Ausgewählte Kapitel der elementaren Zahlentheorie

Lukas Pottmeyer

29. Juni 2023

Vorwort

Das Gerüst dieses Skriptes entstand im Laufe meiner Lehramts-Vorlesung *Ausgewählte Kapitel der elementaren Zahlentheorie* an der Universität Duisburg-Essen im WS17/18. Dies ist eine überarbeitete Version für das Wintersemester 20/21. Wer Fehler entdeckt, kann mich gerne per Mail an

lukas.pottmeyer@uni-due.de

darauf hinweisen.

Lukas Pottmeyer

Mathematisches Vokabelheft

Um Zeit und Nerven zu sparen ist es in der Mathematik nötig gewisse Symbole zur Unterstützung heranzuziehen. Verwenden Sie die folgenden Symbole außschließlich in der angegebenen Bedeutung!

Symbol	Bedeutung
$=$	gleich, ist gleich
$\neq$	ungleich, ist ungleich
$\Rightarrow$	daraus folgt, impliziert
$\Leftarrow$	wird impliziert von
$\Leftrightarrow$	ist äquivalent zu
$\in$	ist Element von, ist in
$\notin$	ist kein Element von, ist nicht in
$\subseteq$	ist enthalten in
$\supseteq$	enthält

Dies sind nur einige der wichtigsten Vokabeln. Ergänzen Sie dieses Vokabelheft nach belieben. Weiter benutzen wir folgende Bezeichnungen für die Zahlbereiche.

$\mathbb{N}$	natürliche Zahlen ohne die Null $\{1, 2, 3, \ldots\}$
$\mathbb{N}_0$	natürliche Zahlen mit Null $\{0, 1, 2, 3, \ldots\}$
$\mathbb{Z}$	ganze Zahlen $\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$

Griechische Buchstaben

In der Mathematik wird viel mit Variablen gearbeitet. Dafür reicht unser herkömmliches lateinisches Alphabet oft nicht aus und es werden auch Buchstaben des griechischen Alaphabets benutzt. In dieser Vorlesung werden wir wahrscheinlich nur sehr wenige griechische Buchstaben benutzen. Der Vollständigkeit halber listen wir trotzdem das gesamte griechische Alphabet auf.

A, α	Alpha
B, β	Beta
Γ, γ	Gamma
Δ, δ	Delta
E, ε	Epsilon
Z, ζ	Zeta
H, η	Eta
Θ, θ	Theta
I, ι	Iota
K, κ	Kappa
Λ, λ	Lambda
M, μ	My
N, ν	Ny
Ξ, ξ	Xi
O, o	Omikron
Π, π	Pi
P, ρ	Rho
Σ, σ	Sigma
T, τ	Tau
Y, υ	Ypsilon
Φ, ϕ	Phi
X, χ	Chi
Ψ, ψ	Psi
Ω, ω	Omega

Inhaltsverzeichnis

Das Symbol

deutet an, dass hier eine geeignete Stelle für eine Pause ist. Sie können aber natürlich auch einfach weiter arbeiten.

Kapitel 1

Modulare Arithmetik

1.1 Grundbegriffe

Hier lernen wir die wichtigsten Bezeichnungen für die ganze Vorlesung. Alles was folgt sollte Ihnen bereits bekannt vorkommen. Insbesondere werden Sie mit Sätzen wie

Drei ist ein Teiler von Sechs.
oder
Sechs ist ein Vielfaches von drei.
oder
Acht ist nicht durch drei teilbar.

vertraut sein. Das wollen wir nun formalisieren, da wir auch von Teilbarkeit sprechen wollen, wenn die Zahlen nicht bereits konkret vorgegeben sind. Wir müssen also mit Variablen arbeiten.

Definition 1.1.1. Seien a, b ganze Zahlen (kurz: seien $a, b \in \mathbb{Z}$). Dann heißt a *Teiler* von b, wenn es eine ganze Zahl k gibt, mit $a \cdot k = b$. Ist a ein Teiler von b, so heißt b *Vielfaches* von a.

Notation 1.1.2. Sind $a, b \in \mathbb{Z}$, dann schreiben wir $a \mid b$, wenn a ein Teiler von b ist, und wir schreiben $a \nmid b$, wenn a kein Teiler von b ist. Weiter heißt a *teilt* b nichts anderes als, dass a ein Teiler von b ist.

Beispiel 1.1.3. Es ist $3 \mid 6$, da $3 \cdot 2 = 6$ und 2 offensichtlich eine ganze Zahl ist. Es ist $3 \nmid 8$, da es keine ganze Zahl b gibt, so dass $3 \cdot b = 8$. Das

ist für viele von Ihnen sicher offensichtlich. Lassen Sie mich trotzdem noch zwei Argumente dafür geben:
Erstens: Es ist $3 \cdot 2 = 6 < 8$ und $3 \cdot 3 = 9 > 8$. Da es keine ganze Zahl zwischen 2 und 3 gibt, erhalten wir nie 3·(ganze Zahl)= 8.
Zweitens: Wenn wir $3 \cdot b = 8$ auflösen, erhalten wir $b = \frac{8}{3} = 2 + \frac{2}{3}$. Da $\frac{2}{3}$ keine ganze Zahl ist, ist auch $b = \frac{8}{3}$ keine ganze Zahl.

Dieses zweite Argument liefert uns eine weitere Beschreibung von Teilbarkeit. Diese halten wir in einem Lemma (was nichts anderes als „Hilfssatz“ bedeutet) fest.

Lemma 1.1.4. *Seien $a, b \in \mathbb{Z}$. Dann gilt $a \mid b$ genau dann, wenn der Bruch $\frac{b}{a}$ eine ganze Zahl ist.*

Hier haben wir einen Baustein kennengelernt, der uns noch oft über den Weg laufen wird: Ein *genau dann wenn*. Immer wenn Sie diesen Baustein lesen, werden zwei Aussagen verglichen. In unserem Fall ist die erste Aussage $a \mid b$, und die zweite Aussage $\frac{b}{a} \in \mathbb{Z}$. Das *genau dann wenn* dazwischen sagt uns nun, dass beide Aussagen *äquivalent* sind; d.h. ist die erste Aussage richtig, dann ist es auch die zweite Aussage UND ist die zweite Aussage richtig, dann ist es auch die erste.
Weiter stellen wir fest, dass alles die Null teilt! Denn für beliebiges $a \in \mathbb{Z}$ gilt immer $a \cdot 0 = 0$ und natürlich ist 0 eine ganze Zahl.
Wir sammeln jetzt ein paar weitere Eigenschaften der Teilbarkeit auf den ganzen Zahlen.

Lemma 1.1.5. *Seien $a, b, c \in \mathbb{Z}$ mit $c \neq 0$. Dann gilt:*

(a) $a \mid b \implies a \mid b \cdot c$

(b) $a \mid b$ *und* $a \mid c \implies a \mid b + c$

(c) $a \mid b \iff a \cdot c \mid b \cdot c$

(d) $a \mid b$ *und* $b \mid c \implies a \mid c$

(e) $1 \mid a$, $-1 \mid a$, $a \mid a$ *und* $-a \mid a$

(f) $a \mid c \implies |a| \leq |c|$

(g) $a \mid b$ *und* $b \mid a \iff a = b$ *oder* $a = -b$

BEWEIS. Wir beweisen nur die Aussagen (e)-(g). Die anderen Beweise können Sie als Übung selber machen.

Zu (e): Es ist also a irgendeine ganze Zahl. Dann ist $a \cdot 1 = 1 \cdot a = a$, was $a \mid a$ und $1 \mid a$ beweist. Genauso zeigt die Gleichung $(-1) \cdot (-a) = (-a) \cdot (-1) = a$ die Teilbarkeiten $-1 \mid a$ und $-a \mid a$.

Zu (f): Sei also $a \mid c$. Die Aussage ist, dass dann der Betrag von a kleiner oder gleich dem Betrag von c ist. Nach Voraussetzung ist $c \neq 0$, also ist c tatsächlich ein Vielfaches von a, das verschieden von Null ist. Insbesondere kann $|c|$ damit nicht kleiner als $|a|$ sein.

Zu (g): Hier muss eine Äquivalenz ($\Longleftrightarrow$) gezeigt werden. Wir müssen also zeigen, dass aus der Aussage links, die Aussage rechts folgt und umgekehrt. Wir fangen mal mit der Aussage rechts an.

Dann ist $a = b$ oder $a = -b$. In beiden Fällen haben wir $a \mid b$ und $b \mid a$ (siehe (e)).

Jetzt starten wir links. Sei also $a \mid b$ und $b \mid a$. Damit gibt es $k, k' \in \mathbb{Z}$ so dass $a \cdot k = b$ und $b \cdot k' = a$ ist. Setzen wir die zweite Gleichung in die erste ein, so erhalten wir

$$\underbrace{(b \cdot k')}_{=a} \cdot k = b \quad \Longrightarrow \quad b \cdot (k' \cdot k) = b \Longrightarrow \quad k' \cdot k = 1.$$

Da k und k' ganze Zahlen sind, müssen beide im Betrag kleiner oder gleich 1 sein. Es folgt $k = k' = 1$ oder $k = k' = -1$. Unsere Gleichung mit der wir gestartet sind war $a \cdot k = b$. Da wir nun wissen dass k nur 1 oder -1 sein kann, erhalten wir wie gewünscht $a = b$ oder $a = -b$.

□

Einschub

Wir haben gesehen, dass die folgenden Aussagen und Bezeichnungen alle das Gleiche bedeuten. Wie immer sind a und b ganze Zahlen:

- a teilt b
- a ist ein Teiler von b
- b ist ein Vielfaches von a
- $a \mid b$
- es gibt ein $k \in \mathbb{Z}$ mit $a \cdot k = b$
- der Bruch $\frac{b}{a}$ ist eine ganze Zahl

Als nächstes kommen wir zu Primzahlen. Was sind das für Zahlen? Die meisten würden wahrscheinlich antworten: Zahlen, die nur durch die Eins und durch sich selbst teilbar sind. Das ist aber leider nicht ganz ausreichend, wie das folgende Beispiel zeigt.

Beispiel 1.1.6. (a) Es ist $1 \mid 1$ (na klar!). Die 1 ist auch nicht durch eine Zahl ≥ 2 teilbar. Aber trotzdem ist die 1 *keine* Primzahl!

(b) Die 5 ist eine Primzahl (na klar!). Aber es gilt $1 \mid 5$, $5 \mid 5$ und $-1 \mid 5$, $-5 \mid 5$. Die 5 hat also vier und nicht nur zwei Teiler. Wir müssen also die negativen Zahlen bei der Definition von Primzahlen mitberücksichtigen.

Definition 1.1.7. Eine positive ganze Zahl p heißt *Primzahl*, wenn gilt

(i) $p \neq 1$, und

(ii) die einzigen Teiler von p sind $1, -1, p, -p$.

Wir wollen in dieser Vorlesung auch den Umgang mit der mathematischen Sprache vertiefen. Dazu übersetzen wir die Bedingung (ii) der obigen Definition, mit Hilfe von Symbolen:

$$\underbrace{a \mid p}_{a \text{ teilt } p} \quad \underbrace{\Longrightarrow}_{\text{dann folgt}} \quad \underbrace{a \in}_{a \text{ ist in}} \{1, -1, p, -p\}.$$

Die geschweiften Klammern begrenzen eine *Menge*. D.h. $\{1, -1, p, -p\}$ ist der Zusammenschluss von genau den Elementen $1, -1, p, -p$. Schauen wir uns den Ausdruck also nochmal in Ruhe an, so sagt er uns:
Wenn a ein Teiler von p ist *dann folgt*, dass a eines der Elemente $1, -1, p, -p$ sein muss. Das bedeutet natürlich nichts anderes als die Aussage (ii) in der Definition von Primzahlen.

Das besondere an den Primzahlen ist, dass sich aus ihnen alle anderen Zahlen zusammensetzen lassen.

Theorem 1.1.8 (Fundamentalsatz der Arithmetik)**.** *Jedes $n \in \mathbb{Z}\backslash\{-1, 0, 1\}$ lässt sich eindeutig schreiben als*

$$n = \pm p_1^{e_1} \cdot \ldots \cdot p_r^{e_r},$$

mit Primzahlen $p_1 < p_2 < \ldots < p_r$ und natürlichen Zahlen $e_1, \ldots, e_r$.

Hier kam schon wieder ein neues mathematisches Symbol vor. Der Ausdruck $\mathbb{Z} \setminus \{-1, 0, 1\}$ bedeutet nichts anderes als *alle ganzen Zahlen OHNE* $-1, 0, 1$. Da sich jede Zahl als Produkt von Primzahlen schreiben lässt, können wir die Primzahlen als die Atome der Welt der ganzen Zahlen betrachten. Der Beweis dieses Theorems wurde bereits in der Arithmetik geführt.

Beispiel 1.1.9. Die ersten paar Primzahlen sind 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, ...
Die Zahl 134901248 ist keine Primzahl. Da diese Zahl mit der Ziffer 8 endet, ist es eine gerade Zahl und daher durch 2 teilbar. Und 2 ist nicht in der Menge $\{1, -1, 134901248, -134901248\}$.

Der letzte Teil des Beispiels enthält eine unscheinbare Bemerkung (die mir sicher alle geglaubt haben), die wir genauer herausarbeiten wollen.

Definition 1.1.10. Eine ganze Zahl heißt *gerade* genau dann, wenn sie durch 2 teilbar ist. Ist eine Zahl nicht durch 2 teilbar, dann heißt sie *ungerade*.

Bemerkung 1.1.11. Mit unserem Wissen über Teilbarkeit können wir nun sofort sagen, dass alle geraden Zahlen von der Form $2 \cdot k$ für ein $k \in \mathbb{Z}$ sind. Wenn wir die Zahlengerade betrachten, dann ist jede zweite Zahl gerade. Die ungerade Zahlen sind nun genau die Nachbarn der geraden Zahlen. Jede ungerade Zahl ist somit von der Form $2 \cdot k + 1$ für ein $k \in \mathbb{Z}$.

Wir erhalten die folgenden Rechenregeln für gerade und ungerade Zahlen.

Lemma 1.1.12. *Es gilt*

(a) Das Produkt von einer geraden Zahl mit irgendeiner anderen ganzen Zahl ist gerade.

(b) Das Produkt von zwei ungeraden Zahlen ist ungerade.

(c) Die Summe von zwei geraden Zahlen ist gerade.

(d) Die Summe von zwei ungeraden Zahlen ist gerade.

(e) Die Summe einer geraden und einer ungeraden Zahl ist ungerade.

Beweis. Wir beweisen nur die ersten zwei Aussagen und benutzen dabei natürlich Bemerkung 1.1.11.

Zu (a): Sei g eine gerade Zahl und sei $a \in \mathbb{Z}$ beliebig. Da g gerade ist, gibt es ein $k \in \mathbb{Z}$ mit $g = 2 \cdot k$. Nun ist

$$g \cdot a = (2 \cdot k) \cdot a = 2 \cdot \underbrace{(k \cdot a)}_{\in \mathbb{Z}}$$

wieder gerade. Das wollten wir zeigen.

Zu (b): Seien u und u' ungerade Zahlen. Dann gibt es $k, k' \in \mathbb{Z}$, mit $u = 2 \cdot k + 1$ und $u' = 2 \cdot k' + 1$. Damit ist nun

$$\begin{aligned} u \cdot u' &= (2 \cdot k + 1) \cdot (2 \cdot k' + 1) = 4 \cdot (k \cdot k') + 2 \cdot k + 2 \cdot k' + 1 \\ &= 2 \cdot \underbrace{(2 \cdot k \cdot k' + k + k')}_{\in \mathbb{Z}} + 1 \end{aligned}$$

eine ungerade Zahl.

Die restlichen Aussagen beweist man ganz genau so. □

Einschub

Wir schreiben Lemma 1.1.12 nochmal etwas lapidar auf. Dazu kürzen wir *gerade* mit g ab, und entsprechend *ungerade* mit u. Dann haben wir

- $g \cdot g = g$
- $u \cdot u = u$
- $g \cdot u = u \cdot g = g$
- $g + g = g$
- $u + u = g$
- $g + u = u + g = u$

Wir haben also Rechenregeln für *Eigenschaften von Zahlen* – nämlich g und u.

Beispiel 1.1.13. Diese einfache Unterscheidung zwischen geraden und ungeraden Zahlen können wir nun benutzen um Fragen zu beantworten, die auf den erten Blick viel schwieriger aussehen. Z.B.:

$$\text{Gibt es eine ganze Zahl } x \text{ mit } 3x^{17} + 7x^8 + 1 = 0? \tag{1.1}$$

Wir unterscheiden wieder nur zwischen geraden und ungeraden Zahlen. Die Koeffizienten 3, 7 und 1 sind alle ungerade. Ist nun x irgendeine gerade Zahl, so ist auch $x^{\text{irgendwas}}$ eine gerade Zahl. Die linke Seite der Gleichung aus (1.1) ergibt dann

$$u \cdot g + u \cdot g + u = g + g + u = g + u = u,$$

also eine ungerade Zahl. Ist x irgendeine ungerade Zahl, so ist auch $x^{\text{irgendwas}}$ eine ungerade Zahl und die linke Seite der Gleichung aus (1.1) ergibt

$$u \cdot u + u \cdot u + u = u + u + u = g + u = u,$$

also schon wieder eine ungerade Zahl. Es ist also ganz egal welches x wir in $3x^{17} + 7x^8 + 1$ einsetzen, wir erhalten *immer* eine ungerade Zahl. Da die Null, aber eine gerade Zahl ist, können wir schließen, dass $3x^{17} + 7x^8 + 1$ *nie* gleich Null ist. Die Antwort auf die Frage lautet also: Nein!

