Elemente der Zahlentheorie

Rainer Vogt

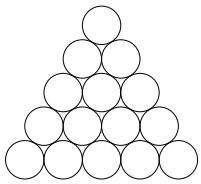
WS 2009/2010

Inhaltsverzeichnis

Teil I
Kleine historische Einführung

1 Dreiecks- und Pyramidenzahlen

Man beginne mit einer Reihe von Kugeln nebeneinander gelegt. Danach legt man in die Zwischenräume eine zweite Reihe usw. bis man ein Dreieck aus Kugeln hat



Sei $k_2(n)$ die Anzahl von Kugeln, die man für das ganze Dreieck benötigt, falls die unterste Reihe n Kugeln enthält.

Schon ca. 500 v. Chr. fragten sich griechische Gelehrte aus der Schule des Pythagoras (ca 570 bis 480), welche Zahlen von der Form $k_2(n)$ sind.

1.1 Definition: $k_2(n)$ heißt n-te **Dreieckszahl**.

Natürlich sind uns diese Dreieckszahlen bekannt:

1.2 $k_2(n) = n + (n+1) + \ldots + 2 + 1 = \frac{n\cdot(n+1)}{2}$

Jetzt können wir aber eine Dimension höher gehen. Wir beginnen mit einem Dreieck, legen dann auf jedes Tripel von Kugeln eine weitere Kugel und erhalten so eine zweite Dreiecksschicht. Man sieht sofort, dass für diese Schicht $k_2(n-1)$ Kugeln benötigt werden. Wir fahren fort, bis wir einen Tretraeder errichtet haben.

1.3 Definition: Die Anzahl $k_3(n)$ der Kugeln im Tetraeder heißt Tetraederzahl.

1.4 Aufgabe: Geben Sie eine Formel im Stil von (1.2) für $k_3(n)$ an und ermitteln Sie mit ihr $k_3(1000)$.

Jetzt vereinfachen wir unsere Fragestellung etwas: Wir beginnen mit einem Quadrat aus n^2 Kugeln und legen darauf eine zweite Lage, indem wir wieder auf die "Zwischenräume" lege. Diese zweite Lage ist dann wieder ein Quadrat mit einer Kante von $(n-1)$ Kugeln.

1.5 Definition: Die Anzahl $p(n)$ der Kugeln in der so entstandenen quadratischen Pyramide heißt **Pyramidenzahl**.

Für $p(n)$ kennen wir aus dem Grundkurs eine Formel

1.6 $p(n) = 1^2 + 2^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}$.

Jetzt stellt sich sofort die Frage, wie es mit Formeln für höhere Exponenten aussieht. Wie kennen vielleicht noch

1.7 $\sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4}$

Die rechten Seiten von (1.6) und (1.7) sind also Polynome in n.

1.8 Bezeichnung: Sei $S(n,r) = 1^r + 2^r + \ldots + (n-1)^r$.
Also $S(n,0) = n-1$, $S(n,1) = \frac{n(n-1)}{2}, \ldots$

1.9 Aufgabe: Zeigen Sie:
$n^{r+1} - 1 = \binom{r+1}{1}S(n,r) + \binom{r+1}{2}S(n,r-1) + \ldots + \binom{r+1}{r+1}S(n,0)$.

Mit Hilfe von (1.9) kann man rekursiv einen polynomialen Ausdruck für $S(n,r)$ finden.

1.10 Definition: Der Koeffizient B_r von n im polynomialen Ausdruck von $S(n,r)$ heißt r-te **Bernoulli-Zahl** (nach Jakob Bernoulli 1655-1705).

1.11 Beispiel:
$B_0 = 1$, da $S(n,0) = n-1$
$B_1 = -\frac{1}{2}$, da $S(n,1) = \frac{n(n-1)}{2} = \frac{n^2}{n} - \frac{n}{2}$
$B_2 = \frac{1}{6}$, da $S(n,2) = \frac{n-1)\cdot n\cdot(2n-1)}{6} = \frac{1}{6}(2n^3 - 3n^2 + n)$
$B_3 = 0$, da $S(n,3)$ keine linearen Terme hat.

1.12 Aufgabe: (1) $B_r = \frac{-1}{r+1}\sum_{k=2}^{r+1} B_{r+1-k}$

(2) Der Koeffizient von n^k im polynomialen Ausdruck von $S(n,r)$ ist

$$\frac{r!B_{r-k+1}}{(r-k+1)!k!} = \binom{r}{k}\frac{B_{r-k+1}}{r-k+1}.$$

(3) Berechnen Sie $B_4, \ldots, B_{10}$.

1.13 Historisches:

(1) Wie schon angedeutet, haben Dreieckszahlen, Tetraederzahlen u.ä. die Phantasie vieler (Hobby-) Mathematiker angeregt, darunter auch große Namen.

Gauß (1777-1855) bewies um 1800, dass sich jedes $n \in \mathbb{N}$ als Summe dreier Dreieckszahlen schreiben läßt.

Beispiel: $9 = 6 + 3 + 0$.

(2) Ein anderes Ergebnis ähnlicher Art ist von Joseph Louis Lagrange (1736-1813) bewiesen: Jedes $n \in \mathbb{N}$ ist Summe von 4 Quadraten (weniger als 4 ist nicht möglich: $7 = 2^2 + 1^2 + 1^2 + 1^2$)

(3) 1875 stellte der Artillerie-Offizier Edouard Lucas (1842-1891) folgende Behauptung auf: Eine quadratische Pyramide aus Kanonenkugeln enthält genau dann eine Quadratzahl von Kanonenkugeln, wenn sie 24 entlang einer Basiskante hat.

Diese Behauptung wurde erst 1918 mit Hilfe der Theorie der elliptischen Funktionen bewiesen. Ein elementarer Beweis erschien erst 1988.

(4) Bernoulli-Zahlen spielen in vielen Bereichen der Mathematik eine Rolle: In der Algebra, hier natürlich insbesondere in der algebraischen Zahlentheorie, in der Analysis in der Potenzreihenentwicklung des hyperbolischen Tangens

$$\frac{x}{e^x - 1} = \sum_{n=0}^{\infty} \frac{B_n}{n!} x^n$$

in der algebraischen Topologie, usw.

(5) Wir schließen mit einer Beobachtung von Nicomachus von Gerasa (ca 100 v. Chr.). Im Dreieck

				1					Summe:	1
			3		5					8
		7		9		11				27
	13		15		17		19			64
21		23		25		27		29		125

ist die Summe der Zahlen der n-ten Zeile genau n^3.

2 Primzahlen

Die klassische Zahlentheorie beschäftigt sich mit den natürlichen Zahlen $N = \{1, 2, \ldots\}$. Wir müssen uns daher auf ein Axiomensystem einigen, das wir zugrundelegen wollen. Hier möchte ich auf bereits bekanntem aufbauen und nehme die Körperaxiome von $\mathbb{Q}$ einschließlich der Ordnungaxiome. Wir definieren $\mathbb{N}$ als die Vielfachen von 1, also

$$n = 1 + 1 + 1 \ldots + 1 \quad n\text{-mal.}$$

Man leitet daraus leicht das Induktionsprinzip und das Wohlordnungsprinzip ab. Mehr wollen wir nicht voraussetzen.

2.1 Definition: $p \in \mathbb{N}$ heißt **Primzahl**, wenn p genau zwei Teiler in $\mathbb{N}$ hat.

2.2 Fundamentalsatz der Zahlentheorie: Jedes $n \in \mathbb{N}$, $n > 1$ ist **eindeutig** als Produkt von Primzahlen

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_r$$

mit $p_1 \leq p_2 \leq \ldots \leq p_r$ darstellbar.

Existenz: Angenommen, nicht jede natürliche Zahl > 1 ist ein Produkt von Primzahlen. Nach dem Wohlordnungsprinzip gibt es einen kleinsten Verbrecher n. Angenommen

$$n = k \cdot l$$

mit $k, l \in \mathbb{N}$, $k, l < n$. Dann sind k und l Produkte von Primzahlen und damit auch n. Also sind n und 1 die einzigen Teiler von n, d.h. n ist selbst prim, da $n > 1$. Widerspruch

Eindeutigkeit: Sei

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_r = q_1 \cdot q_2 \cdot \ldots \cdot q_s$$

mit $p_1 \leq \ldots \leq p_r$ und $q_1 \leq \ldots \leq q_s$ wieder der kleinste Verbrecher. Dann ist $p_1 \neq q_1$, denn andernfalls könnten wir p_1 kürzen und erhielten einen kleineren Verbrecher. O.B.d.A. $p_1 < q_1$. Da 1 keine Primzahl ist, kann n keine Primzahl sein, d.h. $r, s > 1$. Also folgt $n \geq q_1^2 > p_1 \cdot q_1$. Somit

$$1 \leq n - p_1 q_1 < n$$

p_1 und q_1 sind Teiler von n und somit von $n - p_1 q_1$. Da $n - p_1 \cdot q_1 < n$, hat

$$n - p_1 q_1$$

eine eindeutige Primfaktorzerlegung, und da p_1 und q_1 Teiler sind, folgt

$$n - p_1 q_1 = p_1 q_1 \cdot r \quad r \in \mathbb{N}.$$

Es folgt: $n = q_1(p_1 r + p_1)$

$$q_2 \dots q_s = p_1(r+1).$$

Da $q_2 \cdot \ldots \cdot q_s < n$, hat diese Zahl eine eindeutige Primfaktorzerlegung, insbesondere taucht p_1 unter den $q_2, \dots, q_1$ auf. Aber $p_1 < q_i \forall i$ ↯

2.3 Satz: Es gibt unendlich viele Primzahlen.

Beweis: Zu jeder Liste von Primzahlen $p_1, \dots, p_n$ kann man eine weitere finden: Sei q ein Primfaktor von $m = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$. Kein p_i ist Teiler von m, da es sonst Teiler von 1 wäre. Also ist q von $p_1, \dots, p_n$ verschieden. □

2.4 Satz: Zwischen den Primzahlen gibt es beliebig große Lücken. D.h. zu jedem $n \in \mathbb{N}$ gibt es eine Zahl $a_n \in \mathbb{N}$, so dass $a_n + i$ für $1 \leq i \leq n$ nicht prim ist.

Beweis: $a_n = (n+1)! + 1$ tut's, denn $i + 1$ ist Teiler von

$$a_n + i = (n+1)! + (i+1) \quad 1 \leq i \leq n.$$

□

Die Verteilung der Primzahlen ist ein großes Problem der Zahlentheorie und Inhalt zahlreicher Untersuchungen. Im Rahmen dieser Vorlesung werden wir kaum Zeit haben, darauf einzugehen. Wir werden im Weiteren noch folgendes elementares Ergebnis benutzen.

2.5 Division mit Rest: Seien $m, n \in \mathbb{N}^*$. Dann $\exists\, q, r \in \mathbb{R}$, so dass

$$n = q \cdot m + r \quad \text{mit } 0 \leq r \leq m.$$

Beweis: Dies ist klar für $m = 1$. Sei also $m > 1$. Wir beweisen den Satz induktiv:

$$1 = 0 \cdot m + 1 \quad \text{mit } 0 \leq r < m.$$

Induktionsschritt von n auf $n+1$: Sei $n = q \cdot m + r$ mit $r < m$. Dann folgt

$$(n+1) = q \cdot m + (r+1).$$

Ist $r + 1 < m$, sind wir fertig. Anderfalls ist $r + 1 = m$ und

$$(n+1) = q \cdot m + m = (q+1) \cdot m + 0.$$

□

2.6 Historisches:

(1) Satz 2.3 geht auf Euklid von Alexandria zurück ($\sim$ 300 v. Chr.)

(2) Die Eindeutigkeit der Primfaktorzerlegung wurde lange Zeit nicht als Problem erkannt. Erst Gauß gab 1801 einen Beweis.

(3) Die Sätze (2.3) und (2.4) werfen die Frage nach der **Verteilung der Primzahlen** auf: Sei $\pi(x)$ die Anzahl der Primzahlen $\leq x$. Man beschreibe $\pi(x)$.

Definition: Sei $U \subset \mathbb{R}$, x_0 Häufungspunkt von U und $f, g : U \to \mathbb{R}$ seien zwei Funktionen. Wir schreiben

$$f(x) \sim g(x), x \to x_0, \qquad \text{falls } \lim_{x \to x_0} \frac{f(x)}{g(x)} = 1.$$

Primzahlsatz: $\pi(x) \sim \frac{x}{\log x}$, $x \to \infty$.

Da wir in dieser Vorlesung verschiedenste Aspekte der Zahlentheorie ansprechen wollen, bleibt uns keine Zeit für den Beweis dieses Satzes.

Folgendes Resultat von Euler kann ebenfalls als Aussage über dies Dichte der Primzahlen interpretiert werden.

Euler (1737): $\sum\limits_{p \text{ prim}} \frac{1}{p}$ divergiert.

(Beachte $\sum\limits_{n \in \mathbb{N}^*} \frac{1}{n^\alpha}$ konvergiert für $\alpha > 1$.)

(4) Es gibt im Bereich der Primzahlen noch zahlreiche offene Fragen. Eine der bekanntesten ist die Untersuchung von Primzahlzwillingen, d.h. von Paaren von Primzahlen der Form $(2n-1, 2n+1)$. Beispiele sind

$$(3,5), (5,7), (11,13), (17,19), (29,31), (41,43).$$

Ein offenes Problem ist, ob es unendlich viele davon gibt.

Nach Auswertung des damals verfügbaren Zahlenmaterials stellten Godfrey Harold Hardy (1877-1947) und John Edensor Littlewood (1885-1977) folgende Vermutung auf.

Vermutung: Ist $\pi_2(x)$ die Anzahl der Primzahlzwillinge $\leq x$, dann gilt

$$\pi_2(x) \sim 2c \frac{x}{\log^2 x}, \quad x \to \infty.$$

Ist $p_1 = 2$, $p_2 = 3$, $p_3 = 5, \ldots$ die Folge der Primzahlen, dann ist

$$c = \prod_{k=2}^{\infty} \frac{p_k(p_k - 2)}{(p_k - 1)^2} = 0,6601618158\ldots$$

Die Konstante c ist bis auf einen Fehler $< 10^{-40}$ berechnet. Stimmt die Vermutung, gibt es unendlich viele Primzahlzwillinge. Alle bisherigen Computerberechungen unterstützen die Vermutung.

Dass das Problem kompliziert ist, zeigt auch folgendes Ergebnis des norwegischen Mathematikers Viggo Brun (1885-1978).

Brun (1919): $\sum_{\substack{p \text{ Primzahl-} \\ \text{zwilling}}} \frac{1}{p}$ konvergiert.

Der Grenzwert ist unbekannt. Nicely berechnete **alle** Primzahlenzwillinge kleiner als 10^{14} (dabei entdeckte er den berüchtigten Bug des Pentium Processors) und errechnete

$$1,902160578$$

als **heuristischen Schätzwert** für diese Summe.

Weitere Informationen im Anschuß an §3.

3 Perfekte Zahlen

Sei $n = p_1^{r_1} \ldots, p_k^{r_k}$ die Primfaktorzerlegung von n mit $p_1 < p_2 < \ldots < p_k$. Eine Zahl $x \in \mathbb{N}$ ist genau dann ein Teiler von n, wenn

$$x = p_1^{s_1} \ldots p_k^{s_k} \quad \text{mit } 0 \leq s_i \leq r_i \quad i = 1, \ldots, k.$$

Also besitzt n genau

$$d(n) = (r_1 + 1) \cdot (r_2 + 1) \cdot \ldots \cdot (r_k + 1)$$

Teiler. Jeder dieser Teiler trifft genau einmal als Summand im ausmultiplizierten Produkt

$$(1 + p_1 + \ldots + p_1^{r_1}) \cdot (1 + p_2 + \ldots + p_2^{r_2}) \cdot \ldots \cdot (1 + p_k + \ldots + p_k^{r_k})$$

auf. Wir erhalten somit

3.1 Definition und Satz: Sei $n \in \mathbb{N}^*$, sein $d(n)$ die Anzahl der Teiler von n und $s(n)$ die Summe aller Teiler. Dann gilt $d(n) = \prod_{i=1}^{n}(r_i + 1)$ und

$$s(n) = \prod_{i=1}^{k}(1 + p_i + \ldots + p_i^{r_i}) = \prod_{i=1}^{k} \frac{p_i^{r_i+1} - 1}{p_i - 1}$$

falls $u = p_1^{r_i+1} \cdots p_k^{r_k}, p_1 < \ldots < p_k$ die Primfaktorzerlegung von n ist.

3.2 (1) n prim $\leftrightarrow s(n) = n + 1$,

(2) m, n teilerfremd $\Rightarrow s(m \cdot n) = s(m) \cdot s(n)$.

3.3 Definition: Sei $s'(n)$ die Summe der echten Teiler von n, also $s'(n) = s(n) - n$. $n \in \mathbb{N}^*$ heißt **PERFEKT**, falls $s'(n) = n$, d.h. $s(n) = 2n$.

3.4 Beispiel: 6, 28, 496, 8128, 33550336 sind perfekt.

Über perfekte Zahlen ist trotz intensiver Forschung wenig bekannt.

3.5 Offene Probleme

(1) Gibt es ungerade perfekte Zahlen?

(2) Gibt es unendlich viele perfekte Zahlen?

Die folgenden klassischen Ergebnisse summieren fast alles, was über perfekte Zahlen bekannt ist.

3.6 Euklid: Ist $2^m - 1$ prim, dann ist $2^{m-1}(2^m - 1)$ perfekt.

Beweis: Sei $n = 2^{m-1} \cdot (2^m - 1)$. Nach Voraussetzung ist $2^m - 1$ prim. Aus (3.1) und (3.2) folgt, da $n = 2^{m-1} \cdot p$

$$s(n) = \frac{2^m - 1}{2 - 1} \cdot \frac{p^2 - 1}{p - 1} = (2^m - 1) \cdot (p + 1) = (2^m - 1) \cdot 2^m = 2n.$$

□

3.7 Leonhard Euler (1707-1783): Ist n eine gerade perfekte Zahl, dann ist n von der Form $2^{m-1}(2^m - 1)$ mit $2^m - 1$ prim.

Beweis: Sei n perfekt, $n = 2^{m-1} \cdot q$ mit ungeraden q. Jeder Teiler von n hat die Form $2^r \cdot d$ mit $0 \leq r \leq m-1$ und $d|q$. Es folgt

$$s(n) = (1 + 2 + \ldots + 2^{m-1}) \cdot s(q) = (2^m - 1) \cdot s(q) = 2n = 2^m \cdot q.$$

Also

$$q = (2^m - 1)s(q) - (2^m - 1)q = (2^m - 1)(s(q) - q) \qquad (*)$$

Angenommen $s(q) - q > 1$. Dann hat q die verschiedenen Faktoren $s(q) - q$, q und 1, denn

(i) $q > 1$. Anderenfalls wäre $n = 2^{m-1}$ und $s(n) = \sum_{r=0}^{m-1} 2^r = 2^m - 1 \neq 2n$.

(ii) $s(q) - q \neq q$. Anderenfalls wäre $q - (2^m - 1) \cdot q$, also $m = 1$ und dann n ungerade.

Es folgt: $s(q) \geq s(q) - q + q + 1 = s(q) + 1$ ↯
Also folgt $s(q) = q + 1$. Das bedeutet aber, dass q prim ist, und wir erhalten aus $(*)$, dass $q = 2^m - 1$. □

3.8 Folgerung: Da $2^{m-1}(2^m - 1) = \frac{2^m(2^m-1)}{2}$, sind alle geraden perfekten Zahlen auch Dreieckszahlen.

Damit reduziert sich das Suchen nach geraden perfekten Zahlen auf die Suche von Primzahlen der Form $2^m - 1$.

3.9 Definition: Eine Primzahl der Form $2^m - 1$ heißt **Mersenne'sche Primzahl** nach dem Geistlichen Marin Mersenne (1588-1648), der die ersten acht geraden perfekten Zahlen korrekt angegeben hat.

3.10 Satz (Mersenne): $2^m - 1$ ist für $m = 2, 3, 5, 7, 13, 17, 19$ und 31 prim.

Man hätte also gerne einen Algorithmus, mit dem man schnell entscheiden kann, ob $2^m - 1$ prim ist oder nicht. Ein solcher Algorithmus ist von dem im §1 erwähnten Edouard Lucas entdeckt und von Derrick Lehmer (1905-1991) weiterentwickelt werden.

3.11 Lucas-Lehmer: Sei $(a_n)_{n\in\mathbb{N}}$ die Folge mit $a_1 = 4$ und $a_{n+1} = a_n^2 - 2$. Dann gilt: $2^m - 1$ ist für $m > 2$ eine Primzahl, falls $2^m - 1$ Teiler von a_{m-1} ist.

Beispiel: $2^5 - 1$ ist ein Faktor von $a_4 = 37.634$
Wir wollen noch kurz auf eine Variante der Perfektion eingehen.

3.12 Sei $n \in \mathbb{N}^*$. Wir betrachten die Folge

$$n,\ s'(n),\ s'(s'(n)),\ s'(s'(s'(n))),\ \ldots$$

3.13 Beispiel: (1) 12, 16, 15, 9, 4, 3, 1

(2) 25, 6, 6, ...

(3) 220, 284, 220, 284, ... (befreundet)

(4) 12496, 14288, 15472, 14264, 12496, ...

Die Beispiele errechnet man mit Hilfe von Satz 3.1. Es gibt also abbrechende Folgen, Folgen die bei einer perfekten Zahl ankommen und dann konstant bleiben, aber auch periodische Folgen.

3.14 Definition: Eine Zahl n heißt **BEFREUNDET**, falls $s'(s'(n)) = k$, den jeweiligen **FREUND** findet man durch Anwenden von s'. Zahlen in einem periodischen Block der Länge > 2 heißen **SOZIAL**.

3.15 Offene Fragen:

(1) Gibt es unendlich viele befreundete Zahlen?

(2) Gibt es soziale Sequenzen beliebiger Periode?

(3) Gibt es Sequenzen, die weder abbrechen noch periodisch werden? 276 wäre ein Kandidat.

3.16 Historisches:

(1) Perfekte Zahlen haben Zahlenmystiker aller Zeiten fasziniert. Schon Augustin (354-430) schrieb in seiner "Stadt Gottes": 6 ist eine perfekte Zahl aus sich heraus und nicht weil Gott alle Dinge in 6 Tagen erschaffen hat, das Gegenteil triff zu. Gott erschuf die Welt in 6 Tagen, weil diese Zahl perfekt ist, und sie wäre auch perfekt, wenn die Arbeit der 6 Tage nicht existiert..

(2) Bis 1588 waren die perfekten Zahlen aus Beispiel (3.4) die einzig bekannten. Die nächsten drei wurden von Mersenne gefunden (3.10). Mersenne behauptete fälschlicherweise, dass auch $2^{67} - 1$ prim sei.

1903 hielt Frank Nelson Cole einen Vortrag, der aus 2 Rechnungen bestand. Man kann dies allerdings keine Vortrag nennen, weil er kein Wort sagte. Er berechnete wortlos $2^{67} - 1$ und

$$193\,707\,721 \times 761\,838\,257\,287$$

Die Ergebnisse waren gleich. Es kam zu “standing ovations”

(3) Bis 1950 kann man gerade eben 12 perfekte Zahlen. Durch Einsatz von Computern sind bis heute (1. Juli 2009) die ersten 39 geraden perfekten Zahlen und noch 8 weitere bekannt. Man weiß aber nicht, ob noch weitere dazwischen liegen.

Man kennt die ersten 39 Mersenne'schen Primzahlen und noch 8 weitere, von denen man vermutet, dass sie die 40. bis 47. Mersenne'schen Primzahlen sind.

