz 4.4 (Fermats[2] kleiner Satz)
Sei $a \in \mathbb{Z}$, p eine Primzahl. Dann gilt

$$a^p \equiv a \mod p.$$

Ist $p \nmid a$, dann gilt

$$a^{p-1} \equiv 1 \mod p.$$

[2]Nach Pierre de Fermat (1607-1665), ein französischer Mathematiker und Jurist

Satz 4.5 (Euler)
Sei $M \geq 2,\ a \in \mathbb{Z}$ *mit* $\mathrm{ggT}(a, M) = 1$*. Dann gilt*

$$a^{\varphi(M)} \equiv 1 \mod M.$$

Bemerkung: $(\mathbb{Z}/M\mathbb{Z})^*$ ist eine Gruppe der Ordnung $\varphi(M)$. Ist $a \in (\mathbb{Z}/M\mathbb{Z})^*$, dann gilt $a^{\varphi(M)})1$ in $(\mathbb{Z}/M\mathbb{Z})^*$.

4.1 Ordnungen

Sei $M \in \mathbb{Z}_{\geq 2},\ a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, M) = 1$. Wir wissen bereits Datei 9: Ordnungen, Video 4_2

$$a^{\varphi(M)} \equiv 1 \mod M.$$

Sei $E = \{k \in \mathbb{N} \mid a^k \equiv 1 \bmod M\}$. Dann ist $E \neq \emptyset$.

Definition (Ordnung)
Das kleinste Element in E nennen wir die ***Ordnung von* a *modulo* M**.

Notation: $\mathrm{ord}_M(a)$

Beispiel: Seien $M = 5,\ a = 2$. Für welche $k \in \mathbb{N}$ gilt $2^k \equiv 1 \bmod 5$?

$$2^1 \equiv 2,\ 2^2 \equiv 4,\ 2^3 \equiv 3,\ 2^4 \equiv 4 \mod 5$$

Also gilt $\mathrm{ord}_5\, 2 = 4$.

Lemma 4.6
Sei $M \in \mathbb{Z}_{\geq 2},\ a \in \mathbb{Z}$ *mit* $\mathrm{ggT}(M, a) = 1$*. Angenommen* $a^k \equiv 1 \bmod M$*. Dann gilt*

$$\mathrm{ord}_M\, a \mid k.$$

Wir betrachten zunächst eine Verschärfung des Satzes von Euler (4.5): Video 4_3
Sei $M \in \mathbb{Z}_{\geq 2}$ von der Form

$$M = p_1^{k_1} \cdots p_r^{k_r}$$

mit $p_1 < \cdots < p_r$ prim und $k_1, \ldots, k_r \geq 1$. Setze

$$\lambda(M) = \mathrm{kgV}_{1 \leq i \leq r} \left(p_1^{k_i} - p_i^{k_i - 1} \right) = \mathrm{kgV}_{1 \leq i \leq r}\, \varphi\left(p_i^{k_i} \right)$$

Vergleiche mit

$$\varphi(M) = \prod_{i=1}^{r} \left(p_1^{k_i} - p_i^{k_i-1}\right)$$

Unser Ziel ist nun, zu zeigen, dass wir im Satz von Euler $\varphi(M)$ einfach durch $\lambda(M)$ ersetzen können, was kleiner als $\varphi(M)$ sein kann.

Satz 4.7
Sei $M \in \mathbb{Z}_{\geq 2}$ wie oben, d.h.

$$M = p_1^{k_1} \cdots p_r^{k_r}$$

mit $p_1 < \cdots < p_r$ prim und $k_1, \ldots, k_r \geq 1$. Sei $a \in \mathbb{Z}$ mit $\operatorname{ggT}(a, M) = 1$. Dann gilt

$$a^{\lambda(M)} \equiv 1 \mod M.$$

Definition (Primitivwurzel)
Sei $M \geq 2$. Eine ganze Zahl $g \in \mathbb{Z}$ mit $\operatorname{ggT}(M, g) = 1$ und

$$\left\{\bar{g}, \bar{g}^2, \ldots, \bar{g}^{\varphi(M)}\right\} = (\mathbb{Z}/M\mathbb{Z})^*$$

nennen wir ***Primitivwurzel modulo* M**.

Beispiel:

1. 2 ist eine Primitivwurzel modulo 5, denn

$$\left\{2, 2^2, 2^3, 2^4\right\} = (\mathbb{Z}/M\mathbb{Z})^*.$$

2. Gibt es eine Primitivwurzel modulo $M = 15$? In anderen Worten, gibt es $g \in \mathbb{Z}$, $\operatorname{ggT}(g, 15) = 1$, mit $\left\{g, g^2, \ldots, g^{\varphi(15)}\right\} = (\mathbb{Z}/15\mathbb{Z})^*$?
   Bemerke $\varphi(15) = \varphi(5)\varphi(3) = 4 \cdot 2 = 8$, aber $\lambda(15) = \operatorname{kgV}(\varphi(5), \varphi(3)) = 4$.
   Also für $\operatorname{ggT}(g, 15) = 1$ $\left|\left\{g, g^2, \ldots, g^{\varphi(15)}\right\}\right| \leq 4$, denn $g^{\lambda(15)} = g^4 \equiv 1 \bmod 15$.
   Also gibt es keine Primitivwurzel modulo 15.

3. Sei $M = pq$ mit pq, prim, $p, q > 2$. Dann ist $\varphi(M) = (p-1)(q-1)$, aber $\lambda(M) = \operatorname{kgV}(p-1, q-1) < \varphi(M)$. Also gibt es keine Primitivwurzel modulo M.

Im Weiteren wollen wir nun zeigen, dass es im Allgemeinen zu jeder Primzahl auch eine Primitivwurzel gibt. Dafür benötigen wir zunächst folgende Lemmata:

Lemma 4.8
Datei 10: Primitivwurzeln, Video 4_4

Seien $a, b \in (\mathbb{Z}/M\mathbb{Z})^*$ mit $M \in \mathbb{Z}_{\geq 2}$, $A = \operatorname{ord}_M a, B = \operatorname{ord}_M b$. Angenommen

$\mathrm{ggT}(A, B) = 1$, *dann gilt*

$$\mathrm{ord}_M\, ab = AB.$$

Lemma 4.9
Seien $a_1, \ldots, a_m \in (\mathbb{Z}/M\mathbb{Z})^*$ *mit* $M \in \mathbb{Z}_{\geq 2}$ *und* $A = \mathrm{kgV}(\mathrm{ord}_M(a_1), \ldots, \mathrm{ord}_M(a_m))$. *Dann* $\exists\, b \in (\mathbb{Z}/M\mathbb{Z})^*$ *mit* $\mathrm{ord}_M\, b = A$.