1.2 Euklidischer Algorithmus

Auch dieser Abschnitt dient im wesentlichen zur Wiederholung eines wichtigen Verfahrens aus der Artihmetik-Vorlesung.

Abbildung 1.1: Das Buch *die Elemente* von Euklid aus dem 3. Jahrhundert v.C. ist ohne Zweifel eine der bedeutendsten Schriften der Weltliteratur. Bis ins 19. Jahrhundert war es nach der Bibel das meist verbreitete Buch weltweit. Noch im 20. Jahrhundert war es ein gängiges Schulbuch für Mathematik.

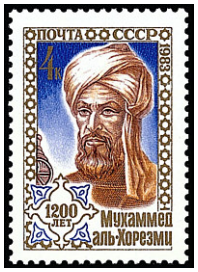


Abbildung 1.2: Um das Jahr 825 verfasste der persische Gelehrte *Abū Ǧa'far Muḥammad b. Mūsā al-Ḫwārazmī* das Lehrbuch *Al-Kitāb al-muḫtaṣar fī ḥisāb al-ǧabr wa-'l-muqābala* (etwa: Das kurzgefasste Buch über die Rechenverfahren durch Ergänzen und Ausgleichen). Dieses Buch präsentiert allgemeine Verfahren zum Lösen von linearen und quadratischen Gleichungen in den positiven reellen Zahlen. Die Wörter *Algebra* und *Algorithmus* leiten sich vom Wort *al-ǧabr* und dem Namen *al-Ḫwārazmī* ab.

Definition 1.2.1. Seien $a, b \in \mathbb{Z}$, mit $b \neq 0$ oder $a \neq 0$. Der *größte gemeinsame Teiler von a und b* ist die größte natürliche Zahl $\mathrm{ggT}(a, b)$ mit $\mathrm{ggT}(a, b) \mid a$ und $\mathrm{ggT}(a, b) \mid b$. Ein $d \in \mathbb{Z}$ mit $d \mid a$ und $d \mid b$ heißt *gemeinsamer Teiler von a und b.*

Beispiel 1.2.2. (a) Es ist $\mathrm{ggT}(68, 68) = 68$, da wir nur nach dem größten Teiler von 68 suchen müssen. Genauso ist $\mathrm{ggT}(a, a) = a$ für jedes $a \in \mathbb{N}$.

(b) Es ist $\mathrm{ggT}(68, 2) = 2$. Der $\mathrm{ggT}(68, 2)$ ist insbesondere ein positiver Teiler der 2. Also kommt nur 1 oder 2 in Frage. Da aber $2 \mid 68$ gilt, ist tatsächlich $2 = \mathrm{ggT}(68, 2)$.

(c) Es ist $\mathrm{ggT}(68, 0) = 68$. Jede Zahl teilt die Null. Also müssen wir wie in (a) nur den größten Teiler von 68 angeben. Dieses Argument liefert auch wieder allgemeiner, dass $\mathrm{ggT}(a, 0) = a$ für alle $a \in \mathbb{N}$ ist.

Euklidischer Algorithmus 1.2.3. Seien $a, b \in \mathbb{N}$, mit $b \neq 0$. Division mit Rest liefert $q, r \in \mathbb{N}_0$ mit $r < b$, so dass $a = qb + r$ gilt. Ist d ein gemeinsamer Teiler von a und b, so gilt mit Lemma 1.1.5 auch $d \mid a - qb = r$. Damit ist d auch ein gemeinsamer Teiler von b und r. Ist umgekehrt d ein gemeinsamer Teiler von b und r, so gilt mit dem gleichen Argument auch

$d \mid qb+r = a$. Damit ist d auch ein gemeinsamer Teiler von a und b. Da somit die gemeinsamen Teiler von a und b ganz genau die gemeinsamen Teilern von b und r sind, gilt insbesondere $\mathrm{ggT}(a,b) = \mathrm{ggT}(b,r)$ und $r < b$.
Wiederholen wir diese Argumentation und schreiben $b = q_1 r + r_1$ mit $r_1 < r$ so gilt $\mathrm{ggT}(a,b) = \mathrm{ggT}(b,r) = \mathrm{ggT}(r,r_1)$. Auf diese Art werden die Reste $r_1, r_2, \ldots$ immer kleiner und somit muss ein $r_i = 0$ sein. Dann ist

$$\mathrm{ggT}(a,b) = \mathrm{ggT}(b,r) = \mathrm{ggT}(r,r_1) = \mathrm{ggT}(r_1,r_2) = \mathrm{ggT}(r_{i-1},0) = r_{i-1}.$$

Beispiel 1.2.4. Wir wollen $\mathrm{ggT}(748,528)$ berechnen.

$$\begin{aligned}
&\text{I} && 748 = 1 \cdot 528 + 220 \\
&\text{II} && 528 = 2 \cdot 220 + 88 \\
&\text{III} && 220 = 2 \cdot 88 + 44 \\
&\text{IV} && 88 = 2 \cdot 44 + 0 \quad \Longrightarrow \ \mathrm{ggT}(748,528) = 44
\end{aligned}$$

Betrachten wir die Gleichungen nun von unten nach oben, so erhalten wir

$$\begin{aligned}
44 &\overset{\text{III}}{=} 220 - 2 \cdot 88 \overset{\text{II}}{=} 220 - 2 \cdot (528 - 2 \cdot 220) = 5 \cdot 220 + (-2) \cdot 528 \\
&\overset{\text{I}}{=} 5 \cdot (748 - 1 \cdot 528) - 2 \cdot 528 = 5 \cdot 748 - 7 \cdot 528
\end{aligned}$$

Dieses *Rückwärtsrechnen* des Euklidischen Algorithmus funktioniert immer. Damit erhalten wir die folgende unscheinbare, aber extrem nützliche Aussage.

Satz 1.2.5. *Seien $a, b \in \mathbb{N}$, dann existieren $x, y \in \mathbb{Z}$ mit* $\mathrm{ggT}(a,b) = x \cdot a + y \cdot b$.

Beispiel 1.2.6. Gibt es $x, y \in \mathbb{Z}$ mit $8 = 68x + 152y$?
Wir ignorieren zunächst die linke Seite und berechnen wie eben den ggT.

$$\begin{aligned}
&\text{I} && 152 = 2 \cdot 68 + 16 \\
&\text{II} && 68 = 4 \cdot 16 + 4 \\
&\text{II} && 16 = 4 \cdot 4 + 0 \quad \Longrightarrow \ \mathrm{ggT}(68,152) = 4
\end{aligned}$$

Rückwärtsrechnen liefert

$$4 \overset{\text{II}}{=} 68 - 4 \cdot 16 \overset{\text{I}}{=} 68 - 4 \cdot (152 - 2 \cdot 68) = 9 \cdot 68 - 4 \cdot 152.$$

Das ist noch nicht ganz das was wir gerne hätten. Multiplizieren wir aber beide Seiten der letzten Gleichung mit 2 so erhalten wir

$$8 = (2 \cdot 9) \cdot 68 - (2 \cdot 4) \cdot 152 = \underbrace{18}_{=x} \cdot 68 + \underbrace{(-8)}_{=y} \cdot 152.$$

Damit haben wir eine Lösung der Ausgangsgleichung gefunden.

Abbildung 1.3: Das Lemma von Bézout ist nach dem französischen Mathematiker *Étienne Bézout* (1730–1783) benannt, der allerdings nicht der erste war, der dieses Resultat kannte. Neben seiner Forschung schrieb Bézou auch einige sehr populäre mathematische Lehrbücher für Studierende anderer Fachrichtungen.

Satz 1.2.7 (Lemma von Bézout)**.** *Seien $a, b, c \in \mathbb{N}$. Dann ist die Gleichung $c = ax + by$ lösbar mit $x, y \in \mathbb{Z}$ genau dann wenn $\text{ggT}(a, b) \mid c$ gilt.*

Beweis. Wie bei jeder „genau-dann-wenn“-Aussage müssen wir zwei Implikationen beweisen.

$\Rightarrow$ Sei also $c = ax+by$ mit $x, y \in \mathbb{Z}$. Per Definition ist $\text{ggT}(a, b)$ sowohl ein Teiler von a als auch von b. Damit gilt aber natürlich auch $\text{ggT}(a, b) \mid ax$ und $\text{ggT}(a, b) \mid by$. Es folg sofort $\text{ggT}(a, b) \mid ax + by = c$. Das mussten wir zeigen.

$\Leftarrow$ Sei nun $\text{ggT}(a, b) \mid c$. Nach Satz 1.2.5 existieren $x', y' \in \mathbb{Z}$ mit $\text{ggT}(a, b) = ax' + by'$. Nach Voraussetzung existiert ein $d \in \mathbb{Z}$ mit $\text{ggT}(a, b) \cdot d = c$. Es folgt

$$c = d \cdot \text{ggT}(a, b) = d(ax' + by') = a(dx') + b(dy').$$

Setzen wir nun $x = dx'$ und $y = dy'$ (beides sind ganze Zahlen), so erhalten wir $c = ax+by$. Damit ist auch die zweite Implikation gezeigt.

□

Korollar 1.2.8. *Seien $a, b \in \mathbb{N}$ mit $\text{ggT}(a, b) = 1$. Für $n \in \mathbb{Z}$ gilt genau dann $ab \mid n$, wenn $a \mid n$ und $b \mid n$ gilt.*

Beweis. Wieder sind zwei Richtungen zu beweisen.

$\Rightarrow$ Offensichtlich ist $a \mid ab$ und $b \mid ab$. Damit folgt aus $ab \mid n$ unmittelbar $a \mid n$ und $b \mid n$. (Für diese Implikation brauchen wir also keine Voraussetzung an $\mathrm{ggT}(a, b)$.)

$\Leftarrow$ Sei nun $a \mid n$ und $b \mid n$. Da $\mathrm{ggT}(a, b) = 1$ ist, existieren $x, y \in \mathbb{Z}$ mit $1 = ax + by$. Multiplizieren wir beide Seiten der Gleichung mit n, so erhalten wir

$$n = anx + bny.$$

Aus $b \mid n$ folgt $b \mid nx$ und somit $ab \mid anx$. Genauso folgt aus $a \mid n$ auch $ab \mid bny$. Zusammen ergibt dies $ab \mid anx + bny = n$.

□

Bemerkung 1.2.9. Die letzte Aussage ist falsch, wenn wir nicht $\mathrm{ggT}(a, b) = 1$ voraussetzen. Denn offensichtlich ist $6 \mid 12$ und $4 \mid 12$, aber $4 \cdot 6 = 24 \nmid 12$.

Noch eine kurze Definition, die Sie alle bereits kennen:

Definition 1.2.10. Zwei ganze Zahlen a und b heißen *teilerfremd* wenn $\mathrm{ggT}(a, b) = 1$ ist.

Einschub

Auch wenn wir es nicht explizit in der Vorlesung verwenden, sollten wir noch eine weitere Bezeichnung erwähnen, die eng mit dem ggT verbunden ist: das *kleinste gemeinsame Vielfache*. Seien wieder $n, k \in \mathbb{N}$ beliebig. Das kleinste gemeinsame Vielfache von n und k bezeichnen wir mit $\mathrm{kgV}(n,k) \in \mathbb{N}$. Wie der Name schon sagt, ist es die Zahl mit den folgenden Eigenschaften

- $n \mid \mathrm{kgV}(n,k)$ und $k \mid \mathrm{kgV}(n,k)$ (d.h. $\mathrm{kgV}(n,k)$ ist ein Vielfaches von n und k), und
- falls $c \in \mathbb{N}$ ein Vielfaches von n und k ist, dann ist $c \geq \mathrm{kgV}(n,k)$ (d.h. es gibt kein kleineres gemeinsames Vielfaches von n und k in $\mathbb{N}$).

Es gilt die schöne Formel $\mathrm{kgV}(n,k) = \frac{n \cdot k}{\mathrm{ggT}(n,k)}$. Da wir wissen, wie man sehr schnell den ggT berechnen kann, wissen wir nun auch, wie man ganz schnell das kgV berechnen kann. Auf den Beweis der Formel verzichten wir; machen Sie sich aber unbedingt klar, dass $\frac{n \cdot k}{\mathrm{ggT}(n,k)}$ tatsächlich ein Vielfaches von n und k ist.

1.3 Kongruenzen

Wir haben bereits bei der Unterscheidung zwischen *gerade* und *ungerade* mit Eigenschaften von Zahlen gerechnet. Das kennen Sie natürlich auch aus Ihrem Alltag. Denn Sie alle wissen, wie viel Uhr es in genau 28 Stunden ist – Sie müssen nur vier Stunden nach vorne rechnen. Genauso wissen Sie welcher Wochentag in genau 23 Tagen ist – der gleiche wie übermorgen.
Für die Uhrzeit wiederholt sich alles nach 24 Stunden. Von Zahlen, die größer sind als 24 können wir also nach und nach 24 abziehen, bis wir irgendwo zwischen 0 und 23 landen. Zum rechnen mit den Stunden genügen also völlig die Zahlen $0, 1, \ldots, 23$. Die 24 ist mit der 0 gleichzusetzen. Das können Sie

sich vorstellen, als ob wir die Zahlengerade gebogen hätten und die 0 und die 24 zusammengeklebt hätten.
Bei den Wochentagen wiederholt sich alles nach 7 Tagen. Hier sind also nur die Zahlen $0, 1, 2, 3, 4, 5, 6$ nötig, da die 7 das gleiche bedeutet (nicht das gleiche ist!) wie die 0.
Ein noch einfacheres Beispiel haben wir letzte Woche schon kennengelernt. Wenn Sie 1111-mal auf einen Lichtschalter drücken, hat das den gleichen Effekt, als ob Sie nur einmal darauf drücken. Hier verändert also 2-mal drücken den Zustand der Glühbirne nicht. Es wird also die 2 mit der 0 identifiziert und alles was übrig bleibt ist die Unterscheidung zwischen geraden und ungeraden Zahlen!

Beispiel 1.3.1. Wir wollen die Beispiele von oben nun mathematisch betrachten.

- Lichtschalter: Wir schreiben

  $$1111 = 555 \cdot 2 + 1.$$

  Da 2-maliges Drücken des Lichtschalters nichts ändert, ändert auch $555 \cdot 2$-maliges Drücken nichts. Damit entspricht 1111-maliges Drücken des Lichtschalters genau einmaligem Drücken. Die Zahl 555 ist für diese Argumentation vollkommen irrelevant. Alles was wir wissen müssen ist

  $$2 \mid 1111 - 1.$$

  Damit bewirkt 1-mal, 3-mal, 5-mal, 7-mal, ... Drücken, immer das gleiche.

- Wochentage: Um herauszufinden welcher Wochentag in 23 Tagen ist, haben Sie (auch wenn Sie es vermutlich anders aufgeschrieben hätten) folgende Rechnung angestellt:

  $$23 = 3 \cdot 7 + 2.$$

  Da in sieben Tagen der gleiche Wochentag ist wie heute, gilt das auch für den Tag in $3 \cdot 7$ Tagen. Also ist in 23 Tagen der gleiche Wochentag wie in zwei Tagen: Übermorgen. Wieder ist die 3 in dieser Argumentation vollkommen egal. Die entscheidende Aussage ist also

  $$7 \mid 23 - 2.$$

Wieder sehen wir, dass in 2, in 9, in 16, in 23, in 30, ... Tagen immer der gleiche Wochentag wie Übermorgen ist.

- Stunden: Um zu wissen, wie viel Uhr es in 28 Stunden ist, kann man

$$28 = 1 \cdot 24 + 4$$

rechnen. Es ist also dieselbe Uhrzeit wie in 4 Stunden. Alles was dafür nötig ist zu wissen, ist

$$24 \mid 28 - 4.$$

Damit ist in 4 Stunden, in 28 Stunden, in 52 Stunden, ... immer die gleiche Uhrzeit.

Dies motiviert (hoffentlich) die folgende Definition.

Definition 1.3.2. Sei $n \in \mathbb{N}$. Zwei Zahlen $a, b \in \mathbb{Z}$ heißen *kongruent modulo* n, falls $n \mid a - b$ gilt. Wir benutzen dafür die Notation $a \equiv b \mod n$.
Die Menge $[a]_n = \{b \in \mathbb{Z} | b \equiv a \mod n\}$ heißt *Restklasse von a modulo n*.
Die Menge aller Restklassen modulo n bezeichnen wir mit $\mathbb{Z}/n\mathbb{Z}$.

Bemerkung 1.3.3. (a) Falls n aus dem Zusammenhang klar ist schreiben wir oft $[a]$ anstatt $[a]_n$.

(b) Ist $a \equiv b \mod n$, so ist auch $b \equiv a \mod n$.

(c) Es ist immer $a \equiv a \mod n$, und $n \equiv 0 \mod n$. Denn $n \mid a - a = 0$ ist korrekt für jedes $n \in \mathbb{N}$, und $n \mid n - 0$ ebenfalls.

(d) Es ist $[a]_n = \{\ldots, a - 2n, a - n, a, a + n, a + 2n, \ldots\}$.