Die größte zur Zeit bekannte Primzahl ist

$$2^{43112608} - 1.$$

Sie wurde 2008 entdeckt und hat 12.978.189 Stellen.

Die größten bekannten Primzahlenzwillinge sind

$$2003663613 \cdot 2^{195000} \pm 1.$$

Sie wurden 2007 entdeckt und haben 58711 Stellen.

(4) $d(n)$ und $s(n)$ sind wie $\pi(n)$, $\pi_2(N)$ zahlentheoretische Funktionen, die man auf ihr asymptotischen Verhalten untersuchen kann.

Definition: Eine zahlentheoretische Funktion f hat die **MAXIMALE GRÖSSENORDNUNG** von g, wenn es zu jedem $\varepsilon > 0$ ein $N(\varepsilon)$ gibt, so dass

(1) $f(n) < (1+\varepsilon)g(n) \quad \forall n > N(\varepsilon)$

(2) $(1-\varepsilon)g(n) < f(n)$ für unendliche viele n.

Es gilt:

(a) $\log d(n)$ hat die maximale Größenordnung $\frac{\log 2 \cdot \log n}{\log(\log n)}$.

(b) Gronwall: $s(n)$ hat die maximale Grßoßenordnung $e^{\gamma} \cdot n \log(\log n)$, wobei $\gamma = \lim\limits_{n\to\infty}(1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n} - \log n) = 0,577\ldots$

4 Diophantische Gleichungen

Diophant von Alexandria ist der bedeutendste, wenn nicht der einzige nennenswerte Algebraiker der Antike. Während in Rom Christenverfolgungen stattfanden, behandelte er in 13 Büchern “Arithmetica” in der 2. Hälfte des

3. Jahrhunderts zahlentheoretische und algebraische Probleme ohne die in der Antike übliche geometrische Einkleidung. Die Bücher widmete er Dionysius, dem Bischof von Alexandria von 247 bis 264.

4.1 Definition: Eine **diophantische Gleichung** (im zahlentheoretischen Sinn) ist eine polynomiale Gleichung in mehreren Unbekannten mit ganzzahligen Koeffizienten.

In dem Bemühen, diophantische Gleichungen zu lösen, entstanden ganze Zweige der Mathematik, allen voran die Algebraische Zahlentheorie und mit ihr die Algebra.
Es gibt keine allgemeinen Lösungstrategien für solche Gleichungen (Yuri Matijasevicz zeigte 1970, dass es kein allgemeines Lösungsverfahren gibt.), sondern nur Methoden, die in vielen, aber nicht in allen Fällen zum Ziel führen. Gesucht werden ganzzahlige Lösungen solcher Gleichungen, aber schon in den einfachsten Fällen, brauchen solche Lösungen nicht zu existieren: Offensichtlich hat

4.2

$$2x + 3 = 2y$$

keine ganzzahlige Lösung, denn die linke Seite ist stets ungerade, während die rechte gerade ist.
Dagegen hat die Gleichung

$$x^2 + y^2 = z^2$$

unendlich viele Lösungen.

4.3 Definition: Eine Lösung (x, y, z) der diophantischen Gleichung

$$x^2 + y^2 = z^2$$

mit $x, y, z \in \mathbb{N}$ heißt **PYTHAGORÄISCHES TRIPEL**. Ist außerdem $\mathrm{ggT}(x, y, z) = 1$, heißt (x, y, z) **PRIMITIVES** pythagoräisches Tripel. Sei $\mathcal{T}$ die Menge der pythagoräischen Tripel, $\mathcal{PT}$ die der primitiven.

Wir wollen $\mathcal{T}$ bestimmen

4.4 Sei (x, y, z) ein pythagoräisches Tripel. Dann gilt

(1) $\forall n \in \mathbb{N}$ ist $(n \cdot x, n \cdot y, n \cdot z)$ ein pythagoräische Tripel.

(2) Ist d Teiler von zwei von x, y, z, so auch vom dritten und $\left(\frac{x}{d}, \frac{y}{d}, \frac{z}{d}\right)$ ist pythagoräisches Tripel

(3) Es gibt ein $n \in \mathbb{N}$ und ein primitives pythagoräisches Tripel $(\overline{x}, \overline{y}, \overline{z})$, so dass $(x, y, z) = (n \cdot \overline{x}, n \cdot \overline{y}, n \cdot \overline{z})$

(1) und (2) sind trivial, (3) folgt aus (1) und (2).
Wir brauchen also nur die Menge der primitiven pythagoräischen Tripel zu bestimmen.

4.5 $(x, y, z) \in \mathcal{PT}$, dann haben x und y verschieden **PARITÄT**, d.h. eine Zahl ist gerade, die andere ungerade.

Beweis: Nach (4.4.2) können x und y nicht beide gerade sein. Sind nun x und y ungerade, also $x = 2k + 1$, $y = 2l + 1$, dann ist

$$z^2 = (2k + 1)^2 + (2l + 1)^2 = 4k^2 + 4k + 4l^2 + 4l + 2.$$

Da z^2 gerade ist, ist auch z gerade und damit 4 ein Teiler von z^2. Folglich muß 4 auch Teiler von 2 sein, ein Widerspruch. □
Sei $\mathcal{PT}' = \{(x, y, z) \in \mathcal{PT}; x \text{ gerade}\}$. Nach dem bisher bewiesenen gilt

$$\mathcal{T} = \{nx, ny, nz) : n \in \mathbb{N}^*, (x, y, z) \in \mathcal{PT}' \text{ oder } (y, x, z) \in \mathcal{PT}'\}.$$

Wir müssen also nur $\mathcal{PT}'$ bestimmen.

4.6 Satz: Sei $U = \{(a, b) \in \mathbb{N}^2; a > b > 0, a \cdot b \text{ gerade }, \text{ggT}(a, b) = 1\}$. Dann ist

$$\varphi : U \to \mathcal{PT}', \quad (a, b) \mapsto (2ab, a^2 - b^2, a^2 + b^2)$$

bijektiv.

Beweis: $\varphi(a, b) \in \mathcal{T}$, denn

$$\begin{aligned} (2ab)^2 + (a^2 - b^2)^2 &= 4a^2b^2 + a^4 - 2a^2b^2 + b^4 = a^4 + 2a^2b^2 + b^4 \\ &= (a^2 + b^2)^2 \end{aligned}$$

Da $\text{ggT}(a, b) = 1$ und $a \cdot b$ gerade ist, haben a und b verschiedene Parität. Also sind $a^2 - b^2$ und $a^2 + b^2$ ungerade. Ist nun p ein Primfaktor von $\text{ggT}(2ab, a^2 - b^2, a^2 + b^2)$, so ist $p > 2$. Da $p|a^2 - b^2$ und $p|a^2 + b^2$, folgt dass p Teiler von $a^2 - b^2 + a^2 + b^2 = 2a^2$ ist. Da $p > 2$, folgt $p|a^2$ und damit $p|a$. Analog teilt p auch $a^2 - b^2 - (a^2 - b^2) = 2b^2$, also b, ein Widerspruch. Es folgt $\varphi(a, b) \in \mathcal{PT}'$.
φ **ist surjektiv:** Sei $(x, y, z) \in \mathcal{PT}'$. Da x gerade ist, ist $x = 2k$. Es folgt

$$4k^2 = x^2 = z^2 - y^2 = (z + y)(z - y).$$

Da x gerade und y ungerade ist, sind z und y ungerade, also $z+y$ und $z-y$ gerade, d.h.

$$z+y=2u \quad z-y=2v.$$

Sei p ein Primfaktor von $\mathrm{ggT}(u,v)$. Dann folgt $2p|z+y$ und $2p|z-y$. Damit teilt $2p$ auch $z+y+(z-y)=2z$ und $z+y-(z-y)=2y$. Es folgt: $p|z$ und $p|y$. Da $\mathrm{ggT}(y,z)=1$, ist dies unmöglich, also sind u und v teilerfremd. Da nun

$$4k^2=(2u)\cdot(2v)=4u\cdot v,$$

ist $k^2=u\cdot v$. Da u und v teilerfremd sind, sind sie selbst Quadratzahlen, also von der Form

$$u=a^2 \quad v=b^2.$$

$$\begin{array}{rcl} \text{Es folgt } 2z & = & 2u+2v, \text{ also } z=u+v=a^2+b^2 \\ 2y & = & 2u-2v, \text{ also } y=u-v=a^2-b^2 \\ x & = & 2k=2a\cdot b \end{array}$$

Da $\mathrm{ggT}(u,v)=1$, ist $\mathrm{ggT}(a,b)=1$. Aus $u>v$ folgt außerdem $a>b>0$. Also ist $(a,b)\in U$ und $\varphi(a,b)=(x,y,z)$.

φ ist injektiv: Sei $\varphi(a_1,b_1)=\varphi(a_2,b_2)$, also

$$\begin{array}{rcl} a_1^2+b_1^2 & = & a_2^2+b_2^2 \\ a_1^2-b_1^2 & = & a_2^2-b_2^2 \end{array} \qquad \text{Es folgt durch addieren } 2a_1^2=2a_2^2.$$

Also $a_1=a_2$, da $a_i>0$ und $b_i>0$. Aus $2a_1b_1=2a_2b_2$ folgt dann $b_1=b_2$. $\square$

4.7 Zur Geschichte: Schon in Mesopotanien konstruierte man pythagoräische Zahlen mit Hilfe der Formel von φ, beschränkte sich dabei aber aus solche a,b deren Primzahlen nur $3,2,5$ enthielten, die Primzahlen in der mesopotanischen Skala 60.

Dass alle pythagoräischen Zahlen so konstruiert werden können, wurde erst durch C.A. Koerbero 1738 bewiesen. Die Injektivität von φ wurde erst von Leopold Kronecker (1823-1891) bemerkt.

Wir haben die diophantische Gleichung $x^2+y^2=z^2$ mit Hilfe einer geeigneten Faktorisierung untersucht, nämlich der Faktorisierung

$$x^2=z^2-y^2=(z+y)\cdot(z-y).$$

Diese Methode führt oft zum Ziel. Wir illustrieren das an einem weitern Beispiel.

4.8 $x^3+y^3=2$

Lösung: $2 = x^3 + y^3 = (x+y) \cdot (x^2 - xy + y^2)$
Wir haben folgende vier Möglichkeiten:

$$\begin{array}{lll} x+y = \pm 1 & \text{und } x^2 - xy + y^2 = \pm 2 & \text{I} \\ x+y = \pm 2 & \text{und } x^2 - xy + y^2 = \pm 1 & \text{II} \end{array}$$

Da $x^2 - xy + y^2 = (x+y)^2 - 3xy$, folgt für

$$\begin{array}{ll} \text{I} & 1 - 3xy = \pm 2 \\ \text{II} & 4 - 3xy = \pm 1 \end{array}$$

Es folgt $(x, y) = (1, 1)$ ist die einzige Lösung in $\mathbb{Z}^2$.

Eine andere Lösungsmethode, die oft zum Ziel führt, ist eine Zerlegung in Restklassen. Wir demonstieren diese Methode an einer diophantischen Gleichung, die erstmals von R Finkelstein und H. London 1971 untersucht wurde.

4.9 $x^3 + 117y^3 = 5$

Lösung: In $\mathbb{Z}/3$ geht die Gleichung in $\overline{z}^{-3} = \overline{2} = \overline{-1}$ über. Da $\overline{0}^3 = \overline{0}$ und $\overline{1}^3 = \overline{1}$, folgt $\overline{x} = \overline{-1}$, d.h. $x = 3m - 1$. Wir erhalten

$$27m^3 - 27m^2 + 9m - 1 = x^3 = -117y^3 + 5 = 9 \cdot (-13y^3) + 5.$$

Bei der Division durch 9 hat x^3 einerseits den Rest -1 (und anderseits den Rest 5. Das ist unmöglich. Also hat (4.9) **keine Lösung**. □

Das Problem hierbei ist natürlich zu erkennen, welche Zahl (hier 3) man für die Restklassenmethode heranziehen sollte.

Auch die Kanonenkurgelaufgabe von Edouard Lucas (1.13.3) ist eine diophantische Gleichung. Er behauptet, dass $x = 24$ die einzige Lösung folgender diophantischer Gleichung ist.

4.10 $(x+1) \cdot x \cdot (2x+1) = 6y^2$

Die elementare Lösung von Anglin aus 1988 macht sich andere diophantische Gleichungen zu nutze:

4.11 Satz: (1) Die Gleichung $2x^4 + 1 = y^2$ hat nur die Lösung $(x, y) = (0, 1)$ in $\mathbb{N}^2$.

(2) Die Gleichung $2x^2 - 1 = y^4$ hat nur die Lösung $(x, y) = (1, 1)$ in $\mathbb{N}^2$.

(3) Die Gleichung $8x^4 + 1 = y^2$ hat nur die Lösung $(x, y) = (0, 1), (1, 3)$ in $\mathbb{N}^2$.

(3) folgt leicht aus (1) und (2), die dagegen nicht ganz so einfach sind. Gegebenenfalls werden wir später den Beweis nachtragen.

Die wohl berühmteste diophantische Gleichung ist die aus "Fermats letztem Satz".

Pierre de Fermat (1601-1665) war Ratsherr im Parlament von Toulouse und betrieb Mathematik nur als Hobby. Er publizierte nur eine mathematische Arbeit. Beim Studium von Bachet's Übersetzung eines der Werke Diophants ins Lateinische stieß er auf die pythagoräische Gleichung

$$x^2 + y^2 = z^2,$$

die wir im Satz (4.6) vollständig lösten. Fermat schrieb auf den Seitenrand folgende Notiz, die in den folgenden Jahrhunderten zahlreiche Mathematiker bis in ihre Träume verfolgte:

"Es ist unmöglich, einen Kubus als Summe zweier Kuben zuschreiben, eine vierte Potenz als Summe zweier vierter Potenzen, oder allemeiner gesagt, irgendeine Potenz über der zweiten als Summe zweier Potenzen gleichen Grades. Ich habe eine wahrhaft wunderbare Beweisführung dieses allgemeinen Satzes entdeckt, der auf diesem Rand nicht Platz findet."

Also

4.12 Fermats letztem Satz: $x^n + y^n = z^n$ hat für $n > 2$ keine Lösung in $\mathbb{Z}\backslash\{0\}$.

Heute glaubt man nicht mehr daran, dass Fermat einen schlüssigen Beweis hatte. Für $n = 4$ hatte er einen Beweis, vielleicht auch für $n = 3$, der aber Euler zugeschrieben wird. (Euler behauptete 1735, einen Beweis zu haben. Veröffentlicht hat er einen Beweis 1770, der allerdings eine zum Glück füllbare Lücke enthielt). Eulers Beweis benutzt Fermat's Methode des **UNENDLICHEN ABSTIEGES**, die dieser im Falle $n = 4$ benutzte.

4.13 Fermat: $x^4 + y^4 = z^2$ hat keine Lösung in $\mathbb{Z}\backslash\{0\}$.

Beweis: Wir dürfen $x, y, z > 0$ voraussetzen. Sei (x, y, x) eine Lösung, so dass z minimal ist. Beachte, dass (x^2, y^2, z) ein pythagoräisches Tripel bilden. Wegen der Minimalität, sind diese Zahlen paarweise teilerfremd und damit auch x, y, z.

Da (x^2, y^2, z) ein primitives pythagoräisches Tripel ist, dürfen wir annehmen, dass x^2 gerade ist. Nach (4.6) gibt es

$$a > b > 0, \quad a \cdot b \text{ gerade}, \quad \text{ggT}(a, b) = 1$$

mit

$$x^2 = 2ab, \quad y^2 = a^2 - b^2, \quad z = a^2 + b^2$$

Es folgt: $b^2 + y^2 = a^2$.

Da $\text{ggT}(a, b) = 1$, ist (b, y, a) ein primitives pythagoräisches Tripel. Da außerdem y ungerade ist, ist b nach (4.5) gerade. Nach (4.6) existieren

$$\begin{array}{lll} & u > v > 0, & u \cdot v \text{ gerade} \quad \text{ggT}(u, v) = 1 \\ \text{mit} & b = 2u \cdot v, & y = u^2 - v^2. \quad a = u^2 + v^2 \end{array}$$

Es folgt

$$x^2 = 4uv(u^2 + v^2).$$

Nun sind u, v und $u^2 + v^2$ paarweise teilerfremd. Denn ist p ein Primteiler von u und $u^2 + v^2$, dann ist p auch Teiler von v^2, ein Widerspruch. Analog für v und $u^2 + v^2$. Es folgt u, v und $u^2 + v^2$ sind Quadratzahlen,

$$u = s^2, \quad v = t^2, \quad u^2 + v^2 = w^2.$$

Es folgt: $s^4 + t^4 = w^2$.

Aber $w^2 = u^2 + v^2 = a < x^2 \leq x^4 < z^2$. Widerspruch zur Minimalität. □

4.14 Folgerung: $x^{4k} + y^{4k} = z^{4k}$ hat keine Lösung in $\mathbb{Z}\backslash\{0\}$.

Die Geschichte von Fermats letztem Satz ist äußerst interessant. Sie führte zur Entwicklung der Algebraische Zahlentheorie.

1825 bewiesen Peter Gustav Lejenne-Dirichlet (1805-1859), also 20-jährig, und unabhängig davon Adrien-Marie Legendre (1752-1833), also 73-jährig, den Fall $n = 5$ nach der Methode von Euler. Der Beweis ist jedoch erheblich komplizierter und macht deutlich, dass mit wachsendem n die Anforderungen an die verwendete Algebra steigen.

4.15 Man beachte, dass es genügt, Fermats Satz für $n = 4$ und $n = p$, p prim $p > 2$ zu beweisen. Der allgemeine Fall folgt wie in (4.14).

1832 bewies Dirichlet den Fall $n = 14$, nachdem er sich vergeblich mit $n = 7$ herumgeplagt hatte.

1839 erledigte Gabriel Lamé (1795-1870) mit großem Einfallsreichtum den Fall $n = 7$.

1847 trug Lamé vor den Mitgliedern der Pariser Akademie einen allgemeinen Beweis vor, indem er die Fermat'sche Gleichung in den sog. ganzen Zahlen eines Kreisteilungskörpers in lineare Terme faktorisierte und dann mit der Methode des unendlichen Abstiegs einen Widerspruch

herbeiführte. Dabei benutzte er, dass die Faktorisierung in lineare Terme im wesentlichen eindeutig ist. Am Ende seiner Rede dankte er Joseph Liouville, dass er ihn auf die Idee gebracht habe, eine solche Faktorisierung mit Hilfe der komplexen Zahlen zu versuchen. Liouville holte Lamé in die Wirklichkeit zurück, indem er ihn auf die entscheidende Lücke im Beweis hinwies (die auch die Lücke im Euler-Beweis war): Woher wußte er, dass die Faktorisierung eindeutig war.

Lamé konnte diese Lücke nicht schließen. Beschämt schrieb er seinem Freund Dirichlet: "Wenn Du nur in Paris gewesen wärest, oder ich in Berlin, dann wäre dies alles nicht geschehen".

In der Tat hätte Dedekind ihn auf eine Arbeit von Ernst Eduard Kummer (1810-1893) aus dem Jahre 1844 in der völlig unbekannten Gratulationsschrift der Universität Breslau zur Jubelfeier der Universität Königsberg hinweisen können, in der Kummer bewies, dass die eindeutige Primfaktorzerlegung nicht in allen Ringen von ganzen Zahlen von Kreisteilungskörpern gilt.

1847 führte Kummer den Begriff der **idealen Zahl** ein, eine Art Zahlbereichserweiterung, aus der sich der Idealbegriff und damit ein entscheidender Zweig der Algebra eintwickelte. Mit seiner Hilfe bewies er den Fermat'schen Satz für alle **regulären** Primzahlen.

4.16 Definition: Eine Primzahl p heißt **REGULÄR**, wenn sie nicht Teiler der Zähler der Bernoulli'schen Zahlen $B_2, B_4, \ldots, B_{p-3}$ ist.

Kummer zeigte in seiner Arbeit von 1847, dass

$$37, 59, 67, 101, 103, 131, 149, 157$$

die einzigen irregulären Primzahlen < 164 sind.

Man beachte, dass Kummer mit seiner Arbeit eine große Klasse von Fällen bewies, nachdem sich Lamé noch 8 Jahre vorher mit dem Fall $n = 7$ lange herumplagte.

Kummers Arbeit stellte bis 1983 den größten einzelnen Fortschritt im Zusammenhang mit Fermat's letztem Satz dar.

1983 bewies Faltings ein allgemeines Ergebnis, aus dem folgt, dass $x^n + y^n = z^n$ für $n > 2$ höchstens endlich viele Lösungen hat. Dafür erhielt er 1986 die Fields-Medaille

Im Herbst 1994 endlich gelang Andrew Wiles eine völlige Lösung von Fermats letztem Satz mit Hilfe sog. Modulformen.

Schlussbemerkungen

Die Zahlentheorie hat sich aus speziellen Fragen über Zahlen, einer daraus entstandenen Zahlenmystik und auch Knobelaufgaben entwickelt. Oft ließen sich diese Fragen mit "ad hoc"-Methoden lösen, manchmal aber waren sie der Ausgangspunkt für die Geburt ganzer Zweige der Mathematik.

In dieser Vorlesung möchte ich einige dieser Aspekte aufgreifen: Neben "ad-ho"-Methoden möchte ich Einblicke in einige dieser Zweige vermitteln, mit deren Methoden zahlentheoretische Probleme lösen und umgekehrt aus zahlentheoretischen Aussagen Schlüsse auf andere mathematische Fragestellungen ziehen.

Teil II
Algebraische Werkzeuge

5 Ringe und Ideale

5.1 Definition: Ein *Ring* ist eine Menge R mit zwei Verknüpfungen, der Addition $+$ und der Multiplikation $\cdot$, so dass folgende Axiome gelten

(1) $(R, +)$ ist abelsche Gruppe, das neutrale Element bezeichnen wir mit 0

(2) $(R, \cdot)$ ist ein Monoid, das neutrale Element bezeichnen wir mit 1

(3) Es gelten die Distributivgesetze

$$a \cdot (b + c) = a \cdot b + a \cdot c, \quad (b + c) \cdot a = b \cdot a + c \cdot a \quad \forall a, b, c \in R$$

Ist $(R, \cdot)$ kommutativ, sprechen wir von einem *kommutativen Ring*.

Konvention: In dieser Vorlesung betrachten wir nur kommutative Ringe, es sei denn, es wird ausdrücklich von nicht kommutativen Ringen gesprochen.

5.2 Definition: $a \in (R, +, \cdot)$ heißt *Einheit*, wenn a bzgl. der Multiplikation ein rechts- und ein linksinverses Element besitzt (die dann gleich sind). Die Gruppe (s. Grundkurs) der Einheiten von $(R, \cdot)$ wird mit R^* bezeichnet.

5.3 Definition: Ein *Unterring* von R ist eine Teilmenge $S \subset R$, so dass S unter den Verknüpfungen $+$ und $\cdot$ auf R selbst ein Ring ist und dasselbe Null- und Einselement besitzt.

5.4 Aufgabe: Sei $S \subset R$, dann ist S genau dann Unterring, wenn

(i) $x, y \in S \Rightarrow x + y \in S$ und $x \cdot y \in S$

(ii) $\pm 1 \in S$

5.5 Definition: $a \in R\{0\}$ heißt *Nullteiler*, wenn es ein $b \neq 0$ gibt, so dass $a \cdot b = 0$. Ist 0 der einzige Nullteiler, heißt R *nullteilerfrei*.

5.6 Definition: Ein *Integritätsring* ist ein kommutativer, nullteilerfreier Ring. Ein Ring R, für den $R^* = R \backslash \{0\}$ heißt *Körper*.