4.2 Primitivwurzeln

Video 4_5

Satz 4.10
Sei p *eine Primzahl. Dann gibt es eine Primitivwurzel modulo* p.

Das bedeutet, dass es $g \in \mathbb{Z}$ (oder $g \in \mathbb{N}$) gibt mit $\{g, g^2, \ldots, g^{p-1}\} = (\mathbb{Z}/p\mathbb{Z})^*$. Wie klein kann man dieses g nun wählen?

Vermutung
Sei p eine Primzahl. Dann gibt es eine Primitivwurzel $g \in \mathbb{N}$ mit $g < 2(\log p)^2$.

Von einem Beweis dieser Vermutung sind wir noch sehr weit enfernt. Doch was ist bisher bekannt? Es gib eine Primitivwurzel $g \in \mathbb{N}$ modulo p mit $g < Cp^{\frac{1}{4}+\varepsilon}$, wobei $C, \varepsilon > 0$ und ε beliebig klein. Dieses Resultat folgt aus Arbeiten von D.A. Burgess aus dem Jahre 1962.

Vermutung (Artin[3])
2 ist eine Primitivwurzel für unendlich viele Primzahlen p.

Eine leicht abgeänderte und „aufgefächerte“ Variante dieser Vermutung stellt der folgende Satz dar, der sich auch tatsächlich beweisen ließ:

Satz (Heath-Brown[4], 1986)
Mindestens eine der Zahlen 2,3,5 ist eine Primitivwurzel für unendlich viele Primzahlen p.

[3]Nach Emil Artin (1898-1962), ein österreichischer Mathematiker
[4]Nach Roger Heath-Brown (geb. 1952), ein britischer Mathematiker

Um den Satz 4.10 nun beweisen zu können bedarf es noch ein wenig Vorbereitung:

Vorlesung 5, 27.04.2021, Video 5_1

Satz 4.11
Sei $P(X) = a_nX^n + \cdots + a_1X + a_0$ mit $a_n, \ldots, a_0 \in \mathbb{Z}$ und p prim. Angenommen $p \nmid a_n$, dann hat die Gleichung $P(X) \equiv 0 \bmod p$ höchstens n verschiedene Lösungen modulo p.

Video 5_2

Für welche $M \in \mathbb{N}_{\geq 2}$ gibt es eine Primitivwurzel modulo M?

Satz 4.12
Sei $k \in \mathbb{N}$ und $p > 2$ eine Primzahl. Dann gibt es eine Primitivwurzel modulo p^k.

Lemma 4.13
Sei p eine ungerade Primzahl und $k \in \mathbb{N}$. Dann gilt

$$(1+p)^{p^{k-1}} \equiv 1 + p^k \mod p^{k+1}.$$

5 Primzahltests

Wir machen nun einen kleinen Ausflug, um die Theorien von Ordnungen und Kongruenzrechnung zu verwenden und uns über Primzahltests zu unterhalten. Eine große Frage hierbei ist, wie man für eine natürliche Zahl $n \in \mathbb{N}$ möglichst schnell herausfinden kann, ob sie eine Primzahl ist oder nicht.[1]

Datei 11: Primzahltests, Video 5_3

Komplexität eines Algorithmus':
$L =$ Zahl der Bits, die für den Input notwendig sind

Beispiel: Um eine natürliche Zahl N zu beschreiben benötigt man $\sim \log_{10} N$ Ziffern im Dezimal oder $\sim \log_2 N$ Bits.

Wir nennen einen Algorithmus polynomiell, wenn seine Laufzeit begrenzt ist durch $c2^a$ mit $c, a > 0$.

Beispiel:

i) Der Euklidische Algorithmus angewandt auf $M, N \in \mathbb{N}$ mit $M < N$ benötigt $\sim c \log_{10} N$ Schritte. Dies ist ein polynomieller Algorithmus.

ii) Um eine Primfaktorzerlegung von $N \in \mathbb{N}$ naiv herzuleiten indem man alle Teiler $\leq \sqrt{N}$ probiert, benötigt man $\sim \sqrt{N} = e^{\frac{\log N}{2}} \cong e^{c2}$ Schritte. Dies nennen wir einen exponentiellen Algorithmus.

Die schnellste Laufzeit für eine Primfaktorzerlegung ist in $\sim c_1 e^{c_2 \sqrt[3]{\log N \log\log N}}$ Schritten möglich mit $c_1, c_2 > 0$.

Fragestellung: Wie kann man schnell testen, ob eine natürliche Zahl $N \in \mathbb{N}$ prim ist?

Fermats kleiner Satz (4.4) besagt, dass für $N \in \mathbb{N}, a \in \mathbb{Z}, N \nmid a, N$ prim, $A^{N-1} \equiv 1 \bmod N$ gilt. (Achtung: Die Rückrichtung gilt hierbei im Allgemeinen nicht!)

Definition
Eine natürliche Zahl N mit $a^{N-1} \equiv 1 \bmod N$ für alle $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, N) = 1$ nennen wir eine Carmichael Zahl[2].

[1] Dieses Kapitel ist nicht klausurrelevant.
[2] Nach Robert Daniel Carmichael (1879-1967), US-amerikanischer Mathematiker

Satz (Alford[3], Granville[4], Pomerance[5], 1951)
Es gibt unendlich viele Carmichael Zahlen.

Fragestellung: Weitere Eigenschaften von Primzahlen?

Satz 5.1 (Rabin[6])
Video 5_4 *Sei N ungerade, $a \in \mathbb{Z}$, $N \nmid a$. Angenommen $N-1 = 2^k \cdot m$ mit m ungerade. Ist N prim, dann gilt*

$$a^m \equiv 1 \mod N$$

oder es gilt $0 \leq j \leq k-1$ mit

$$a^{2^j m} \equiv -1 \mod N.$$

Satz
Sei N ungerade, $a \in \mathbb{Z}$, $N \nmid a$ und $N-1 = 2^k m$ mit m ungerade. Ist $a^m \not\equiv 1 \bmod N$ und $a^{2^j m} \not\equiv -1 \bmod N$ für alle $0 \leq j \leq k-1$, dann ist N zusammengesetzt.

Definition
In diesem Fall nennen wir a einen Zeugen für die Zusammengesetztheit von N.

Satz
Sei N ungerade und zusammengesetzt, Dann sind mindestens 75% der Zahlen $1, 2, \ldots, N-1$ Zeugen für die Zusammengesetztheit von N.