Lemma 1.3.4. *Seien $a, b \in \mathbb{Z}$ und $n \in \mathbb{N}$ beliebig. Dann ist genau dann $a \equiv b \mod n$, wenn $[a]_n = [b]_n$ ist.*

Beweis. Wieder müssen zwei Implikationen gezeigt werden.

$\Rightarrow$ Sei also $a \equiv b \mod n$. Das bedeutet $n \mid a - b$. Wir wählen irgendein Element $c \in [a]_n$ (Beachte, dass $[a]_n$ eine *Menge* von Zahlen ist). Wieder bedeutet das nichts anderes als $n \mid a - c$. Damit gilt aber auch

$$n \mid (a - c) - (a - b) = b - c,$$

was gerade $b \equiv c \mod n$ bedeutet. Es ist also auch $c \in [b]_n$. Wir haben gezeigt, dass jedes Element aus $[a]_n$ auch in $[b]_n$ liegt. Genauso sieht man, dass auch jedes Element aus $[b]_n$ in $[a]_n$ liegt. Die Restklassen $[a]_n$ und $[b]_n$ sind also gleich.

$\Leftarrow$ Diese Richtung ist per Definition schon klar. Wenn $[a]_n = [b]_n$ ist, dann ist insbesondere $b \in [a]_n$, was nichts anderes als $a \equiv b \mod n$ bedeutet.

□

Bemerkung 1.3.5. Es ist $\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots, [n-1]\}$. Denn: Ist $k \in \mathbb{Z}$, so existieren nach Division mit Rest Elemente $q \in \mathbb{Z}$ und $r \in \mathbb{N}_0$ mit $k = q \cdot n + r$ und $r \in \{0, 1, 2, \ldots, n-1\}$. Da $n \mid q \cdot n = k - r$, ist somit $k \equiv r \mod n$ und folglich $[k] = [r] \in \{[0], [1], \ldots, [n-1]\}$.
Insbesondere besteht $\mathbb{Z}/n\mathbb{Z}$ aus genau n verschiedenen Elementen.

Muss ab jetzt jeder Wissen!

Für $a, b \in \mathbb{Z}$ und $n \in \mathbb{N}$ gelten die folgenden Äquivalenzen:

$$\begin{aligned} n \mid a - b &\iff a \equiv b \mod n \\ &\iff \text{es existiert ein } k \in \mathbb{Z} \text{ mit } a = k \cdot n + b \\ &\iff [a]_n = [b]_n \end{aligned}$$

Diesen Kasten können Sie als Vokabelheft auffassen. Hier werden vier Welten miteinander verbunden: Kongruenzen, Restklassen, Teilbarkeit und Division mit Rest. Wir werden sehen, dass mal die eine Welt praktischer ist als die andere, aber was sie festhalten sollten ist, dass sich alles was Sie mit Kongruenzen oder Restklassen ausdrücken können (und möglicherweise auf den ersten Blick kompliziert erscheint) auch nur mit Hilfe von Teilbarkeiten ausdrücken lässt!

Kongruenzen verhalten sich gutartig unter den bekannten Verknüpfungen $+$ und $\cdot$ auf $\mathbb{Z}$.

Proposition 1.3.6. *Sei $n \in \mathbb{N}$ und $a, a', b, b' \in \mathbb{Z}$, mit $a \equiv a' \mod n$ und $b \equiv b' \mod n$. Dann gilt*

(i) $a + b \equiv a' + b' \mod n$ *und*

(ii) $a \cdot b \equiv a' \cdot b' \mod n$.

Beweis. Laut unserer Voraussetzungen existieren $k, l \in \mathbb{Z}$, so dass $a = k \cdot n + a'$ und $b = l \cdot n + b'$ gilt. Wir beweisen nur Teil (i). Teil (ii) können Sie als Übung selbst erledigen.
Es ist $a + b = kn + a' + ln + b' = (k + l)n + a' + b'$. Damit ist $n \mid (k + l)n = (a + b) - (a' + b')$ und es gilt wie geünscht $a + b \equiv a' + b' \mod n$. □

Und was nützt uns das? Nehmen wir irgendein Element a' aus $[a]_n$ und irgendein b' aus $[b]_n$, so gilt $\underbrace{[a' + b']_n = [a + b]_n}_{\Leftrightarrow a+b \equiv a'+b' \mod n}$ und $[a'b']_n = [ab]_n$. Damit sind die folgenden Verknüpfungen sinnvoll definiert (in der Mathematik sagt man auch *wohldefiniert*):

$$[a]_n + [b]_n = [a + b]_n \quad \text{und} \quad [a]_n \cdot [b]_n = [a \cdot b]_n$$

Beispiel 1.3.7.

- Wir rechnen in $\mathbb{Z}/24\mathbb{Z}$. Dort gilt z.B. $[17]+[10] = [27] = [3]$ (denn $24 \mid 27 - 3$) und $[7] \cdot [6] = [42] = [-6] = [18]$.
- Wir wollen $[25^{1234}]_{13}$ berechnen. Zuerst 25^{1234} zu berechnen würde uns sehr lange aufhalten. Mit der letzten Proposition haben wir aber

  $$[25^{1234}]_{13} = [25]_{13}^{1234} = [25 - 2 \cdot 13]_{13}^{1234} = [-1]_{13}^{1234} = [(-1)^{1234}]_{13}.$$

  Nun ist (-1) hoch einer geraden Zahl natürlich gleich 1. Es folgt also $[25^{1234}]_{13} = [1]_{13}$.

  Das Schöne an Proposition 1.3.6 ist daher, dass wir immer mit dem kleinsten Repräsentanten rechnen dürfen. Wenn wir in $\mathbb{Z}/n\mathbb{Z}$ rechnen ist es also nicht nötig mit Zahlen zu rechnen, die viel größer als n sind!

Wir wenden dieses Wissen an um ganz elegant ein paar Teilbarkeitsbedingungen zu beweisen.

Satz 1.3.8. *Eine Zahl $n \in \mathbb{N}$ ist genau dann durch 3 teilbar, wenn ihre Quersumme durch 3 teilbar ist.*

BEWEIS. Wir können n im Dezimalsystem eindeutig schreiben als $n = n_0 + n_1 \cdot 10^1 + n_2 \cdot 10^2 + \ldots + n_k \cdot 10^k$, mit $n_0, \ldots, n_k \in \{0, \ldots, 9\}$. Die Quersumme von n ist dann $n_0 + n_1 + \ldots + n_k$.
Nun ist $10 \equiv 1 \mod 3$ und damit aber auch

$$1 \equiv 1^2 \equiv 10^2 \equiv 10^2 \cdot 1 \equiv 10^3 \equiv \cdots \equiv 10^k \mod 3.$$

Das ist schon alles was wir für den Beweis wissen müssen. Denn nun folgt

$$\begin{aligned} 3 \mid n \quad &\iff \quad 0 \equiv n \equiv n_0 + n_1 \cdot \underbrace{10^1}_{\equiv 1} + n_2 \cdot \underbrace{10^2}_{\equiv 1} + \ldots + n_k \cdot \underbrace{10^k}_{\equiv 1} \mod 3 \\ &\iff \quad 0 \equiv n_0 + \ldots + n_k \mod 3 \\ &\iff \quad 3 \mid n_0 + \ldots + n_k. \end{aligned}$$

Das wollten wir zeigen. □

Was die Quersumme einer Zahl ist, wissen wir alle. Wenn wir ein $n \in \mathbb{N}$ wieder im Dezimalsystem schreiben als $n = n_0 + n_1 \cdot 10^1 + n_2 \cdot 10^2 + \ldots + n_k \cdot 10^k$, mit $n_0, \ldots, n_k \in \{0, \ldots, 9\}$, dann ist die *alternierende Quersumme* die Summe

$$n_0 - n_1 + n_2 - n_3 + n_4 - \ldots + (-1)^k n_k.$$

Das heißt nichts anderes, als dass das Vorzeichen vor jeder Ziffer immer zwischen + und − wechselt. (Sie müssen sich diesen Namen nicht merken, Sie müssen nur die Aussage des nächsten Satzes verstehen!)

Satz 1.3.9. *Eine Zahl $n \in \mathbb{N}$ ist genau dann durch 11 teilbar, wenn ihre alternierende Quersumme durch 11 teilbar ist.*

BEWEIS. Wir schreiben n wieder im Dezimalsystem als $n = n_0 + n_1 \cdot 10^1 + n_2 \cdot 10^2 + \ldots + n_k \cdot 10^k$, mit $n_0, \ldots, n_k \in \{0, \ldots, 9\}$.
Nun ist $10 \equiv -1 \mod 11$, denn $11 \mid 10 - (-1) = 11$. Damit ist $10^\ell \equiv (-1)^\ell \mod 11$ für jedes $\ell \in \mathbb{N}$.
Das ist wieder alles was wir für den Beweis wissen müssen. Denn nun folgt

$$\begin{aligned} 11 \mid n \quad &\iff \quad 0 \equiv n \equiv n_0 + n_1 \cdot \underbrace{10^1}_{\equiv -1} + n_2 \cdot \underbrace{10^2}_{\equiv (-1)^2} + \ldots + n_k \cdot \underbrace{10^k}_{\equiv (-1)^k} \mod 11 \\ &\iff \quad 0 \equiv n_0 - n_1 + n_2 - \ldots + (-1)^k n_k \mod 11 \\ &\iff \quad 11 \mid n_0 - n_1 + n_2 - \ldots + (-1)^k n_k. \end{aligned}$$

Das wollten wir zeigen. □

Beispiel 1.3.10. Die Zahl 13405832 ist somit durch 11 teilbar, denn es ist

$$1 - 3 + 4 - 0 + 5 - 8 + 3 - 2 = 0$$

durch 11 teilbar.

Warnung

In $\mathbb{Z}/n\mathbb{Z}$ können wir zwar sinnvoll rechnen, es gibt aber wesentliche Unterschiede zum Rechnen in $\mathbb{Z}$. In $\mathbb{Z}/24\mathbb{Z}$ gilt zum Beispiel

- $[2] \neq [0]$ und $[12] \neq [0]$, aber $[2] \cdot [12] = [24] = [0]$.
- $[7] \cdot [6] = [42] = [18 + 24] = [18] = [3] \cdot [6]$, aber $[7] \neq [3]$.

Im Allgemeinen darf also in $\mathbb{Z}/n\mathbb{Z}$ nicht gekürzt werden!

Bemerkung 1.3.11. Es gibt in $\mathbb{Z}/24\mathbb{Z}$ kein Element x mit $x \cdot [6] = [1]$, denn sonst wäre

$$[7] = \underbrace{x \cdot [6]}_{=[1]} \cdot [7] = x \cdot [18] = \underbrace{x \cdot [6]}_{=[1]} \cdot [3] = [3],$$

was offensichtlich nicht stimmt. Wir wollen im folgenden klären für welche (und für wie viele) Restklassen $[a] \in \mathbb{Z}/n\mathbb{Z}$ eine Restklasse $[b] \in \mathbb{Z}/n\mathbb{Z}$ existiert, mit $[a] \cdot [b] = [1]$. Das wird uns etwas länger beschäftigen.

Beispiel 1.3.12. In $\mathbb{Z}/6\mathbb{Z}$ gilt:

- $[1] \cdot [1] = [1]$
- $[2] \cdot [1] = [2] \neq [1]$, $[2] \cdot [2] = [4] \neq [1]$, $[2] \cdot [3] = [0] \neq [1]$, $[2] \cdot [4] = [2] \neq [1]$, $[2] \cdot [5] = [4] \neq [1]$
- Genauso wie eben können wir auch durch ausprobieren zeigen, dass $[3] \cdot [a] \neq [1]$ ist für alle $[a] \in \mathbb{Z}/6\mathbb{Z}$.
- Für $[a] \in \mathbb{Z}/6\mathbb{Z}$ beliebig ist $[4] \cdot [a] = [2] \cdot [2a] \neq [1]$.
- $[5] \cdot [5] = [-1] \cdot [-1] = [1]$

Definition 1.3.13. Sei $n \in \mathbb{N}$. Ein Element $[a]$ aus $\mathbb{Z}/n\mathbb{Z}$ heißt *invertierbar*, wenn ein $[b] \in \mathbb{Z}/n\mathbb{Z}$ existiert, so dass $[a] \cdot [b] = [1]$ gilt. Das Element $[b]$ heißt in diesem Fall *(multiplikatives) Inverses* von $[a]$ und wird auch mit $[a]^{-1}$ bezeichnet. Die Menge aller invertierbarer Elemente aus $\mathbb{Z}/n\mathbb{Z}$ bezeichnen wir mit $(\mathbb{Z}/n\mathbb{Z})^*$.

Beispiel 1.3.14. Wie eben gesehen ist $(\mathbb{Z}/6\mathbb{Z})^* = \{[1], [5]\}$.

Bemerkung 1.3.15. (a) Wenn Sie in einem Raum mit anderen Studierenden sind und Sie die Information haben „der mit den blonden Haaren heißt Tom“, wann können Sie dann zweifelsfrei sagen, wer Tom ist? Genau! Wenn es nur eine männliche Person mit blonden Haaren im Raum gibt. Genauso macht auch unsere Namensgebung $[a]^{-1}$ nur Sinn, wenn es tatsächlich nur ein Element $[b]$ in $\mathbb{Z}/n\mathbb{Z}$ gibt mit $[a] \cdot [b] = [1]$.

Das ist aber schnell eingesehen: Angenommen es gäbe zwei solcher Elemente $[a] \cdot [b] = [1]$ und $[a] \cdot [c] = [1]$. Dann ist insbesondere

$$[a] \cdot [b] = [a] \cdot [c].$$

Wir multiplizieren beide Seiten mit $[b]$ und erhalten

$$[b] \cdot [a] \cdot [b] = [b] \cdot [a] \cdot [c].$$

Nun ist aber $[b] \cdot [a] = [b \cdot a] = [a \cdot b] = [a] \cdot [b] = [1]$. Es folgt

$$[b] = [1] \cdot [b] = [1] \cdot [c] = [c].$$

Damit gibt es tatsächlich für jedes invertierbare $[a] \in \mathbb{Z}/n\mathbb{Z}$ genau ein Inverses. Diesem Element können wir jetzt den Namen Tom... ähhh... $[a]^{-1}$ geben.

(b) Gibt es Elemente in $\mathbb{Z}/n\mathbb{Z}$ von denen wir ohne weitere Rechnung immer wissen, dass sie invertierbar sind? Dazu genügt es sich die ganzen Zahlen anzuschauen. Für welche ganzen Zahlen a gibt es eine ganze Zahl b mit $a \cdot b = 1$? Klar! Nur 1 und -1 (denn $1 \cdot 1 = 1 = (-1) \cdot (-1)$). Damit sind auch in $\mathbb{Z}/n\mathbb{Z}$ immer $[1]$ und $[-1] = [n-1]$ invertierbar!

Einschub

Die Rechnung aus Bemerkung 1.3.15(a) zeigt uns noch etwas: Invertierbare Elemente dürfen immer gekürzt werden!

„Kürzen“ = „mit einem Inversen multiplizieren“

Theorem 1.3.16. *Sei $n \in \mathbb{N}$ beliebig. Eine Restklasse $[a] \in \mathbb{Z}/n\mathbb{Z}$ ist genau dann invertierbar, wenn* $\mathrm{ggT}(a, n) = 1$ *gilt.*

Beweis. Wir beweisen wieder die beiden nötigen Implikationen.

$\Rightarrow$ Sei also $[a] \in \mathbb{Z}/n\mathbb{Z}$ invertierbar. Dann existiert per Definition ein $[b] \in \mathbb{Z}/n\mathbb{Z}$ mit $[a] \cdot [b] = [a \cdot b] = [1]$. Das bedeutet (Vokabelheft!), dass ein $k \in \mathbb{Z}$ existiert mit $1 = kn + ab$. Die Gleichung $1 = xn + ya$ ist also lösbar mit $x, y \in \mathbb{Z}$. Damit folgt aus dem Lemma von Bezout 1.2.7 $\mathrm{ggT}(a, n) \mid 1$ – also $\mathrm{ggT}(a, n) = 1$. Das war zu zeigen.

$\Leftarrow$ Sei nun $\mathrm{ggT}(a, n) = 1$. Schon wieder mit dem Lemma von Bézout 1.2.7 existieren $k, b \in \mathbb{Z}$ mit $1 = ab + kn$. Betrachten wir diese Gleichung modulo n, erhalten wir

$$1 \equiv ab + \underbrace{kn}_{\equiv 0} \equiv ab \mod n.$$

Das bedeutet gerade $[1] = [ab] = [a] \cdot [b] \in \mathbb{Z}/n\mathbb{Z}$. Damit ist $[a]$ invertierbar.

□

Der Beweis sagt uns sogar, wie wir ein Inverses (falls es existiert) berechnen können: mit dem Lemma von Bezout!