5.7 Definition: Eine Abbildung $f : R \to S$ von Ringen heißt *Homomorphismus von Ringen*, wenn

$$f(x+y) = f(x) + f(y) \quad f(x \cdot y) = f(x) \cdot f(y) \quad \forall x, y \in R$$

und

$$f(1_R) = 1_S$$

5.8 Ist $f : R \to S$ ein Ringhomomorphismus und $T \subset S$ ein Unterring, dann ist $f(R)$ ein Unterring von S und $f^{-1}(T)$ ein Unterring von R.

Der Beweis ist dem Leser überlassen.

5.9 Definition: Sei R ein Ring. Eine Teilmenge $J \subset R$ heißt *Ideal*, wenn gilt

(i) J ist eine Untergruppe von $(R, +)$.

(ii) $r \cdot J \subset J \; \forall r \in R$ (D.h. ist $r \in R$ und $x \in J$, dann ist $r \cdot x \in J$.)

Sei J ein Ideal. Wir definieren eine Relation $\sim$ auf R durch

$$x \sim y \iff x - y \in J.$$

Dies ist eine Äquivalenzrelation:
$x \sim x$, denn $x - x = 0 \in J$, da J Untergruppe von $(R, +)$ ist.
$x \sim y \Rightarrow y \sim x$, denn
$x \sim y \Rightarrow x - y \in J \Rightarrow -(x - y) = y - x \in J \Rightarrow y \sim x$
$x \sim y \wedge y \sim z \Rightarrow x \sim z$, denn
$x \sim y \wedge y \sim z \Rightarrow (x - y \in J) \wedge (y - z) \in J \Rightarrow (x - y) + (y - z) = x - z \in J \Rightarrow x \sim z$.
Sei $\overline{x}$ die Äquivalenzklasse von x. Dann gilt

$$\overline{x} = \{x \in R; y - x \in J\} = \{y; y \in x + J\} = x + J.$$

Wir kennen diese Klassen als Nebenklassen des Normalteilers J der Gruppe $(R, +)$.
Da J Untergruppe von $(R, +)$ ist, gilt $J + J = J$. Da J Ideal ist, gilt $x \cdot J \subset J$ für alle $x \in R$. Es folgt

$$\begin{aligned} (x + J) + (y + J) &= x + y + J + J = (x + y) + J \\ (x + J) \cdot (y + J) &= x \cdot y + x \cdot J + y \cdot J + J \cdot J \subset x \cdot y + J + J + J = x \cdot y + J \end{aligned}$$

Da die Nebenklassen eine disjunkte Zerlegung von R bilden, wird durch die übliche Addition und Multiplikation jedem Paar von Nebenklassen **eindeutig** eine neue Nebenklasse zugeordnet. D.h. ist R/J die Menge dieser Nebenklassen, dann definieren

$$\begin{aligned} \overline{x} + \overline{y} &= \overline{x+y} \\ \overline{x} + \cdot \overline{y} &= \overline{x \cdot y} \end{aligned}$$

zwei Verknüpfungen auf R/J. Wir haben das bereits im Grundkurs bei den Ringen $\mathbb{Z}/n$ kennen gelernt.

5.10 Satz: Sei J ein Ideal in einem Ring R. Dann gilt

(i) die Menge R/J der Nebenklassen $\overline{x} = x + J$ ist unter

$$\overline{x} + \overline{y} = \overline{x+y} \text{ und } \overline{x} \cdot \overline{y} = \overline{x \cdot y}$$

ein Ring.

(ii) Die Projektion $p : R \to R/J$, $x \mapsto \overline{x}$, ist eine Ringhomomorphismus, und $\operatorname{Kern} p := \{x \in R;\ p(x) = \overline{0}\} = J$.

Beweis: (i) $\overline{0}$ ist das neutrale Element der Addition und $\overline{1}$ das der Multiplikation. Wir beweisen exemplarisch das Distributivgesetz. Die anderen Axiome werden analog angezeigt.

$$\begin{aligned} \overline{x} \cdot (\overline{y} + \overline{z}) &= \overline{x} \cdot \overline{y+z} = \overline{x \cdot (y+z)} = \overline{x \cdot y + x \cdot z} \\ &= \overline{x \cdot y} + \overline{x \cdot z} = \overline{x} \cdot \overline{y} + \overline{x} \cdot \overline{z} \end{aligned}$$

(ii)
$$\begin{aligned} p(x+y) &= \overline{x+y} = \overline{x} + \overline{y} = p(x) + p(y) \\ p(x \cdot y) &= \overline{x \cdot y} = p(x) \cdot p(y) \\ p(1) &= \overline{1} \end{aligned}$$

$x \in \operatorname{Kern} p \iff \overline{x} = \overline{0} \iff x \in J.$ □

5.11 Beispiel: (1) Ist $f : R \to S$ ein Ringhomomorphismus, dann ist

$$\operatorname{Kern} f = \{x \in R; f(x) = 0\}$$

ein Ideal. Umgekehrt ist nach 5.10 jedes Ideal Kern eines Ringhomomorphismus.

(2) Jede Untergruppe U von $(\mathbb{Z}, +)$ ist Ideal des Ringes $(\mathbb{Z}, +, \cdot)$.

(3) $\{0\}$ und R sind die *trivialen Ideale* eines Ringes R.

(4) Ein Körper $\mathbb{K}$ hat nur die trivialen Ideale: Ist $J \subset \mathbb{K}$ ein Ideal und $J \neq \{0\}$, dann ist $J = K$. Sei $x \neq 0$ aus J und $r \in \mathbb{K}$, dann ist $r = (r \cdot x^{-1}) \cdot x \in J$.

5.12 Aufgaben: (1) Ist $\{J_\alpha : \alpha \in A\}$ eine Familie von Idealen in R, dann ist $\bigcup_{\alpha \in A} J_\alpha$ ein Ideal.

(2) Sind I und J Ideale von R, dann ist $I + J$ ein Ideal.

5.13 Definition und Satz: Sei $A \subset R$ eine Teilmenge. Das kleinste Ideal $I(A)$ von R, das A enthält, heißt das von A *erzeugte Ideal*. Es gilt

$$I(A) = \bigcap \{U \subset R;\ U \text{ Ideal },\ A \subset U\}$$

Ein Ideal, das von einem einzigen Element erzeugt wird, heißt *Hauptideal*. Statt $I(\{a\})$ schreiben wir nur (a).

5.14 $(a) = R \cdot a$

Beweis: Da $a \in (a)$ und (a) ein Ideal ist, ist $r \cdot a \in (a)$ für alle $r \in R$, also $R \cdot a \subset (a)$. Weiter ist $R \cdot a$ ein Ideal, denn

(i) $R \cdot a \neq \emptyset$

(ii) mit $r_1 \cdot a$, $r_2 \cdot a \in R \cdot a$ ist $r_1 \cdot a - r_2 \cdot a = (r_1 - r_2) \cdot a \in R \cdot a$. Also ist $R \cdot a$ Untergruppe von $(R, +)$.

(iii) mit $r_1 \cdot a$ ist auch $r \cdot (r_1 \cdot a) = (r \cdot r_1) \cdot a \in R \cdot a$, also ist $R \cdot a$ ein Ideal. $R \cdot a$ enthält $a = 1 \cdot a$. Da (a) das kleinste Ideal ist, das a enthält, folgt $R \cdot a = (a)$.

□

5.15 Definition: Ein *Hauptidealring* oder PID (für "principal ideal domain") ist ein Integritätsring, in dem jedes Ideal ein Hauptideal ist.

5.16 Beispiel: $\mathbb{Z}$ ist ein Hauptring. Wir wissen aus dem Grundkurs, dass jede Untergruppe von der Form $n \cdot \mathbb{Z}$ ist, also nach 5.14 ein Hauptideal ist. Die Faktorringe $\mathbb{Z}/(n \cdot \mathbb{Z})$ sind die bekannten Restklassenringe.

5.17 Ein Ringhomomorphismus $f : R \to S$ ist genau dann injektiv, wenn Kern $f = \{0\}$.

Beweis: Ist f injektiv und $f(x) = 0$, dann ist $x = 0$, da auch $f(0) = 0$. Ist umgekehrt $\operatorname{Kern} f = \{0\}$, dann gilt

$$f(x) = f(y) \iff f(x-y) = f(x)-f(y) = 0 \iff x-y \in \operatorname{Kern} f \iff x = y.$$

□

5.18 Homomorphiesatz: Ist $f : R \to S$ ein Ringhomomorphismus, dann gibt es genau einen Ringhomomorphismus $\overline{f} : R/\operatorname{Kern} f \to S$, so dass

$$f = \overline{f} \circ p : R \to R/\operatorname{Kern} f \to S$$

$\overline{f}$ ist injektiv.

Beweis: Angenommen: $\overline{f}$ existiert. Dann gilt

$$\overline{f}(\overline{x}) = \overline{f}(p(x)) = f(x) \qquad (*)$$

Damit ist $\overline{f}$ durch f festgelegt.
Wir müssen zeigen, dass $(*)$ wohldefiniert ist, d.h. gilt $\overline{x} = \overline{y}$, dann muss

$$f(x) = \overline{f}(\overline{x}) = \overline{f}(\overline{y}) = f(y)$$

gelten.

$$\overline{x} = \overline{y} \iff x-y \in \operatorname{Kern} f \iff f(x-y) = f(x)-f(y) = 0 \iff f(x) = f(y)$$

$\overline{f}$ ist ein Ringhomomorphismus: Nach $(*)$ gilt

$$\overline{f}(\overline{x} + \overline{y}) = \overline{f}(\overline{x+y}) = f(x+y) = f(x) + f(y) = \overline{f}(\overline{x}) = \overline{f}(\overline{y})$$

Analog $\overline{f}(\overline{x} \cdot \overline{y}) = \overline{f}(\overline{x}) \cdot \overline{f}(\overline{y})$ und $\overline{f}(\overline{1}) = 1_S$.
Weiter gilt: $\overline{x} \in \operatorname{Kern} \overline{f} \iff \overline{f}(\overline{x}) = 0 \iff f(x) = 0 \iff x \in \operatorname{Kern} f \iff \overline{x} = \overline{0}$.
Nach 5.16 ist $\overline{f}$ injektiv. □

6 Polynomringe

Sei R ein Ring. Mit $R[X]$ bezeichnen wir den *Polynomring* über R. Seine Elemente sind Polynome

$$p = a_0 + a_1X + a_2X + \ldots + a_nX^n$$

mit $a_i \in R$. Ist $a_n \neq 0$, heißt a_n *Leitkoeffzient* von p und n der *Grad* von p. Ist ein $a_i = 0$, wird es in der Regel im Ausdruck p weggelassen.
Aus dem Grundkurs wissen wir, dass $R[X]$ mit den Verknüpfungen

$$p + q = (a_0 + b_0) + (a_1 + b_1) \cdot X + \ldots + (a_n + b_n) \cdot X^n$$
$$p \cdot q = c_0 + c_1 X + \ldots \cdot c_{m+n} X^{m+n} \text{ mit } c_i = \sum_{j=0}^{i} a_j \cdot b_{i-j}$$

einen Ring bildet, wobei $p = a_0 + a_1 X + \ldots + a_n X^n$ und $q = b_0 + b_1 X + \ldots + b_m X^m$. Hier ist $r = \max(m, n)$ und $a_i = 0$ für $i > n$ und $b_j = 0$ für $j > m$.
Wir fassen R als Unterring von $R[X]$ auf: $r \in R$ wird mit dem Polynom r vom Grad 0 identifiziert.

6.1 Für Polynome $p, q \in R[X]$ gilt

(1) $\operatorname{grad}(p + q) \leq \max(\operatorname{grad} p, \operatorname{grad} q)$

(2) $\operatorname{grad}(p \cdot q) \leq \operatorname{grad} p + \operatorname{grad} q$

(3) Sind a und b die Leitkoeffizienten von p bzw. q, dann gilt in (2) Gleichheit, falls $a \cdot b \neq 0$. Ist R Integritätsring, ist das immer der Fall.

Aus den Gradformen erhält man sofort

6.2 (1) $R[X]$ Integritätsring $\iff$ R Integritätsring

(2) R Integritätsring $\Rightarrow R^* = R[X]^*$

(3) $R[X]$ ist niemals ein Körper.

6.3 Division mit Rest: Seien $f = \sum_{i=0}^{n} a_i X^i$ und $g = \sum_{i=1}^{m} b_i X^i$ aus $R[X]$ mit $a_n \neq 0$ und $b_m \in R^*$. Dann gibt es Polynome $q, r \in R[X]$, so dass

$$f = q \cdot g + r \text{ mit } r = 0 \text{ oder } \operatorname{grad} r < \operatorname{grad} g.$$

Beweis: 1. Fall $n < m$: $f = 0 \cdot g + f$, also $q = 0$, $r = f$
2. Fall $n \geq m$: Induktion nach n.
Für $n = 0$ ist $f = a_0$, $g = b_0$. Also

$$a_0 = (a_0 b_0^{-1}) \cdot b_0 + 0, \quad \text{d.h. } q = a_0 \cdot b_0^{-1} \text{ und } r = 0.$$

Induktionsschritt von n − 1 nach n: Sei $p := a_n \cdot b_m^{-1} \cdot X^{n-m}$

$$\begin{aligned} f &= a_n X^n + a_{n-1} X^{n-1} + \ldots + a_0 \\ p \cdot g &= a_n X^n + a_n b_m^{-1} b_{m-1} X^{n-1} + \ldots + a_n b_m^{-1} b_0 X^{n-m}. \end{aligned}$$

Also ist $f_1 := f - p \cdot g$ ein Polynom vom Grad $< n$. Also gibt es q_1 und r in $R[X]$ mit

$$f - p \cdot g = f_1 = q_1 \cdot g + r \quad \text{mit } r = 0 \text{ oder } \operatorname{grad} r < \operatorname{grad} g.$$

Es folgt $f = (q_1 + p) \cdot g + r$. □

6.4 Definition: Ein Element $z \in R$ heißt *Nullstelle* des Polynoms $p = \sum_{i=1}^{n} a_i X^i \in R[X]$, falls $\sum_{i=1}^{b} a_i \cdot z^i =: p(z) = 0$ in R ist.

6.5 Ist z Nullstelle von $p \in R[X]$, dann ist $(X - z)$ Teiler von p.

Beweis: Wir dividieren p durch $(X - z)$ mit Rest $r \in R[X]$:

$$p = q \cdot (x - z) + r \quad \text{mit } r = 0 \text{ oder } \operatorname{grad} r < 1.$$

Dann ist r konstant. Da z Nullstelle von p ist, folgt

$$0 = p(z) = q(z) \cdot (z - z) + r = r.$$

Also ist $p = q \cdot (X - z)$. □

Aus dem Gradformeln erhalten wir

6.6 Satz: Ist R ein Integritätsring und $p \in R[X]$ vom Grad n, dann hat p höchstents n Nullstellen.

Teil III

Kongruenzen

7 Simultane lineare Kongruenzen

Ziel dieses Paragraphen ist es, simultane lineare Kongruenzen zu lösen, d.h. Lösungen für ein Spektrum von Kongruenzen zu finden.

7.1
$$\begin{aligned} a_1 \cdot x &\equiv b_1 \mod m_1 \\ a_2 \cdot x &\equiv b_2 \mod m_2 \\ &\vdots \\ a_r \cdot x &\equiv b_r \mod m_r \end{aligned}$$

wobei $m_i \in \mathbb{N}$, und $a_i, b_i \in \mathbb{Z}$, $i = 1, \ldots, r$.

Wir erinnern daran, dass ("a kongruent b modulo m")

$$a \equiv b \mod m$$

bedeutet, dass $m \dashv a - b$, oder anders ausgedrückt, dass

$$[a]_m = [b]_m \text{ in } \mathbb{Z}/m,$$

d.h. wir untersuchen einfache lineare Gleichungssyteme in $\mathbb{Z}/m$.
Aus dem Grundkurs wissen wir

7.2 Satz: (1) $\mathbb{Z}/m$ ist genau dann ein Körper, wenn m prim ist

(2) Für $m > 1$ ist $(\mathbb{Z}/m)^* = \{\overline{x} \in \mathbb{Z}/m;\ \text{ggT}(x, m) = 1\}$

(3) Für $m > 1$ gilt: $\overline{x} \in \mathbb{Z}/m$ ist Nullteiler $\iff$ $\text{ggT}(x, m) > 1$

(4) $\mathbb{Z}/m = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\}$

Bei unseren Untersuchungen wird der ggT eine große Rolle spielen. Deshalb gehen wir zunächst auf ihn ein.

7.3 Definition: Seien $m_1, m_2, \ldots, m_r \in \mathbb{Z}$.
d heißt *größter gemeinsamer Teiler* von $m_1, \ldots, m_r$, wir schreiben

$$d = \text{ggT}(m_1, \ldots, m_r)$$

wenn gilt

(1) $d \dashv m_i$, $i = 1, \ldots, r$

(2) $z \dashv m_i$, $i = 1, \ldots, r \Rightarrow z \dashv d$

v heißt *kleinstes gemeinsames Vielfache* von $m_1, \ldots, m_r$, wir schreiben

$$v = \text{kgV}(m_1, \ldots, m_r)$$

wenn gilt

(1) $m_i \dashv v$, $i = 1, \ldots, r$

(2) $m_i \dashv z$, $i = 1, \ldots, r \Rightarrow v \dashv z$

Bemerkung: d und v sind nur bis auf Vorzeichen bestimmt. Um Eindeutigkeit zu erreichen, nehmen wir die positiven Werte.

7.4 Lemma: (1) $(m_1)+(m_2)+\ldots+(m_r)=(d)$ mit $d=\mathrm{ggT}(m_1,\ldots,m_r)$

(2) $(m_1)\cap(m_2)\cap\ldots\cap(m_r)=(v)$ mit $v=\mathrm{kgV}(m_1,\ldots,m_r)$

(3) $d=\mathrm{ggT}(m_1,\ldots,m_r)$ besitzt eine Darstellung

$$d=\sum_{i=1}^{r} l_i\cdot m_i \qquad \text{mit } l_i\in\mathbb{Z}.$$

(4) m,n *coprim* (d.h. $\mathrm{ggT}=(m,n)=1$) $\iff$ $\exists k,l\in\mathbb{Z}$ mit $km+ln=1$

Beweis: (1) Da $\mathbb{Z}$ Hauptidealring ist, gibt es ein $d\in\mathbb{N}$, so dass $(m_1)+\ldots+(m_r)=(d)$.

$$(m_1)+\ldots+(m_r)=d \quad\Rightarrow\quad m_i\in(d)\ \forall i \quad\Rightarrow\quad d\dashv m_i\ \forall i.$$

Weiter gilt

$$z\dashv m_i\ \forall i\Rightarrow\ m_i\in(z)\ \forall i\ \Rightarrow\ (m_1)+\ldots+(m_r)\subset(z)\ \Rightarrow\ d\in(z)\ \Rightarrow\ z\dashv d$$

Also ist $d=\mathrm{ggT}(m_1,\ldots,m_r)$.
(2) Analog
(3) Da $d\in(m_1+\ldots+(m_r)$ gibt es eine Darstellung $d=\sum_{i=1}^{r} l_i\cdot m_i$.
(4) m,n coprim $\Rightarrow \mathrm{ggT}(m,n)=1\Rightarrow\exists k,l\in\mathbb{Z}$ mit $1=k\cdot m+l\cdot n$ nach (3).
Gilt umgekehrt $1=k\cdot m+l\cdot n$, folgt $1\in(m)+(n)$, also

$$\mathbb{Z}=(1)\subset(m)+(n)\subset\mathbb{Z}=(1),$$

d.h. $(m)+(n)=(1)$ und damit $\mathrm{ggT}(m,n)=1$ nach (1). □

7.5 Hier haben wir impliziet benutzt: Für $a,b\in\mathbb{Z}$ gilt

$$(a)=(b)\iff a=\pm b.$$

Beweis: "$\Leftarrow$" klar
"$\Rightarrow$" $(a)=(b)\Rightarrow a\in(b)\wedge b\in(a)\Rightarrow\exists k,l\in\mathbb{Z}$, so dass $a=k\cdot l$ und $b=l\cdot a$.
Es folgt $a=k\cdot l\cdot a$. Ist $a\neq 0$, folgt $k\cdot l=1$, also $k=l=1$ oder $k=l=-1$.
□
Wir kommne zur Lösung von Kongruenzungleichungen. Wir beginnen mit dem einfachsten Fall

7.6 $$a \cdot x \equiv b \mod m$$

Problem 1: Finde alle $x \in \mathbb{Z}$, die diese Kongruenz erfüllen.
Problem 2: Fasse diese Kongruenz als Gleichung

$$[a]_m \cdot x = [b]_m$$

in $\mathbb{Z}/m$ auf und bestimme ihre Lösungsmenge in $\mathbb{Z}/m$.
Fangen wir mit Problem 1 an:

$$a \cdot x \equiv b \mod m \Leftrightarrow \exists y \in \mathbb{Z} \text{ mit } a \cdot x + m \cdot y = b$$

Wir müssen also die diophantische Gleichung

7.7

$$a \cdot x + m \cdot y = b$$

lösen. Eine solche Lösung existiert genau dann, wenn

$$b \in (a) + (m) = (d) \quad \text{mit} \quad d = \text{ggT}(a, m)$$

Wir erhalten die
Lösbarkeitsbedingung: Die Gleichung 7.7 hat genau dann Lösungen, wenn $d = \text{ggT}(a, m)$ Teiler von b ist.
Ist die Lösbarkeitsbedingun erfüllt, vereinfachen wir die Gleichung 7.7, indem wir durch d teilen. Wir erhalten die äquivalente Gleichung

$$a' \cdot x + m' \cdot y = b',$$

wobei $a = a' \cdot d,\ m = m' \cdot d$ und $b = b' \cdot d$ ist. Wie wir oben bereits festgestellt haben, ist $x \in \mathbb{Z}$ genau dann Lösung dieser Gleichung, wenn

7.8

$$a' \cdot x \equiv b' \mod m'$$

Da $\text{ggT}(a', m') = 1$, ist $[a']_{m'}$ in $\mathbb{Z}/m'$ invertierbar. Damit hat 7.8 in $\mathbb{Z}/m'$ genau eine Lösung, die wir erhalten, indem wir die Gleichung mit dem Inversen $[k]_{m'}$ von $[a']_{m'}$ multiplizieren. Um k zu finden, bestimmen wir mit Hilfe des euklidischen Algorithmuses ein Darstellung

$$1 = \text{ggT}(a', m') = k \cdot a' + l \cdot m' \quad \text{mit } k,\ l \in \mathbb{Z}$$

Dann ist $[k]_{m'} = [a']_{m'}^{-1}$. Damit erhalten wir die

Antwort zu Problem 1: Falls die Lösbarkeitsbedingung erfüllt ist, löst $x \in \mathbb{Z}$ die Kongruenz 7.6 genau dann, wenn

$$x \equiv k \cdot b \mod m' \qquad \text{also} \qquad x \equiv k \cdot \frac{b}{d} \mod \frac{m}{d},$$

wobei k durch die Darstellung $1 = k \cdot \frac{a}{d} + l \cdot \frac{m}{d}$ mit $k,\ l \in \mathbb{Z}$ gegeben ist. Als Lösungsmenge erhalten wir

$$\mathbb{L} = x_0 + \frac{m}{d} \cdot \mathbb{Z} \quad \text{mit } x_0 = k \cdot \frac{b}{d}$$

Unter diesen sind genau

$$x_0,\ x_1 = x_0 + \frac{m}{d},\ x_2 = x_0 + 2 \cdot \frac{m}{d},\ \ldots,\ x_{d-1} = x_0 + (d-1) \cdot \frac{m}{d}$$

die modulo m verschiedenen, so dass wir auch die Antwort auf Problem 2 erhalten.