Idee: Führe den Rabin-Test mit k zufällig gewählten Zahlen a aus. Ist N zusammengesetzt, dann ist die Wahrscheinlichkeit, dass wir einen Zeugen nach k Schritten finden $\geq 1 - \left(\frac{1}{4}\right)^k$

Bemerkung: Wenn die verallgemeinerte Riemann-Hypothese gilt, dann gibt es für zusammengesetzte N einen Zeugen $a < 2(\log N)^2$. Dies führt zu einem polynomiellen Algorithmus, der die Zusammengesetztheit von N erkennt.

[5]William Robert Alford (1937-2003), ein US-amerikanischer Mathematiker
[5]Andrew James Granville (geb. 1962), ein britisch-kanadischer Mathematiker
[5]Carl Bernard Pomerance (geb. 1944), ein US-amerikanischer Mathematiker
[6]Nach Michael O. Rabin (geb. 1931), ein israelischer Informatiker

5.1 Die Pollard'sche ρ-Methode

[7]

Datei 12: Pollard-ρ-Methode, Video 5_5

Angenommen $N \in \mathbb{N}$ ist zusammengesetzt. Unser Ziel ist, einen echten Teiler von N zu finden.

Sei $b \in \mathbb{Z}$ und betrachte die Folge $x_0, x_1, x_2, \dots$ von Restklassen modulo N, definiert auch $x_0 = 1, x_{i+1} \equiv x_i^2 + b \bmod N$ für $i \geq 0$.

Sei $\nu(m)$ für $m \in \mathbb{N}$ die größte Potenz von 2, die kleiner als m ist.

Beispiel: $\nu(5) = 4, \nu(8) = 4, \nu(12) = 8$

Wir berechnen $\mathrm{ggT}(x_i - x_{nu(i)}, N)$. Unsere Erwartung ist, dass wenn wir das für $i < 4,5N^{\frac{1}{4}}$ tun die Wahrscheinlichkeit, dass wir einen echten Teiler von N gefunden haben, $> \frac{1}{2}$ ist.

Hemiasdb Sei $p \leq \sqrt{N}$ ein Primteiler von N und $q = \lfloor\sqrt{2p}\rfloor + 1$. Betrachte $x_0, x_1, \dots, x_q$ modulo q.

1. Ziel: Finde $0 \leq k, l \leq q$ mit $x_k - x_l \equiv 0 \bmod p$.

Die Wahrscheinlichkeit, dass alle $x_0, x_1, \dots, x_q$ modulo p verschieden sind ist $\left(1 - \frac{1}{p}\right) \cdot \left(1 - \frac{2}{p}\right) \cdots \left(1 - \frac{q}{p}\right)$. Wie groß ist das?

$$\begin{aligned}
\log \left(1 - \frac{1}{p}\right) \cdot \left(1 - \frac{2}{p}\right) \cdots \left(1 - \frac{q}{p}\right) &= \sum_{r=1}^{q} \log \left(1 - \frac{r}{q}\right) \\
&\leq - \sum_{r=1}^{q} \frac{r}{p} = -\frac{1}{2}\frac{q(q+1)}{p} \\
&< -1
\end{aligned}$$

Die Wahrscheinlichkeit, dass $x_0, x_1, \dots, x_q$ modulo p paarweise verschieden sind, ist also $< e^{-1} < \frac{1}{2}$

Bemerkung: $q < \sqrt{2\sqrt{N}} + 2 < 1,5N^{\frac{1}{4}}$

Unser Problem ist nun, dass wir gerne $\mathrm{ggT}(x_k - x_l, N)$ für alle $0 \leq k, l \leq q$ berechnen würden, dies wären jedoch $\sim N^{\frac{1}{4}} \cdot N^{\frac{1}{4}} \sim N^{\frac{1}{2}}$ Berechnungen!

Idee: Ist

$$x_k \equiv x_l \mod p,$$

so auch

[7] Nach John M. Pollard (geb. 1941), ein britischer Mathematiker

$$\begin{aligned} x_{k+1} &\equiv x_{l+1} \mod p \\ x_{k+2} &\equiv x_{l+2} \mod p \\ &\vdots \end{aligned}$$

Angenommen, wir haben $l < k$ mit $x_k \equiv x_l \bmod p$ und $0 \leq l, k \leq q$. Wähle $m \in \mathbb{N}$ mit

$$2^{m-1} < \max\{l, k-l\} \leq 2^m.$$

Dann gilt

$$x_{k-l} \equiv x_{2^m} \mod p$$

und

$$\begin{aligned} k - l + 2^m &< k - l + 2\max\{l, k-l\} \\ &\leq 4,5 N^{\frac{1}{4}} \end{aligned}$$

6 Quadratreste

Bisher haben wir lineare Kongruenzgleichungen Vorlesung 6, 30.04.2021, Datei 13: Quadratreste, Teil 1, Video 6_1

$$ax + b \equiv 0 \mod M$$

mit $a, b \in \mathbb{Z},\ M \in \mathbb{N}$ betrachtet. Nun wollen wir uns die Frage stellen, was passiert, wenn wir zu quadratische Kongruenzgleichungen übergehen.

Seien $a, b, c \in \mathbb{Z},\ M \in \mathbb{N}_{\geq 2}$. Wann hat die Gleichung

$$ax^2 + bx + c \equiv 0 \mod M$$

eine Lösung? Laut dem chinesischen Restsatz genügt es, $M = p^k$ mit p prim zu betrachten. Wir beginnen mit dem einfachsten Fall

$$x^2 \equiv a \mod p$$

Definition (quadratischer (Nicht-)Rest)
Sei $a \in \mathbb{Z},\ p$ prim mit $p \nmid a$. Dann nennen wir a einen ***quadratischen Rest/Nichtrest*** modulo p, falls $x^2 \equiv a \bmod p$ lösbar ist/keine Lösung hat.

Beispiel: $p = 7$: Quadratische Reste: 1,2 ,4
Quadratische Nichtreste: 3,5,6

$p = 5$: Quadratische Reste: 1,4
Quadratische Nichtreste: 2,3

Satz 6.1
Sei p eine ungerade Primzahl. Dann gibt es $\frac{p-1}{2}$ quadratische Reste und $\frac{p-1}{2}$ quadratische Nichtreste modulo p.

Definition (Legendre[1] Symbol)

Video 6_2 Sei p eine ungerade Primzahl und $a \in \mathbb{Z}$. Wir definieren das ***Legendre Symbol*** als

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{falls } a \equiv x^2 \bmod p \text{ eine Lösung hat} \\ -1 & \text{falls } a \text{ ein quadratischer Nichtrest modulo } p \text{ ist} \\ 0 & p \mid a \end{cases}$$

Beispiel: Sei $p = 7$:
$\left(\frac{1}{7}\right) = \left(\frac{2}{7}\right) = \left(\frac{4}{7}\right) = 1$
$\left(\frac{7}{7}\right) = 0$
$\left(\frac{3}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{1}{6}\right) = -1$

Satz 6.2
Sei p eine ungerade Primzahl, $a, b \in \mathbb{Z}$. Dann gilt

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

Datei 14: Quadratreste, Teil 2, Video 6_3

Fragestellung: Wie lassen sich die Legendre Symbole berechnen?