Beispiel 1.3.17. Was ist das Inverse von $[11] \in \mathbb{Z}/28\mathbb{Z}$? Zunächst sehen wir, dass $[11]$ invertierbar ist, da $\mathrm{ggT}(11, 28) = 1$ ist (11 ist eine Primzahl und $11 \nmid 28$). Wir starten den Euklidischen Algorithmus – einmal vorwärts einmal rückwärts:

vorwärts:

$$\begin{aligned} 28 &= 2 \cdot 11 + 6 \\ 11 &= 1 \cdot 6 + 5 \\ 6 &= 1 \cdot 5 + 1 \\ 5 &= 5 \cdot 1 + 0 \end{aligned}$$

rückwärts:

$$\begin{aligned} 1 &= 6 - 5 = 6 - (11 - 6) = 2 \cdot 6 - 11 \\ &= 2 \cdot (28 - 2 \cdot 11) - 11 \\ &= 2 \cdot 28 - 5 \cdot 11. \end{aligned}$$

Die Gleichung auf der rechten Seite betrachten wir wieder modulo 28 und erhalten $1 \equiv -5 \cdot 11 \mod 28$. Dies bedeutet

$$[1] = [-5] \cdot [11].$$

Damit ist $[11]^{-1} = [-5] = [23]$.

Wie bereits angekündigt wollen wir zählen, wie viele Elemente in $\mathbb{Z}/n\mathbb{Z}$ es gibt, die invertierbar sind. Da $(\mathbb{Z}/n\mathbb{Z})^*$ genau die Menge der invertierbaren Elemente ist, müssen wir also zählen, wie viele Elemente $(\mathbb{Z}/n\mathbb{Z})^*$ enthält. Da diese Zahl eine wichtige Rolle einnimmt, bekommt sie wieder einen Namen.

Definition 1.3.18. Für $n \in \mathbb{N}$ setzen wir $\varphi(n)$ als Anzahl von Elementen in $(\mathbb{Z}/n\mathbb{Z})^*$. Formal bedeutet das $\varphi(n) = |\,(\mathbb{Z}/n\mathbb{Z})^*\,|$. Die Abbildung φ (Phi), die jedes $n \in \mathbb{N}$ auf $\varphi(n)$ abbildet heißt *Eulersche-Phi-Funktion.*

Über Abbildungen werden wir in kürze noch genauer sprechen.

Abbildung 1.4: Der Schweizer *Leonhard Euler* (1707–1783) war einer der begabtesten und produktivsten Mathematiker aller Zeiten. Seine Werke wurden in mehr als 70 Bänden veröffentlicht und enthalten mehr als 800 Resultate. Selbst seine Erblindung 1771 (die er mit den Worten „Nun habe ich weniger Ablenkung“ kommentiert haben soll) beeinträchtigte seine Produktivität nicht. Die meiste Zeit arbeitete er in St. Petersburg.

Bemerkung 1.3.19. Nach Theorem 1.3.16 gilt

$$\varphi(n) = |\{k \in \{0, 1, 2, \ldots, n-1\} : \mathrm{ggT}(k, n) = 1\}|.$$

In Worten: $\varphi(n)$ ist gleich der Anzahl der Elemente zwischen Null und $n-1$, die teilerfremd zu n sind.
Denn: Jedes Element in $\mathbb{Z}/n\mathbb{Z}$ ist von der Form $[k]$ mit $k \in \{0, 1, \ldots, n-1\}$. Ein solches $[k] \in \mathbb{Z}/n\mathbb{Z}$ ist genau dann invertierbar, wenn $\mathrm{ggT}(k, n) = 1$ gilt. Insgesamt ist also $(\mathbb{Z}/n\mathbb{Z})^* = \{[k]_n : k \in \{0, \ldots, n-1\} \text{ und } \mathrm{ggT}(k, n) = 1\}$. Die Behauptung folgt sofort.

Beispiel 1.3.20. Es ist

- $\varphi(6) = |\,(\mathbb{Z}/6\mathbb{Z})^*\,| \overset{1.3.12}{=} |\{[1], [5]\}| = 2$
- $\varphi(8) = |\{k \in \{0, 1, 2, \ldots, 7\} : \mathrm{ggT}(k, 8) = 1\}| = |\{1, 3, 5, 7\}| = 4$
- Wir wollen $\varphi(25)$ berechnen. Wir müssen also wissen, wie viele Elemente aus $\{0, \ldots, 24\}$ teilerfremd zur 25 sind. Wir benutzen einen tollen Trick: Wir zählen die Elemente, die uns eigentlich nicht interessieren. Da die Menge $\{0, \ldots, 24\}$ genau 25 Elemente enthält, sehen wir

$$\varphi(25) = 25 - \begin{array}{l}\text{„Anzahl der Elemente zwischen 0 und 24,}\\ \text{die NICHT teilerfremd zu 25 sind“}\end{array} \tag{1.2}$$

  Aber was sind nun die Elemente, die einen gemeinsamen Teiler (ungleich der 1) mit 25 haben? Die 25 hat nur die positiven Teiler $1, 5, 5^2$. Es ist also jeder positive Teiler von 25 (außer der 1) durch 5 teilbar. Damit sind die Zahlen, die nicht teilerfremd zur 25 sind ganz genau die Vielfachen von 5. Zwischen 0 und 24 sind das genau $0, 5, 10, 15, 20$ – also genau fünf Stück. Es folgt

$$\varphi(25) = 25 - 5 = 20.$$

Aber was ist $\varphi(15000)$? Die Eulersche-φ-Funktion für große Zahlen zu berechnen wird uns noch etwas in Anspruch nehmen.

Genau wie wir gerade $\varphi(25)$ berechnet haben, kann man ganz allgemein die folgende Aussage beweisen.

Proposition 1.3.21. *Sei p eine Primzahl und $k \in \mathbb{N}$. Dann gilt $\varphi(p^k) = p^{k-1} \cdot (p-1)$.*

BEWEIS. Wir wissen schon, dass wir die Elemente aus $\{0, \ldots, p^k - 1\}$ zählen müssen, die teilerfremd zu p^k sind. Genau, wie in (1.2) erhalten wir

$$\varphi(p^k) = p^k - \begin{array}{l}\text{„Anzahl der Elemente zwischen 0 und } p^k - 1,\\ \text{die NICHT teilerfremd zu } p^k \text{ sind“}\end{array} \tag{1.3}$$

Da die positiven Teiler von p^k genau die Zahlen $1, p, p^2, \ldots, p^k$ sind, ist jeder positive Teiler außer der 1 durch p teilbar. Damit sind die Zahlen, die nicht teilerfremd zu p^k sind, ganz genau die Vielfachen von p. Diese sind

$$0 \ , \ p \ , \ 2 \cdot p \ , \ 3 \cdot p \ , \ 4 \cdot p \ , \ \ldots \ , \ (p^{k-1} - 1) \cdot p$$

Hier hören wir auf, da das nächste Vielfache $p^{k-1} \cdot p = p^k$ größer ist als $p^k - 1$. Damit sind die gerade aufgelisteten Zahlen genau die Elemente aus $\{0, \ldots, p^k - 1\}$ die nicht teilerfremd zu p^k sind. Wie viele sind das nun? Klar: p^{k-1}. Dank (1.3) wissen wir daher

$$\varphi(p^k) = p^k - p^{k-1} = p^{k-1} \cdot (p - 1).$$

□

Korollar 1.3.22. *Für jede Primzahl p ist $\varphi(p) = p - 1$. Insbesondere ist $(\mathbb{Z}/p\mathbb{Z})^* = \{[1], [2], \ldots, [p-1]\}$.*

Mit der Eulerschen-Phi-Funktion haben wir hier schon eine Abbildung kennengelernt. Da wir auch noch weiter mit Abbildungen arbeiten werden, nutzen wir die Gelegenheit ein paar bekannte Grundbegriffe zu wiederholen.

Einschub

Eine *Abbildung (oder Funktion)* f zwischen zwei Mengen M und N ordnet jedem Element aus M genau ein Element aus N zu. Wir schreiben dafür

$$f : M \longrightarrow N \quad ; \quad m \mapsto f(m).$$

Eine solche Abbildung f heißt:

- *injektiv*, falls keine zwei verschiedenen Elemente aus M auf das selbe Element aus N abgebildet werden. Formal bedeutet das: $f(m) = f(m') \Longrightarrow m = m'$.
- *surjektiv*, falls es für jedes $n \in N$ mindestens ein $m \in M$ gibt, mit $f(m) = n$.
- *bijektiv*, falls f sowohl injektiv als auch surjektiv ist.

Beispiel 1.3.23. (a) Ordnen wir jeder Person im Moodle-Kurs ihr Geburtsdatum zu, so ist dies eine Abbildung der Menge aller angemeldeten Personen in die Menge der Daten seit dem 01.01.1920. Denn *jede*r* hat *genau ein* Geburtsdatum und niemand von Ihnen ist älter als 100 Jahre. Diese Abbildung ist nicht surjektiv, da niemand von Ihnen am 01.01.1920 geboren wurde. Die Abbildung ist injektiv genau dann wenn keine zwei von Ihnen das gleiche Geburtsdatum haben.[1]

(b) Ist $f : \mathbb{Z}/12\mathbb{Z} \longrightarrow \mathbb{Z}/3\mathbb{Z}$; $[a]_{12} \mapsto [a]_3$ eine Abbildung? Wir müssen überprüfen, ob jedes $[a]_{12}$ auch wirklich nur auf ein einziges Element aus $\mathbb{Z}/3\mathbb{Z}$ abgebildet wird. D.h.: Wir müssen testen ob die folgende Aussage gilt

$$[a]_{12} = [a']_{12} \quad \Longrightarrow \quad \underbrace{f([a]_{12})}_{=[a]_3} = \underbrace{f([a']_{12})}_{=[a']_3}.$$

Aus $[a]_{12} = [a']_{12}$ folgt $12 \mid a - a'$. Da auch $3 \mid 12$ gilt, folgt auch $3 \mid a - a'$ und somit wie gewünscht $f([a]_{12}) = [a]_3 = [a']_3 = f([a']_{12})$. Damit ist f eine Abbildung.

[1] Das berühmte Geburtstagsparadoxon besagt, dass die Wahrscheinlichkeit dafür dass zwei Personen am gleichen Tag Geburtstag feiern (ohne Jahreszahl) bereits ab 23 Personen grösser als 50% ist.

(c) Ist $f : \mathbb{Z}/12\mathbb{Z} \longrightarrow \mathbb{Z}/5\mathbb{Z}$; $[a]_{12} \mapsto [a]_5$ eine Abbildung? Die Antwort ist *Nein!*. Denn es gilt $[1]_{12} = [13]_{12}$, aber $f([1]_{12}) = [1]_5 \neq [3]_5 = [13]_5 = f([13]_{12})$.

Genau wie im Beispiel zeigt man das folgende Lemma.

Lemma 1.3.24. *Es gibt genau dann eine Abbildung* $f : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/k\mathbb{Z}$ *;* $[a]_n \mapsto [a]_k$*, wenn* $k \mid n$ *gilt.*

Bemerkung 1.3.25. Wir haben gesehen, dass $[a]_{12} \mapsto [a]_3$ eine Abbildung beschriebt, $[a]_{12} \mapsto [a]_5$ hingegen nicht. Wir veranschaulichen das, was dabei passiert, in einer ganz anderen Situation: Wir nehmen an, dass jede*r hier im Kurs eine Lieblingsserie hat, über die er/sie sehr gut Bescheid weiß. Nun betrachten wir alle Personen, die die selbe Lieblingsserie haben, als eine *Restklasse* (modulo Serien). Dann ist jede Person in so einer Restklasse ein Repräsentant für die zugehörige Serie. Z.B. könnten wir haben

- Anna, Bahar, Esther und Enes sind Repräsentanten für Game of Thorones
- Frederic und Hatice sind Repräsentanten für Breaking Bad
- Jennifer, Kübra und Lukas sind Repräsentanten für Peaky Blinders

D.h.

- [Anna] = [Bahar] = [Esther] = [Enes]
- [Frederic] = [Hatice]
- [Jennifer] = [Kübra] = [Lukas]

Fragen wir nun jede Person nach der Anzahl der Staffeln ihrer Lieblingsserie, so sagen alle Repräsentanten einer Restklasse das gleiche. Die Zuordnung (Restklasse $\mapsto$ Anzahl der Staffeln) beschreibt daher eine Abbildung, da die Antwort unabhängig davon ist, welchen Repräsentanten der Restklasse wir fragen!
Fragen wir hingegen nach dem Lieblingscharakter der Serie, so werden unterschiedliche Repräsentanten einer Restklasse auch unterschiedlich Antworten! (z.B. könnte Anna mit Jon und Bahar mit Arya antworten.) Es ist also

nicht möglich jeder Restklasse *genau einen* Lieblingscharakter zuzuordnen, da die Antwort immer vom gewählten Representanten abhängt! Damit ist duch die Zuordnung (Restklasse $\mapsto$ Lieblingscharakter) KEINE Abbildung beschrieben!
Das gleiche passiert auch in Beispiel 1.3.23: Egal welchen Repräsentanten aus $[1]_{12}$ wir fragen, was er modulo 3 ergibt, ist die Antwort immer die gleiche: 1. Fragen wir hingegen unterschiedliche Repräsentanten aus $[1]_{12}$ was sie modulo 5 ergeben, so erhalten wir auch unterschiedliche Antworten: 1 antwortet 1 und 13 antwortet 3.
Diesen schönen Vergleich hat Alexander Graf gefunden.

Wir kommen nun langsam zurück zu invertierbaren Elementen. Unser Ziel ist es noch immer die Anzahl von invertierbaren Elementen in $\mathbb{Z}/n\mathbb{Z}$ zu berechnen.

Definition 1.3.26. Für $n, k \in \mathbb{N}$ definieren wir das *kartesische Produkt* von $\mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Z}/k\mathbb{Z}$ als Menge aller geordneter Paare (x, y) mit $x \in \mathbb{Z}/n\mathbb{Z}$ und $y \in \mathbb{Z}/k\mathbb{Z}$. Wir schreiben dafür

$$\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z} = \{([a]_n, [b]_k) | [a]_n \in \mathbb{Z}/n\mathbb{Z} \text{ und } [b]_k \in \mathbb{Z}/k\mathbb{Z}\}.$$

Beispiel 1.3.27. Die Menge $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ besteht genau aus den Elementen

$$\begin{array}{lll} ([0]_2, [0]_3) & ([0]_2, [1]_3) & ([0]_2, [2]_3) \\ ([1]_2, [0]_3) & ([1]_2, [1]_3) & ([1]_2, [2]_3) \end{array}$$

Bemerkung 1.3.28. Es ist klar, dass gilt $|\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z}| = |\mathbb{Z}/n\mathbb{Z}| \cdot |\mathbb{Z}/k\mathbb{Z}| = n \cdot k$. (Beachten Sie z.B. das rechteckige Schema aus dem letzten Beispiel.)

Beispiel 1.3.29. Wir haben in Lemma 1.3.24 gesehen, dass es eine Abbildung

$$f : \mathbb{Z}/12\mathbb{Z} \longrightarrow \mathbb{Z}/3\mathbb{Z} \quad ; \quad [a]_{12} \mapsto [a]_3$$

und eine Abbildung

$$g : \mathbb{Z}/12\mathbb{Z} \longrightarrow \mathbb{Z}/4\mathbb{Z} \quad ; \quad [a]_{12} \mapsto [a]_4$$

Abbildung 1.5: Das kartesiche Produkt ist nach dem französischen Philosophen, Mathematiker und Naturwissenschaftler *René Descartes* (1596–1650; lat: Renatus Cartesius) benannt. Descartes studierte Jura, verbrachte die Zeit nach seinem Examen jedoch mit Reisen auf denen er durch zahlreiche Gespräche den Ruf eines Universalgelehrten erlangte. Sein philosophischer Grundsatz „Ich denke, also bin ich“ ist jedem vertraut.

gibt. Diese Abbildungen können wir zusammensetzen zu einer Abbildung

$$\Psi : \mathbb{Z}/12\mathbb{Z} \longrightarrow \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \quad ; \quad [a]_{12} \mapsto ([a]_3, [a]_4).$$

Dann ist

$$\begin{array}{lll} \Psi([0]_{12}) = ([0]_3, [0]_4) & \Psi([1]_{12}) = ([1]_3, [1]_4) & \Psi([2]_{12}) = ([2]_3, [2]_4) \\ \Psi([3]_{12}) = ([0]_3, [3]_4) & \Psi([4]_{12}) = ([1]_3, [0]_4) & \Psi([5]_{12}) = ([2]_3, [1]_4) \\ \Psi([6]_{12}) = ([0]_3, [2]_4) & \Psi([7]_{12}) = ([1]_3, [3]_4) & \Psi([8]_{12}) = ([2]_3, [0]_4) \\ \Psi([9]_{12}) = ([0]_3, [1]_4) & \Psi([10]_{12}) = ([1]_3, [2]_4) & \Psi([11]_{12}) = ([2]_3, [3]_4) \end{array}$$

Wir stellen fest, dass Ψ bijektiv ist! Das ist kein Zufall, wie wir gleich sehen werden. Weiter sehen wir, dass $[a]_{12}$ invertierbar ist, genau dann wenn $[a]_3$ und $[a]_4$ invertierbar sind. Damit besitzt $(\mathbb{Z}/12\mathbb{Z})^*$ genau so viele Elemente wie es Paare von invertierbaren Elementen aus $\mathbb{Z}/3\mathbb{Z}$ und $\mathbb{Z}/4\mathbb{Z}$ gibt. Es folgt $\varphi(12) = \varphi(3) \cdot \varphi(4) = (3-1) \cdot 2 \cdot (2-1) = 4$. Natürlich ist auch das keine Zufall. Das werden wir später in Satz 1.3.32 allgemein beweisen.

Jetzt kommen wir erst einmal zur Bijektivität der Abbildung.