Wir fassen zusammen:

7.9 Zusammenfassung: Sei $d = \mathrm{ggT}(a, m)$ und $k, l \in \mathbb{Z}$, so dass $d = k \cdot a + l \cdot m$, also $1 = k \cdot \frac{a}{d} + l \cdot \frac{m}{d}$. Die Kongruenz

$$a \cdot x \equiv b \mod m$$

ist genau dann lösbar, wenn $d \dashv b$. In diesem Fall gibt es genau d zueinander inkongruente Lösungen modulo m, nämlich

$$x_0,\ x_1 + x_0 + \frac{m}{d},\ x_2 = x_0 + \frac{2m}{d}, \ldots,\ x_{d-1} = x_0 + \frac{(d-1)m}{d} \qquad \text{mit } x_0 = k \cdot \frac{b}{d}.$$

Die Lösungsmenge der Kongruenz in $\mathbb{Z}$ ist

$$\mathbb{L} = x_0 + \frac{m}{d} \cdot \mathbb{Z} = \{x_0, \ldots, x_{d-1}\} + m \cdot \mathbb{Z}$$

Für die Lösung des Problems 7.1 bemühen wir den

7.10 Chinesischer Restesatz: Seien $m_1, \ldots, m_r \in \mathbb{Z}$ paarweise teilerfremd und sei $m = m_1 \cdot \ldots \cdot m_r$. Dann ist

$$\begin{array}{rcl} f : \mathbb{Z}/m & \to & \mathbb{Z}/m_1 \times \ldots \times \mathbb{Z}/m_r \\ [x]_m & \mapsto & ([x]_{m_1}, \ldots, [x]_{m_r}) \end{array}$$

ein Isomorphismus von Ringen, wobei die Ringstrukturen der rechten Seite durch komponentenweise Addition und Multiplikation gegeben ist.

Beweis: Da die Ringstruktur auf $R = \mathbb{Z}/m_1 \times \ldots \times \mathbb{Z}/m_r$ durch komponentenweise Addition und Multiplikation gegeben ist, ist

$$g := \mathbb{Z} \to R, \quad x \mapsto ([x]_{m_1}, \ldots, [x]_{m_r})$$

ein Ringhomomorphismus. Sein Kern ist

$$\operatorname{Kern} g = (m_1) \cap (m_2) \cap \ldots \cap (m_r) = (m)$$

nach 7.4, weil $m = \operatorname{kgV}(m_1, \ldots, m_r)$. Aus dem Isomorphiesatz folgt, dass

$$f = \overline{g} : \mathbb{Z}/m \to R$$

injektiv ist. Da $\mathbb{Z}/m$ und R gleich viele Elemente haben, ist f ein Isomorphismus. □

7.11 Folgerung: Sind $m_1, \ldots, m_r \in \mathbb{N}$ paarweise teilerfremd und ist $d_i = \operatorname{ggT}(a_i, m_i)$ Teiler von b_i für $i = 1, \ldots, r$, dann besitzt 7.1 Lösungen.
Gilt

$$a_i \cdot x_i \equiv b_i \mod m_i \quad i = 1, \ldots, r$$

dann gibt es genau eine Lösung x modulo $m = m_1 \cdot m_2 \cdot \ldots \cdot m_r$, so dass

$$x \equiv x_i \mod m_i.$$

Beweis: Nach 7.9 finden wir genau dann ein x_i, so dass

$$a_i \cdot x_i \equiv b_i \mod m_i,$$

wenn $d_i \dashv b_i$ ist. Sind $x_1, \ldots, x_r$ gefunden, dann gibt es nach dem chinesischen Restesatz genau ein x modulo m, so dass

$$x \equiv x_i \mod m_i.$$

□

7.12 Bemerkung: Sind $m_1, \ldots, m_r \in \mathbb{Z}$ nicht paarweise teilerfremd, dann zeigt unser Beweis, dass

$$\begin{array}{rcl} f : \mathbb{Z}/v & \to & \mathbb{Z}/m_1 \times \ldots \times \mathbb{Z}/m_r \\ [x]_v & \mapsto & ([x]_{m_1}, \ldots, [x]_{m_r}) \end{array}$$

noch injektiv ist, wobei $v = \operatorname{kgV}(m_1, \ldots, m_r)$.

Im Grundkurs haben wir gelernt, mit Hilfe des euklidischen Algorithmus eine Darstellung des $d = \mathrm{ggT}(a, m)$ der Form

$$d = k \cdot a + l \cdot b \qquad k, l \in \mathbb{Z}$$

zu bestimmen. Mit Hilfe dieses Verfahrens kann man auch eine Darstellung der Form

$$d = k_1 \cdot a_1 + \ldots + k_r \cdot a_r \qquad k_1, \ldots, k_r \in \mathbb{Z}$$

für $d = \mathrm{ggT}(a_1, a_2, \ldots, a_r)$ finden, denn

7.13 Aufgabe: $\mathrm{ggT}(a_1, \ldots, a_r) = \mathrm{ggT}(\mathrm{ggT}(a_1, \ldots, a_{r-1}), a_r)$

7.14 Verfahren zum Auffinden der Lösungen von 7.1:
Zunächst lösen wir die Kongruenzen

$$a_i \cdot x_i \equiv b_i \mod m_i, \text{ falls } d_i = \mathrm{ggT}(a_i, m_i) \dashv b_i.$$

Ist d_i kein Teiler von m_i für ein i, dann ist 7.1 nicht lösbar. Wir bestimmen die modulo $\frac{m_i}{d_i}$ eindeutige Lösung x_i, indem wir die Kongruenz zunächst durch Division durch d_i vereinfachen. Sei $m_i' = \frac{m_i}{d_i}$.
Sind nun $m_1', \ldots, m_r'$ paarweise teilerfremd und ist $m = m_1' \cdot \ldots \cdot m_r'$, dann ist

$$\mathrm{ggT}\left(\frac{m}{m_1'}, \frac{m}{m_2'}, \ldots, \frac{m}{m_r'}\right) = 1.$$

Wir bestimmen $l_1, \ldots, l_r \in \mathbb{Z}$, so dass

$$1 = l_1 \cdot \frac{m}{m_1'} + \ldots + l_r \frac{m}{m_r'}.$$

Da $m_i' \dashv \frac{m}{m_j'}$ für $j \neq i$, folgt $1 \equiv l_i \cdot \frac{m}{m_i'} \mod m_i'$. Wir erhalten:

7.15 Für $x = \sum_{i=1}^{r} x_i \cdot l_i \cdot \frac{m}{m_i}$ gilt $x \equiv x_i \mod m_i'$. D.h. dieses x löst das System 7.1, da x_i die Kongruenz $\frac{a_i}{d_i} \cdot x_i \equiv \frac{b_i}{d_i} \mod m_i'$ und damit die Kongruenz $a_i \cdot x_i \equiv b_i \mod m_i$ löst.

Nach dem chinesischen Restesatz ist dieses x modulo m das einzige Element, das $x \equiv x_i$ für $i = 1, \ldots, r$ erfüllt. Als Lösungsmenge von 7.1 in $\mathbb{Z}$ erhalten wir somit

$$\mathbb{L} = \left\{ \sum_{i=1}^{r} x_i \cdot l_i \cdot \frac{m}{m_i'} \right\} + m \cdot \mathbb{Z}$$

Damit haben wir ein Lösungsverfahren von 7.1 für den Fall, dass $m_1, \ldots, m_r$ paarweise teilerfremd sind.

Aber auch im Fall, dass die m_i nicht paarweise coprim sind, können wir 7.10 zur Bestimmung der Lösungen einsetzen. Wir demonstrieren das an einem Beispiel

7.16 Beispiel:

$$\begin{array}{lll} (1) & 6x \equiv 6 & \mod 8 \\ (2) & 3x \equiv 9 & \mod 18 \end{array}$$

$\mathrm{ggT}(6,8) = 2 \dashv 6$ und $\mathrm{ggT}(3,18) = 3 \dashv 9$. Also haben beide Gleichungen Lösungen. Wir vereinfachen die Kongruenzen und erhalten das äquivalente System

$$\begin{array}{lll} (3) & 3x \equiv 3 & \mod 4 \\ (4) & x \equiv 3 & \mod 6 \end{array}$$

Da $[3]_4$ in $\mathbb{Z}/4$ inverierbar ist, ist (3) äquivalent zu

$$(5) \quad x \equiv 1 \qquad \mod 4$$

Damit sind die Lösungen $x_1 = 1$ und $x_2 = 3$ von (5) und (4) sofort ablesbar.

Während wir im Verfahren 7.14 den chinesischen Restesatz von rechts nach links angewandt haben, nutzen wir jetzt die umgekehrte Richtung: Aus 7.10 folgt

$$x \equiv 3 \mod 6 \iff (x \equiv 3 \mod 2) \wedge (x \equiv 3 \mod 3).$$

Damit ist unser System äquivalent zu

(a) $x \equiv 1 \mod 4$

(b) $x \equiv 1 \mod 2$

(c) $x \equiv 0 \mod 3$

Die Lösungen von (a) lösen auch (b), also ist (b) überflüssig. Es bleibt

(I) $x \equiv 1 \mod 4$

(II) $x \equiv 0 \mod 3$

Jetzt können wir unser Verfahren anwenden: $m = 4 \cdot 3 = 12,\ m_1' = 4,\ m_2' = 3.$

$$1 = l_1 \cdot 3 + l_2 \cdot 4 = -1 \cdot 3 + 1 \cdot 4.$$

Modulo 12 ist die Lösung also

$$x = -3 \cdot x_1 + 4 \cdot x_2 = -3 \cdot 1 + 4 \cdot 0 = -3$$

Als Gesamtlösungsmenge erhalten wir

$$\mathbb{L} = -3 + 12 \cdot \mathbb{Z}$$

Aufgabe: Lösen Sie

$$\begin{aligned} 6x &\equiv 6 \mod 8 \\ 3x &\equiv 12 \mod 18 \end{aligned}$$

Zum Abschluss beweisen wir zwei Resultate von separatem Interesse. Zunächst einen Satz, der John Wilson (1741-1793) zugeschrieben wird. Allerdings wurde er von diesem nur vermutet und dann von Joseph-Louis Lagrange (1736-1813) bewiesen.

7.17 Satz von Wilson: Sei $n > 1$ aus $\mathbb{N}$. Dann gilt

$$(n-1)! \equiv -1 \mod n \iff n \text{ prim.}$$

Beweis: "$\Leftarrow$" Sei $n = p$ prim. Im Körper $\mathbb{Z}/p$ sind $\overline{1}, \ldots, \overline{p-1}$ von $\overline{0}$ verschieden, besitzen also genau ein Inverses. Es gilt

$$\overline{x} = \overline{x}^{-1} \iff \overline{x}^2 = \overline{1} \iff \overline{x}^2 - \overline{1} = (\overline{x}+\overline{1})(\overline{x}-\overline{1}) = \overline{0} \iff \overline{x} = \overline{1} \text{ oder } \overline{x} = -\overline{1}.$$

Damit sind genau $\overline{1}$ und $\overline{p-1}$ zu sich selbst invers. Die übrigen Elemente können wir zu Paaren ordnen, die zueinander invers sind. Es folgt

$$\overline{(p-1)!} = \overline{1} \cdot \overline{p-1} = -\overline{1} \qquad \text{in } \mathbb{Z}/p = \mathbb{Z}/n$$

"$\Rightarrow$" Sei $n = p \cdot q$ mit $1 < p, q < n$ und $(n-1)! \equiv -1 \mod n$. Dann folgt natürlich auch: $(n-1)! \equiv -1 \mod p$.
Aber $(n-1)! = (n-1) \cdot (n-2) \cdot \ldots \cdot p \cdot (p-1) \cdot \ldots \cdot 1 \equiv 0 \mod p$, ein Widerspruch. □
Das zweite Resultat ist wesentlich jünger. Es wurde 1949 von P.A. Clement publiziert.

7.18 Satz: Satz von Clement: $4((n-1)!+1)+n \equiv 0 \mod n(n+2) \iff (n, n+2)$ ist ein Primzahlzwilling..

Beweis: 1. Fall: n gerade. Dann ist $(n, n+2)$ kein Primzahlzwilling. Wir müssen also zeigen, dass die Kongruenz keine Lösung hat.

Sei $n = 2k$. Angenommen die Kongruenz gilt, dann gilt auch

$$\begin{aligned} 4((n-1)!+1)+n &\equiv 0 \mod n \\ 4(2k-1)!+4 &\equiv 0 \mod 2k, \quad \text{da } n \equiv 0 \mod n \\ 2(2k-1)!+2 &\equiv 0 \mod k \quad \text{(Division durch 2)} \\ 2 &\equiv 0 \mod k, \quad \text{da } k \nmid (2k-1)! \end{aligned}$$

Also ist $k = 1$ oder 2 und damit $n = 2$ oder 4. Für diese n ist die Ausgangskongruenz nicht erfüllt.

2. Fall: n ungerade: Dann gilt $\text{ggT}(n, n+2) = 1$, und nach 7.10 ist die Kongruenz äquivalent zum System der Kongruenzen

$$\begin{aligned} \text{(I)} \quad & 4((n-1)!+1)+n \equiv 0 \mod n \\ \text{(II)} \quad & 4((n-1)!+1)+n \equiv 0 \mod n+2. \end{aligned}$$

Da $[4]_n$ Einheit in $\mathbb{Z}/n$ ist und $[n]_n = [0]_n$ ist (I) äquivalent zu

$$(n-1)!+1 \equiv 0 \mod n.$$

Nach dem Satz von Wilson ist das genau dann der Fall, wenn n prim ist.

Da $[n]_{n+2} = [-2]_{n+2}$ ist (II) äquivalent zu

$$4(n-1)!+4-2 \equiv 0 \mod n+2.$$

Da $[n]_{n+2} = [-2]_{n+2}$ und $[n+1]_{n+2} = [-1]_{n+2}$ Einheiten in $\mathbb{Z}/(n+2)$ sind, kann ich diese Gleichung mit $n \cdot (n+1)$ multiplizieren und erhalte eine äquivalente Kongruenz

$$0 \equiv 4(n+1)!+2 \cdot n \cdot (n+1) \equiv 4(n+1)!+2 \cdot (-2) \cdot (-1) \mod n+2$$

Da $[4]_{n+2}$ Einheit in $\mathbb{Z}/n+2$ ist, ist diese Kongruenz äquivalent zu

$$(n+1)!+1 \equiv 0 \mod n+2.$$

Nach dem Satz von Wilson ist dies äquivalent dazu, dass $n+2$ prim ist. □

8 Lineare diophantische Gleichungen

Die Ergebnisse des vergangenen Abschnitts versetzen uns in die Lage, wenigstens lineare diophantische Gleichungen zu lösen. Gesucht werden also Lösungen in $\mathbb{Z}^n$ der Gleichung

8.1 $a_1 \cdot x_1 + a_2 \cdot x_2 + \ldots + a_n \cdot x_n = b \quad \text{mit} \quad a_i,\ b \in \mathbb{Z},\ i = 1, \ldots, n.$

Wir beginnen mit der einfachen Gleichung

8.2 $ax + my = b, \quad a, b, m \in \mathbb{Z}.$

Rechnen wir modulo m geht die Gleichung über in

$$a \cdot x \equiv b \qquad \text{mod } m.$$

Wir wissen aus 7.9 und dessen Beweis, dass diese Gleichung genau dann lösbar ist, wenn $d = \text{ggT}(a, m)$ ein Teiler von b ist. Ist

$$d = k \cdot a + l \cdot m$$

dann ist x genau dann eine Lösung von 8.2, wenn x die Form

$$x = k \cdot \frac{b}{d} + \frac{t \cdot m}{d} = x_0 + \frac{t \cdot m}{d} \quad \text{mit} \quad x_0 = \frac{k \cdot b}{d} \quad \text{und} \quad t \in \mathbb{Z}$$

hat. Setzen wir das in 8.2 ein, erhalten wir

$$a \cdot x_0 + m \cdot y_0 \ = b$$

$$m \cdot y_0 = b - a \cdot x_0 = \frac{b \cdot d - a \cdot k \cdot b}{d} \ = \frac{b(d - a \cdot k)}{d} = \frac{b \cdot l \cdot m}{d}$$

Also

$$y_0 = \frac{l \cdot b}{d}.$$

Allgemeiner haben wir

$$\begin{aligned} b &= a \cdot \left(x_0 + \frac{t \cdot m}{d} \right) + m \cdot y = a \cdot x_0 + \frac{a \cdot t \cdot m}{d} + m \cdot y \\ &= b - m \cdot y_0 + \frac{a \cdot t \cdot m}{d} + m \cdot y \end{aligned}$$

Also

$$m \cdot y = m \cdot y_0 - \frac{a \cdot t \cdot m}{d}$$

und somit

$$y = y_0 - \frac{a \cdot t}{d} \quad t \in \mathbb{Z}.$$

Wir fassen zusammen

8.3 Satz: Die diophantischen Gleichung

$$a \cdot x + m \cdot y = b \quad a, b, m \in \mathbb{Z}$$

hat genau dann Lösungen $(x, y) \in \mathbb{Z}^2$, wenn $d = \text{ggT}(a, m)$ Teiler von b ist. Ist $d = k \cdot a + l \cdot m$ und $d \dashv b$, dann ist

$$\mathbb{L} = \left\{ \left(\frac{k \cdot b + t \cdot m}{d}, \frac{l \cdot b - a \cdot t}{d} \right) ; t \in \mathbb{Z} \right\}$$

die Lösungsmenge.

Bei der Lösung der Gleichung 8.1 hilft uns der folgende Satz.

8.4 Satz: Seien $a_1, \ldots, a_n$ von 0 verschiedene Zahlen aus $\mathbb{Z}$ und sei $d = \text{ggT}(a_1, \ldots, a_n)$. Dann gilt

(1) die diophantische Gleichung

$$a_1 \cdot x_1 + \ldots + a_n \cdot x_n = c \qquad (*)$$

hat genau dann Lösungen $(x_1, \ldots, x_n) \in \mathbb{Z}^n$, wenn $d \dashv c$.

(2) Es gelte $d \dashv c$. Sei $\mathbb{L} \subset \mathbb{Z}^n$ die Lösungsmenge der Gleichung $(*)$ und $\mathbb{L}' \subset \mathbb{Z}^{n+1}$ die Lösungsmenge des Systems der diophantischen Gleichungen mit $a = \text{ggT}(a_{n-1}, a_n)$

$$\begin{aligned} a_1 \cdot x_1 + \ldots + a_{n-2} \cdot x_{n-2} + ay &= c \\ a_{n-1} \cdot x_{n-1} + a_n \cdot x_n - ay &= 0 \end{aligned}$$

Dann sind die Abbildungen

$$\begin{aligned} &\varphi : \mathbb{L} \to \mathbb{L}', \quad (x_1, \ldots, x_n) \mapsto (x_1, \ldots, x_n, y) \text{ mit } y = \tfrac{1}{a}(a_{n-1}x_{n-1} + a_n x_n) \\ &\psi : \mathbb{L}' \to \mathbb{L}, \quad (x_1, \ldots, x_n, y) \mapsto (x_1, \ldots, x_n) \end{aligned}$$

bijektiv und zueinander invers.

Beweis: (1) Die Gleichung hat genau dann eine Lösung, wenn $c \in (a_1) + \ldots (a_n) = (d)$, d.h. wenn $d \dashv c$.
(2) Für $(x_1, \ldots, x_n) \in \mathbb{L}$ und $y = \frac{1}{a}(a_{n-1}x_{n-1} + a_n x_n)$ gilt

$$\begin{aligned} a_1x_1 + \ldots + a_{n-2}x_{n-2} + ay &= a_1x_1 + \ldots + a_{n-2}x_{n-2} + a_{n-1}x_{n-1} + a_nx_n = c \\ a_{n-1}x_{n-1} + a_nx_n - ay &= a_{n-1}x_{n-1} + a_nx_n - a_{n-1}x_{n-1} - a_nx_n = 0 \end{aligned}$$

Also ist $\varphi(x_1, \ldots, x_n) \in \mathbb{L}'$, denn $y \in \mathbb{Z}$, da $d = \mathrm{ggT}(a_1, \ldots, a_n)$. Ist $(x_1, \ldots, x_n) \in \mathbb{L}'$, dann ergibt die Addition der Gleichungen

$$\begin{array}{rcl} a_1x_1 + \ldots + a_{n-2}x_{n-2} + a \cdot y & = & c \\ a_{n-1} \cdot x_{n-1} + a_x \cdot x_n - a \cdot y & = & 0 \\ \hline a_1x_1 + \ldots\ldots\ldots\ldots + a_n \cdot x_n & = & c \end{array} \qquad (**)$$

Also ist $\psi(x_1, \ldots x_n, y) = (x_1, \ldots, x_n) \in \mathbb{L}$. Weiter gilt $\psi \circ \varphi = \mathrm{id}_{\mathbb{L}}$ und

$$\varphi \circ \psi(x_1, \ldots, x_n, y) = \varphi(x_1, \ldots, x_n) = (x_1, \ldots, x_n, y')$$

mit $y' = \frac{1}{a}(a_{n-1} \cdot x_{n-1} + a_n \cdot x_n) = y$ nach $(**)$. Also sind φ und ψ zueinander inverse Abbildungen. □

8.5 Lösungsverfahren: (Wir benutzen die Bezeichungen des Satzes.)
Zunächst prüfen wir die **Lösbarkeitsbedingung:** Sei $d_0 = \mathrm{ggT}(a_1, \ldots, a_n)$. Die diophantische Gleichung hat genau dann eine Lösung, wenn $d_0 \dashv c$.
Ist das der Fall, fahren wir wie folgt fort:
1. Schritt: (a) Wir vereinfachen die Gleichung, indem wir durch d_0 teilen. Wir erhalten die neue Gleichung

$$a'_1 \cdot x_1 + \ldots + a'_n \cdot x_n = c'$$

(b) Sei $d_1 = \mathrm{ggT}(a'_2, \ldots, a'_n)$. Wir lösen die Gleichung

$$a'_1 \cdot x_1 + d_1 \cdot y_1 = c'$$

mit Hilfe von 8.3.
2. Schritt: Wir wenden den ersten Shritt auf die Gleichung

$$a'_2 \cdot x_2 + \ldots + a'_n \cdot x_n = d_1 \cdot y_1$$

an: Wir vereinfachen sie, indem wir durch d_1 teilen. Wir erhalten

$$a''_2 \cdot x_2 + \ldots + a''_n \cdot x_n = y_1$$

Sei $d_2 = \mathrm{ggT}(a''_3, \ldots, a''_n)$. Wir lösen die Gleichung

$$a''_2 \cdot x_2 + d_2 \cdot y_2 = y_1$$

mit Hilfe von 8.3 und fahren fort. Der erste Schritt bestimmt x_1, der zweite x_2 usw.. Im $(n-1)$-ten Schritt bestimmen wir x_{n-1} und x_n.

8.6 Beispiel: $6 \cdot x_1 + 15 \cdot x_2 + 6 \cdot x_3 = 9$

$d = \text{ggT}(6, 15, 6) = 3$ teilt 9. Also gibt es Lösungen. Natürlich betrachten wir jetzt nicht mehr die Ausgangsgleichung, sondern teilen erst einmal durch den ggT. Wir erhalten die äquivalente Gleichung

$$2 \cdot x_1 + 5 \cdot x_2 + 2 \cdot x_3 = 3.$$

$a = \text{ggT}(5, 2) = 1$. Nach dem Lösungsverfahren lösen wir zunächst die Gleichung

$$2x_1 + y = 3$$

lösen. Ihre Lösungsmenge (wir lösen nach y auf) ist $\mathbb{L}_1\{(x_1, y) = (t_1, 3 - 2t_1); t_1 \in \mathbb{Z}\}$.