Satz 6.3 (Euler)
Sei p eine ungerade Primzahl, $a \in \mathbb{Z}$ mit $p \nmid a$. Dann gilt

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p.$$

Korollar 6.4
Sei p eine ungerade Primzahl. Dann gilt

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \textit{für } p \equiv 1 \bmod 4 \\ -1 & \textit{für } p \equiv -1 \bmod 4 \end{cases}$$

[1] Nach Adrien-Marie Legendre (1752-1833), ein französischer Mathematiker

Satz 6.5 (Quadratische Reziprozität)
Seien p, q ungerade Primzahlen mit $p \neq q$. Dann gilt

Datei 15: Quadratreste, Teil 3, Video 6_4

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Satz 6.6
Sei p eine ungerade Primzahl. Dann gilt

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & p \equiv \pm 1 \bmod 8 \\ -1 & p \equiv \pm 3 \bmod 8 \end{cases}$$

Beispiel:

$$\begin{aligned} \left(\frac{-70}{11}\right) &= \left(\frac{5}{11}\right)\left(\frac{7}{11}\right)\left(\frac{-1}{11}\right)\left(\frac{2}{11}\right) \\ &= \left(\frac{11}{5}\right)(-1)\left(\frac{11}{7}\right)(-1)(-1) \\ &= \left(\frac{1}{5}\right)(-1)\left(\frac{4}{7}\right) \\ &= -1 \end{aligned}$$

Beispiel: Bestimme $\left(\frac{3}{p}\right)$ für ungerade Primzahlen $p \neq 3$.

Fall 1: $p \equiv 1 \bmod 4$. Dann gilt

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$$

und $\left(\frac{3}{p}\right) = 1 \iff p \equiv 1 \bmod 3$.

Fall 2: $p \equiv -1 \bmod 4$. Dann gilt

$$\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right)$$

und $\left(\frac{3}{p}\right) = 1 \iff p \equiv 2 \bmod 3$.

Insgesamt folgt also

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & p \equiv \pm 1 \mod 12 \\ -1 & p \equiv \pm 5 \mod 12 \end{cases}$$

Satz 6.7
Es gibt unendlich viele Primzahlen $p \equiv 1 \mod 4$.

Video 6_5 ***Beobachtung:*** Das Legendre Symbol $\left(\frac{a}{p}\right)$ ist beinahe periodisch in p.

Satz 6.8
Sei $a \in \mathbb{Z} \setminus \{0\}$, p, q ungerade Primzahlen mit $p \nmid a$ und $q \nmid a$. Angenommen $a \equiv 1 \mod 4$ und $p \equiv q \mod |a|$, oder $a \not\equiv 1 \mod 4$ und $p \equiv q \mod 4|a|$, dann gilt

$$\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$$

Lemma 6.9
Seien $u_1, \ldots, u_r \in \mathbb{Z}$ ungerade. Dann gilt

$$\sum_{i=1}^{r} \frac{u_i - 1}{2} \equiv \frac{u_1 \cdots u_r - 1}{2} \mod 2$$

und

$$\sum_{i=1}^{r} \frac{u_i^2 - 1}{8} \equiv \frac{(u_1 \cdots u_r)^2 - 1}{8} \mod 2$$

Satz 6.10
Vorlesung 7, 04.05.2021 Video 7_2 *Sei p eine Primzahl mit $p \equiv -1 \mod 4$ und wir nehmen an, dass $2p+1$ ebenfalls prim ist. Dann gilt*

$$2p + 1 \mid 2^p - 1.$$

Dieser Satz sagt insbesondere, dass für $p > 3$ in diesem Fall $2^p - 1$ keine Primzahl ist. Er vor allem relevant in der noch offenen Frage, ob es unendlich viele Mersenne[2]-Primzahlen (also Primzahlen der Form $2^p - 1$) gibt.

Satz 6.11 (Pépin[3]-Test)
Definiere $F_n := 2^{2^n} + 1$ für $n \in \mathbb{N}$. Dann gilt, dass F_n genau dann prim ist, wenn gilt

$$3^{\frac{1}{2}(F_n - 1)} \equiv -1 \mod F_n.$$

[2]Nach Marin Mersenne (1588-1648), ein französischer Theologe, Mathematiker und Musiktheoretiker
[3]Nach Théophile Pépin (1826-1904), ein französischer Mathematiker

Die im Satz 6.11 definierten Zahlen F_n werden Fermat-Zahlen genannt. Bisher ist noch unbekannt, ob unendlich viele der Fermat-Zahlen auch Primzahlen sind. Fermat hatte seinerzeit behauptet, alle Fermat-Zahlen seien Primzahlen, dies wurde allerdings von Euler widerlegt, der zeigte, dass F_5 nicht prim ist. Inzwischen wird angenommen, dass tatsächlich lediglich $F_0, \dots, F_4$ prim sind. Da die Fermat-Zahlen allerdings durch die doppelte Exponentialität so dünn sind ist es sehr schwer, sie tatsächlich zu überprüfen. Die kleinste bisher ungetestete Fermat-Zahl ist F_{33}, welche 2.585.287.973 Stellen hat.

Lemma 6.12 (Gauß'sches Lemma)
Sei $p > 2$ eine Primzahl. Wir nennen $1, 2, \dots, \frac{p-1}{2} \bmod p$ positive Restklassen und $-1, -2, \dots, -\frac{p-1}{2} \bmod p$ negative Restklassen mod$p$. Sei $a \in \mathbb{Z}$ mit $p \nmid a$ und μ die Zahl der negativen Restklassen in der Folge $a, 2a, \dots, \frac{p-1}{2}a \bmod p$. Dann gilt — Datei 16: Quadratische Reziprozität, Video 7_3

$$\left(\frac{a}{p}\right) = (-1)^{\mu}.$$

Beispiel: $\left(\frac{3}{5}\right)$:
$1, 2$ positive Restklassen modulo 5
$3, 4$ negative Restklassen modulo 5
$3 \cdot 1 \equiv -2,\ 3 \cdot 2 \equiv 1$. Das heißt in diesem Beispiel haben wir $\mu = 1$ und $\left(\frac{3}{5}\right) = (-1)^{\mu} = -1$.