Theorem 1.3.30 (Chinesischer Restsatz)**.** *Seien $k, n \in \mathbb{N}$ teilerfremd. Dann ist die Abbildung*

$$\Psi : \mathbb{Z}/nk\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z} \quad ; \quad [a]_{nk} \mapsto ([a]_n, [a]_k)$$

bijektiv.

Beweis. Wir zeigen die Injektivität. Sei dazu $\Psi([a]_{nk}) = \Psi([b]_{nk})$. D.h.: $([a]_n, [a]_k) = ([b]_n, [b]_k)$. Dann ist $n \mid (a-b)$, $k \mid (a-b)$ und $\mathrm{ggT}(n,k) = 1$. Es folgt aus Korollar 1.2.8, dass $nk \mid (a-b)$ gilt – also $[a]_{nk} = [b]_{nk}$. Damit ist Ψ injektiv.
Da sowohl $\mathbb{Z}/nk\mathbb{Z}$ als auch $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z}$ genau $n \cdot k$ Elemente besitzen, folgt aus der Injektivität bereits die Bijektivität von Ψ. Denn: Da Ψ injektiv ist, sind alle $n \cdot k$-vielen Elemente $\Psi([a]_{nk}) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z}$ verschieden. Damit

existiert für nk verschiedene Elemente aus $([a]_n, [b]_k) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z}$ (also für alle Elemente) ein Element aus $\mathbb{Z}/nk\mathbb{Z}$ welches von Ψ auf $([a]_n, [b]_k)$ abgebildet wird. □

Abbildung 1.6: Die Schrift *Sunzi Suanjing* wurde wahrscheinlich zwischen dem 3. und 5. Jahrhundert n.C. vom chinesischen Gelehrten Sun-Zi verfasst und enthält im dritten Kapitel die älteste bekannte Version des *chinesischen Restsatzes* (das erklärt den Namen des Satzes).

Beispiel 1.3.31. Wir möchten alle ganzen Zahlen m finden, für die $m \equiv 2 \mod 35$ und $m \equiv 4 \mod 12$ gilt. (Wir suchen also alle $m \in \mathbb{Z}$ mit $([m]_{35}, [m]_{12}) = ([2]_{35}, [4]_{12})$.)

1. Schritt: Bestimme $x, y \in \mathbb{Z}$, mit $1 = 35x + 12y$.

Das machen wir natürlich mit dem Euklidischen Algorithmus und dem Lemma von Bézout:

$$\begin{aligned} 35 &= 2 \cdot 12 + 11 \\ 12 &= 1 \cdot 11 + 1 \\ 11 &= 11 \cdot 1 + 0 \end{aligned}$$

$$\begin{aligned} 1 &= 12 - 11 = 12 - (35 - 2 \cdot 12) \\ &= -1 \cdot 35 + 3 \cdot 12. \end{aligned}$$

2. Schritt: Wir setzen $e = -1 \cdot 35$ und $f = 3 \cdot 12$, und stellen fest

$$\begin{aligned} e &\equiv 0 \mod 35 & e &\equiv 1 \mod 12 \\ f &\equiv 1 \mod 35 & f &\equiv 0 \mod 12. \end{aligned}$$

Es ist klar, dass $e \equiv 0 \mod 35$ und $f \equiv 0 \mod 12$ gilt, da e ein Vielfaches von 35 und f ein Vielfaches von 12 ist. Weiter sind e und f nach dem 1.

Schritt gerade so gewählt, dass $e + f = 1$ gilt. Damit ist insbesondere

$$e \equiv 1 - f \equiv 1 \mod 12 \quad \text{und} \quad f \equiv 1 - e \equiv 1 \mod 35.$$

Für diese beiden Schritte waren die Ausgangswerte 2 und 4 volkommen irrelevant. Die kommen erst jetzt ins Spiel, wenn wir aus unseren Werten e und f eine Lösung der beiden Kongruenzen zusammenpuzzeln.

3. Schritt: Das Element $m = 4 \cdot e + 2 \cdot f = -140 + 72 = -68$ erfüllt $m \equiv 2 \mod 35$ und $m \equiv 4 \mod 12$.

Mit dem 2. Schritt sehen wir

- $m \equiv 4 \cdot e + 2 \cdot f \equiv 4 \cdot 0 + 2 \cdot 1 \equiv 2 \mod 35$ und
- $m \equiv 4 \cdot e + 2 \cdot f \equiv 4 \cdot 1 + 2 \cdot 0 \equiv 4 \mod 12$.

Bis jetzt haben wir eine(!) Lösung der beiden Kongruenzen gefunden. Wir interessieren uns aber für *alle* Lösungen.

4. Schritt: Die Menge $[m]_{12\cdot 35} = [-68]_{420}$ ist die Menge aller Zahlen $\ell \in \mathbb{Z}$ mit $\ell \equiv 2 \mod 35$ und $\ell \equiv 4 \mod 12$.

Nach dem 3. Schritt, wissen wir, dass $m = -68$ die gewünschten Kongruenzen erfüllt. Sei ℓ irgendeine weitere Zahl, die die Kongruenzen erfüllt. Dann gilt $([-68]_{35}, [-68]_{12}) = ([\ell]_{35}, [\ell]_{12})$. Die Abbildung

$$\Psi : \mathbb{Z}/420\mathbb{Z} \longrightarrow \mathbb{Z}/35\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z} \quad ; \quad [a]_{420} \mapsto ([a]_{35}, [a]_{12})$$

ist nach dem Chinesischen Restsatz bijektiv (und damit insbesondere injektiv). Insbesondere folgt aus $\Psi([-68]_{420}) = ([2]_{35}, [4]_{12}) = \Psi([\ell]_{420})$ bereits $[-68]_{420} = [\ell]_{420}$ und somit $\ell \in [-68]_{420}$.

In Beispiel 1.3.29 haben wir festgestellt, dass die Restklasse $[a]_{12}$ genau dann invertierbar ist, wenn sowohl $[a]_3$ als auch $[a]_4$ invertierbar sind. Das zeigen wir nun allgemein.

Satz 1.3.32. *Seien $n, k \in \mathbb{N}$ teilerfremd und $a \in \mathbb{Z}$ beliebig. Dann ist $[a]_{nk}$ genau dann invertierbar, wenn $[a]_n$ und $[a]_k$ invertierbar sind.*

BEWEIS. Nach Theorem 1.3.16 genügt es zu zeigen, dass $\mathrm{ggT}(a, nk) = 1$ genau dann gilt, wenn $\mathrm{ggT}(a, n) = 1$ und $\mathrm{ggT}(a, k) = 1$. Dafür beweisen wir die nötigen Implikationen

$\Rightarrow$ Sei also $\mathrm{ggT}(a, nk) = 1$. Jeder gemeinsame Teiler von a und n, ist auch ein gemeinsamer Teiler von a und nk (da offensichtlich $n \mid nk$ gilt). Da aber nach Voraussetzung a und nk teilerfremd sind, muss dies auch für a und n gelten. Genauso argumentiern wir um auch $\mathrm{ggT}(a, k) = 1$ zu erhalten.

$\Leftarrow$ Sei nun $\mathrm{ggT}(a, n) = 1 = \mathrm{ggT}(a, k)$. Dann existieren nach dem Lemma von Bezout 1.2.7 $x, y, v, w \in \mathbb{Z}$ mit

$$1 = ax + ny \quad \text{und} \quad 1 = av + kw$$

Damit ist auch

$$\begin{aligned} 1 = 1 \cdot 1 &= (ax + ny) \cdot (av + kw) = axav + axkw + nyav + nykw \\ &= a \cdot \underbrace{(xav + xkw + nyv)}_{\in \mathbb{Z}} + (nk) \cdot \underbrace{(yw)}_{\in \mathbb{Z}}. \end{aligned}$$

Wieder mit Satz 1.2.7 folgt $\mathrm{ggT}(a, nk) = 1$. Das war zu zeigen.

□

Damit werden invertierbare Elemente aus $\mathbb{Z}/nk\mathbb{Z}$ durch die Abbildung aus dem Chinesischen Restsatz 1.3.30 genau auf Paare von invertierbaren Elementen aus $\mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Z}/k\mathbb{Z}$ abgebildet. Da die Abbildung bijektiv ist, gibt es damit genau so viele invertierbare Elemente in $\mathbb{Z}/nk\mathbb{Z}$ wie Paare von invertierbaren Elementen aus $\mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Z}/k\mathbb{Z}$. Zusammengefasst erhalten wir:

Korollar 1.3.33. *Sind $n, k \in \mathbb{N}$ teilerfremd, dann gilt $\varphi(nk) = \varphi(n) \cdot \varphi(k)$.*

Beispiel 1.3.34. Was ist nun $\varphi(15000)$? Alle zu 15000 teilerfremden Zahlen aufzulisten wäre sehr sehr aufwendig. Es gilt aber

$$\begin{aligned} \varphi(15000) = \varphi(15 \cdot 1000) &= \varphi(2^3 \cdot 3 \cdot 5^4) \\ &\overset{\mathrm{ggT}(2^3, 3 \cdot 5^4) = 1}{=} \varphi(2^3) \cdot \varphi(3 \cdot 5^4) \overset{\mathrm{ggT}(3, 5^4) = 1}{=} \varphi(2^3) \cdot \varphi(3) \cdot \varphi(5^4) \\ &\overset{1.3.21}{=} 2^2 \cdot (2-1) \cdot (3-1) \cdot 5^3 \cdot (5-1) = 4000 \end{aligned}$$

Bemerkung 1.3.35. Da wir eine Formel für die Eulersche-Phi-Funktion an Primzahlpotenzen p^k haben, ist es damit ganz einfach $\varphi(n)$ zu berechnen, wenn wir die Primfaktorzerlegung von n kennen. Kennen wir die Primfaktorzerlegung nicht, dann ist die Berechnung von $\varphi(n)$ für großes n extrem aufwendig. Diese kleine Feststellung wird für die Verschlüsselungstheorie, die wir im nächsten Kapitel kennenlernen von entscheidender Bedeutung sein.

Wir wollen die Eulersche-Phi-Funktion nun benutzen um weiter das Rechnen auf $\mathbb{Z}/n\mathbb{Z}$ zu lernen. Eine wichtige Sache, die wir bereits kennengelernt haben, ist dass wir bei der Multiplikation und der Addition von Restklassen in $\mathbb{Z}/n\mathbb{Z}$ auf Zahlen, die deutlich größer sind als n verzichten können. Aber was ist, wenn wir hohe Potenzen von Restklassen berechnen wollen? Sagen wir $[2]_{11}^{1000002}$. Können wir dann auch den Exponenten reduzieren, um die Rechnung viel einfacher zu machen? Glücklicherweise lautet die Antwort oft „ja“! Entscheidend dafür ist das folgende Theorem.

Theorem 1.3.36 (Satz von Euler)**.** *Sei $n \in \mathbb{N}$ beliebig und $[a] \in (\mathbb{Z}/n\mathbb{Z})^*$. Dann ist $[a]^{\varphi(n)} = [1]$.*

Den Beweis führen wir etwas weiter unten. Lassen Sie uns kurz überlegen, warum die Voraussetzung $[a] \in (\mathbb{Z}/n\mathbb{Z})^*$ zwingend erforderlich ist: Wenn $[a]^{\varphi(n)} = [1]$ gilt, dann ist das nichts anderes als $[a] \cdot [a]^{\varphi(n)-1} = [1]$. Damit ist $[a]$ invertierbar (und $[a]^{\varphi(n)-1}$ ist das zugehörige Inverse). Damit kann die Gleichung $[a]^{\varphi(n)} = [1]$ tatsächlich nur für invertierbare Elemente, also für $[a] \in (\mathbb{Z}/n\mathbb{Z})^*$ gelten.
Ein Element $[a] \in \mathbb{Z}/n\mathbb{Z}$ ist genau dann in $(\mathbb{Z}/n\mathbb{Z})^*$, wenn $\mathrm{ggT}(a, n) = 1$ ist (siehe Satz 1.3.32). Benutzen wir diese Charakterisierung und unser Vokabelheft, so impliziert der Satz von Euler sofort:

Korollar 1.3.37. *Sei $n \in \mathbb{N}$ und $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, n) = 1$. Dann gilt $a^{\varphi(n)} \equiv 1 \mod n$.*

Beispiel 1.3.38. Wir kommen zurück zur Frage was $[2]^{1000002} \in \mathbb{Z}/11\mathbb{Z}$ ergibt. Wir wissen $\varphi(11) = 11 - 1 = 10$ und $[2] \in (\mathbb{Z}/11\mathbb{Z})^*$, da $\mathrm{ggT}(2, 11) = 1$

ist. Teilen wir den Exponenten 1000002 mit Rest durch 10, so erhalten wir $1000002 = 10 \cdot 100000 + 2$. Somit ist

$$[2]^{1000002} = [2]^{10\cdot 100000+2} = [2]^{10\cdot 100000} \cdot [2]^2 = (\underbrace{[2]^{10}}_{=[1]})^{100000} \cdot [2]^2 = [2]^2 = [4].$$

Korollar 1.3.39 (kleiner Satz von Fermat)**.** *Für eine Primzahl p gilt $a^p \equiv a$ mod p für alle $a \in \mathbb{Z}$.*

Beweis. Übung. □

Abbildung 1.7: *Pierre de Fermat* (1607–1665) war ein französischer Jurist und war dennoch einer der führenden Mathematiker des 17. Jahrhunderts. Daher gilt er auch als *König der Hobby-Mathematiker*. Besondere Bekanntheit erlangte er durch den so genannten großen Satz von Fermat; eine Vermutung zu der er behauptete einen wunderschönen beweis zu kennen, die aber ert 1994 bewiesen werden konnte.

Wir fangen nun an den Beweis vom Satz von Euler vorzubereiten.

Lemma 1.3.40. *Sei $n \in \mathbb{N}$ und $[a] \in (\mathbb{Z}/n\mathbb{Z})^*$ beliebig. Dann gilt*

(a) $[a] \cdot [b] \in (\mathbb{Z}/n\mathbb{Z})^*$ für alle $[b] \in (\mathbb{Z}/n\mathbb{Z})^*$.

(b) Die Abbildung $\tau_{[a]} : (\mathbb{Z}/n\mathbb{Z})^* \longrightarrow (\mathbb{Z}/n\mathbb{Z})^*$; $[b] \mapsto [a] \cdot [b]$ ist bijektiv.

Beweis. Wir beweisen die Aussagen nacheinander.

Zu (a): Seien $[a], [b] \in (\mathbb{Z}/n\mathbb{Z})^*$ und seien $[c], [d] \in \mathbb{Z}/n\mathbb{Z}$ mit $[a] \cdot [c] = [1]$ und $[b] \cdot [d] = [1]$. Dann gilt

$$([a] \cdot [b]) \cdot [cd] = ([a] \cdot [b]) \cdot \underbrace{([c] \cdot [d])}_{\in \mathbb{Z}/n\mathbb{Z}} = ([a] \cdot [c]) \cdot ([b] \cdot [d]) = [1] \cdot [1] = [1].$$

Damit ist wie behauptet $[a] \cdot [b] \in (\mathbb{Z}/n\mathbb{Z})^*$.

Zu (b): Nach Teil (a) ist tatsächlich $\tau_{[a]}([b]) \in (\mathbb{Z}/n\mathbb{Z})^*$. Damit ist $\tau_{[a]}$ sinnvoll definiert. Wir zeigen, dass $\tau_{[a]}$ injektiv ist. Es ist

$$\begin{aligned} \tau_{[a]}([b]) = \tau_{[a]}([c]) \quad &\Longrightarrow \quad [a] \cdot [b] = [a] \cdot [c] \\ &\Longrightarrow \quad \underbrace{[a]^{-1} \cdot [a]}_{=[1]} \cdot [b] = \underbrace{[a]^{-1} \cdot [a]}_{=[1]} \cdot [c] \quad \Longrightarrow \quad [b] = [c]. \end{aligned}$$

Damit ist $\tau_{[a]}$ injektiv. Es ist zu beachten, dass das nur funktioniert da $[a]^{-1}$ nach Voraussetzung existiert!

Wir beweisen noch, dass $\tau_{[a]}$ surjektiv ist. Sei dazu $[b] \in (\mathbb{Z}/n\mathbb{Z})^*$ beliebig. Dann ist auch $[a]^{-1} \cdot [b] \in (\mathbb{Z}/n\mathbb{Z})^*$. Insbesondere ist somit $\tau_{[a]}([a]^{-1} \cdot [b]) = [a] \cdot ([a]^{-1} \cdot [b]) = [b]$. Wir haben gezeigt, dass jedes Element aus $(\mathbb{Z}/n\mathbb{Z})^*$ von $\tau_{[a]}$ getroffen wird. Damit ist $\tau_{[a]}$ auch surjektiv und damit bijektiv.

□

Beweis vom Satz von Euler 1.3.36. Sei $[a] \in (\mathbb{Z}/n\mathbb{Z})^*$ beliebig. Nach Lemma 1.3.40 ist die Abbildung

$$\tau_{[a]} : (\mathbb{Z}/n\mathbb{Z})^* \longrightarrow (\mathbb{Z}/n\mathbb{Z})^* \quad ; \quad [b] \mapsto [a] \cdot [b]$$

bijektiv. Das bedeutet, dass jedes Element aus $(\mathbb{Z}/n\mathbb{Z})^*$ genau einem Element der Form $\tau_{[a]}([b])$ entspricht. Es gilt also

$$(\mathbb{Z}/n\mathbb{Z})^* = \{\tau_{[a]}([b]) \mid [b] \in (\mathbb{Z}/n\mathbb{Z})^*\}$$

und alle Elemente $\tau_{[a]}([b])$, mit $[b] \in (\mathbb{Z}/n\mathbb{Z})^*$, sind verschieden. Damit gilt die folgende Aussage

Das Produkt von allen Elementen aus $(\mathbb{Z}/n\mathbb{Z})^*$ ist das gleiche wie das Produkt von allen Elementen der Form $\tau_{[a]}([b])$, mit $[b] \in (\mathbb{Z}/n\mathbb{Z})^*$.