Dann haben wir die Gleichung

$$5x_2 + 2x_3 = a \cdot y = 3 - 2t_1$$

zu lösen. Sei $D = \text{ggT}(5, 2) = 1 = 5 - 2 \cdot 2$. Nach 8.3 erhalten wir die Lösungen

$$(x_2, x_3) = (3 - 2t_1 + 2t_2,\ -2 \cdot (3 - 2t_1) - 5 \cdot t_2).$$

Damit erhalten wir als Lösungen der Ausgangsgleichung

$$(x_1, x_2, x_3) = (t_1, 3 - 2t_1 + 2t_2, -6 + 4t_1 - 5t_2), \quad t_1, t_2 \in \mathbb{Z}.$$

9 Die prime Restklassengruppe

9.1 Definition: Sei $m > 1$ aus $\mathbb{N}$. Die *prime Restklassengruppe* modulo m ist die Gruppe $(\mathbb{Z}/m)^*$ der Einheiten im Ring $\mathbb{Z}/m$.

Wir wollen diese Gruppe bestimmen.

Sei nun $m = p_1^{r_1} \cdot \ldots \cdot p_k^{r_k}$ die Primfaktorzerlegung von m, wobei $p_1 < p_2 < \ldots < p_k$. Wir setzen $m_i = p_i^{r_i}$.

Nach dem chinesischen Restesatz haben wir einen Isomorphismus

$$\mathbb{Z}/m \cong \mathbb{Z}/m_1 \times \ldots \times \mathbb{Z}/m_k$$

von Ringen. Es folgt

9.2 $(\mathbb{Z}/m)^* \cong (\mathbb{Z}/m_1 \times \ldots \times \mathbb{Z}/m_k)^* = (\mathbb{Z}/m_1)^* \times \ldots \times (\mathbb{Z}/m_k)^*$

Es genügt daher, $(\mathbb{Z}/p^r)^*$ mit p prim zu bestimmen. Unsere erste Frage gilt der Anzahl ihrer Elemente:

9.3 Für $p \geq 2$ prim gilt $|(\mathbb{Z}/p^r)^*| = (p-1) \cdot p^{r-1}$.

Beweis: $[k]_{p^r} \in (\mathbb{Z}/p^r)^* \iff \text{ggT}(k,p) = 1$. Nun sind

$$p, 2p, 3p, \ldots, p^{r-1} \cdot p$$

genau die durch p teilbaren Elemente eines Repräsentantensystems $\{1,\ 2, \ldots,\ p^r\}$ von $\mathbb{Z}/p^r$. Also gibt es $p^r - p^{r-1} = (p-1)p^{r-1}$ Elemente, die nicht durch p teilbar sind. □

Wir beginnen jetzt mit $(\mathbb{Z}/p)^*$, aber benötigen dafür noch algebraische Resultate, die wir zum Teil aus dem Grundkurs kennen.

Sei $(G, \cdot)$ eine Gruppe und $x \in G$.

9.4 Definition: Die *Ordnung* $\text{ord}(x)$ von $x \in G$ ist die Anzahl der Elemente der von x erzeugten Untergruppe $\langle x \rangle$ von G, d.h. die Ordnung von $\langle x \rangle$.

9.5 Satz: Sei $\text{ord}(x) = k \in \mathbb{N}$, $k > 1$. Dann ist k die kleinste Zahl aus $\mathbb{N}$, für die $x^k = e$ (e ist das neutrale Element von G).

Beweis: Da $\langle x \rangle$ endlich ist, muss es in der Folge

$$e = x^0, x^1, x^2, \ldots$$

nach höchstens k Schritten Wiederholungen geben. Wir betrachten die erste Wiederholung $x^r = x^s$ mit $r < s$, d.h. $x^0, x^1, \ldots, x^{s-1}$ sind alle verschieden.

Behauptung: $r = 0$ und $s = k$.

Beweis: Es gilt $x^0 = x^{s-r}$. Da es sich um die erste Wiederholung handelt ist $s - r = s$, also $r = 0$. Da $x^s = e$, sind $x^0, x^1, \ldots, x^{s-1}$ alle Elemente aus $\langle x \rangle$, d.h. $s = k$. □

9.6 Lemma: Sei $(G, \cdot)$ eine Gruppe, $x \in G$.
(1) Ist $\text{ord}(x) = k$ und $x^n = e$, dann gilt $k \dashv n$.
(2) Ist p prim, $x^{p^{k-1}} \neq 1$ und $x^{p^k} = 1$, dann ist $\text{ord}(x) = p^k$.

Beweis: (1) Wir teilen n durch k mit Rest

$$n = q \cdot k + r \text{ mit } 0 \leq r < k.$$

Es gilt

$$e = x^n = x^{q \cdot k} \cdot x^r = (x^k)^q \cdot x^r = e \cdot x^r = x^r.$$

Da $r < k$ und k die kleinste Zahl aus $\mathbb{N}$ ist, für die $x^k = e$, folgt $r = 0$.

(2) Da $x^{p^k} = 1$, ist $\mathrm{ord}(x)$ Teiler von p^k, also $\mathrm{ord}(x) = p^s$ mit $s \leq k$. Falls $s < k$, gibt es ein $r \geq 0$, so dass $k - 1 = s + r$. Es folgt

$$x^{p^{k-1}} = x^{p^{s+r}} = x^{p^s \cdot p^r} = \left(x^{p^s}\right)^{p^r} = 1^{p^r} = 1,$$

ein Widerspruch. Also ist $s = k$. □

9.7 Lemma: Sei $(G, \cdot)$ eine abelsche Gruppe und seien $a_1, \ldots, a_n \in G$ Elemente mit $\mathrm{ord}(a_i) = k_i \in \mathbb{N}$, $i = 1, \ldots, n$. Sei $v = \mathrm{kgV}(a_1, \ldots, a_n)$. Dann gibt es ein $a \in G$ der Ordnung v.

Beweis: Da $\mathrm{kgV}(k_1, \ldots, k_n) = \mathrm{kgV}(k_1, \mathrm{kgV}(k_2, \ldots, k_n))$, genügt es den Fall zweier Elemente a, b mit $\mathrm{ord}(a) = k$ und $\mathrm{ord}(b) = l$ zu behandeln.

1. Fall: $\mathrm{ggT}(k, l) = 1$. Dann ist $\mathrm{kgV}(k, l) = k \cdot l$. Sei $r = \mathrm{ord}(a \cdot b)$. Dann gilt

$$(a \cdot b)^{k \cdot l} = a^{k \cdot l} \cdot b^{k \cdot l} = (a^k)^l \cdot (b^l)^k = e.$$

es folgt: $r \dashv k \cdot l$ nach 9.6.

Aus

$$a^{l \cdot r} = a^{l \cdot r} \cdot e = a^{l \cdot r} \cdot b^{l \cdot r} = (a \cdot b)^{l \cdot r} = e$$

folgt $k \dashv l \cdot r$ nach 9.6. Da $\mathrm{ggT}(k.l) = 1$, folgt $k \dashv r$. Genauso zeigt man, dass $l \dashv r$. Also ist r gemeinsames Vielfaches von k und l und damit $r = k \cdot l$, da $r \dashv k \cdot l$. Also $\mathrm{ord}(a \cdot b) = k \cdot l$.

2. Fall: Seien $k = p_1^{r_1} \cdot \ldots \cdot p_k^{r_k}$ und $l = p_1^{s_1} \cdot \ldots \cdot p_k^{s_k}$ schwache Primfaktorzerlegungen von k und l mit $0 \leq r_i, s_i$. Sei k_0 das Produkt aller $p_i^{r_i}$, für die $r_i \geq s_i$, und l_0 das Produkt aller $p_i^{s_i}$, für die $r_i < s_i$. Dann gilt

$$k_0 \dashv k, \quad l_0 \dashv l, \quad \mathrm{kgV}(k, l) = k_0 \cdot l_0, \quad \mathrm{ggT}(k_0, l_0) = 1$$

Also gibt es $k_1,\ l_1 \in \mathbb{Z}$, so dass $k = k_0 \cdot k_1$ und $l = l_0 \cdot l_1$. Da $\mathrm{ord}(a^{k_1}) = k_0$, $\mathrm{ord}(b^{l_1}) = l_0$ und $\mathrm{ggT}(k_0, l_0) = 1$, folgt aus Fall 1, dass $\mathrm{ord}(a^{k_1} \cdot b^{l_1}) = k_0 \cdot l_0 = \mathrm{kgV}(k, l)$.

□

9.8 Satz: Sei $\mathbb{K}$ ein Körper und $G \subset (\mathbb{K}^*, \cdot)$ eine endliche Untergruppe. Dann ist G zyklisch.

Beweis: Sei $G = \{a_1, \ldots, a_n\}$, $\mathrm{ord}(a_i) = r_i$ und $m = \mathrm{kgV}(r_1, \ldots, r_n)$. Nach 9.7 gibt es ein Element x der Ordnung m in G. Da dann $x^m = 1$, sind $x, x^2, \ldots, x^m = 1$ verschiedene Nullstellen des Polynoms $X^m - 1$. Da dieses Ploynom höchstens m Nullstellen haben kann, gibt es keine weiteren. Da nun $\mathrm{ord}(a_i) \dashv m$, gilt $a_i^m = 1$, so dass a_i Nullstelle von $X^m - 1$ ist. Also ist a_i eine Potenz von x. Es folgt $G = \langle x \rangle$. □

9.9 Folgerung: $(\mathbb{Z}/p)^*$ ist zyklisch der Ordnung $p-1$, also

$$((\mathbb{Z}/p)^*, \cdot) \cong (\mathbb{Z}/p-1, +).$$

Wir wenden uns jetzt $(\mathbb{Z}/p^r)^*$ für $r \geq 2$ zu und beginnen mit $p = 2$. Da $r \geq 2$, ist 4 Teiler von 2^r. Wir betrachten die von $[5]_{2^r}$ (multiplikativ) erzeugte Untergruppe $\langle 5 \rangle$ von $(\mathbb{Z}/2^r)^*$, d.h.

$$\langle 5 \rangle = \{[5^k]_{2^r}; k \in \mathbb{N}_0\}$$

zur Vereinfachung der Schreibweise schreiben wir oft x statt $[x]_{2^r}$. Da $5 \equiv 1 \mod 4$, ist $5^k \equiv 1 \mod 4$, d.h. $\langle 5 \rangle$ ist enthalten in der Restklasse $[1]_4$, also

$$\langle 5 \rangle \subset \{1, 5, 9, \ldots, 2^r - 3\} \subset (\mathbb{Z}/2^r)^*.$$

Die übrigen Einheiten $\{3, 7, 9, \ldots, 2^r - 1\}$ von $\mathbb{Z}/2^r$ werden von den Elementen

$$\{-1, -5, -9, \ldots, -(2^r - 3)\}$$

repräsentiert.

9.10 Satz: Für die Untergruppe $\langle 5 \rangle$ von $(\mathbb{Z}/2^r)^*$, $r \geq 2$, gilt

$$\langle 5 \rangle = \{1, 5, 9, \ldots, 2^r - 3\}.$$

Als Folgerung erhalten wir

9.11 Satz: Für $r \geq 2$ gilt

$$\begin{array}{rcl} (\mathbb{Z}/2^r)^* & \cong & \{\pm 1\} \times \langle 5 \rangle \cong (\{\pm 1\}, \cdot) \times (\{1, 5, 9, \ldots, 2^r - 3\}, \cdot) \\ & = & (\mathbb{Z}/2, +) \times (\mathbb{Z}/2^{r-2}, +) \end{array}$$

Beweis: $(\mathbb{Z}/2^r)^*) = \{1, 3, 5, \ldots, 2^r - 1\} = \{\pm 1, \pm 5, \pm 9, \ldots, \pm(2^r - 3)\}$. Damit ist $|\langle 5 \rangle|$ die Hälfte der Anzahl der ungeraden Zahlen von 0 bis $2^r - 1$. Also folgt $|\langle 5 \rangle| = 2^{r-2}$. Der Isomorphismus ist durch die offensichtliche Abbildung

$$f : \{\pm 1\} \times \langle 5 \rangle \to (\mathbb{Z}/2^r), \quad (\pm 1, 5^k) \mapsto \pm 5^k$$

gegeben. Man sieht sofort, dass f ein surjektiver Homomorphismus ist. Da beide Seiten gleichviel Elemente haben, ist f ein Isomorphismus. □

Beweis von 9.10: (A) Wir zeigen durch Induktion: Für $k \geq 0$ gilt $5^{2^k} - 1 = 2^{k+2} \cdot q$ mit ungeradem q.

Für $k = 0$ gilt $5^{2^0} - 1 = 5 - 1 = 4 = 2^2 \cdot 1$

Induktionsschritt:
Voraussetzung: $5^{2^k} - 1 = 2^{k+2} \cdot q_1$, q_1 ungerade
Behauptung: $5^{2^{k+1}} - 1 = 2^{k+3} \cdot q$, q ungerade
Beweis: $5^{2^{k+1}} - 1 - (5^{2^k} + 1)(5^{2^k} - 1) = 2^{k+2} \cdot q_1 \cdot (5^{2^k} + 1)$
Nun gilt $5^{2^k} + 1 \equiv 1 + 1 = 2 \mod 4$. Also ist $5^{2^k} + 1$ durch 2, aber nicht durch 4 teilbar, d.h.$5^{2^k} + 1 = 2 \cdot q_2$. mit q_2 ungerade. Die Behauptung folgt jetzt mit $q = q_1 \cdot q_2$.
Folgerung: $\mathrm{ord}([5]_{2^r} = 2^{r-2}$. Da $|\{1, 5, 9, \ldots, 2^r - 3\}| = 2^{r-2}$ folgt der Satz.
Beweis: $5^{2^{r-3}} = 1 + 2^{r-1} \cdot q_1$ mit ungeradem q_1 und $5^{2^{r-2}} = 1 + 2^r \cdot q_2$ mit ungeradem q_2. Es folgt $5^{2^{r-3}} \not\equiv 1 \mod 2^r$, aber $5^{2^r} \equiv 1 \mod 2^r$. Nach 9.6 ist $\mathrm{ord}([5]_{2^r} = 2^{r-2}$.

Betrachten wir nun den Fall $p > 2$.

9.12 Für $p \geq 2$ prim gilt $|(\mathbb{Z}/p^r)^*| = (p-1) \cdot p^{r-1}$.

Beweis: $[k]_{p^r} \in (\mathbb{Z}/p^r)^* \iff \mathrm{ggT}(k, p) = 1$. Nun sind

$$p, 2p, 3p, \ldots, p^{r-1} \cdot p$$

genau die durch p teilbaren Elemente eines Repräsentantensystems $\{1,\ 2, \ldots,\ p^r\}$ von $\mathbb{Z}/p^r$. Also gibt es $p^r - p^{r-1} = (p-1)p^{r-1}$ Elemente, die nicht durch p teilbar sind. □
Wir betrachten jetzt den Reduktionshomomorphismus

$$\pi : \mathbb{Z}/p^r \to \mathbb{Z}/p, \quad [x]_{p^r} \mapsto [x]_p.$$

Dieser ist ein **surjektiver** Ringhomomorphismus, der $(\mathbb{Z}/p^r)^*$ auf $(\mathbb{Z}/p)^*$ abbildet, denn beide Gruppen enthalten die Elemente $[x]$, für die $\mathrm{ggT}(x, p) = 1$ ist. Wir wollen den Kern von

$$\pi^* : (\mathbb{Z}/p^r)^* \to (\mathbb{Z}/p)^*, \quad [x]_{p^r} \mapsto [x]_p$$

bestimmen. Da $|(\mathbb{Z}/p)^*| = p - 1$, ist $|\operatorname{Kern} \pi^*| = p^{r-1}$ nach 9.11.

9.13 Lemma: Für $p > 2$ prim ist $\operatorname{Kern} \pi^*$ ist zyklisch, multiplikativ erzeugt von $[p+1]_{p^r}$, also $\operatorname{Kern} \pi^* = \langle [p+1]_{p^r} \rangle \subset (\mathbb{Z}/p^r)^*$.

Beweis: Wir gehen wie im Beweis von 9.9 vor und zeigen zunächst durch Induktion nach k:
(A) Ist $p > 2$ prim und $k \geq 0$, dann gilt

$$(1 + px)^{p^k} = 1 + p^{k+1} \cdot y \quad \text{mit } y = x \mod p.$$

Für $k = 0$ gilt $(1 + px)^{p^0} = 1 + px$.

Induktionsschritt:

Voraussetzung: $(1 + px)^{p^k} = 1 + p^{k+1} \cdot y_1$ mit $y_1 \equiv x \mod p$

Behauptung: $(1 + px)^{p^{k+1}} = 1 + p^{k+2} \cdot y$ mit $y \equiv x \mod p$

Beweis:

$$\begin{array}{lll} (1+px)^{p^{k+1}} = ((1+px)^{p^k})^p & = & (1+p^{k+1}\cdot y_1)^p = (1+pz)^p \\ = 1 + ppz + \binom{p}{2}p^2z^2 + \binom{p}{3}p^3z^3 \ldots & = & 1 + p^2z(1 + \binom{p}{2}z + pz^2 \cdot \text{Rest}) \\ = 1 + p^2z(1+w) & = & 1 + p^{k+2}y_1(1+w) \end{array}$$

mit $z = p^k y_1$ und $w = \binom{p}{2}z + pz^2 \cdot \text{Rest}$.

$w \equiv 0 \mod p$, da $p - 1$ gerade ist, also $p \dashv \binom{p}{2}$.

Wir erhalten die Behauptung mit $y = y_1 \cdot (1 + w) \equiv y_1 \equiv x \mod p$.

$[p+1]_{p^r} \in \operatorname{Kern} \pi^*$, denn $\pi^*([p+1]_{p^r}) = [p+1]_p = [1]_p$ ist das neutrale Element von $(\mathbb{Z}/p)^*$. Da $|\operatorname{Kern} \pi^*| = p^{r-1}$ ist $[p+1]_{p^r}^{p^{r-1}} = [1]_{p^r}$ nach dem Satz von Lagrange. Da $(p+1)^{p^{r-2}} = 1 + p^{r-1} \cdot y$ mit $y \equiv 1 \mod p$, ist $[p+1]_{p^r}^{p^{r-2}} \neq [1]_{p^r}$. Nach 9.6 ist $\operatorname{ord}[p+1]_{p^r} = p^{r-1}$. Damit erzeugt $[p+1]_{p^r}$ ganz $\operatorname{Kern} \pi^*$. □

9.14 Satz: Ist $p > 2$ prim und $r \geq 2$, dann ist $(\mathbb{Z}/p^r)^*$ zyklisch der Ordnung $(p-1) \cdot p^{r-1}$, erzeugt von $[p+1]_{p^r} \cdot a$, wobei $a \in (\mathbb{Z}/p^r)^*$ ein Element der Ordnung $p - 1$ ist, so dass $\pi^*(a)$ die Gruppe $(\mathbb{Z}/p)^*$ erzeugt.

Zum Beweis benötigen wir noch ein algebraisches Resultat.

9.15 Satz: Ist $(G, \cdot)$ eine zyklische Gruppe der Ordnung n, erzeugt von $x \in G$, und ist $\operatorname{ggT}(r, n) = 1$, dann gilt auch $G = \langle x^r \rangle$.

Beweis: Da jedes Element aus G eine Potenz von x ist, genügt es zu zeigen, dass x eine Potenz von x^r ist. Da $\operatorname{ggT}(r, n) = 1$, gibt es $k, l \in \mathbb{Z}$, so dass $1 = k \cdot r + l \cdot n$. Es folgt

$$x = x^{kr+ln} = (x^r)^k \cdot (x^n)^l = (x^r)^k.$$

□

Beweis von 9.14: Sei z Erzeuger von $(\mathbb{Z}/p)^*$, also $\operatorname{ord}(z) = p - 1$ und $x = [p+1]_{p^r}$ der Erzeuger von $\operatorname{Kern} \pi^*$. Da π^* surjektiv ist, gibt es ein $y \in (\mathbb{Z}/p^r)^*$, so dass $\pi^*(y) = z$. Dann ist $y^{p-1} \in \operatorname{Kern} \pi^*$, da $\pi^*(y^{p-1}) = z^{p-1} = 1$. Die Ordnung von y^{p-1} teilt $|\operatorname{Kern} \pi^*| = p^{r-1}$, also $\operatorname{ord}(y^{p-1}) = p^s$ mit $s \leq r - 1$. Es folgt $y^{(p-1)\cdot p^s} = 1$, so dass $\operatorname{ord}(y^{p^s}) \dashv p - 1$ nach 9.5. Da $\pi^*(y^{p^s}) = z^{p^s}$ und $\operatorname{ggT}(p-1, p^s) = 1$, ist z^{p^s} Erzeuger von $(\mathbb{Z}/p)^*$ nach 9.15, also $\operatorname{ord}(z^{p^s}) = p-1$. Es folgt $\operatorname{ord}(y^{p^s}) \geq p-1$. Wir erhalten $\operatorname{ord}(y^{p^s}) = p-1$.

Da $\mathrm{ggT}(p-1, p^{r-1}) = 1$ ist

$$x \cdot y^{p^s} \text{ Erzeuger von } (\mathbb{Z}/p^r)^*,$$

wie im Beweis von 9.6 gezeigt wurde. □

9.16 Definition: Die "zahlentheoretische Funktion"

$$\varphi : \mathbb{N} \longrightarrow \mathbb{R}$$

$\varphi(n) = |\{d \in \mathbb{N};\ d \leq n \text{ und } \mathrm{ggT}(d, n) = 1\}|$ heißt *Euler'sche φ-Funktion.*

9.17 Da $\varphi(n) = |\mathbb{Z}/n)^*|$, folgt aus 9.2 und 9.11:
Ist $n = p_1^{r_1} \cdot \ldots \cdot p_k^{r_k}$ die Primfaktorzerlegung von n mit $p_1 < p_2 < \ldots < p_k$ und $r_i \geq 1$, dann gilt

$$\varphi(n) = \prod_{i=1}^{k} (p_i - 1) p_i^{r_i - 1} = \prod_{i=1}^{k} p^{r_i} \left(1 - \frac{1}{p_i}\right) = n \cdot \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

9.18 Definition: Ein Element $a \in (\mathbb{Z}/n)^*$ heißt *Primitivwurzel* modulo n, falls a ganz $(\mathbb{Z}/n)^*$ erzeugt, d.h. $\langle a \rangle = (\mathbb{Z}/n)^*$ bzw. $\operatorname{ord} a = \varphi(n)$.

Unsere Untersuchungen liefern

9.19 Satz: $(\mathbb{Z}/n)^*$ hat genau dann eine Primitivwurzel, wenn $n = 2,\ 4,\ p^r$ oder $2p^r$ ist, wobei $p > 2$ prim und $r \geq 1$ ist.

Beweis: Sei $n = 2,\ 4,\ p^r$ oder $2p^r$ mit $p > 2$ prim und $r \geq 1$. Wir müssen zeigen, dass $(\mathbb{Z}/n)^*$ zyklisch ist. Für $n = 2,\ 4,\ p^r$ folgt dies aus 9.10 und 9.14. Für $n = 2p^r$ folgt mit 9.2

$$(\mathbb{Z}/2p^r)^* \cong (\mathbb{Z}/2)^* \times (\mathbb{Z}/p^r)^* \cong (\mathbb{Z}/p^r)^*$$

das wiederum zyklisch ist.
Ist n von anderer Form, zeigen wir im nächsten Satz, dass die Ordnung eines Elements von $(\mathbb{Z}/n)^*$ Teiler von $\frac{1}{2}\varphi(n)$ ist, d.h. $(\mathbb{Z}/n)^*$ ist nicht zyklisch. □

9.20 Satz: Sei $n \in \mathbb{N}$, $n > 1$ und $n \neq 2,\ 4,\ p^r,\ 2p^r$ mit $p > 2$ prim. Dann gilt für alle $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, n) = 1$

$$a^{\frac{1}{2}\varphi(n)} \equiv 1 \mod n.$$

Beweis: Aus $\mathrm{ggT}(a, n) = 1$ folgt $[a]_n \in (\mathbb{Z}/n)^*$. Sei $l = \operatorname{ord}([a]_n)$.