Definition (Untere Gaußklammer)
Sei $x \in \mathbb{R}$. Wir definieren — Video 7_5

$$\lfloor x \rfloor = \max\{m \in \mathbb{Z} \mid m \leq x\}.$$

Beispiel: $\lfloor 3 \rfloor = 3,\ \lfloor 2,8 \rfloor = 2$

Lemma 6.13
Sei $p > 2$ eine Primzahl, $a \in \mathbb{Z}$ mit $2 \nmid a$ und $p \nmid a$. Sei

$$S(a, p) := \sum_{s=1}^{\frac{p-1}{2}} \left\lfloor \frac{as}{p} \right\rfloor.$$

Dann gilt

$$\left(\frac{a}{p}\right) = (-1)^{S(a,p)}.$$

6.1 Das Jacobi-Symbol

Vorlesung 8, 07.05.2021 Video 8_2

Motivation: schnelle Berechnung von Legendre Symbolen. Angenommen p ist eine (große) Primzahl, $n < p$ und wir wollen $\left(\frac{n}{p}\right)$ berechnen. Unsere Strategie sah dafür sah bisher wie folgt aus:

Nehme eine Primfaktorzerlegung von $n = q_1 \cdot q_2 \cdots q_r$ mit $q_1, \dots, q_r$ prim. Dann gilt

$$\left(\frac{n}{p}\right) = \left(\frac{q_1}{p}\right)\left(\frac{q_2}{p}\right)\cdots\left(\frac{q_r}{p}\right)$$

Wende jetzt quadratische Reziprozität an.

Problem: Wir müssen für dieses Vorgehen zunächst eine Primfaktorzerlegung von n finden.

Definition (Jacobi-Symbol)
Sei $n \in \mathbb{N}$ ungerade und $m \in \mathbb{Z}$ mit $\mathrm{ggT}(m, n) = 1$. Sei $n = p_1 p_2 \cdots p_r$ mit $p_1, \dots, p_r$ Primzahlen. Dann definieren wir

$$\left(\frac{m}{n}\right) = \left(\frac{m}{p_1}\right)\left(\frac{m}{p_2}\right)\cdots\left(\frac{m}{p_r}\right).$$

Achtung: Ist $\left(\frac{m}{n}\right) = 1$, dann wissen wir im Allgemeinen noch nicht, ob die Kongruenz $m \equiv x^2 \bmod n$ eine Lösung hat!

Beispiel:

$$\begin{aligned}\left(\frac{-1}{21}\right) &= \left(\frac{-1}{7}\right)\left(\frac{-1}{3}\right)\\ &= (-1)(-1)\\ &= 1,\end{aligned}$$

aber $x^2 \equiv -1 \bmod 21$ hat keine Lösung!

Satz 6.14 (Eigenschaften von Jacobi-Symbolen)
Seien $m, n \in \mathbb{N}$ ungerade mit $\mathrm{ggT}(m, n) = 1$. Dann gilt

i) $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$

ii) $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$

iii) $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{(m-1)(n-1)}{4}}$

7 Summen von Quadraten

7.1 Summen von zwei Quadraten

Vorlesung 9, 11.05.2021

Die Frage, mit der wir uns in diesem Kapitel beschäftigen wollen, ist welche natürlichen Zahlen wir als Summe von zwei Quadraten schreiben können.

Beispiel: $5 = 1^2 + 2^2$
$3 = \square + \square? \implies$ keine Lösung
$2 = 1^2 + 1^2$
$4 = 2^2 + 0^2$

Lemma 7.1
Seien $a, b \in \mathbb{Z}$, p eine ungerade Primzahl mit $p \nmid ab$ und $p \mid a^2 + b^2$. Dann gilt

$$p \equiv 1 \mod 4.$$

Korollar
Ist $p \geq 3$ prim, $p = a^2 + b^2$ mit $a, b \in \mathbb{Z}$, dann gilt $p \equiv 1 \bmod 4$.

Satz 7.2 (Fermat)
Sei p eine Primzahl mit $p \equiv 1 \bmod 4$. Dann gibt es $a, b \in \mathbb{Z}$ mit $p = a^2 + b^2$.

Lemma 7.3
Angenommen $m, n \in \mathbb{Z}$ mit $m = a^2 + b^2$ und $n = c^2 + d^2$ für gewisse $a, b, c, d \in \mathbb{Z}$. Dann ist auch $m \cdot n$ die Summe von zwei ganzzahligen Quadraten.

Wie können wir nun alle $n \in \mathbb{N}$ finden, die wir als Summe von zwei Quadraten schreiben können?

Korollar 7.4
Sei $n \in \mathbb{N}$. Dann gilt $n = a^2 + b^2$ für $a, b \in \mathbb{Z}$ genau dann, wenn n die Form

$$n = 2^k m^2 p_1 \cdots p_r$$

mit $k \geq 0$, $m \in \mathbb{Z}$, $p_1, \ldots, p_r$ Primzahlen mit $p_i \equiv 1 \bmod 4$ hat.

Satz 7.5 (Verschärfung von Satz 7.2)
Sei $n \in \mathbb{N}$ und definiere

$$r_2(n) = \left|\left\{(x, y) \in \mathbb{Z}^2 \mid n = x^2 + y^2\right\}\right|.$$

i) $\frac{r_2(n)}{4}$ *ist eine multiplikative Funktion.*

ii) Sei p prim und $k \in \mathbb{N}$. Dann gilt

$$\frac{r_2(p^k)}{4} = \begin{cases} k+1 & \text{für } p \equiv 1 \bmod 4 \\ 0 & \text{für } p \equiv 3 \bmod 4 \text{ und } k \text{ ungerade} \\ 1 & \text{für } p \equiv 4 \bmod 4 \text{ und } k \text{ gerade} \\ 1 & \text{für } p = 2 \end{cases}$$

Beispiel: $p \equiv 3 \bmod 4$ ✓
$p = 2, 2 = (\pm 1)^2 + (\pm 1)^2$
Ist $p \equiv 1 \bmod 4$ mit $p = a^2 + b^2$, dann sind auch $(\pm a, \pm b), (\pm b, \pm a)$ Lösungen.

Satz 7.6 (Dirichlet)
Sei $n \in \mathbb{N}$. Dann gilt

$$r_2(n) = 4 \sum_{\substack{d \mid n \\ d \equiv 1 \bmod 2}} (-1)^{\frac{d-1}{2}}$$

7.2 Summen von vier Quadraten

Fragestellung: Angenommen, wir wollen ***jedes*** $n \in \mathbb{N}$ schreiben als

$$n = \square + \square + \square + \square + \square + \square + \ldots$$

Wie viele Quadrate benötigt man mindestens?

Beobachtung: 4 Quadrate sind ausreichend.

Satz 7.7 (Lagrange[1] 1770)
Jede natürliche Zahl n kann als Summe vn vier ganzzahligen Quadraten geschrieben werden.