Dias ist das Kernargument in diesem Beweis. Stellen Sie also sicher, dass Sie es nachvollziehen können.
Wir formulieren diese Aussage nun mathematisch. Dazu sei

$$(\mathbb{Z}/n\mathbb{Z})^* = \{[a_1], [a_2], \ldots, [a_{\varphi(n)}]\}.$$

(Beachten Sie, dass $(\mathbb{Z}/n\mathbb{Z})^*$ per Definition genau $\varphi(n)$ Elemente besitzt.) Dann ist

$$\begin{aligned}[a_1]\cdot[a_2]\cdot\ldots\cdot[a_{\varphi(n)}] &= \tau_{[a]}([a_1])\cdot\tau_{[a]}([a_2])\cdot\ldots\cdot\tau_{[a]}([a_{\varphi(n)}])\\ &= ([a]\cdot[a_1])\cdot\ldots\cdot([a]\cdot[a_{\varphi(n)}])\\ &= [a]^{\varphi(n)}\cdot([a_1]\cdot[a_2]\cdot\ldots\cdot[a_{\varphi(n)}]) \qquad (1.4)\end{aligned}$$

Weiter haben wir in Lemma 1.3.40 gesehen, dass das Produkt von invertierbaren Elementen wieder invertierbar ist. Insbesondere ist $[a_1]\cdot\ldots\cdot[a_{\varphi(n)}]$ invertierbar und es existiert ein $[b]\in\mathbb{Z}/n\mathbb{Z}$ mit $([a_1]\cdot[a_2]\cdot\ldots\cdot[a_{\varphi(n)}])\cdot[b]=[1]$. Multiplizieren wir nun (1.4) mit $[b]$ so erhalten wir

$$[1]=([a_1]\cdot\ldots\cdot[a_{\varphi(n)}])\cdot[b]=[a]^{\varphi(n)}\cdot([a_1]\cdot[a_2]\cdot\ldots\cdot[a_{\varphi(n)}])\cdot[b]=[a]^{\varphi(n)}.$$

Das war zu zeigen. □

Beispiel 1.3.41. Was sind die letzten beiden Ziffern von 3333^{4444}? Benutzen Sie ruhig Ihren Taschenrechner, aber der wird Ihnen nicht viel nützen. Die letzten beiden Ziffern einer natürlichen Zahl a sind stets kongruent zu a modulo 100. Dies sehen wir sofort an einem Beispiel: $12345 \equiv 123\cdot 100 + 45 \equiv 45 \mod 100$. Wir müssen also eine Zahl zwischen 0 und 99 finden, die kongruent zu 3333^{4444} modulo 100 ist.
Da $3333 \equiv 33 \mod 100$ ist, erhalten wir in einem ersten Schritt

$$3333^{4444} \equiv 33^{4444} \mod 100. \qquad (1.5)$$

Leider ist 33^{4444} immer noch viel zu groß. Um den Exponenten zu verkleinern, benutzen wir nun den Satz von Euler. Dazu berechnen wir $\varphi(100) = \varphi(2^2\cdot 5^2) = \varphi(2^2)\cdot\varphi(5^2) = 2\cdot(2-1)\cdot 5\cdot(5-1) = 40$ und $\mathrm{ggT}(33,100)=1$. Es ist also $33^{40}\equiv 1 \mod 100$. Es folgt

$$33^{4444} \equiv 33^{40\cdot 111+4} \equiv (33^{40})^{111}\cdot 33^4 \equiv 33^4 \mod 100 \qquad (1.6)$$

Damit haben wir das Problem beträchtlich vereinfacht, da wir nun nur noch die letzten beiden Ziffern von 33^4 berechnen müssen. Damit hat Ihr Taschenrechner sicher keine Probleme mehr... wir allerdings auch nicht! Wir berechnen einfach

$$\begin{aligned}33^2 &\equiv (30+3)^2 \equiv 900+180+9 \equiv 9\cdot 100+100+80+9 \equiv 89 \mod 100\\ 33^4 &\equiv (33^2)^2 \equiv 89^2 \equiv (-11)^2 \equiv 121 \equiv 21 \mod 100 \qquad (1.7)\end{aligned}$$

Setzen wir nun die Gleichungen (1.5), (1.6) und (1.7) zusammen erhalten wir:

$$3333^{4444} \equiv 33^{4444} \equiv 33^4 \equiv 21 \mod 100.$$

Damit endet die gigantisch große Zahl 3333^{4444} auf die Ziffern 21.

Kapitel 2

Kryptographie

Kryptographie (altgriechisch etwa: *verborgen schreiben*) ist die Theorie von verschlüsselter Kommunikation. Diese hat eine sehr lange Tradition, war aber möglicherweise noch nie so bedeutend wie heute, wo fast jegliche Kommunikation über das Internet erfolgt. Eine große Herausforderung wurde in den 1970er Jahren gemeistert: Geheime Datenübertragung zwischen zwei Partein die sich noch nie getroffen haben und deren gesamte Kommunikation mitgelesen wird. Dies scheint auf den ersten Blick vollkommen unmöglich, wir werden aber ein Verfahren kennenlernen, welches genau das leistet. Dafür benutzen wir die Zahlentheorie, die wir im letzten Kapitel studiert haben.

2.1 Anfänge der Kryptographie

Im folgenden haben wir immer das gleiche Setting: Person 1 (Mia) möchte eine Nachricht an Person 2 (Pia) schicken und Person 3 (Lea) möchte diese Nachricht mitlesen.
Am sichersten ist die Kommunikation natürlich, wenn Lea nicht weiß, dass überhaupt eine Kommunikation stattfindet. Das ist im Allgemeinen aber ziemlich unrealistisch.
Es ist natülich auch möglich Nachrichten zu verstecken (in Bildern, mit Zitronensaft schreiben, ...). Dies wird *Steganographie* genannt und ist nicht Teil der Vorlesung, da wir dieses Verstecken nicht „berechnen“ können.
Die Nachricht, die Mia verschicken möchte nennen wir *Klartext*. Diesen Klartext verändert Mia zu einer *Chiffre*, diesen Vorgang nennen wir *Verschlüsselung*. Pia erhält die Chiffre von Mia und kann daraus den Klartext

wiederherstellen. Diesen Vorgang nennen wir *Entschlüsselung*. Es soll für Pia natürlich sehr einfach sein, die Chiffre zu verschlüsseln. Umgekehrt sollte es für Lea extrem schwierig (idealerweise sogar unmöglich) sein den Klartext aus der Chiffre zu gewinnen.

Caesar-Kryptosystem 2.1.1. Wir identifizieren das Alphabet mit den Elementen aus $\mathbb{Z}/26\mathbb{Z}$. Dies machen wir folgendermaßen.

A entspricht $[1]_{26}$, B entspricht $[2]_{26}$, ..., Y entspricht $[25]_{26}$, Z entspricht $[26]_{26} = [0]_{26}$. Allgemein entspricht also der i-te Buchstabe des Alphabets dem Element $[i]_{26}$.

Nun einigen sich Mia und Pia auf einen geheimen Buchstaben, z.B. auf den Buchstaben E. Dieser Buchstabe ist der *Schlüssel* von Pia und Mia. Mia verschlüsselt ihren Klartext nun indem sie jeden Buchstaben der Nachricht mit dem Element $\text{E}\hat{=}[5]_{26}$ *addiert*. D.h. der Buchstabe A wird durch $\text{A}+\text{E}\hat{=}[1]_{26} + [5]_{26} = [6]_{26}\hat{=}\text{F}$ verschlüsselt, B durch $\text{B}+\text{E}\hat{=}[2]_{26} + [5]_{26} = [7]_{26}\hat{=}\text{G}$, ..., V durch $\text{V}+\text{E}\hat{=}[22]_{26} + [5]_{26} = [27]_{26} = [1]_{26}\hat{=}\text{A}$, ..., Z durch $\text{Z}+\text{E}\hat{=}[26]_{26} + [5]_{26} = [5]_{26}\hat{=}\text{E}$. Dies entspricht einer Verschiebung des Alphabets um 5 Stellen. Möchte sie nun (aus welchen gründen auch immer) das Wort „Pampelmuse“ an Pia schicken, so rechnet sie

Schlüssel:	E	E	E	E	E	E	E	E	E	E
Klartext:	P	A	M	P	E	L	M	U	S	E
Chiffre:	U	F	R	U	J	Q	R	Z	X	J

Die Chiffre lautet also UFRUJQRZXJ. Wenn Lea diese Chiffre abfängt, aber nicht weiß mit welchem Buchstaben sie verschlüsselt wurde, hat sie ein bisschen was zu tun um die Nachricht zu lesen. Pia hingegen kennt den Schlüssel E und kann die Nachricht entschlüsseln in dem sie von jedem Buchstaben der Chiffre das Element $\text{E}\hat{=}[5]_{26}$ abzieht. D.h.:

$$
\begin{array}{lrcl}
\text{U-E} & \hat{=}[21]_{26} - [5]_{26} = [16]_{26}\hat{=} & & \text{P} \\
\text{F-E} & \hat{=}[6]_{26} - [5]_{26} = [1]_{26}\hat{=} & & \text{A} \\
\text{R-E} & \hat{=}[18]_{26} - [5]_{26} = [13]_{26}\hat{=} & & \text{M} \\
\text{U-E} & \hat{=}[21]_{26} - [5]_{26} = [16]_{26}\hat{=} & & \text{P} \\
\text{J-E} & \hat{=}[10]_{26} - [5]_{26} = [5]_{26}\hat{=} & & \text{E} \\
\text{Q-E} & \hat{=}[17]_{26} - [5]_{26} = [12]_{26}\hat{=} & & \text{L} \\
\text{R-E} & \hat{=}[18]_{26} - [5]_{26} = [13]_{26}\hat{=} & & \text{M} \\
\text{Z-E} & \hat{=}[26]_{26} - [5]_{26} = [21]_{26}\hat{=} & & \text{U} \\
\text{X-E} & \hat{=}[24]_{26} - [5]_{26} = [19]_{26}\hat{=} & & \text{S} \\
\text{J-E} & \hat{=}[10]_{26} - [5]_{26} = [5]_{26}\hat{=} & & \text{E}
\end{array}
$$

Damit kennt Pia den Klartext PAMPELMUSE.

Abbildung 2.1: Das obige Kryptosytem ist tatsächlich nach dem Feldherren *Gaius Julius Caesar* (100v.Chr.–44v.Chr.) benannt. Er soll diese Art der Verschlüsselung mit dem Schlüssel C, also einer Verschiebung des Alphabets um 3 Buchstaben, für seine militärische Korrespondenz genutzt haben.

Die Vorteile dieses Verfahrens sind, dass der Schlüßel fast keinen Speicherplatz benötigt; bzw. leicht zu merken ist. Auch ist die Ver- und Entschlüsselung sehr einfach und dadurch auch sehr schnell. Allerdings ist das Verfahren sehr unsicher. Denn:

- es gibt pro Chiffre nur 26 mögliche Klartexte, die man im Zweifel alle ausprobieren kann.
- ist ein einziger Buchstabe richtig entschlüsselt, so kennt man sofort den Schlüssel (und kann damit die ganze Nachricht entschlüsseln).
- Bei etwas längeren Texten oder mehreren kurzen Texten, ist der mit Abstand häufigste Buchstabe ein E, der etwa 17,4% aller Buchstaben in einem deutschen Text ausmacht (der nächst häufigste ist das N mit einem Anteil von etwa 9,78%). Damit wird der hüfigste Buchstabe der Chiffre höchst wahrscheinlich das E repräsentieren. Damit gilt *fast* immer

$$\text{Schlüssel} = \text{„häufigster Buchstabe der Chiffre“ - E}$$

Natürlich identifizieren wir bei dieser Rechnung wieder die Buchstaben mit den Elementen aus $\mathbb{Z}/26\mathbb{Z}$.

Das Verfahren wird deutlich sicherer, wenn wir nicht nur einen sondern mehrere Buchstaben als Schlüssel verwenden.

Vigenère-Kryptosystem 2.1.2. Wieder wird das Alphabet mit den Elementen aus $\mathbb{Z}/26\mathbb{Z}$ identifiziert. Nun einigen sich Pia und Mia auf den Schlüssel KRYP. Mia verschlüsselt ihren Klartext in dem sie den ersten Buchstaben mit K addiert, den zweiten mit R, den dritten mit Y und den vierten mit P. Dann fängt sie wieder von vorne an und verschlüsselt den fünften Buchstaben mit K, ...

Schlüssel:	K	R	Y	P	K	R	Y	P	K	R
Klartext:	P	A	M	P	E	L	M	U	S	E
Chiffre:	A	S	L	F	P	D	L	K	D	W

Liest Lea die Chiffre ASLFPDLKDW, hat sie *fast* keine Chance daraus den Klartext abzuleiten. Pia hingegen kennt den Schlüssel KRYP. Daher weiß sie:

$$\text{Klartext} = \text{Chiffre - KRYPKRYPKR}$$

$$\begin{array}{lcl}
\text{A-K} & \hat{=}[1]_{26} - [11]_{26} = [-10]_{26} = [16]_{26}\hat{=} & \text{P} \\
\text{S-R} & \hat{=}[19]_{26} - [18]_{26} = [1]_{26}\hat{=} & \text{A} \\
\text{L-Y} & \hat{=}[12]_{26} - [25]_{26} = [-13]_{26} = [13]_{26}\hat{=} & \text{M} \\
\text{F-P} & \hat{=}[6]_{26} - [16]_{26} = [-10]_{26} = [16]_{26}\hat{=} & \text{P} \\
\text{P-K} & \hat{=}[16]_{26} - [11]_{26} = [5]_{26}\hat{=} & \text{E} \\
\text{D-R} & \hat{=}[4]_{26} - [18]_{26} = [-14]_{26} = [12]_{26}\hat{=} & \text{L} \\
\text{L-Y} & \hat{=}[12]_{26} - [25]_{26} = [-13]_{26} = [13]_{26}\hat{=} & \text{M} \\
\text{K-P} & \hat{=}[11]_{26} - [16]_{26} = [-5]_{26} = [21]_{26}\hat{=} & \text{U} \\
\text{D-K} & \hat{=}[4]_{26} - [11]_{26} = [-7]_{26} = [19]_{26}\hat{=} & \text{S} \\
\text{W-R} & \hat{=}[23]_{26} - [18]_{26} = [5]_{26}\hat{=} & \text{E}
\end{array}$$

Damit kann Pia die Nachricht lesen. Eine einfache Häufigkeitsanalyse wie beim Caesar-Kryptosystem nützt nichts, da der gleiche Buchstabe durch verschiedene Buchstaben verschlüsselt werden kann; z.B. ist das erste P in Pampelmuse durch ein A chiffriert und das zweite P durch ein F.

Abbildung 2.2: Die Vigenère Verschlüsselung ist benannt nach *Blaise de Vigenère* (1523–1596), einem französischen Diplomaten, der einige Werke zur Kryptographie verfasst hat. Der Ursprung dieses Kryptosystems geht allerdings zurück auf eine Schrift von Johannes Trithemius (1462–1516).

In diesem Beispiel ist der Klartext nicht wesentlich länger als der Schlüssel. Normalerweise ist das ganz anders und die Nachricht ist viel länger als der Schlüssel. Dann hat Lea eine gute Chance, die Nachricht zu entschlüssel, wie das nächste Beispiel zeigt.

Beispiel. Lea fängt die folgende Chiffre ab

OWQ AONCTSE FFC TYC WRUF OAD XUELDD YTFDD MEJDYN HWQ MISD ZC VPKSUH DSDDAP RTH MNZNUHPF LQCPFYUCE

Eine einfache Häufigkeitsanalyse der Buchstaben hilft hier nicht weiter. Also machen wir eine etwas(!) schwierigere Häufigkeitsanalyse. Wir benutzen, dass es viele Buchstabenpaare gibt, die oft vorkommen. Die häufigsten sind EN, EI, ER, CH, NN, ...

Die entscheidende Beobachtung ist nun: Kommt nun eine Buchstabenfolge zweimal in einem Text vor und werden beide Folgen gleich verschlüsselt, so muss der Abstand zwischen den Buchstabenfolgen ein Vielfaches der Schlüssellänge sein.

In unserer Chiffre finden wir dreimal die Folge DD. Der Abstand zwischen den ersten beiden ist fünf Buchstaben lang, der Abstand zwischen der zweiten und der dritten, ist 25 Buchstaben lang. Wir gehen also davon aus, dass die Schlüssellänge ein Teiler von 5 und von 25 ist. Damit bekommen wir die Vermutung, dass der Schlüssel aus genau fünf Buchstaben besteht!