(1) $n = 2^r$ mit $r \geq 3$. Nach 9.10 gilt

$$((\mathbb{Z}/2p^r)^*, \cdot) \cong (\mathbb{Z}/2, +) \times (\mathbb{Z}/2^{r-2}, +).$$

Es folgt: $l \dashv 2^{r-2} = \text{kgV}(2, 2^{r-2})$

(2) $n = 2^r \cdot p^s$ mit $r > 1$, $s \geq 1$. Dann folgt aus 9.2, 9.10, 9.14

$$((\mathbb{Z}/n)^*, \cdot) \cong (\mathbb{Z}/2, +) \times (\mathbb{Z}/2^{r-2}, +) \times (\mathbb{Z}/(p-1) \cdot p^{s-1}, +)$$

Mit $k = \text{kgV}(2, 2^{r-2}, (p-1)p^{s-1})$ gilt nach 9.6

$$[a^k]_n = 1 \quad \text{in } (\mathbb{Z}/n)^*.$$

Da $p-1$ gerade ist, gilt $k = \text{kgV}(2^{r-2}, (p-1)p^{s-1}) \dashv 2^{r-2} \cdot (p-1) \cdot p^{s-1}$. Da $\varphi(n) = 2 \cdot 2^{r-2} \cdot (p-1) \cdot p^{s-1}$, folgt $k \dashv \frac{1}{2}\varphi(n)$ und damit die Behauptung.

(3) $n = 2^{r_0} \cdot p_1^{r_1} \cdot \ldots \cdot p_l^{r_l}$ mit $l \geq 2$, $2 < p_1 < \ldots < p_l$ prim, $r_i \geq 1$ für $i > 0$. Dann ist

$$((\mathbb{Z}/n)^*, \cdot) \cong (\mathbb{Z}/2^{r_0})^*, \cdot) \times (\mathbb{Z}/(p_1-1) \cdot p_1^{r_1-1}, +) \times \ldots \times (\mathbb{Z}/(p_l-1) \cdot p_l^{r_l-1}, +)$$

Wieder gilt $[a^k]_n = 1$ für $k = \text{kgV}(\varphi(2^{r_0}), (p_1-1) \cdot p_1^{r^1-1}, \ldots, (p_l-1) \cdot p_l^{r_l-1})$ und $\varphi(n) = \varphi(2^{r_0}) \cdot (p_1-1) \cdot p_1^{r^1-1} \cdot \ldots \cdot (p_l-1) \cdot p_l^{r_l-1}$. Da (p_i-1) gerade ist und $l \geq 2$, folgt $k \dashv \frac{1}{2}\varphi(n)$ und damit die Behauptung.

□

Allgemein gilt nach dem Satz von Lagrange (s. auch den Grundkurs)

9.21 Kleiner Femat'scher Satz: Ist $n > 1$ aus $\mathbb{N}$ und $a \in \mathbb{Z}$ mit $\text{ggT}(a, n) = 1$, dann gilt

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

Ist insbesondere p prim und kein Teiler von $a \in \mathbb{Z}$, gilt

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

10 Ein Ausflug in die Kryptographie

Dieser Abschnitt ist dem Skript "Elemente der Algebra und Zahlentheorie", Wintersemester 2006/2007, von Prof. T. Römer entnommen. Das wiederum

folgt der Vorlesung *Codierungstheorie und Kryptographie* von Prof. W. Bruns (s. Osnabrücker Schriften zur Mathematik).

Die Kryptographie entwickelt *Kryptosysteme* um "Information" geheimzuhalten. Dies ist immer dann von Interesse, wenn Nachrichten über *unsichere Kanäle* übermittelt werden müssen. Unbefugte Dritte haben hier die Möglichkeit, gesendete Nachrichten zu empfangen und evtl. sogar verfälscht weiterzuleiten. Militär, Diplomatie und Geheimdienste sind immer Anwendungsbereiche von Kryptosystemen gewesen. Aber insbesondere seit dem 19. Jahrhundert wurden auch Kryptosysteme von der Wirtschaft benötigt, da z.B. Nachrichten von Telegraphisten im Morse-Code offen über Telegraphenleitungen gesendet wurden. Heute benutzen wir Kryptosysteme im Internet, bei Geldautomaten und an vielen weiteren Stellen.

Das folgende Diagramm beschreibt abstrakt das Zusammenwirken der Komponenten eines Kryptosystems

Nun bestehen eine Reihe von Problemen. Zunächst muss der Sender identifiziert werden können. Aber es muss z.B. auch sichergestellt sein, dass die gesendete Nachricht tatsächlich die Nachricht ist, die der Sender gesendet hat. Ein wichtiges Prinzip der Kryptographie lautet, dass *der Gegner das Verfahren kennt*. Man darf sich also nicht auf die Geheimhaltung des Chiffrier- und des Dechiffrierverfahrens verlassen. Für die Sicherheit ist es mindestens erforderlich, dass es dem Gegner nicht gelingt, bei bekanntem Geheimtext den Schlüssel zu finden. Dies setzt offensichtlich einen sehr großen Schlüsselraum voraus, insbesondere seit es möglich ist, mit Computerhilfe sehr viele Schlüssel in kurzer Zeit zu probieren. Für Fragestellungen dieser Art und ihre Lösungen wird auf die Literatur zur Kryptographie verwiesen.

Zunächst stellen wir hier klassische Kryptosysteme vor.

10.1 Beispiel: (Caesar-Chiffre) Eine der ältesten bekannten Chiffren ist die sogenannte "Caesar-Chiffre", die Gaius Julius Caesar zugeschrieben wird. Hierbei fasst man die 26 Buchstaben des (deutschen) Alphabets als Repräsentanten der Elemente von $\mathbb{Z}/26$ auf: wobei z.B. A der Restklasse von 0, B der Restklasse von 1 usw. entspricht. Nun wählt man als Schlüssel einen Buchstaben aus und "addiert" ihn zu jedem Buchstaben des Klartexts, um den Geheimtext zu erhalten:

Klartext	`veni vidi vici`
Schlüssel	`EEEE EEEE EEEE`
Geheimtext	`ZIRM ZMHM ZMGM`

Durch diese Chiffre wird der Klartext vor den Augen eines Mitlesers verborgen. Aber es tritt das Problem auf, dass der Schlüsselraum zu klein ist. Man kann einfach alle möglichen 26 Schlüssel ausprobieren um den Klartext zu erhalten.

Eine Verbesserung ist:

10.2 Beispiel: (Monoalphabetische Substitution) Die Caesar-Chiffre können wir als eine Permutation des Alphabets betrachten. Sie ist gerade eine zyklische Verschiebung um eine gewisse Anzahl an Stellen. Nun können wir den Schlüsselraum vergrößert, wenn wir beliebige Permutationen des Alphabets als Schlüssel zulassen. Wir erhalten dann nämlich $26! \approx 4 \cdot 10^{26}$ mögliche Schlüssel. Um sich den Schlüssel merken zu können, wird meist ein Schlüsselwort vereinbart, welches unter den Anfang des Alphabets geschrieben wird, wobei mehrfach auftretende Buchstaben nur bei ihrem ersten Erscheinen berücksichtigt werden. Danach schreibt man die im Schlüsselwort nicht vorkommenden Buchstaben der Reihe nach unter die restlichen Buchstaben des Alphabets, wobei wir mit dem Buchstaben beginnen, der auf den letzten im Schlüsselwort vorkommenden Buchstaben des Alphabets folgt. (Das kann man variieren.) Bei Verwendung des Schlüsselworts POMPEIUS ergibt sich folgende Permutation:

Klartextalphabet	`abcdefghijklmnopqrstuvwxyz`
Geheimtextalphabet	`POMEIUSTVWXYZABCDFGHJKLNQR`

Diese Chiffre führt dann also zu folgender Verschlüsselung:

Klartext	`mathe ist toll`
Geheimtext	`ZPHTI VGH HBYY`

Chiffren dieser Art heißen *monoalphabetische Substitutionen*, weil man dem Klartextalphabet ein einziges Geheimtextalphabet gegenüber stellt.

Monoalphabetische Substitutionen haben jedoch einen entscheidenden Schwachpunkt. Die Verteilung der Häufigkeit der einzelnen Buchstaben wird gegenüber dem Klartext nur permutiert. Wir betrachten folgende Tabellen, die die Häufigkeit der einzelnen Buchstaben im Deutschen und im Englischen angeben. (In der Literatur findet man auch geringfügig andere Angaben, da diese Statistiken von den Texte abhängen, die ausgezählt worden sind.)

Buchstabe	Häufigkeit in %	
	Deutsch	Englisch
a	6,5	8,2
b	1,9	1,5
c	3,1	2,8
d	5,1	4,3
e	17,4	12,7
f	1,7	2,2
g	3,0	2,0
h	4,8	6,1
i	7,5	7,0
j	0,3	0,2
k	1,2	0,8
l	3,4	4,0
m	2,5	2,4

Buchstabe	Häufigkeit in %	
	Deutsch	Englisch
n	9,8	6,7
o	2,5	7,5
p	0,8	1,9
q	0,02	0,1
r	7,0	6,0
s	7,3	6,3
t	6,2	9,1
u	4,4	2,8
v	0,7	1,0
w	1,9	2,4
x	0,03	0,2
y	0,04	2,0
z	1,1	0,1

Nun wird man eine Häufigkeitstabelle der Einzelzeichen des Geheimtextes anfertigen und diesen dann ihrer Häufigkeit gemäß Buchstaben des Klartextes zuweisen. Bei kurzen Texten treten natürlich Abweichungen zwischen den erwarteten und den beobachteten Häufigkeiten auf, so das die Zuordnung nicht immer auf Anhieb möglich ist. Bei langen Texten stimmen in der Regel die beobachteten Häufigkeiten der häufigsten Buchstaben gut mit den erwarteten überein. Hat man einige Buchstaben entdeckt, so experimentiert man, um weitere Zuordnungen finden.

Also ist auch die monoalphabetische Substitution nicht sicher. Viele weitere klassische Chiffren wurden alle gebrochen. Es tritt jedoch noch ein weiteres Problem auf. Die klassischen Verfahren (wie die Beispiele) sind alles *symmetrische Verfahren*. Die Teilnehmer müssen sich auf einen Schlüssel einigen, der dann über einen sicheren Kanal übertragen werden muss. Erstaunlicherweise kann man dieses Problem elegant umgehen.

Man muss den Gegner ja nicht daran hindern Klartexte zu verschlüsseln. Er soll nur Geheimtexte nicht entschlüsseln können. Das Grundprinzip sogenannnter *asymmetrische Verfahren* mit öffentlichem Schlüssel ist folgendes (nach Diffie und Hellman):

(1) Jeder Teilnehmer A konstruiert eine Funktion E_A, mit Hilfe der man Klartexte verschlüsseln kann. Diese Funktion soll eine *Einwegfunktion mit Falltür* sein. Eine nur A bekannte Zusatzinformation soll nur ihm eine Funktion D_A liefern mit $D_A = E_A^{-1}$.

(2) Der Teilnehmer A gibt E_A bekannt und hält D_A geheim.

(3) Will nun ein anderer Teilnehmer B eine Nachricht P an A senden, so verschlüsselt er sie mittels E_A und sendet den Chiffretext $C = E_A(P)$ an A.

(4) Wenn A den Chiffretext C empfängt, wendet er die nur ihm bekannte Entschlüsselung D_A an und erhält $P = D_A(E_A(P))$ zurück.

Zunächst ist nicht klar, ob Funktionen E_A und D_A existieren, die die gewünschten Eigenschaften haben. Mit Hilfe der Zahlentheorie lässt sich diese Idee jedoch realisieren. Das sogenannte *RSA-Kryptosystem* arbeitet wie folgt. ("Alice" und "Bob" werden hierbei in der Literatur zur Kryptographie häufig als Bezeichnung von Personen A und B verwendet.)

(1) Alice wählt zufällig zwei sehr große Primzahlen p und q.

(2) Alice berechnet $m_A = pq$ und $\varphi(m_A) = (p-1)(q-1)$. Die Zahl m_A wird auch der *RSA-Modul* von Alice genannt.

(3) Alice wählt nun eine zu $\varphi(m)$ teilerfremde Zahl $1 \leq e_A < \varphi(m)$, die *Verschlüsselungs-Exponent* genannt wird.

(4) Alice bestimmt als *Entschlüsselungs-Exponenten* die Zahl d_A, $1 \leq d_A < \varphi(m_A)$ mit $e_A d_A \equiv 1 \mod \varphi(m_A)$.

(5) Alice gibt m_A und e_A öffentlich bekannt, hält aber d_A, p, q und $\varphi(m_A)$ geheim.

(6) Will nun Bob eine Nachricht an Alice senden, so stellt er den Klartext zunächst als eine Folge von Zahlen $n_1, \ldots, n_r$ zwischen 0 und $m_A - 1$ dar. Dann bestimmt er zu jeder dieser Zahlen n_i den Geheimtext

$$c_i \equiv n_i^{e_A} \mod m_A$$

und sendet die Folge $c_1, \ldots, c_r$ an Alice. (Jede der Restklassen wird dabei natürlich durch c_i mit $0 \leq c_i \leq m_A - 1$ repräsentiert.)

(7) Alice empfängt $c_1, \ldots, c_r$, bildet die Potenzen

$$c_i^{d_A} \equiv n_i \mod m_A$$

und erhält $n_1, \ldots, n_r$ zurück (die dann noch in die ursprüngliche Nachricht umgewandelt werden müssen).

10.3 Beispiel: Wir wählen $p = 3$, $q = 11$, also $m = 33$. Es ist $(p-1)(q-1) = 20$ und daher kann $e = 3$ als Verschlüsselungs-Exponent verwendet werden. Wegen $3 \cdot 7 \equiv 1 \mod 20$, ergibt sich der Verschlüsselungs-Exponent $d = 7$. Für den Klartext $n = 13$ erhalten wir den Geheimtext $c \equiv 13^3 \equiv 19 \mod 33$, und wie gewünscht ist $c^7 \equiv 13 \mod 33$.

Wir zeigen nun, dass das Verfahren wirklich funktioniert. Nach Wahl von d_A gilt ja

$$e_A d_A \equiv 1 \mod \varphi(m_A),$$

und daher

$$e_A d_A = t\,\varphi(m_A) + 1$$

mit einer ganzen Zahl $t \geq 0$. Dann ist mit $m = m_A$

$$c_i^{d_A} \equiv n_i^{e_A d_A} \equiv n_i^{t\varphi(m)+1} \equiv \left(n_i^{\varphi(m)}\right)^{(t-1)} n_i^{\varphi(m)+1} \equiv n_i^{\varphi(m)(t-1)} n_i \equiv \cdots \equiv n_i \mod m$$

Hierbei haben wir ausgenutzt, dass $n_i^{\varphi(m)+1} \equiv n_i \mod m$ gilt, was wir in den Übungen beweisen werden.

Für die praktische Anwendung müssen eine Reihe von weiteren Problemen gelöst werden:

(1) Es müssen große Primzahlen gefunden werden und daher sind gute Primzahltests nötig.

(2) Die Arithmetik, wie schnelles Potenzieren, muss geeignet implementiert werden.

Das RSA-System ist gebrochen, wenn es jemandem gelingt, die Zahl m_A in ihre Teiler p und q zu zerlegen. Die scheint bisher ein schwieriges Problem zu sein. Man kann allerdings nicht beweisen, ob die Dechiffrierung wirklich die Zerlegung des RSA-Moduls erfordert. Daher ist nicht bekannt, ob das Brechen des RSA-Systems ebenso schwierig ist wie die Primfaktorzerlegung. Wir haben gesehen, dass die Zahlentheorie ein wesentlicher Faktor des RSA-Systems ist. Wir beenden an dieser Stelle die Diskussion von Kryptosystemen und verweisen für weitere Ergebnisse auf die Literatur.

Der Vollständigkeit halber behandeln wir abschließend Probleme der Codierungstheorie. Diese sind einerseits ähnlicher Natur, wie die der Kryptographie, aber unterscheiden sich andererseits wesentlich in den eigentlichen Ziele. Man möchte Information über einen "Kanal" versenden. Hierbei interessiert uns erstmal nicht, ob jemand anderes die Information lesen kann, oder nicht.

Das Grundproblem lässt sich wie folgt beschreiben:

Nun existieren folgende Probleme:

- Bei der Übertragung können Störungen auftreten (Rauschen, Kratzen, ...);
- Man möchte Fehler erkennen (z.B. Strichcode)
- und oft auch korrigieren können (z.B. CD oder Satellitenübertragung).

Nun gliedert sich ein codierungstheoretisches Problem im wesentlichen in drei Teile:

- Konstruktion eines Codes, der wie gewünscht Fehler erkennt und korrigiert;
- Konstruktion eines Codierers;
- Konstruktion eines Decodierers.

Nebenbedingungen:

- Wenig Kosten;
- Schnelligkeit.

Weitere Aspekte sind die bereits behandelte Kryptographie, oder die Quellcodierung, deren Ziel es ist Daten in eine effiziente Form zu bringen.

10.4 Beispiel:

$$\begin{array}{cccccccc} 00 & & 000 & & & & & \\ 10 & \longrightarrow & 101 & \longrightarrow & 111 & \longrightarrow & ? \\ 01 & & 011 & & & & & \\ 11 & & 110 & & & & & \end{array}$$

Die Idee ist, dass der Codierer dasjenige Bit hinzufügt, so dass die Quersumme Gerade wird. Macht der Kanal höchstens einen Fehler, so kann dieser erkannt werden. Es ist aber nicht möglich diesen zu korrigieren.

10.5 Beispiel:

$$\begin{array}{lcllcl} 00 & & 000000 & & & \\ 10 & \longrightarrow & 101010 & \longrightarrow & 101011 & \longrightarrow \quad 10 \\ 01 & & 010101 & & & \\ 11 & & 111111 & & & \end{array}$$

Hier ist nun die Idee, den Code dreimal zu wiederholen. Passiert höchstens ein Fehler, so kann dieser richtig decodiert werden. Aber dies ist mit sehr hohe Kosten verbunden.

10.6 Beispiel:

$$\begin{array}{lcllcl} 00 & & 00000 & & & \\ 10 & \longrightarrow & 01101 & \longrightarrow & 01100 & \longrightarrow \quad 10 \\ 01 & & 10110 & & & \\ 11 & & 11011 & & & \end{array}$$

Auch hier kann ein Fehler korrigiert werden, aber mit weniger Aufwand!

Die grundlegenden Definitionen für Codes sind nun:

10.7 Definition: Sei F eine endliche Menge mit $q = |F|$ Elementen. Eine Teilmenge $C \neq \emptyset$ von $F^n = \{(u_1, \ldots, u_n) : u_i \in F\}$ heißt *(Block-) Code* über dem *Alphabet* F. Die Elemente von C heißen *Codewörter*. Die Zahl n heißt die *Länge* von C. Für $q = 2$ (bzw. $q = 3$) nennen wir C auch einen *binären* (bzw. *ternären*) Code. Ist $|C| = 1$, so sagen wir, dass C trivial ist.

In der Regel setzen wir $F = \{0, \ldots, q-1\}$.

10.8 Definition: Sei C ein Code der Länge n über F mit $|F| = q$. Dann heißt $R(C) = \frac{log_q|C|}{n}$ die *Informationsrate* von C.

Ist $C \subset F^n$, dann folgt $|C| \leq q^n$. Gilt dann z.B. $|C| = q^k$, ergibt sich $R(C) = \frac{k}{n}$.

10.9 Beispiel: Der Code

$$C = \{(c, \ldots, c) \in F^n : c \in F\} \subset F^n$$

heißt *Wiederholungscode* der Länge n. Man kann sich überlegen, dass C bis zu $\frac{n-1}{2}$ Fehler korrigieren kann. Aber dies kostet einen sehr hohen Preis, da nur ein Zeichen bei n Zeichen Informationen trägt. Es gilt $R(C) = \frac{1}{n}$.

Das allgemeine Ziel der Codierungstheorie ist die Konstruktion eines Codes $C \subset F^n$ mit großer Informationsrate $R(C)$, der möglichst viele Fehler erkennen kann. Diese Ziele widersprechen sich natürlich.

Hier wollen wir nun eine Klasse von Codes betrachten, die sich einfach mit Hilfe der elementaren Zahlentheorie beschreiben lassen, die aber trotzdem viele Anwendungen im Alltag haben.

10.10 Definition: Seien $\pi_1, \ldots, \pi_n$ bijektive Abbildungen von $\mathbb{Z}/q$ auf $\mathbb{Z}/q$ und $[a] \in \mathbb{Z}/q$. Sei nun

$$C = \{([c_1], \ldots, [c_n]) \in (\mathbb{Z}/q)^n : \sum_{i=1}^{n} \pi_i([c_i]) = [a] \text{ in } \mathbb{Z}/q\}.$$

C heißt ein *Kontrollcode* mit der *Kontrollgleichung* $\sum_{i=1}^{n} \pi_i(c_i) = a$.

10.11 Satz: Ein Kontrollcode C kann einen Fehler erkennen.

Beweis: Seien $\pi_1, \ldots, \pi_n$ bijektive Abbildungen von $\mathbb{Z}/q$ auf $\mathbb{Z}/q$ und

$$C = \{([c_1], \ldots, [c_n]) \in (\mathbb{Z}/q)^n : \sum_{i=1}^{n} \pi_i([c_i]) = [a] \text{ in } \mathbb{Z}/q\}.$$

Für $0 \leq c_j < q$ lässt sich die Restklasse von c_j mittels

$$\pi_j([c_j]) = [a] - \sum_{i=1, i \neq j}^{n} \pi_i([c_i])$$

berechnen. □

10.12 Beispiel: (ISBN-Code) Es ist $F = \{0, 1, \ldots, 9, X\}$. Hierbei entspricht X der 10.

Betrachte z.B. $0-19-853803-0$. Durch die erste Ziffer wird die Sprachregion definiert. Hierbei steht 0 für Englisch und 3 für Deutsch. Die nächsten zwei Ziffern sind für den Verlag bestimmt. Danach folgt eine Buchnummer. Die ersten 9 Ziffern $c_1, \ldots, c_9$ sind Elemente von $\{0, \ldots, 9\}$. Die die zehnte Ziffer berechnet sich aus

$$10c_1 + 9c_2 + \cdots + 2c_9 + c_{10} \equiv 0 \mod 11.$$

Daher können wir den ISBN-Code also als eine Teilmenge von

$$\{([c_1], \ldots, [c_{10}]) \in (\mathbb{Z}/11)^{10} : \sum_{i=1}^{10} (11 - i)[c_i] = [0]\}$$

auffassen. Hierbei ist zu beachten, dass $(11-i)$ eine bijektive Abbildung auf $\mathbb{Z}/11\mathbb{Z}$ ist. Der ISBN-Code ist also ein Kontrollcode und erkennt daher einen Fehler. Er erkennt auch die Vertauschung von 2 beliebigen Stellen.