Lemma 7.8
Ist $m = \square + \square + \square + \square$ und $n = \square + \square + \square + \square$, dann gilt auch

$$mn = \square + \square + \square + \square.$$

Mit diesem Lemma können wir uns als Ziel setzen, jede beliebige Primzahl p als Summe von maximal vier Quadraten zu schreiben.

Lemma 7.9
Sei $p > 2$ prim. Dann gibt es $m \in \mathbb{N}$ mit $m < p$ und

$$mp = \square + \square + \square + \square.$$

7.3 Summen von drei Quadraten

Fragestellung: Für welche $n \in \mathbb{N}$ genügen uns sogar schon 3 Quadrate?

Vorlesung 10, 14.05.2021

Erste Beobachtung: $\square \equiv 0, 1, 4 \mod 8$.

- Ist $n \in \mathbb{N}$ mit $n \equiv 7 \mod 8$, dann $n \neq \square + \square + \square$
- Angenommen $n \in \mathbb{N}$ mit $n = a^2 + b^2 + c^2$ mit $a, b, c \in \mathbb{Z}$ und $4 \mid n$. Dann haben wir
$$0 \equiv n \equiv a^2 + b^2 + c^2 \mod 4.$$
Daraus folgt $2 \mid a$, $2 \mid b$, $2 \mid c$, also
$$\frac{n}{4} = \left(\frac{a}{2}\right)^2 + \left(\frac{b}{2}\right)^2 + \left(\frac{c}{2}\right)^2$$

Folgerung: Ist $n = (8k + 7) \cdot 4^l$ mit $k \in \mathbb{Z}_{\geq 0}$, $l \in \mathbb{Z}_{\geq 0}$, dann ist $n \neq \square + \square + \square$.

[1]Nach Joseph-Louis Lagrange (1736-1813), ein italienischer Mathematiker und Astronom

Satz 7.10 (Gauß[2])
Jedes $n \in \mathbb{N}$, das nicht die Form $n = 4^l(8k+7)$ mit $k, l \in \mathbb{Z}_{\geq 0}$ hat, kann als Summe von drei Quadraten geschrieben werden.

Eine Anwendung: Dreieckszahlen, also Zahlen der Form

$$a_n = \frac{n(n+1)}{2}.$$

Korollar 7.11
Jede natürliche Zahl $n \in \mathbb{N}$ kann als Summe von drei Dreieckszahlen geschrieben werden, das heißt $n = \triangle + \triangle + \triangle$.

Allgemeiner: Sei $F(x_1, \dots, x_k) \in \mathbb{Z}[x_1, \dots, x_k]$ ein homogenes Polynom von Grad 2, z.B. $x_1^2 + x_3x_4 + x_2^2 + \dots$

Fragestellung: Wann kann man jede natürliche Zahl schreiben als $n = F(x_1, \dots, x_k)$ mit $x_1, \dots, x_k \in \mathbb{Z}$?

Um diese Frage beantworten zu können benötigen wir zunächst etwas Terminologie:

- Wir nennen F ***positiv definit***, falls $F(x_1, \dots, x_k) > 0$ für alle $(x_1, \dots, x_k) \in \mathbb{R}^k \setminus \{0\}$.
- Wir nennen F ***gerade***, falls jeder Koeffizient von x_ix_j mit $i \neq j$ gerade ist.

Satz (15-Satz von Conway[3] und Schneeberger[4], 1993)
Sei $F(x_1, \dots, x_k)$ eine gerade positiv definite quadratische Form mit ganzen Koeffizienten. Falls F die Zahlen $n = 1, \dots, 15$ darstellt, dann stellt F alle natürlichen Zahlen dar.

Satz (290-Theorem von Bhargava[5] und Hanke[6], 2005)
Sei F eine positiv definite quadratische Form mit ganzzahligen Koeffizienten. Falls F die Zahlen $n = 1, \dots, 290$ darstellt, dann stellt F jede natürliche Zahl dar.

[2] Nach Carl Friedrich Gauß (1777-1855), ein deutscher Mathematiker, Statistiker, Astronom, Geodät und Physiker
[4] John Horton Conway (1937-2020), ein britischer Mathematiker
[4] William Allan Schneeberger (geb. 1970), Promotionsstudent Conways
[6] Manjul Bhargava (geb. 1974), ein kanadischer Mathematiker
[6] Jonathan Hanke, ein US-amerikanischer Mathematiker

7.4 Das Waringsche Problem

Satz (Jacobi)
Jedes $n \in \mathbb{N}$ kann geschrieben werden als

$$n = \square + \square + \square + \square.$$

Fragestellung: Was passiert bei höheren Potenzen? Welche Zahlen können beispielsweise geschrieben werden als

$$n = a^3 + b^3 + c^3 + d^3?$$

Satz (Hilbert[7])
Sei $k \in \mathbb{Z}_{\geq 2}$. Dann gibt es eine natürliche Zahl $g(k)$, sodass jedes $n \in \mathbb{N}$ als Summe von höchstens $g(k)$ positiven k-ten Potenzen geschrieben werden kann. Das heißt für jedes $n \in \mathbb{N}$ gibt es $s \leq g(k),\ x_1, \ldots, x_s \in \mathbb{N}$ mit $n = x_1^k + x_2^k + \ldots + x_s^k$.

Fragestellung: Was ist der kleinstmögliche Wert für $g(k)$?

Definition
Sei $g(k)$ die kleinstmögliche natürliche Zahl in Hilberts Satz.

Beispiel: $g(2) = 4$ (Jacobi + Gauß)
$g(3) = 9$
$g(4) = 19$
$g(5) = 37$

Beobachtung: $g(k)$ wächst schnell in k, manchmal wegen kleinen Werten von n.

Beispiel: Schreibe $2^k - 1 = x_1^k + \ldots + x_s^k$ mit $x_i \in \mathbb{N}$. Dann gilt $x_1 = 1$ und $s = 2^k - 1$. Es folgt $g(k) \geq 2^k - 1$.

Idee: Ist $k = 3$, dann kann jedes $n \in \mathbb{N} \setminus \{23, 239\}$ als Summe von acht Kuben geschrieben werden.

[7] Nach David Hilbert (1862-1943), ein deutscher Mathematiker

Definition
Für $k \geq 2$ sei $G(k)$ die kleinste natürliche Zahl, sodass jedes hinreichend große $n \in \mathbb{N}$ als Summe von höchstens $G(k)$ positiven k-ten Potenzen geschrieben werden kann.