Stimmt die Vermutung, dann wird jeder fünfte Buchstabe mit dem gleichen Buchstaben des Schlüssels addiert. D.h. der erste Buchstabe wird genau so verschlüsselt wie der sechste, und wie der elfte, und wie der 16te, ... Weiter

wird der zweite Buchstabe genau so verschlüsselt wie der siebte, und wie der zwölfte, ...
Damit gilt vermutlich:

- ONFCOETEHSPDPNPPE wurde mit dem 1. Buchstaben des Schlüssels chiffriert
- WCFWALFJWDKSRZFF wurde mit dem 2. Buchstaben des Schlüssels chiffriert
- QTCRDDDDQZSDTNLY wurde mit dem 3. Buchstaben des Schlüssels chiffriert
- ASTUXDDYMCUDHUQU wurde mit dem 4. Buchstaben des Schlüssels chiffriert
- OEYFUYMNIVHAMHCC wurde mit dem 5. Buchstaben des Schlüssels chiffriert

Wir haben also *eine* Vigenère-Chiffre in *fünf* Caesar-Chiffren zerlegt. Nun können wir also wieder eine Häufigkeitsanalyse durchführen. In der ersten Buchstabenfolge sind die häufigsten Buchstaben P und E. Wir vermuten also, dass gilt

1. Buchstabe des Schlüssels + E = P oder =E, bzw.
1. Buchstabe des Schlüssels = P-E =K oder = E-E = Z.

Genau so sehen wir für die Buchstabenfolgen 2, 3 und 4, dass vermutlich gilt

2. Buchstabe des Schlüssels = F-E =A oder = W-E = R.
3. Buchstabe des Schlüssels = D-E =Y.
4. Buchstabe des Schlüssels = U-E =P oder = D-E = Y.

In der fünften Buchstabenfolge sticht kein Buchstabe hervor. Mit unserem bisherigen Wissen können wir aber entweder den Schlüssel erraten (da wir uns in dem Kapitel über Kryptographie befinden, und der Anfang KRYP kompatibel mit unseren Vermutungen ist, wird es sich wohl um den Schlüssel KRYPT handeln), oder wir testen einfach die acht möglichen

Schlüsselanfänge und füllen jeden fünften Buchstaben aus dem Kontext hinzu. In jedem Fall erhalten wir den Klartext

DER KUCKUCK UND DER ESEL DIE HATTEN EINEN STREIT
WER WOHL AM BESTEN SAENGE ZUR SCHOENEN MAIENZEIT

Ist die Nachricht viel länger als der Schlüssel, lässt sich auf die eben beschriebene Methode jede Vigenère-Chiffre entschlüsseln.

2.2 RSA-Verfahren

Die Verfahren zur Verschlüsselung aus dem letzen Abschnitt haben eine gravierende Schwachstelle: Es muss sich zunächst geheim auf einen Schlüssel geeinigt werden. Aber wie soll das funktionieren wenn die gesamte Kommunikation überwacht wird?
Wenn Sie sich im Internet Ihr Lieblingsmathebuch mit Ihrer Kreditkarte bestellen möchten, macht es wenig Sinn erst zur Geschäftsstelle von a...n zu fahren um sich dort auf einen geheimen Schlüssel zu einigen.
Bevor wir ein Verfahren vorstellen, wie man sicher kommunizieren kann obwohl alles mitgehört wird, brauchen wir noch ein bisschen Zahlentheorie.

Lemma 2.2.1. *Seien p und q zwei verschiedene Primzahlen und sei $k \in \mathbb{N}$ beliebig. Für alle $a \in \mathbb{Z}$ gilt $a^{k\varphi(p\cdot q)+1} \equiv a \mod pq$.*

Beweis. Wir betrachten die gewünschte Kongruenz zunächst nur modulo p. Gilt $p \mid a$, so ist natürlich $a \equiv 0 \equiv a^{k\varphi(p\cdot q)+1} \mod p$. Sei nun $p \nmid a$. Dann folgt (da p eine Primzahl ist), dass $\mathrm{ggT}(a,p) = 1$ ist. Damit gilt mit dem Satz von Euler 1.3.36 $a^{\varphi(p)} \equiv 1 \mod p$. Es folgt

$$a^{k\varphi(p\cdot q)+1} \equiv \left(a^{\varphi(p)}\right)^{k\varphi(q)} \cdot a \equiv 1^{k(q-1)} \cdot a \equiv a \mod p$$

Es gilt also für alle $a \in \mathbb{Z}$ die Behauptung $p \mid a^{k\varphi(p\cdot q)+1} - a$. Durch Vertauschen der Rollen von p und q, folgt genauso $q \mid a^{k\varphi(p\cdot q)+1} - a$. Da p und q teilerfremd sind, folgt

$$p \cdot q \mid a^{k\varphi(p\cdot q)+1} - a \quad \Longleftrightarrow \quad a^{k\varphi(p\cdot q)+1} \equiv a \mod pq.$$

Das war zu zeigen. □

RSA-Kryptosystem 2.2.2. Kommen wir nun zum Ablauf des RSA-Verfahrens. Wie immer möchte Mia eine Nachricht an Pia schicken.

- Pia wählt ganz geheim zwei verschiedene Primzahlen p und q. Diese sind geheim und werden nicht verraten und bilden Pias *privaten Schlüssel*. Dann bildet Pia $N = p \cdot q$ und wählt ein $e \in \{2, \dots, N\}$ mit $\mathrm{ggT}(\varphi(N), e) = 1$. Hier ist es wichtig zu beachten, dass Pia natürlich $\varphi(N) = (p-1) \cdot (q-1)$ kennt!

- Die Werte N und e werden nun ganz öffentlich bereitgestellt. Sie bilden Pias *öffentlichen Schlüssel*. Zum Beispiel stellt sie diese Werte auf Ihre Homepage.

- Mia transferiert nun ihre Nachricht in ein Element $m \in \{1, \dots, N-1\}$. Sollte ihre Nachricht zu lang sein, so unterteilt sie sie einfach in mehrere Nachrichten von geeigneter Länge.

- Nun berechnet Mia ein $c \in \{1, \dots, N-1\}$ mit $c \equiv m^e \mod N$ und schickt diesen Wert an Pia.

- Pia weiß, dass $\varphi(N) = (p-1) \cdot (q-1)$ ist. Damit kann sie ein Element $d \in \mathbb{N}$ berechnen mit $d \cdot e \equiv 1 \mod \varphi(N)$. Dieses d nennen wir Pias *Dechiffrierzahl*. Hierfür benötigt Pia die Voraussetzung $\mathrm{ggT}(e, \varphi(N)) = 1$.

- Mit diesem d ist die Entschlüsselung so gut wie fertig. Es gilt nämlich $e \cdot d = k \cdot \varphi(N) + 1$ für ein $k \in \mathbb{N}$. Damit kann Pia mit der Rechnung

$$c^d \equiv m^{e \cdot d} \equiv m^{k \cdot \varphi(N)+1} \overset{2.2.1}{\equiv} m \mod N$$

  leicht Mias Nachricht rekonstruieren.

Beispiel 2.2.3. Wir geben zwei Beispiele mit kleinen Zahlen an. Die Zahlen sind zwar verhältnismässig klein, aber man kann die Beispiele trotzdem nur mit einigem Aufwand per Hand rechnen. Daher erlauben wir den Einsatz von Rechnern. Man kann zum Beispiel den Modulo-Rechner benutzen, der unter https://www.mtholyoke.edu/courses/quenell/s2003/ma139/

js/powermod.html bereitgestellt wird. Ein Rechner speziell für das RSA-Verfahren, steht z.B. unter https://www.cryptool.org/de/cto/highlights/rsa-step-by-step.html bereit.

(a) Pia wählt

- privater Schlüssel $p = 7$ und $q = 11$
- öffentlicher Schlüssel $N = 77$ und $e = 7$

Es ist tatsächlich $N = p \cdot q$ und $e = 7$ ist teilerfremd zu $\varphi(77) = 60$.

Als nächstes berechnet Pia die Dechiffrierzahl d. Dies macht Sie natürlich mit dem Euklidischen Algorithmus 1.2.3:

$$\begin{aligned} 60 &= 8 \cdot 7 + 4 \\ 7 &= 1 \cdot 4 + 3 \\ 4 &= 1 \cdot 3 + 1 \end{aligned}$$

Damit folgt nämlich $1 = 4-3 = 4-(7-4) = 2\cdot 4-7 = 2\cdot(60-8\cdot 7)-7 = 2\cdot 60-17\cdot 7$. Betrachten wir diese Gleichung modulo $\varphi(77) = 60$ erhalten wir $1 \equiv -17 \cdot 7 \equiv 43 \cdot 7 \mod 60$.

Es ist somit $d = 43$.

Pia hat also die Schlüssel gewählt, bereitgestellt und ihre Dechiffrierzahl berechnet. Jetzt erst ist Mia dran. Mia möchte nun $m = 30$ an Pia schicken.

Verschlüsselung: Sie berechnet $m^e \equiv 30^7 \equiv 2 \mod 77$.

Mia schickt also die Chiffre $c = 2$ an Pia.

Entschlüsselung: Pia erhält $c = 2$ und möchte Mias Nachricht m erhalten. Sie berechnet also $c^d \equiv 2^{43} \equiv 30 \mod 77$. Damit hat Pia tatsächlich die Nachricht $m = 30$ erhalten.

Bei diesem Beispiel kann man sich noch fragen, warum das ganze sicher sein soll. Es sind doch gefühlt alle Informationen für jeden verfügbar. Wenn wir die Zahlen nur ganz leicht vergrößern, sieht es schon anders aus.

(b) Pia wählt die Primzahlen 157 und 211. Dann ist $N = 33127$ und $\varphi(N) = 156 \cdot 210 = 32760$. Weiter wählt sie $e = 11$ und macht ihren

$$\text{öffentlichen Schlüssel } (N, e) = (33127, 11)$$

bekannt. Es ist

$$\begin{aligned} 32760 &= 2978 \cdot 11 + 2 \\ 11 &= 5 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

Damit folgt $1 = 11 - 5 \cdot 2 = 11 - 5 \cdot (32760 - 2978 \cdot 11) = 14891 \cdot 11 - 5 \cdot \underbrace{32760}_{=\varphi(N)}$. Insbesondere weiß Pia nun $14891 \cdot 11 \equiv 1 \mod \varphi(N)$.

$$\text{Sie setzt daher } d = 14891.$$

Mia möchte nun ihre Handy-PIN $m = 7353$ an Pia schicken. Dazu berechnet sie modulo $N = 33127$

$$c \equiv m^e \equiv 7353^{11} \equiv 10289 \mod 33127$$

Dieses c sendet sie an Pia. Pia berechnet dann modulo $N = 33127$

$$c^d \equiv 10289^{14891} \equiv 7353 \equiv m \mod 33127.$$

und erhält Mias Handy-PIN.

Bemerkung 2.2.4. Angenommen Lea hätte die Nachricht c erhalten. Sie kennt außerdem die Werte N und e, da diese öffentlich sind. Damit weiß sie, dass Mias Nachricht m die Kongruenz $m^e \equiv c \mod N$ erfüllt. Dies wäre ganz einfach zu lösen, wenn sie das Element d mit $d \cdot e \equiv 1 \mod \varphi(N)$ kennen würde. Aber sie kennt nicht einmal $\varphi(N)$.
Können Sie ohne weiteres aus $N = 33127$ aus obigem Beispiel den Wert $\varphi(N)$ ablesen? Ich nicht!
Um $\varphi(N)$ effektiv berechnen zu können, müssen wir die Primfaktorzerlegung $N = p \cdot q$ kennen. Üblicherweise sind p und q beides Primzahlen der Größenordnung 2^{1024}.

Einschub

Der schnellste PC Deutschlands steht in Stuttgart und heißt Hawk. Er schafft 26 Billiarden ($= 26 \cdot 10^{15}$) Rechenschritte pro Sekunde. Um aus einem gegebenen $N = p \cdot q \approx 2^{2048}$ die Primteiler p und q herauszufinden, könnten wir N durch jede natürliche Zahl kleiner gleich 2^{1024} teilen und sehen ob wir einen Teiler gefunden haben.
Wie lange würde Hawk dafür brauchen? Die Antwort ist ungefähr $\frac{2^{1024}}{26 \cdot 10^{15}}$ Sekunden. Das sind ca. $2,19 \cdot 10^{284}$ Jahre. Unsere Sonne verglüht in spätestens $8 \cdot 10^9$ Jahren. Damit ist das RSA-Verfahren nach bisherigem Wissensstand sehr sicher. Wie es aussieht, wenn Quantencomputer alltagstauglich werden, ist hingegen eine andere Frage.

Ohne die Kenntnis von p und q scheint es also sehr schwierig zu sein, die RSA-Verschlüsselung zu knacken. Es ist allerdings nicht bekannt ob man tatsächlich N faktorisieren können muss um das RSA-Verfahren zu knacken. Möglicherweise haben die NSA oder Lea bereits einen anderen Weg gefunden...



Abbildung 2.3: Das RSA-Verfahren ist benannt nach *Ronald Rivest* (*1947; links), *Adi Shamir* (*1952; mitte) und *Leonard Adleman* (*1945; rechts), die dieses Verfahren 1977 als erste veröffentlichten. Alle drei wurden dafür mit dem Turing-Award (der höchsten Auszeichung für Informatiker) ausgezeichnet. Bereits 1973 wurde ein äquivalentes Verfahren von *C. Cocks* (*1950), einem Mitarbeiter des britischen Nachrichtendienstes, erfunden. Dies wurde erst 1997 bekannt, da seine Entdeckung bis dahin unter Geheimhaltung stand (und trotzdem nie genutzt wurde). In der Zwischnzeit hatten Rivest, Shamir und Adleman basierend auf RSA eine Sicherheitsfirma gegründet und diese für über $2,5 \cdot 10^8$\$ verkauft.

Bemerkung 2.2.5. Das RSA-Verfahrens basiert darauf, dass es zwar ganz einfach ist aus zwei Primzahlen p und q das Produkt $N = p \cdot q$ zu berechnen, es aber unfassbar schwierig (bis unmöglich) ist, aus dem Produkt N wieder die beiden Primzahlen p und q zu rekonstruieren. Im Einschub oben, haben wir ausgerechnet wie lange der schnellste PC Deutschlands brauchen würde um diese Primzahlen ganz naiv zu finden (länger als unsere Erde existieren wird!). Es ist natürlich auch möglich, die Teiler nicht von unten nach oben (ist 2 ein Teiler von N, ist 3 ein Teiler von N,....) zu testen, sondern von oben nach unten. Dazu könnte man $\sqrt{N}$ berechnen und dann testen ob N durch eine ganze Zahl nah an $\sqrt{N}$ teilbar ist. Dann finden wir sehr schnell einen Teiler von N, falls p und q sehr nah bei einander sind. In der Praxis muss daher darauf geachtet werden, dass p und q weit genug auseinander sind (sprich, dass $p - q$ hinreichend groß ist).

Das RSA-Verfahren kann geknackt werden, wenn der Angreifer, also Lea, $\varphi(N)$ kennt, da damit die alles entscheidende Dechiffrierzahl berechnet werden kann. Das nächste Lemma besagt, dass es tatsächlich genau so schwierig ist $\varphi(N)$ zu berechnen, wie die Primteiler p und q von N zu finden.

Lemma 2.2.6. *Seien N und e der öffentliche Schlüssel eines RSA-Verfahrens. Dann kennen wir den privaten Schlüssel p und q, genau dann wenn wir $\varphi(N)$ kennen.*

Beweis. Wenn wir den privaten Schlüssel p und q kennen, dann kennen wir natürlich auch $(p-1) \cdot (q-1) = \varphi(pq) = \varphi(N)$. Als nächstes müssen wir noch zeigen, dass wir aus $\varphi(N)$ auch die Zahlen p und q konstruieren können.
Es ist

$$N - \varphi(N) + 1 = pq - (p-1)(q-1) + 1 = p + q \quad \text{und} \quad N = p \cdot q. \tag{2.1}$$

Diese Werte sind uns also bekannt, wenn wir $\varphi(N)$ kennen. Nun sind aber p und q genau die Nullstellen des Polynoms

$$(x-p) \cdot (x-q) = x^2 - (p+q)x + pq \overset{(2.1)}{=} x^2 - (N - \varphi(N) + 1)x + N.$$

(D.h.: Wenn wir p oder q für x einsetzen kommt Null heraus.) Aber die Nullstellen eines quadratischen Polynoms sind schnell berechnet. Benutzen wir

die pq-Formel oder quadratische Ergänzung erhalten wir, dass die Nullstellen des Polynoms gegeben sind durch

$$\pm\sqrt{\left(\frac{N-\varphi(N)+1}{2}\right)^2 - N} + \frac{N-\varphi(N)+1}{2}.$$

Also finden wir mit dieser Formel unsere Primzahlen p und q, mit $N = p \cdot q$. □

Bemerkung 2.2.7. Das RSA-Verfahren wird z.B. immer dann benutzt wenn Sie im Adressfeld Ihres Browsers den Anfang `https://` sehen (achten Sie mal auf der Moodle-Seite darauf). Die Verschlüsselung die offiziell von WhatsApp benutzt wird, funktioniert ähnlich zum RSA-Verfahren.