Ein weiteres Beispiel ist ein Code, der auf einigen EC-Karten eingesetzt wurde bzw. wird:

10.13 Beispiel: (Kontonummer-Code) Für $a \in \mathbb{N}$ sei $Q(a)$ die Quersumme. Definiere

$$\phi\colon \mathbb{Z}/10 \to \mathbb{Z}/10,\ [a] \mapsto [Q(2a)].$$

ϕ ist eine Permutation von $\mathbb{Z}/10$, also insbesondere eine bijektive Abbildung, da die Elemente von $\mathbb{Z}/10$ wie folgt abgebildet werden:

[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]
[0]	[2]	[4]	[6]	[8]	[1]	[3]	[5]	[7]	[9]

Nun definieren wir

$$\begin{aligned} & C \\ = \ & \{([c_1],\dots,[c_n]) \in (\mathbb{Z}/10)^n : c_n + Q(2c_{n-1}) + c_{n-2} + Q(2c_{n-3}) + \cdots \equiv 0 \bmod 10 \\ = \ & \{([c_1],\dots,[c_n]) \in (\mathbb{Z}/10)^n : [c_n] + [Q(2c_{n-1})] + [c_{n-2}] + [Q(2c_{n-3})] + \cdots = [0]. \end{aligned}$$

C ist 1-fehlererkennend, da C ein Kontrollcode ist. C erkennt aber auch das Vertauschen zweier Ziffern, sofern diese nicht 0 und 9 sind.

Mittels der Codierungstheorie kann Information vor Fehlern bei der Übertragung über gestörte Kanäle geschützt werden. Für wirklich gute Codes muss deutlich mehr Mathematik eingesetzt werden!

Teil IV

Approximationen irrationaler Zahlen

11 Kettenbrüche

Wenden wir den euklidischen Algorithmus auf das Paar 46 und 32 an, erhalten wir

$$\begin{array}{lll} 46 = 1 \cdot 32 + 14 & \text{und damit} & \frac{46}{32} = 1 + \frac{14}{32} \\ 32 = 2 \cdot 14 + 4 & \text{und damit} & \frac{32}{14} = 2 + \frac{4}{14} \\ 14 = 3 \cdot 4 + 2 & \text{und damit} & \frac{14}{4} = 3 + \frac{2}{4} \\ 4 = 2 \cdot 2 + 0 & \text{und damit} & \frac{4}{2} = 2 + 0 \end{array}$$

Da $\frac{14}{32}$ der Kehrwert von $\frac{32}{14}$ ist, $\frac{4}{14}$ der Kehrwert von $\frac{14}{4}$ usw., erhalten wir

$$\frac{46}{32} = 1 + \frac{1}{2 + \frac{4}{14}} = 1 + \frac{1}{2 + \frac{1}{3 + \frac{2}{4}}} = 1 + \frac{1}{2 + \frac{1}{3 + \frac{1}{2}}}$$

Im allgemeinen Fall haben wir für r_0 und r_1

$$\begin{array}{rcll} r_0 & = & a_0 \cdot r_1 + r_2 & \text{mit} \quad 0 < r_2 < r_1 \\ r_1 & = & a_1 \cdot r_2 + r_3 & \text{mit} \quad 0 < r_3 < r_2 \\ & \vdots & & \\ r_k & = & a_k \cdot r_{k+1} + r_{k+2} & \text{mit} \quad 0 < r_{k+2} < r_{k+1} \\ & \vdots & & \\ r_n & = & a_n \cdot r_{n+1} + 0 & \end{array}$$

und somit

$$\frac{r_0}{r_1} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}$$

Da $r_{k+1} < r_k$ für $k > 0$, sind alle $a_i > 0$ für $i > 0$.

Einen solchen Ausdruck nennen wir einen Kettenbruch. Wir wollen aber nicht nur Kettenbrüche mit ganzen Zahlen studieren, sondern definieren allgemeiner

11.1 Definition: Ein *Kettenbruch* ist ein formaler Ausdruck der Form

$$[a_0; a_1, a_2, \ldots] := a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_1 + \cfrac{1}{\ddots}}}$$

mit $a_i \in \mathbb{R}$, wobei a_0 beliebig ist und die $a_1, a_2, \ldots > 0$ sind.
Ein Kettenbruch kann *endlich* sein:

$$[a_0; a_1, a_2, \ldots, a_k] := a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_k}}}$$

In diesem Fall nennen wir k die *Länge* des Kettenbruchs $[a_0; a_1, a_2, \ldots, a_k]$. Wir lassen auch *unendliche Kettenbrüche* $[a_0; a_1, a_2, \ldots]$ zu und verstehen darunter die Folge ihrer *Abschnitte* $([a_0; a_1, a_2, \ldots, a_n])_{n\in\mathbb{N}_0}$.

Über die Konvergenz von unendlichen Kettenbrüchen werden wir uns später Gedanken machen.

11.2 Satz: Definiere $p_{-1} = 1,\ p_0 = a_0$ und $p_k = a_k p_{k-1} + p_{k-2}$ $k \geq 1$
$q_{-1} = 0,\ q_0 = 1$ und $q_k = a_k q_{k-1} + q_{k-2}$ $k \geq 1$

Dann gilt

$$[a_0; a_1, a_2, \ldots, a_k] = \frac{p_k}{q_k}$$

11.3 Bezeichnung: $\frac{p_k}{q_k}$, $k \geq 0$, heißt k-ter *Näherungsbruch* des Kettenbruchs $[a_0; a_1, a_2, \ldots]$. Dieser heißt *konvergent*, wenn die Folge $\left(\frac{p_k}{q_k}\right)_{k\in\mathbb{N}}$ konvergiert.

Beweis: Induktion: $[a_0] = a_0 = \frac{p_0}{q_0}, \quad [a_0; a_1] = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1} = \frac{p_1}{q_1}$
Induktionsschritt von n nach $n+1$, $n \geq 1$:
Voraussetzung: $[a_0; a_1, a_2, \ldots, a_n] = \frac{p_n}{q_n}$
Behauptung: $[a_0; a_1, a_2, \ldots, a_{n+1}] = \frac{p_{n+1}}{q_{n+1}}$
Beweis: $[a_0; a_1, a_2, \ldots, a_{n+1}] = [a_0; a_1, a_2, \ldots, a_{n-1}, a_n + \frac{1}{a_{n+1}}]$. Gesucht wird der n-te Näherungsbruch $\frac{\bar{p}_n}{\bar{q}_n}$ der rechten Seite. Die k-ten Näherungsbrüche

beider Seiten sind für $k \leq n-1$ gleich.

$$\frac{\overline{p}_n}{\overline{q}_n} = \frac{\left(a_n + \frac{1}{a_{n+1}}\right) p_{n-1} + p_{n-2}}{\left(a_n + \frac{1}{a_{n+1}}\right) q_{n-1} + q_{n-2}} = \frac{a_{n+1}(a_n p_{n-1} + p_{n-2}) + p_{n-1}}{a_{n+1}(a_n q_{n-1} + q_{n-2}) + q_{n-1}}$$

$$= \frac{a_{n+1}p_n + p_{n-1}}{a_{n+1}q_n + q_{n-1}} = \frac{p_{n+1}}{q_{n+1}}.$$

□

11.4 Lemma: (1) Für $k \geq 0$ gilt $q_k > 0$ und

$$p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1}$$

(2) Für $k \geq 1$ gilt

(i) $q_k p_{k-2} - p_k q_{k-2} = (-1)^{k-1} a_k$

(ii) $\frac{p_k}{q_k} - \frac{p_{k-1}}{q_{k-1}} = \frac{(-1)^{k-1}}{q_k \cdot q_{k-1}}$

(3) Für $k \geq 2$ gilt $\frac{p_k}{q_k} - \frac{p_{k-2}}{q_{k-2}} = \frac{(-1)^k a_k}{q_k \cdot q_{k-2}}$

Beweis: $q_0 = 1$. Da alle $a_k > 0$ für $k \geq 1$, ist $q_k > 0$ für $k \geq 0$. Aus den Formen 11.2 erhält man

$$p_k \cdot q_{k-1} = a_k p_{k-1} q_{k-1} + p_{k-2} q_{k-1} \qquad q_k \cdot p_{k-2} = a_k q_{k-1} p_{k-2} + q_{k-2} p_{k-2}$$
$$q_k \cdot p_{k-1} = a_k q_{k-1} p_{k-1} + q_{k-2} p_{k-1} \qquad p_k \cdot q_{k-2} = a_k p_{k-1} q_{k-2} + p_{k-2} q_{k-2}$$

Subtrahiere die Gleichungen voneinander

$$\begin{aligned} p_k \cdot q_{k-1} - q_k \cdot p_{k-1} &= p_{k-2} q_{k-1} - q_{k-2} p_{k-1} = -(p_{k-1} q_{k-2} - q_{k-1} p_{k-2}) \\ &= \ldots = (-1)^k (p_0 q_{-1} - q_0 p_{-1}) = (-1)^{k-1}. \end{aligned}$$

Im zweiten Fall erhalten wir

$$q_k p_{k-2} - p_k q_{k-2} = a_k (q_{k-1} p_{k-2} - p_{k-1} q_{k-2}) = a_k (-(-1)^{k-2}) = (-1)^{k-1} a_k$$

Damit sind (1) und (2(i)) gezeigt.
Dividieren wir (1) durch $q_k \cdot q_{k-1} \neq 0$, erhalten wir (2(ii)), und dividieren wir (2(i)) durch $q_k q_{k-2} \neq 0$, erhalten wir (3). □

11.5 Folgerung: Ist $\alpha = [a_0; a_1, \ldots, a_m]$ und $2k+1 < m$, $k \geq 1$, so gilt

$$\frac{p_{2k-2}}{q_{2k-2}} < \frac{p_{2k}}{q_{2k}} < \alpha < \frac{p_{2k+1}}{q_{2k+1}} < \frac{p_{2k-1}}{q_{2k-1}}$$

Beweis: Nach 11.4.3 ist $\frac{p_{2k}}{q_{2k}} - \frac{p_{2k-2}}{q_{2k-2}} = \frac{(-1)^{2k}a_k}{q_{2k}q_{2k-2}} > 0$, so dass $\frac{p_{2k}}{q_{2k}} > \frac{p_{2k-2}}{q_{2k-2}}$.
Analog zeigt man die rechte Ungleichung. Weiterhin gilt nach 11.4.2

$$\frac{p_{2k+1}}{q_{2k+1}} - \frac{p_{2k}}{q_{2k}} = \frac{(-1)^{2k}}{q_{2k+1}q_{2k}} > 0.$$

□

Besonderes Interesse gilt Kettenbrüchen mit ganzzahligen Elementen.

11.6 Definition: Ein Kettenbruch mit *natürlichen Elementen* ist ein endlicher Kettenbruch $[a_0; a_1, \ldots, a_m]$ oder ein unendlicher Kettenbruch $[a_0; a_1, a_2, \ldots]$ mit $a_0 \in \mathbb{Z}$ und $a_i \in \mathbb{N}$ für $i \geq 1$. Im endlichen Fall wird außerdem verlangt, dass $a_m \geq 2$.

Ist im endlichen Fall $a_m = 1$, so ist $[a_0; a_1, \ldots, a_m] = [a_0; a_1, \ldots, a_{m-1} + 1]$, so dass man einen neuen Kettenbruch mit $a_{m-1} \geq 2$ erhält!

11.7 Für einen unendlichen Kettenbruch mit natürlichen Elementen gilt

$$q_{n+1} > q_n \geq n \quad \forall n \geq 1 \quad \text{und} \quad q_1 = a_1 \geq q_0 = 1.$$

Beweis: Induktiv zeigen wir $q_n \geq n$: $q_0 = 1$, $q_1 = a_1 \geq 1$, $q_2 = a_2 \cdot q_1 + q_0 \geq q_1 + q_0 \geq 2$.
Induktionsschritt: Aus $n \geq 2$ und $q_n \geq n$ folgt $q_{n+1} \geq n + 1$. denn

$$q_{n+1} = a_{n+1}q_n + q_{n-1} \geq q_n + q_{n-1} \geq n + n - 1 \geq n + 1$$

Es folgt $q_n < q_{n+1}$ für $n \geq 1$, denn $q_{n+1} = a_{n+1}q_n + q_{n-1} \geq q_n + q_{n-1} > q_n$, weil $q_{n-1} \geq 1$ für $n \geq 1$. □

11.8 Satz: Jeder Kettenbruch mit natürlichen Elementen ist konvergent.

Beweis: Im endlichen Fall ist das klar. Im unendlichen Fall ist zu zeigen, dass die Folge $\left(\frac{p_n}{q_n}\right)_{n\in\mathbb{N}}$ der Näherungsbrüche konvergiert. Sei also $s > 0$. Für $k > n$ gilt nach 11.4 und 11.7

$$\begin{aligned}\left|\tfrac{p_k}{q_k} - \tfrac{p_n}{q_n}\right| &\leq \sum_{i=n}^{k-1}\left|\tfrac{p_{i+1}}{q_{i+1}} - \tfrac{p_i}{q_i}\right| = \sum_{i=n}^{k-1}\tfrac{1}{q_{i+1}\cdot q_i} \leq \sum_{i=n}^{k-1}\tfrac{1}{(i+1)i} = \sum_{i=n}^{k-1}\left(\tfrac{1}{i} - \tfrac{1}{i+1}\right)\\ &= \tfrac{1}{n} - \tfrac{1}{k} < \tfrac{1}{n} < s \text{ für } n > n_0 = \tfrac{1}{s}.\end{aligned}$$

Damit ist das Cauchy-Konvergenzkriterium erfüllt. □

11.9 Satz: Jedes $\alpha \in \mathbb{R}$ lässt sich **eindeutig** als Kettenbruch mit natürlichen Elementen darstellen. Der Kettenbruch ist genau dann endlich, wenn α rational ist.

Die Eindeutigkeitsforderung macht die Zusatzbedingung an a_m im endlichen Fall in Def. 11.6 nötig.

Beweis: Sei $[x] = \max\{k \in \mathbb{Z}; k \leq x\}$. D.h. $[x]$ ist die größte ganze Zahl $\leq x$.

Existensnachweis: Setze $a_0 = [\alpha]$. Ist $\alpha = [\alpha]$ sind wir fertig. Sonst gilt

$$\alpha = a_0 + \frac{1}{r_1} \quad \text{mit } r_1 > 1, \quad \text{also } \alpha = [a_0; r_1].$$

Ist $r_1 \in \mathbb{N}$, sind wir fertig. Sonst setzen wir

$$a_1 = [r_1], \quad r_1 = a_1 + \frac{1}{r_2} \quad \text{mit } r_2 > 1, \quad \text{also } \alpha = [a_0; a_1, r_2].$$

Ist $r_2 \in \mathbb{N}$, sind wir fertig. Sonst fahren wir fort.

Ist jedes $r_n \notin \mathbb{N}$, ist der resultierende Kettenbruch unendlich. Im anderen Fall erhalten wir einen endlichen Kettenbruch

$$\alpha = [a_0; a_1, \ldots, a_m]$$

mit $a_m \geq 2$.

Ist $\alpha \in \mathbb{Q}$, so ist $r_1 \in \mathbb{Q}$. Ist $r_i \in \mathbb{Q}$, so ist $r_{i+1} \in \mathbb{Q}$, so dass jedes r_i von der Form

$$r_i = \frac{s_i}{t_i} \quad s_i, t_i \in \mathbb{N}, \quad \text{ggT}(s_i, t_i) = 1$$

ist. Weiter gilt nach Konstruktion

$$\begin{aligned} 0 &\leq r_i - a_i = \frac{1}{r_{i+1}} < 1 \\ 0 &\leq \frac{s_i}{t_i} - a_i = \frac{s_i - t_i a_i}{t_i} = \frac{z_i}{t_i} < 1. \end{aligned}$$

Also $z_i < t_i$ und $r_{i+1} = \frac{t_i}{z_i}$. Nach Kürzen ist $r_{i+1} = \frac{s_{i+1}}{t_{i+1}}$. Es folgt $t_{i+1} \leq z_i < t_i$, so dass der Prozess abbrechen muss, d.h. $r_k \in \mathbb{N}$ für genügend großes k.

Für einen Kettenbruch mit natürlichen Elementen sind die p_n und q_n ganzzahlig, d.h. $\frac{p_n}{q_n} \in \mathbb{Q}$. Ist der Kettenbruch endlich, folgt

$$\alpha = [a_0; a_1, \ldots, a_m] = \frac{p_m}{q_m} \in \mathbb{Q}.$$

Für den unendlichen Fall bleibt zu zeigen, dass der gefundene Kettenbruch die Zahl α darstellt. Nach Konstruktion gilt

$$\alpha = [a_0; a_1, \ldots, a_n, r_{n+1}] \quad a_0 \in \mathbb{Z}, a_i \in \mathbb{N} \text{ für } 1 \leq i \leq n, r_{n+1} > 1.$$

Sei $\frac{p_n}{q_n}$ der n-te Näherungsbruch des unendlichen Kettenbruchs. Dann gilt

$$\begin{aligned} \alpha - \frac{p_n}{q_n} &= \frac{r_{n+1}p_n + p_{n-1}}{r_{n+1}q_n + q_{n-1}} - \frac{p_n}{q_n} = \frac{q_n r_{n+1} p_n + q_n p_{n-1} - r_{n+1} q_n p_n - p_n q_{n-1}}{q_n(r_{n+1}q_n + q_{n-1})} \\ &= \frac{p_{n-1}q_n - p_n q_{n-1}}{q_n(r_{n+1}q_n + q_{n-1})} = \frac{(-1)^n}{q_n(r_{n+1}q_n + q_{n-1})} \end{aligned}$$

Also

$$\left|\alpha - \frac{p_n}{q_n}\right| = \frac{1}{q_n(r_{n+1}q_n + q_{n-1})} < \frac{1}{q_n(a_{n+1}q_n + q_{n-1})} = \frac{1}{q_n \cdot q_{n+1}} = \frac{1}{n^2} \rightsquigarrow 0 \qquad (*)$$

Eindeutigkeit: Seien $\alpha = [a_0; a_1, a_2, \ldots] = [b_0; b_1, b_2, \ldots]$ zwei Entwicklungen von α in Kettenbrüche mit natürlichen Elementen, die endlich oder unendlich sein können. Wir zeigen induktiv, dass $a_i = b_i \; \forall i$.

$a_0 = b_0$: Aus der Definition eines Kettenbruchs folgt, dass $a_0 = b_0 = [\alpha]$, denn $a_1 \geq 1$, also ist der erste Nenner > 1.

Induktionsschritt: Sei $a_i = b_i$ für $0 \leq i \leq n$. Dann gilt auch $a_{n+1} = b_{n+1}$

Seien $\frac{p_k}{q_k}$ und $\frac{p'_k}{q'_k}$ die Näherungsbrüche beider Kettenbrüche. Diese sind nach Induktion für $k \leq n$ gleich. Sei

$$r_{n+1} = [a_{n+1}; a_{n+2}, \ldots], \qquad r'_{n+1} = [b_{n+1}; b_{n+2}, \ldots]$$

Dann gilt

$$\alpha = \frac{r_{n+1}p_n + p_{n-1}}{r_{n+1}q_n + q_{n-1}} = \frac{r'_{n+1}p'_n + p'_{n-1}}{r'_{n+1}q'_n + q_{n-1}}$$

und somit

$$(r_{n+1} \cdot p_n + p_{n-1}) \cdot (r'_{n+1} \cdot q_n + q_{n-1}) = (r'_{n+1} \cdot p_n + p_{n-1}) \cdot (r_{n+1} \cdot q_n + q_{n-1}).$$

Ausmultipliziert gibt das

$$r_{n+1} \cdot r'_{n+1} \cdot p_n \cdot q_n + r'_{n+1} \cdot p_{n-1} \cdot q_n + r_{n+1} \cdot p_n \cdot q_{n-1} = r'_{n+1} \cdot r_n \cdot p_n \cdot q_n + r_{n+1} \cdot p_{n-1} \cdot q_n + r'_{n+1} \cdot p_n \cdot q_n.$$

Also $(r'_{n+1} - r_{n+1}) \cdot (p_{n-1}q_n - p_n \cdot q_{n-1}) = 0$

Es folgt $r'_{n+1} = r_{n+1}$, weil $p_{n-1} \cdot q_n - p_n \cdot q_{n-1} = (-1)^n$ nach 11.4.

Wie oben folgt jetzt $a_{n+1} = [r_{n+1}] = [r'_{n+1}] = b_{n+1}$. □

Dieser Satz liefert ausgesprochen gute Approximationen irrationaler Zahlen durch rationale. In der Zeile (*) des letzten Beweises haben wir statt $<$ das Gleichheitszeichen, falls $r_{n+1} = a_{n+1} \in \mathbb{N}$ ist. Wir halten fest:

11.10 Satz: Für den n-ten Näherungsbruch der Entwicklung von α in einen Kettenbruch mit natürlichen Elementen gilt

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

falls dessen Länge $\geq n+1$ ist. Das Gleichheitszeichen gilt genau dann, wenn seine Länge $n+1$ ist.

Im nächsten Abschnitt zeigen wir, dass diese Approximation einer irrationalen Zahl α durch eine rationale Zahl $\frac{p}{q}$ in gewissem Sinne optimal ist.

12 Approximationen irrationaler Zahlen durch rationale

12.1 Satz: Sei $\alpha \in \mathbb{R}$ beliebig und $r \geq 1$. Dann gibt es $p, q \in \mathbb{Z}$, so dass

$$|q \cdot \alpha - p| < \frac{1}{r} \qquad \text{wobei} \quad 1 \leq q \leq r.$$

Beweis: Ist $\alpha \in \mathbb{Q}$, $\alpha = \frac{a}{b}$ mit $1 \leq b \leq r$, folgt $|b \cdot \alpha - a| = 0 < \frac{1}{r}$.
Sei also α irrational oder rational mit $b > r$. Bestimme in der Kettenbruchentwicklung von α ein n, so dass $q_n \leq r < q_{n+1}$. Nach 11.7 gibt es ein solches n für jeden unendlichen Kettenbruch und damit nach 11.9 für jedes $\alpha \notin \mathbb{Q}$. Ist dagegen $\alpha = \frac{a}{b} \in \mathbb{Q}$ mit $b > r$ und $\alpha = [a_0; a_1, \ldots, a_m]$ seine Kettenbruchentwicklung, dann ist $\alpha = \frac{a}{b} = \frac{p_m}{q_m}$. Da $\frac{a}{b}$ ein gekürzter Bruch ist, gilt $b \leq q_m$. Also gibt es auch in diesem Fall ein solches n, weil $b > r$ ist. Aus 11.10 folgt jetzt

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

□

12.2 Definition: Eine gekürzte rationale Zahl $\frac{a}{b}$ mit $b \in \mathbb{N}$ heißt *beste Approximation* von $\alpha \in \mathbb{R}$, wenn für alle $\frac{p}{q} \in \mathbb{Q}$ mit $1 \leq q \leq b$ und $\frac{p}{q} \neq \frac{a}{b}$

$$\left|\alpha - \frac{a}{b}\right| < \left|\alpha - \frac{p}{q}\right|.$$

D.h. jede gekürzte rationale Zahl mit kleinerem Nenner oder gleichem Nenner, aber anderem Zähler als $\frac{a}{b}$ ist eine schlechtere Approximation von α.