Bekannt: $G(2) = 4,\ G(4) = 16,\ G(3) \leq 7.$

Lemma 7.12
$G(3) \geq 4$

Satz (Wooley[8] 1992)
Es gibt eine Konstante $C \in \mathbb{R}$ *mit*

$$G(k) \leq k \log k + k \log\log k + Ck.$$

Lemma

$$r_k(n) = \int_0^1 T(\alpha)^s e^{-2\pi i \alpha n}\, d\alpha$$

7.5 Quadratische Gleichungen in 2 Variablen über $\mathbb{Q}$

Seien $a, b, c, d, e, f \in \mathbb{Z}$ und betrachte die Gleichung

$$Q(x, y) = ax^2 + bxy + cy^2 + dx + ey + f = 0$$

Beispiel: Hyperbel $x^2 - y^2 = 1$
Parabel $2x^2 = y$
Ellipsen $x^2 + 2y^2 = 3$
Vereinigung von zwei Geraden $(x - 2y + 1)(2x - y) = 0$

Wir nennen $Q(x, y)$ ***reduzibel*** über $\mathbb{Q}$ oder $\mathbb{C}$, falls $Q(x, y) = f(x, y)g(x, y)$ mit $\operatorname{grad} f \geq 1$ und $\operatorname{grad} g \geq 1$ und $f, q \in \mathbb{Q}[x, y]$ oder $\mathbb{C}[x, y]$.

Satz 7.13
Seien $a, b, c, d, e, f \in \mathbb{Z}$. *Falls* $ax^2 + bxy + cy^2 + dx + ey + f = 0$ *eine rationale Lösung hat und über* $\mathbb{C}$ *irreduzibel ist, dann hat die Gleichung unendlich viele Lösungen.*

[8] Nach Trevor Wooley (geb. 1964), ein britischer Mathematiker

Beispiel:

$$C : x^2 + 2y^2 = 3$$

hat den rationalen Punkt $(x_0, y_0) = (1, 1)$. Berechne die Gerade L durch $P = (x_0, y_0)$ mit Steigung $m \in \mathbb{Q}$.

$$L = \begin{cases} x = x_0 + t \\ y = y_0 + t \cdot m \end{cases}$$

Schnitt von L und C:

$$\begin{aligned} (x_0 + t)^2 + 2(y_0 + tm)^2 &= 3 \\ (1 + t)^2 + 2(1 + tm)^2 &= 3 \\ \iff 2t + t^2 + 4tm + 2t^2m^2 &= 0 \\ t(t + 2tm^2 + 2 + 4m) &= 0 \end{aligned}$$

$$\begin{aligned} \implies t &= 0 \text{ oder} \\ t &= -\frac{2 + 4m}{1 + 2m^2} \end{aligned}$$

P' ist gegeben durch

$$\begin{aligned} x_1 &= 1 - \frac{2 + 4m}{2 + 2m^2} = \frac{2m^2 - 4m - 1}{1 + 2m^2} \\ y_1 &= 1 - m\frac{2 + 4m}{1 + 2m^2} \\ &= \frac{-2m^2 - 2m + 1}{1 + 2m^2} \end{aligned}$$

Alle rationalen Lösungen von $x^2 + 2y^2 = 3$ können beschrieben werden durch

$$(x, y) = \left(\frac{2m^2 - 4m - 1}{1 + 2m^2}, \frac{-2m^2 - 2m + 1}{1 + 2m^2} \right)$$

für $m \in \mathbb{Q}$.

8 Kettenbrüche

8.1 Endliche Kettenbrüche

Vorlesung 11, 18.05.2021

Zunächst: wir betrachten Kettenbrüche als Ausdrücke der Form

$$b_0 + \frac{1}{b_1 + \frac{1}{b_2 + \cdots + \frac{1}{b_n}}}$$

mit $b_0 \in \mathbb{Z}$, $b_1, \ldots, b_n \in \mathbb{N}$. Als Kurzschreibweise benutzen wir die Notation

$$\langle b_0, b_1, \ldots, b_n \rangle.$$

Bemerkung: Der Wert eines endlichen Kettenbruchs ist gleich einer rationalen Zahl.

Lemma 8.1
Jede rationale Zahl kann als endlicher Kettenbruch geschrieben werden.

Caveat: Die Darstellung einer rationalen Zahl in der Form eines endlichen Kettenbruchs ist im allgemeinen nicht eindeutig:

$$\langle 0, 1, 1 \rangle = \frac{1}{1 + \frac{1}{1}} = \frac{1}{2} = \langle 0, 2 \rangle$$

Bemerkung: i) $a_m = \left\lfloor \frac{r_{m-1}}{r_m} \right\rfloor$ und $\frac{r_{m+1}}{r_m} = \left\{ \frac{r_{m-1}}{r_m} \right\} = \frac{r_{m-1}}{r_m} - \left\lfloor \frac{r_{m-1}}{r_m} \right\rfloor$.

ii) $\frac{r_1}{r_2} = \langle a_2, a_3, \ldots, a_k \rangle$ oder im Allgemeinen

$$\frac{r_{m-1}}{r_m} = \langle a_m, a_{m+1}, \ldots, a_k \rangle$$

Beispiel: Wir wollen $\frac{137}{33}$ als Kettenbruch darstellen.

$$\begin{aligned} 137 &= 4 \cdot 33 + 5 & \qquad \frac{137}{33} &= 4 + \frac{5}{33} \\ 33 &= 6 \cdot 5 + 3 & \frac{33}{5} &= 6 + \frac{3}{5} \\ 5 &= 1 \cdot 3 + 2 & \frac{5}{3} &= 1 + \frac{2}{3} \\ 3 &= 1 \cdot 2 + 1 & \frac{3}{2} &= 1 + \frac{1}{2} \end{aligned}$$

Also ist $\frac{137}{33} = \langle 4, 6, 1, 1, 2 \rangle$

8.2 Unendliche Kettenbrüche

Sei $\alpha \in \mathbb{R} \setminus \mathbb{Q}$. Unser Ziel ist es, α in der Form

$$\alpha = \langle a_0, a_1, a_2, \dots \rangle$$

zu schreiben. Hierfür verwenden wir den Algorithmus aus Lemma 8.1:
Sei $\alpha_0 = \alpha$.

$$a_0 = \lfloor \alpha_0 \rfloor, \ \alpha_1 = \frac{1}{\{\alpha_0\}},$$

also

$$\begin{aligned} \alpha &= a_0 + \{\alpha_0\} \\ &= a_0 + \frac{1}{\frac{1}{\{\alpha_0\}}} \\ &= a_0 + \frac{1}{\alpha_1} \end{aligned}$$

$$a_1 = \langle \alpha_1 \rangle, \ \alpha_2 = \frac{1}{\{\alpha_1\}} \implies \alpha_1 = a_1 + \frac{1}{\alpha_2}$$

$$a_2 = \langle \alpha_2 \rangle, \ \alpha_3 = \frac{1}{\{\alpha_2\}}$$

$$\vdots$$

$$a_n = \langle \alpha_n \rangle, \ \alpha_{n+1} = \frac{1}{\{\alpha_n\}} \text{ für } n \geq 0$$