12.3 Satz: (Lagrange) Ist $\frac{p_n}{q_n}$, $n \geq 1$, der n-te Näherungsbruch der Kettenbruchentwicklung von α, dann gilt für alle $\frac{p}{q} \in \mathbb{Q}$ mit $1 \leq q \leq q_n$ und $\frac{p}{q} \neq \frac{p_n}{q_n}$

$$|q_n\alpha - p_n| < |q\alpha - p|$$

12.4 Folgerung: $\frac{p_n}{q_n}$ ist eine beste Approximation von α, denn dividiert man die Ungleichung durch q_n erhält man

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n}|q\alpha - p| = \frac{q}{q_n}\left|\alpha - \frac{p}{q}\right| \leq \left|\alpha - \frac{p}{q}\right|$$

. □

Beweis: Für $\alpha = \frac{p_n}{q_n}$ ist die Behauptung klar. Sei also $\alpha \neq \frac{p_n}{q_n}$ für alle n.
Das Gleichungssystem

$$\begin{array}{lrcl} \text{I} & p_n \cdot x + p_{n-1} \cdot y & = & p \\ \text{II} & q_n \cdot x + q_{n-1} \cdot y & = & q \end{array}$$

hat genau eine Lösung, und diese ist ganzzahlig: Nach 11.4 gilt:

$$q_{n-1} \cdot I - p_{n-1} \cdot II = (p_n \cdot q_{n-1} - p_{n-1} \cdot q_n) \cdot x = (-1)^{n-1} \cdot x = q_{n-1} \cdot p - p_{n-1} \cdot q$$

$$p_n \cdot II - q_n \cdot I = (p_n \cdot q_{n-1} - q_n \cdot p_{n-1}) \cdot y = (-1)^{n-1} \cdot y = p_n \cdot q - q_n \cdot p.$$

Angenommen $y = 0$, dann ist $\frac{p_n}{q_n} = \frac{p}{q}$, ein Widerspruch. Also ist $y \neq 0$.
Ist $x = 0$, so ist $y > 0$, weil $q_{n-1} \geq 1$ und $q \geq 1$.
Ist $x \neq 0$, so haben x und y verschiedene Vorzeichen: Da $q \geq 1$, können nicht beide negativ sein, und weil $q_n \geq q$, können nicht beide positiv sein. Aus den Gleichungen folgt

$$\begin{array}{rcll} q\alpha - p & = & q_n\alpha x + q_{n-1}\alpha y - p_n x - p_{n-1} y & \\ & = & x(q_n\alpha - p_n) + y(q_{n-1}\alpha - p_{n-1}) & (*) \end{array}$$

Nach 11.5 gilt entweder

$$\frac{p_n}{q_n} \leq \alpha \leq \frac{p_{n-1}}{q_{n-1}}, \text{ also } q_{n-1} \cdot \alpha - p_{n-1} \leq 0 \text{ und } q_n \cdot \alpha - p_n \geq 0$$

oder

$$\frac{p_{n-1}}{q_{n-1}} \leq \alpha \leq \frac{p_n}{q_n}, \text{ also } q_{n-1} \cdot \alpha - p_{n-1} \geq 0 \text{ und } q_n \cdot \alpha - p_n \leq 0$$

In beiden Fällen haben $q_n\alpha - p_{n-1}$ und $q_{n-1}\alpha - p_{n-1}$ verschiedene Vorzeichen. Damit sind die Summanden $(*)$ beide positiv oder beide negativ. Es folgt

$$|q\alpha - p| = |x(q_n\alpha - p_n)| + |y(q_{n-1}\alpha - p_{n-1})| \geq |q_{n-1}\alpha - p_{n-1}|.$$

Nach unserer Kettenbruchentwicklung gilt $\alpha = [a_0; a_1, \ldots, a_n, r_{n+1}]$ mit $r_{n+1} > 1$. Also

$$\alpha = \frac{p_n r_{n+1} + p_{n-1}}{q_n r_{n+1} + q_{n-1}} \qquad r_{n+1} \cdot \alpha q_n + \alpha q_{n-1} = r_{n+1} p_n + p_{n-1},$$

also $|q\alpha - p| \geq |q_{n-1}\alpha - p_{n-1}| = r_{n+1} \cdot |p_n - \alpha q_n| > |\alpha q_n - p_n|$. □

12.5 Beispiel: Beste Approximationen von $\sqrt{2}$

$$\sqrt{2} = 1 + (\sqrt{2} - 1) = 1 + \frac{(\sqrt{2} - 1)(\sqrt{2} + 1)}{1 + \sqrt{2}} = 1 + \frac{1}{2 + (\sqrt{2} - 1)}$$

Der Kettenbruch wird somit *periodisch*: $\sqrt{2} = [1; 2, 2, 2, 2, \ldots]$
Wir berechnen die Näherungsbrüche:

$$\begin{aligned}
\frac{p_1}{q_1} &= \frac{2 \cdot 1 + 1}{2 \cdot 1} = \frac{3}{2} & \left|\sqrt{2} - \frac{p_1}{q_1}\right| &< \frac{1}{2 \cdot 5} &&= 0,1 \\
\frac{p_2}{q_2} &= \frac{2 \cdot 3 + 1}{2 \cdot 2 + 1} = \frac{7}{5} & \left|\sqrt{2} - \frac{7}{5}\right| &< \frac{1}{5 \cdot 12} &&< 0,017 \\
\frac{p_3}{q_3} &= \frac{2 \cdot 7 + 3}{2 \cdot 5 + 2} = \frac{17}{12} & \left|\sqrt{2} - \frac{17}{12}\right| &< \frac{1}{12 \cdot 29} &&< 0,003
\end{aligned}$$

letzteres weil $q_4 = 2 \cdot 12 + 5 = 29$.

12.6 Beste Approximationen von π: Die Kettenbruchentwicklung von π ist unbekannt. Man rechnet aus, dass $\pi = [3; 7, 15, 1, 292, \ldots]$

$$\begin{aligned}
\frac{p_1}{q_1} &= \frac{7 \cdot 3 + 1}{7 \cdot 1} = \frac{22}{7} & \left|\pi - \frac{22}{7}\right| &< \frac{1}{7 \cdot 106} &&< 0,0014 \\
\frac{p_2}{q_2} &= \frac{15 \cdot 22 + 3}{15 \cdot 7 + 1} = \frac{333}{106} & \left|\pi - \frac{333}{106}\right| &< \frac{1}{106 \cdot 113} &&< 8,4 \cdot 10^{-5} \\
\frac{p_3}{q_3} &= \frac{1 \cdot 333 + 22}{1 \cdot 106 + 7} = \frac{355}{113} & \left|\pi - \frac{355}{113}\right| &< \frac{1}{113 \cdot 33102} &&< 2,7 \cdot 10^{-7}
\end{aligned}$$

$$q_4 = 292 \cdot 113 + 106 = 33102$$

Wir sehen, dass diese Näherungsbrüche π erstaunlich gut approximieren. Um so überraschender ist es, dass diese Näherungen für π schon bekannt waren, bevor die Theorie der Kettenbrüche entwickelt wurde:

Archimedes (287 - 212 v.Chr.) arbeitete mit dem Näherungsbruch $\frac{22}{7}$, aber kannte noch andere bessere Approximationen von π.

Ptolemäus (85 - 165 n.Chr.) benutzte die Approximation $\frac{333}{106}$.

Der Chinese **Tsu-Chung-Chi** (3. Jahrhundert n.Chr.) kannte die Approximationen $\frac{22}{7}$ und $\frac{355}{113}$.

12.7 Definition: $\alpha \in \mathbb{R}$ ist durch rationale Zahlen *zur Ordnung* n approximierbar, wenn es eine Konstante $C(\alpha)$ gibt, die nur von α abhängt, so dass

$$\left|\alpha - \frac{p}{q}\right| < \frac{C(\alpha)}{q^n}$$

für unendlich viele $\frac{p}{q} \in \mathbb{Q}$ ($n \in \mathbb{N}$)

12.8 Sei $\alpha \in \mathbb{R}$ durch rationale Zahlen zur Ordnung n approximierbar, und $\delta > 0$. Dann gibt es im Intervall $[\alpha - \delta, \alpha + \delta]$ unendlich viele $\frac{p}{q} \in \mathbb{Q}$, so dass

$$\left|\alpha - \frac{p}{q}\right| < \frac{C(\alpha)}{q^n}. \qquad (*)$$

Beweis: Die Ungleichung in 12.7 ist äquivalent zu

$$\alpha - \frac{C(\alpha)}{q^n} < \frac{p}{q} < \alpha + \frac{C(\alpha)}{q^n}.$$

Zu fest gewähltem $q \in \mathbb{N}$ kann es nur endlich viele $p \in \mathbb{Z}$ geben, die das erfüllen. Also muss die Ungleichung $(*)$ für unendlich viele verschiedene q gelten. Ist nun q groß genug, dann ist

$$\frac{C(\alpha)}{q^n} < \delta.$$

□

12.9 Satz: (1) $\alpha \in \mathbb{Q}$ ist approximierbar zur Ordnung 1 und zu keiner höheren Ordnung.

(2) Jede irrationale Zahl ist zur Ordnung 2 approximierbar.

Beweis: Sei $\alpha = \frac{a}{b}$ mit $b \in \mathbb{N}$, $\mathrm{ggT}(a,b) = 1$. Nach 8.3 hat die Gleichung

$$aq - bp = 1$$

unendliche viele Lösungen p, q in $\mathbb{Z}$. Nach 7.4.4 ist $\mathrm{ggT}(p,q) = 1$. Für $q \neq 0$ (das ist immer der Fall, wenn $\alpha \notin \mathbb{Z}$) folgt

$$\frac{a}{b} - \frac{p}{q} = \frac{1}{b \cdot q}$$

und somit für $q > 0$

$$\left| \frac{a}{b} - \frac{p}{q} \right| = \frac{1}{b \cdot q} < \frac{2}{q} \qquad (*)$$

Für negative q ist $q' = -q > 0$, so dass mit $p' = -p$ gilt $\frac{a}{b} - \frac{p'}{q'} = -\frac{1}{b \cdot q'}$. Wir erhalten

$$\left| \frac{a}{b} - \frac{p'}{q'} \right| = \frac{1}{b \cdot q'} < \frac{2}{q'} \qquad (*)$$

Die Ungleichungen $(*)$ haben also mit $C(\alpha) = 2$ unendlich viele Lösungen $\frac{p}{q}$ bzw. $\frac{p'}{q'}$ in $\mathbb{Q}$.
Indem wir gegebenenfalls p und q durch $-p$ und $-q$ ersetzen, dürfen wir annehmen, dass $b, q > 0$ sind. Ist $\frac{a}{b} \neq \frac{p}{q}$, folgt

$$\left| \frac{a}{b} - \frac{p}{q} \right| = \frac{|aq - bp|}{bq} \geq \frac{1}{bq}$$

Eine Approximation der Ordnung 2 mit $c = C(\alpha)$ erfordert

$$\frac{1}{b \cdot q} \leq \frac{|aq - bp|}{bq} < \frac{c}{q^2} \quad \text{also} \quad q \leq q|aq - bp| < cb \qquad (**)$$

Dafür ist $q < cb$ eine notwendige Bedingung, die nur für endlich viele q gelten kann. Für festes q ist $(**)$ offensichtlich für höchstens endlich viele p erfüllt.
Teil (2): Ist α irrational, hat α nach 11.9 eine unendliche Kettenbruchentwicklung mit natürlichen Elementen. Für die Näherungsbrüche gilt

$$\left| \alpha - \frac{p_n}{q_n} \right| \leq \frac{1}{q_n^2}.$$

Also ist α von der Ordnung 2 appoximierbar mit $C(\alpha) = 2$. $\square$

13 Algebraische Zahlen

13.1 Definition: $\alpha \in \mathbb{R}$ heißt *algebraisch vom Grad n*, wenn α Nullstelle eines Polynoms $f \neq 0$ aus $\mathbb{Q}[X]$ vom Grade n ist, aber nicht von einem Polynom kleineren Grades aus $\mathbb{Q}[X]$. Ist $\alpha \in \mathbb{R}$ nicht algebraisch, dann heißt α *transzendent*.

13.2 Definition: Eine Menge X heißt *abzählbar*, wenn sie leer ist oder es eine surjektive Abbildung $\mathbb{N} \to X$ gibt. Gibt es keine solche Abbildung und ist $X \neq \emptyset$, heißt X *überabzählbar*.

13.3 Lemma: (1) $\mathbb{N}^k$ ist abzählbar für $k \in \mathbb{N}$

(2) Ist X abzählbar und $f : X \to Y$ surjektiv, dann ist Y abzählbar.

(3) Ist X abzählbar und $Y \subset X$, dann ist Y abzählbar.

(4) Ist J abzählbar und $\{M_j; j \in J\}$ eine Familie abzählbarer Mengen M_j, dann ist $\bigcup\limits_{j \in J} M_j$ abzählbar.

(5) $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Q}[X]$ sind abzählbar.

Beweis: (1) Aus der eindeutigen Primfaktorzerlegung von n folgt, dass n eindeutig von der Form $n = 2^k \cdot q$ mit $k \geq 0$ und ungeradem q ist. Dann ist $l = \frac{q+1}{2} \in \mathbb{N}$, also $n = 2^k \cdot (2l - 1)$. Wir definieren

$$\psi : \mathbb{N} \longrightarrow \mathbb{N} \times \mathbb{N}, \quad n \mapsto (k + 1, l).$$

Dann ist ψ surjektiv: $(s, t) = \psi(2^{s-1} \cdot (2t - 1))$ und $2^{s-1} \cdot (2t - 1) \in \mathbb{N}$. Für $k > 2$ ist

$$\mathbb{N} \xrightarrow{\psi} \mathbb{N}^2 \xrightarrow{\psi \times \mathrm{id}} \mathbb{N}^3 \xrightarrow{\psi \times \mathrm{id}} \mathbb{N}^4 \longrightarrow \ldots \longrightarrow \mathbb{N}^k$$

surjektiv.

(2) Nach Voraussetzung haben wir eine surjektive Abbildung $g : \mathbb{N} \to X$. Dann ist $f \circ g : \mathbb{N} \to Y$ surjektiv.

(3) Ist $Y \neq \emptyset$, wählen wir ein $y_0 \in Y$. Dann ist

$$f : X \to Y, \quad x \mapsto \begin{cases} x, & \text{falls } x \in Y \\ y_0, & \text{falls } x \notin Y \end{cases}$$

surjektiv. Nach (2) ist Y abzählbar.

(4) Nach Voraussetzung gibt es surjektive Abbildungen

$$f_j : \mathbb{N} \longrightarrow M_j, \quad g : \mathbb{N} \longrightarrow J.$$

Dann ist die Abbildung

$$h : \mathbb{N} \times \mathbb{N} \longrightarrow \bigcup_{j \in M} M_j, \quad (k, l) \mapsto f_{g(k)}(l)$$

surjektiv: Ist $x \in M_j$, $l \in \mathbb{N}$, so dass $f_j(l) = x$, und $k \in \mathbb{N}$, so dass $g(k) = j$, dann ist $h(k, l) = f_j(l) = x$. Nach (2) ist $\bigcup\limits_{j \in M} M_j$ abzählbar.

(5) $\mathrm{id} : \mathbb{N} \longrightarrow \mathbb{N}$ ist surjektiv.

$$f : \mathbb{N} \longrightarrow \mathbb{Z}, \quad n \mapsto \begin{cases} \frac{n-1}{2}, & n \text{ ungerade} \\ -\frac{n}{2}, & n \text{ gerade} \end{cases}$$

ist surjektiv.

$$\mathbb{N} \times \mathbb{N} \xrightarrow{f \times \mathrm{id}} \mathbb{Z} \times \mathbb{N} \xrightarrow{g} \mathbb{Q} \quad \text{mit} \quad g(p, q) = \frac{p}{q}$$

ist surjektiv. Also ist $\mathbb{Q}$ abzählbar.
Sei $P_n \subset \mathbb{Q}[X]$ die Menge der Polynome vom Grad n. Dann ist

$$\mathbb{Q}^n \times \mathbb{Q}^* \longrightarrow P_n, \quad (a_0, \ldots, a_n) \mapsto \sum_{i=0}^{n} a_i X^i$$

ein Isomorphismus. Da $\mathbb{Q}$ und $\mathbb{Q}^*$ abzählbar sind, ist nach (1) auch $\mathbb{Q}^n \times \mathbb{Q}^*$, also auch P_n abzählbar. Nach (4) ist dann

$$\mathbb{Q}[X] = \{0\} \cup \bigcup_{n=0}^{\infty} P_n.$$

abzählbar. □

13.4 Satz: (1) Die Menge $\mathbb{A}$ der algebraischen Zahlen in $\mathbb{R}$ ist abzählbar.

(2) $\mathbb{R}$ ist überzählbar.

(3) Die Menge $\mathbb{T}$ der transzendenten Zahlen in $\mathbb{R}$ ist überabzählbar.

Beweis: (1) $\mathbb{A} \subset \mathbb{R}$ ist die Menge der reellen Nullstellen aller Polynome aus $P = \mathbb{Q}[X] \backslash \{0\}$. Für $f \in P$ sei $N(f)$ die Menge der Nullstellen. Nach 6.6 ist $|N(f)| \leq \operatorname{grad} f$; insbesondere ist $N(f)$ abzählbar. Da P abzählbar ist, ist

$$\mathbb{A} = \bigcup_{f \in P} N(f)$$

nach 13.3.4 abzählbar.

(2) Wir zeigen: Es gibt keine surjektive Abbildung $f : \mathbb{N} \to \mathbb{R}$.

Zu jedem f konstruieren wir eine reelle Zahl x zwischen 0 und 1, die nicht von f getroffen wird. Die Dezimalbruchentwicklung von x hat die Form

$$x = \sum_{j=1}^{\infty} a_j \cdot \frac{1}{10^j}, \quad 0 \leq a_j \leq 9.$$

Ist $f(k) = n + \sum b_k \frac{1}{10^j}$ die Dezimalbruchentwicklung von $f(k)$ mit $n \in \mathbb{N}_0$, wählen wir $a_k = 7$, falls $b_k \leq 5$, und $a_k = 3$, falls $b_k > 5$. Dann ist

$$|f(k) - x| \geq \frac{1}{10^k}$$

also $f(k) \neq x$. Da das für alle $k \in \mathbb{N}$ gilt, ist x nicht im Bild von f.

(3) Wäre $\mathbb{T}$ abzählbar, wäre auch $\mathbb{R} = \mathbb{A} \cup \mathbb{T}$ abzählbar. □

Obwohl es also mehr transzendente als algebraische Zahlen gibt, ist es schwer, eine solche zu finden. Die Eulersche Zahl e und die Kreiszahl π sind transzendent. Der Beweis dieser Aussage ist so kompliziert, dass er den Rahmen dieser Vorlesung sprengt.

Für e wurde das erst 1873 von Charles Hermite (1822-1901) und für π im Jahr 1882 von Ferdinand von Lindemann (1852-1939) bewiesen.

Wir wollen nun transzendente Zahlen mit Hilfe einer Verallgemeinerung des Satzes 12.9 finden.

13.5 Satz (Liouville 1809-1882): Eine algebraische Zahl $\alpha \in \mathbb{R}$ vom Grad n ist nicht zu einer Ordnung $> n$ durch rationale Zahlen approximierbar.

Beweis: Für $n = 1$ ist das in 12.9 gezeigt. Sei also $n > 1$ und somit $\alpha \notin \mathbb{Q}$. Sei $f \neq 0$ ein Polynom aus $\mathbb{Q}[X]$ vom Grad n, das α als Nullstelle hat. Indem wir mit dem Hauptnenner der Koeffizienten multiplizieren, dürfen wir annehmen, dass $f \in \mathbb{Z}[X]$. Sei also

$$f = a_n \cdot X^n + \ldots + a_0 \in \mathbb{Z}[X]$$

von minimalem Grad $n > 0$, so dass $f(\alpha) = 0$. Nach 6.5 ist

$$f = (X - \alpha) \cdot g \quad \text{in } \mathbb{R}[X].$$

Angenommen, $g(\alpha) = 0$, dann gibt es ein $h \in \mathbb{R}[X]$, so dass

$$g = (X - \alpha) \cdot h \quad \text{in } \mathbb{R}[X].$$

Aus $f = (X-\alpha)^2 \cdot h$ folgt durch Differenzieren:

$$f' = 2(X-\alpha)\cdot h + (X-\alpha)^2 \cdot h' = (X-\alpha)\cdot(2h + (X-\alpha)\cdot h'),$$

dass $f'(\alpha) = 0$. Da aber $\operatorname{grad} f' = \operatorname{grad} f - 1$, ist das unmöglich.
Da g ein reelles Polynom mit $g(\alpha) \neq 0$, gibt es ein Intervall

$$J = [\alpha - \delta, \alpha + \delta] \quad \text{mit } \delta > 0,$$

so dass $g(x) \neq 0 \ \forall x \in J$ (hier machen wir eine Anleihe aus der Analysis, die Sie aus der Schule oder der Vorlesung "Elemente der Analysis" kennen sollten). Als weitere Anleihe aus der Analysis brauchen wir noch: g ist auf J beschränkt, d.h. es gibt ein $M > 0$ so das

$$|g(x)| < M \quad \forall x \in J$$

Sei nun $\frac{p}{q} \in \mathbb{Q} \cap J$. Dann folgt

$$\left|\alpha - \frac{p}{q}\right| = \left|\frac{f\left(\frac{p}{q}\right)}{g\left(\frac{p}{q}\right)}\right| \overset{(*)}{=} \frac{|a_n \cdot p^n + a_{n-1}\cdot p^{n-1}\cdot q + \ldots + a_n \cdot q^n|}{q^n \cdot |g(\frac{p}{q})|} > \frac{1}{M \cdot q^n}. \tag{A}$$

In $(*)$ erweitern wir mit q^n.
Angenommen, α ist durch rationale Zahlen der Ordnung $n+1$ approximierbar, dann gibt es nach 12.8 ein $C(\alpha) > 0$, so dass für unendlich viele $\frac{p}{q} \in \mathbb{Q} \cap J$ gilt

$$\left|\alpha - \frac{p}{q}\right| < \frac{C(\alpha)}{q^{n+1}}.$$

Wie wir im Beweis von 12.8 gesehen haben, muss es unendlich viele verschiedene solche q geben. Da $q \in \mathbb{N}$, gibt es unendlich viele q mit $q > C(\alpha) \cdot M$. Für $\frac{p}{q}$ mit solchen q gilt nach (A)

$$\frac{1}{M \cdot q^n} < \left|\alpha - \frac{p}{q}\right| < \frac{C(\alpha)}{q^{n+1}} = \frac{1}{q^n} \cdot \frac{C(\alpha)}{q} < \frac{1}{q^n \cdot M},$$

ein Widerspruch. □

13.6 Satz: $\alpha = \frac{1}{10^{1!}} + \frac{1}{10^{2!}} + \frac{1}{10^{3!}} + \ldots = \sum_{k=1}^{\infty} \frac{1}{10^{k!}}$ ist transzendent.

Beweis: Sei $\alpha_n = \frac{p_n}{q_n}$ die Summe der ersten n Summanden. Dann ist $\alpha_n \in \mathbb{Q}$, und es gilt

$$\begin{aligned} 0 < \alpha < \alpha_n = \sum_{k=n+1}^{\infty} \frac{1}{10^{k!}} &= \frac{1}{10^{(n+1)!}} \cdot \left(1 + \frac{1}{10^{n+2}} + \ldots\right) \\ &< \frac{1}{10^{(n+1)!}} \cdot \left(1 + \frac{1}{2} + \frac{1}{4} + \ldots\right) = \frac{2}{10^{(n+1)!}} \end{aligned}$$

Sei $N \in \mathbb{N}$ und $n > N$. Dann gilt

$$10^{(n+1)!} = (10^{n!})^{n+1} = q_n^{n+1} > q_n^{N+1},$$

so dass

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{2}{q_n^{n+1}} < \frac{2}{q_n^{N+1}} \quad \forall n > N.$$

Also ist α von der Ordnung N approximierbar. Da N beliebig ist, kann α nach 13.5 nicht algebraisch sein. □