Bemerkung: Es gilt für $i \geq 0$:

$$0 < \{\alpha_i\} < 1$$

Also $\alpha_{i+1} = \frac{1}{\{\alpha_i\}} > 1$ und $a_{i+1} = \langle \alpha_{i+1} \rangle \in \mathbb{N}$.
Nach n Schritten

$$\begin{aligned} \alpha &= \langle a_0, a_1, a_2, \ldots, a_{n-1}, \alpha_n \rangle \\ &= a_0 + \cfrac{1}{a_1 + \frac{1}{a_2 + \cdots + \frac{1}{a_n}}} \end{aligned}$$

Bemerkung: Ist $\alpha \in \mathbb{R} \setminus \mathbb{Q}$, dann gilt $\alpha_n \neq 0 \; \forall \, n \in \mathbb{N}$.

Ist $\alpha = \langle a_0, a_1, a_2, \ldots, a_{n-1}, \alpha_n \rangle$ wie oben, so nennen wir als Konvention die a_i ***Elemente*** des Kettenbruchs.

Fragestellung: Warum würde man $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ überhaupt als Kettenbruch schreiben wollen?

Idee: Die Elemente eines Kettenbruchs geben sehr gute Approximationen für die durch den Kettenbruch dargestellte Zahl.

Definition (Teilbruch)
Sei $\alpha \in \mathbb{R} \setminus \mathbb{Q}$, $\alpha = \langle a_0, a_1, a_2, \ldots \rangle$. Dann nennen wir für $n \in \mathbb{Z}_{\geq 0}$

$$\frac{p_n}{q_n} = \langle a_0, a_1, a_2, \ldots, a_n \rangle$$

den **n-*ten Kettenbruch*** von α.

Beispiel:

$$\begin{aligned}
\sqrt{2} &= \lfloor\sqrt{2}\rfloor + \{\sqrt{2}\} \\
&= \lfloor\sqrt{2}\rfloor + \frac{1}{\frac{1}{\sqrt{2}}} \\
a_0 &= \lfloor\sqrt{2}\rfloor = 1 \\
\alpha_1 &= \frac{1}{\{\sqrt{2}\}} \\
&= \frac{1}{\sqrt{2}-1} = \frac{\sqrt{2}+1}{(\sqrt{2}-1)(\sqrt{2}+1)} \\
&= \sqrt{2}+1 \\
a_1 &= \lfloor\alpha_1\rfloor = 2 \\
\alpha_2 &= \frac{1}{\{\alpha_1\}} = \frac{1}{\sqrt{2}-1} \\
a_2 &= \lfloor\alpha_2\rfloor = \lfloor\alpha_1\rfloor = 2
\end{aligned}$$

Es folgt $\sqrt{2} = \langle 1, 2, 2, 2, \dots\rangle$
Teilbrüche:

$$\begin{aligned}
\frac{p_0}{q_0} &= 1 \\
\frac{p_1}{q_1} &= \langle 1, 2\rangle \\
&= 1 + \frac{1}{2} \\
\frac{p_2}{q_2} &= \langle 1, 2, 2\rangle \\
&= 1 + \frac{1}{2+\frac{1}{2}}
\end{aligned}$$

$$\sqrt{2} = 1,4142\dots, \quad \left|\sqrt{2} - \frac{p_2}{q_2}\right| = 0,01421\dots$$

Satz 8.2
Sei $a_0 \in \mathbb{Z}, \ a_1, a_2, \dots \in \mathbb{N}$. Definiere eine Folge p_n, q_n für $n \geq -2$ wie folgt:

$$\begin{aligned}
p_{-2} &= 0 & q_{-2} &= 1 \\
p_{-1} &= 1 & q_{-1} &= 0
\end{aligned}$$

$$\begin{aligned}
p_n &= a_n p_{n-1} + p_{n-2} \\
q_n &= a_n q_{n-1} + q_{n-2}.
\end{aligned}$$

Sei $n \geq 0$ und $x \in \mathbb{R}$ mit $xq_n + q_{n-1} \neq 0$. Dann gilt

$$\langle a_0, a_1, \ldots, a_n, x \rangle = \frac{xp_n + p_{n-1}}{xq_n + q_{n-1}}$$

Bemerkung: i) Die Brüche $\frac{p_n}{q_n}$ sind Teilbrüche von $\langle a_0, a_1, a_2, \ldots \rangle$.

ii) Wir können in der Notation von Satz 8.2 α_n berechnen, wenn wir $\alpha \in \mathbb{R}$ und seine Teilbrüche kennen:

$$\begin{aligned} \alpha &= \langle a_0, a_1, \ldots, a_n, a_{n+1} \rangle \\ &= \frac{\alpha_{n+1} p_n + p_{n-1}}{\alpha_{n+1} q_n + q_{n-1}} \\ \implies \alpha_{n+1} &= -\frac{p_{n-1} - \alpha q_{n-1}}{p_n - \alpha q_n} \end{aligned}$$

8.3 Approximationseigenschaften von Kettenbrüchen

Satz 8.3
Sei $\alpha = \langle a_0, a_1, a_2, \ldots \rangle$ mit $a_0 \in \mathbb{Z}$, $a_1, a_2, \ldots \in \mathbb{N}$. Angenommen p_n, q_n, $n \in \mathbb{Z}_{\geq 2}$ sind wie in Satz 8.2 definiert. Dann gilt für $n \geq 0$

$$p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1}$$

und

$$\alpha - \frac{p_n}{q_n} = \frac{(-1)^n}{q_n(\alpha_{n+1} q_n + q_{n-1})}$$

Korollar
$\alpha > \frac{p_n}{q_n}$ *für n gerade*
$\alpha < \frac{p_n}{q_n}$ *für n ungerade*

Korollar
Mit der gleichen Notation wie oben gilt

$$\left| \alpha - \frac{p_n}{q_n} \right| < \frac{1}{q_n q_{n+1}} < \frac{1}{q_n^2}.$$

Die wollen wir nun mit Approximationen vergleichen, die aus der Dezimalentwicklung entstehen. Wir schreiben im Dezimalsystem

$$\alpha = b_0, b_1 b_2 b_3 \dots b_n b_{n+1} \dots$$

Dann gilt

$$|\alpha - b_0, b_1 b_2 b_3 \dots b_n| \leq 0,00\dots01 = 10^{-n}$$

Definitionen