Kapitel 3

Komplexe Zahlen

Die reellen Zahlen $\mathbb{R}$ sind Ihnen allen geläufig. Sie haben ein paar schöne Eigenschaften. Die wichtigste ist, dass man in $\mathbb{R}$ (genau wie in $\mathbb{Q}$) rechnen kann; d.h. es gibt eine Addition und eine Multiplikation, die die Kommuatitv-, Assoziativ- und Distributivgesetzte erfüllen. Weiter besitzt jedes $r \in \mathbb{R} \setminus \{0\}$ ein Inverses r^{-1}. Dieses Inverse ist genauso definiert wie in $\mathbb{Z}/n\mathbb{Z}$, denn es ist die (eindeutige) reelle Zahl mit $r \cdot r^{-1} = 1$.

Wir dürfen auch Wurzeln aus positiven Zahlen ziehen, was in $\mathbb{Q}$ im allgemeinen nicht funktioiniert, da $\sqrt{2} \in \mathbb{R} \setminus \mathbb{Q}$ ist.

Bei seinem Studium von quadratischen Gleichungen kannte Muḥammad al-Ḫwārazmī (siehe 1.2) weder die Null noch negative Zahlen. Es war also nicht möglich die Gleichungen $x^2 - 2x - 1 = 0$ und $x^2 + 2x - 1 = 0$ auf die gleiche Art und Weise zu behandeln, stattdessen wurden die Gleichungen $x^2 = 2x + 1$ und $x^2 + 2x = 1$ als unterschiedliche Fälle betrachtet. Aus heutiger Sicht ist das relativ umständlich, da in beiden Fällen die pq-Formel (oder quadratische Ergänzung) angewendet werden kann, die einem die Lösungen liefert.

Wir machen aber auch noch eine Fallunterscheidung bei der Betrachtung von quadratischen Gleichungen. Denn anders als bei den Gleichungen oben, betrachten wir die Gleichung $x^2 + 1 = 0$ als nicht lösbar, da die Lösung $x = \pm\sqrt{-1}$ wäre, aber das ist keine reelle Zahl mehr.

In diesem Kapitel beschäftigen wir uns mit der mutigen Überlegung, dass auch diese Fallunterscheidung nicht wirklich notwendig ist. Dazu müssen wir aber neue Zahlen kennenlernen – die komplexen Zahlen.

3.1 Grundlagen

Mit der Motivation von eben, können wir uns fragen, was diese neuen Zahlen erfüllen sollen. Kurz vor Weihnachten erstellen wir also eine Wunschliste.

Wunschliste 3.1.1. Wir wünschen uns für die neuen Zahlen,

- ein Element i mit $i^2 = -1$ (damit $x^2 + 1 = 0$ nicht länger als unlösbar gelten muss)
- dass die reellen Zahlen $\mathbb{R}$ benutzt werden (die haben wir ja schon verstanden)
- dass wir rechnen können. Also brauchen wir auch Elemente der Form $a + i$ und $b \cdot i$ mit $a, b \in \mathbb{R}$
- jetzt brauchen wir aber auch noch die Elemente $a + b \cdot i$ mit $a, b \in \mathbb{R}$
- dass wir so viele Eigenschaften von $\mathbb{R}$ haben wie möglich. Insbesondere möchten wir

$$(a+b\cdot i)+(a'+b'\cdot i) \overset{\text{kommutativ}}{=} (a+a')+b\cdot i+b'\cdot i \overset{\text{distributiv}}{=} (a+a')+(b+b')\cdot i \tag{3.1}$$

und

$$\begin{aligned}(a+b\cdot i)\cdot(a'+b'\cdot i) &\overset{\text{distributiv}}{=} aa'+a\cdot(b'\cdot i)+(b\cdot i)\cdot a'+(b\cdot i)\cdot(b'\cdot i)\\ &\overset{\text{assoziativ}}{=} aa'+(ab')\cdot i+(a'b)\cdot i+(bb')\cdot \underbrace{i^2}_{=-1} = (aa'-bb')+(ab'+a'b)\cdot i\end{aligned}$$

Einschub

Das ist erstmal nur eine Wunschliste! Jetzt müssen wir noch zeigen, dass tatsächlich alle unsere Wünsche (zumindest die oben genannten) erfüllt werden können.

Wir versuchen also folgende Definition.

Definition 3.1.2. Die Menge $\mathbb{C} = \{a + b \cdot i \mid a, b \in \mathbb{R}\}$, wobei $i^2 = -1$ gilt, heißt die Menge der *komplexen Zahlen*. Die Addition auf $\mathbb{C}$ ist gegeben durch

$$(a + b \cdot i) + (a' + b' \cdot i) = (a + a') + (b + b') \cdot i$$

Die Addition in den Klammern der rechten Seite ist dabei die bekannte Addition auf $\mathbb{R}$. Die Multiplikation ist definiert durch

$$(a + b \cdot i) \cdot (a' + b' \cdot i) = (a \cdot a' - b \cdot b') + (a \cdot b' + a' \cdot b) \cdot i$$

Auch hier sind die Rechnungen in den Klammern auf der rechten Seite die bekannten Rechnungen auf $\mathbb{R}$.

Lemma 3.1.3. *In den komplexen Zahlen $\mathbb{C}$ gelten die folgenden Rechenregeln. Seien dazu $u = a + b \cdot i, v = c + d \cdot i, w = e + f \cdot i \in \mathbb{C}$ beliebig. Dann ist*

(i) $(0 + 0 \cdot i) + u = u$

(ii) *(Kommutativität bzgl. +)* $u + v = v + u$

(iii) *(Assoziativität bzgl. +)* $u + (v + w) = (u + v) + w$

(iv) $u + (-a + (-b) \cdot i) = 0 + 0 \cdot i$

(v) $(1 + 0 \cdot i) \cdot u = u$

(vi) *(Kommutativität bzgl. ·)* $u \cdot v = v \cdot u$

(vii) *(Assoziativität bzgl. ·)* $u \cdot (v \cdot w) = (u \cdot v) \cdot w$

(viii) *(Distributivgesetz)* $u \cdot (v + w) = u \cdot v + u \cdot w$

Beweis. Es geht nur darum die Aussagen nachzurechnen. Wir machen das exemplarisch für Punkt (vi). Es ist

$$u \cdot v = (a + b \cdot i) \cdot (c + d \cdot i) \overset{Def.\cdot}{=} (ac - bd) + (ad + bc) \cdot i$$

und

$$v \cdot u = (c + d \cdot i) \cdot (a + b \cdot i) \overset{Def.\cdot}{=} (ca - db) + (da + cb) \cdot i$$

Da $ac - bd = ca - db$ und $ad + bc = da + cb$ ist (a, b, c, d sind reelle Zahlen und wir dürfen mit diesen so rechnen wie wir es gewohnt sind), ist somit $u \cdot v = v \cdot u$. □

Notation 3.1.4. Wir schreiben ab jetzt $a \cdot i$ für $0 + a \cdot i$, und a für $a + 0 \cdot i$. Damit fassen wir $\mathbb{R}$ als Teilmenge von $\mathbb{C}$ auf. Weiter schreiben wir $a - b \cdot i$ für $a + (-b) \cdot i$ und i für $1 \cdot i$. Für $u, v \in \mathbb{C}$ setzen wir $u - v = u + (-1) \cdot v$.

Wir kommen zurück zur Motivation der komplexen Zahlen. Wir wollten gerne in der Lage sein ohne Rücksicht auf mögliche Einschränkungen Wurzeln zu ziehen. Was ist nun $\sqrt{-5}$? Es muss ein Element $x \in \mathbb{C}$ sein, mit $x^2 = -5$. So ein Element kennen wir aber: $x = \sqrt{5} \cdot i$, denn es ist

$$(\sqrt{5} \cdot i)^2 = (\sqrt{5})^2 \cdot i^2 = 5 \cdot (-1) = -5.$$

Wir hatten i als Repräsentant für $\sqrt{-1}$ eingeführt. Auch damit sieht man schnell $\sqrt{-5} = \sqrt{5 \cdot (-1)} = \sqrt{5} \cdot \sqrt{-1} = \sqrt{5} \cdot i$. Wir können in den komplexen Zahlen also aus *allen* reellen Zahlen eine Quadratwurzel ziehen.

Proposition 3.1.5. *Jede quadratische Gleichung $x^2+ax+b = 0$ mit $a, b \in \mathbb{R}$ hat eine Lösung in $\mathbb{C}$.*

Beweis. Wir betrachten also $x^2 + ax + b = 0$. Mit quadratischer Ergänzung ist dies äquivalent zu

$$(x+\frac{a}{2})^2 - \frac{a^2}{4} + b = 0 \quad \Longleftrightarrow \quad (x+\frac{a}{2})^2 = \frac{a^2}{4} - b \quad \Longleftrightarrow \quad x = \pm\sqrt{\frac{a^2}{4} - b} - \frac{a}{2}.$$

Da $\frac{a^2}{4} - b$ eine reelle Zahl ist, können wir die Wurzel in $\mathbb{C}$ ziehen und somit haben wir eine Lösung gefunden □

Beispiel 3.1.6. Wir lösen die Gleichung $x^2 + 2x + 3 = 0$. Diese Gleichung ist äquivalent zu

$$(x+1)^2 - 1 + 3 = 0 \quad \Longleftrightarrow \quad (x+1)^2 = -2 \quad \Longleftrightarrow \quad x + 1 = \pm \underbrace{\sqrt{-2}}_{\sqrt{2} \cdot i}$$

Es ist somit $x = \pm\sqrt{-2} - 1 = -1 \pm \sqrt{2} \cdot i$.

Es gilt sogar noch viel mehr als die letzte Proposition. Wir können nicht nur sämtliche quadratische Gleichungen in $\mathbb{C}$ lösen, sondern alle polynomiellen Gleichungen über den reellen Zahlen.

Theorem 3.1.7 (Fundamentalsatz der Algebra)**.** *Seien $a_0, \ldots, a_n \in \mathbb{R}$ beliebig. Es existiert eine komplexe Zahl $z \in \mathbb{C}$ mit*

$$a_n \cdot z^n + a_{n-1} \cdot z^{n-1} + \ldots + a_1 \cdot z + a_0 = 0.$$

Es gibt viele verschiedene Beweise von diesem Resultat. Allerdings würde jeder einzelne den Rahmen dieser Vorlesung sprengen.

Definition 3.1.8. Sei $z = a + b \cdot i \in \mathbb{C}$. Dann heißt $\overline{z} = a - b \cdot i \in \mathbb{C}$ die *komplex-konjugierte Zahl zu* z. Weiter nennen wir $a = Re(z)$ den *Realteil* von z und $b = Im(z)$ den *Imaginärteil* von z.

Lemma 3.1.9. *Sei* $z = a + b \cdot i \in \mathbb{C}$. *Es gilt*

(a) $z = \overline{z} \in \mathbb{R} \iff z \in \mathbb{R}$

(b) $z\overline{z} = a^2 + b^2 \in \mathbb{R}$

Beweis. Wir rechnen einfach nach.

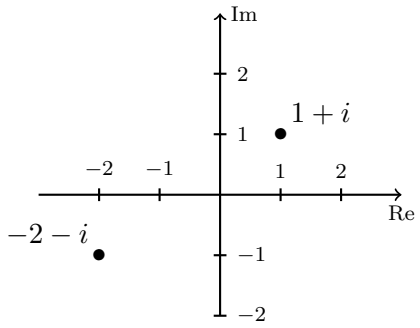
Zu (a):

$$\begin{aligned} z = \overline{z} &\iff a + b \cdot i = a - b \cdot i \\ &\iff (a - a) + (2b) \cdot i = 0 \\ &\iff b = 0 \\ &\iff z = a \in \mathbb{R} \end{aligned}$$

Zu (b): $z \cdot \overline{z} = (a + b \cdot i) \cdot (a - b \cdot i) = a^2 - b^2 \cdot \underbrace{i^2}_{=-1} = a^2 + b^2$

□

Konstruktion 3.1.10. Wir möchten die komplexen Zahlen geometrisch deuten. Dazu stellen wir fest, dass eine komplexe Zahl im wesentlichen durch zwei reelle Zahlen a und b gegeben ist; nämlich den Realteil und den Imaginärteil. Zwei reelle Zahlen kennen wir bereits als Punkte in einem Koordinatensystem (a/b). Damit können wir komplexe Zahlen als Ebene darstellen, wir sprechen auch von der *komplexen Zahlenebene*. Beachten Sie, dass das wunderbar unsere Anschauung der reellen Zahlen als Zahlengerade erweitert!



Wir können die komplexen Zahlen also auch geometrisch deuten. z.B. ist der Abstand von $z = -2-1\cdot i$ zum Nullpunkt gegeben durch $\sqrt{(-2)^2 + (-1)^2} = \sqrt{5}$. Allgemein ist der Abstand von $a + b \cdot i$ zum Nullpunkt gegeben durch $\sqrt{a^2 + b^2}$. Das ist offensichtlich, falls $a = 0$ oder $b = 0$. Der allgemeine Fall folgt aus dem Satz des Pythagoras, nachdem wir das Dreieck mit den Punkten 0, a, $a + b \cdot i$ eingezeichnet haben. Dieses Dreieck hat offensichtlich einen rechten Winkel. Die Seite des Dreiecks, die 0 und a verbindet hat die Länge $|a|$, und die Strecke, die a und $a+b\cdot i$ verbindet, hat die Länge $|b|$. Der Abstand zwischen $a+b\cdot i$ ist die Länge der Hypothenuse im Dreieck. Nennen wir diesen Abstand x, dann gilt mit Pythagoras $x^2 = |a|^2 + |b|^2 = a^2 + b^2$. Wurzelziehen, liefert nun den gesuchten Wert.

Definition 3.1.11. Der *Betrag* einer komplexen Zahl $z = a + b \cdot i$ ist $|z| = \sqrt{a^2 + b^2} \overset{3.1.9}{=} \sqrt{z \cdot \overline{z}}$.

Lemma 3.1.12. *Seien $u, v \in \mathbb{C}$. Dann gilt*

(a) $\overline{u \cdot v} = \overline{u} \cdot \overline{v}$

(b) $\overline{u + v} = \overline{u} + \overline{v}$

(c) $|u \cdot v| = |u| \cdot |v|$

Beweis. Teil (a) und (b) rechnet man einfach nach, was wir hier weglassen. Teil (c) folgt nun durch

$$|u \cdot v| = \sqrt{u \cdot v \cdot \overline{u \cdot v}} \overset{(a)}{=} \sqrt{u \cdot \overline{u} \cdot v \cdot \overline{v}} = \sqrt{u \cdot \overline{u}} \cdot \sqrt{v \cdot \overline{v}} = |u| \cdot |v|.$$

□

Eine schöne Eigenschaft auf den reellen Zahlen ist, dass wir durch jedes Element ungleich Null teilen dürfen bzw. teilen können. Dies gilt glücklicherweise auch auf den komplexen Zahlen, wie wir nun sehen werden.

Proposition 3.1.13. *Ist $u \neq 0$ eine komplexe Zahl, so existiert ein Element $u^{-1} \in \mathbb{C}$ mit $u \cdot u^{-1} = 1$.*
D.h.: Jedes Element in $\mathbb{C} \setminus \{0\}$ besitzt ein Inverses!

BEWEIS. Wenn $u = a + b \cdot i \neq 0$ ist, ist $u \cdot \overline{u} = a^2 + b^2 \in \mathbb{R} \setminus \{0\}$. Damit existiert das Element $\frac{1}{u \cdot \overline{u}} \in \mathbb{R} \subseteq \mathbb{C}$. Es ist also auch $\overline{u} \cdot \frac{1}{u \cdot \overline{u}} \in \mathbb{C}$ und es gilt

$$u \cdot \left(\overline{u} \cdot \frac{1}{u \cdot \overline{u}} \right) = 1.$$

□

Merken!

Das Inverse von $u \in \mathbb{C} \setminus \{0\}$ ist stets $\frac{\overline{u}}{|u|^2}$.

Beispiel 3.1.14. Was ist das Inverse von $1 + i$? Die gerade gezeigt Formel liefert

$$(1+i)^{-1} = \frac{1}{1+i} = \frac{1-i}{(1+i)\cdot(1-i)} = \frac{1-i}{1^2+1^2} = \frac{1}{2} - \frac{1}{2} \cdot i$$

Wie können wir $\frac{1+5\cdot i}{3-2\cdot i}$ in die Form $a+b\cdot i$ bringen? Wir erweitern den Bruch mit $(3+2\cdot i)$ und erhalten

$$\frac{1+5\cdot i}{3-2\cdot i} = \frac{(1+5\cdot i)\cdot(3+2\cdot i)}{(3-2\cdot i)\cdot(3+2\cdot i)} = \frac{(3-10)+(2+15)\cdot i}{3^2+2^2} = \frac{-7}{13} + \frac{17}{13} \cdot i.$$

3.2 Die Gauß'schen Zahlen

Eigentlich beschäftigen wir uns in der Zahlentheorie mit den ganzen Zahlen. Zu Beginn der Vorlesung haben wir uns mit den Mengen $\mathbb{Z}/n\mathbb{Z}$ beschäftigt und haben daraus Informationen über die ganzen Zahlen erhalten. Grob gesagt,

haben wir kleinere „Zahlbereiche“ benutzt um Aussagen über $\mathbb{Z}$ zu treffen. Wir wollen in diesem Abschnitt zeigen, dass wir auch größere Zahlbereiche benutzen können um $\mathbb{Z}$ zu studieren. Dazu wollen wir $\mathbb{Z}$ erweitern, und zwar genau so wie wir die reellen Zahlen erweitert haben um die komplexen Zahlen zu erhalten.

Definition 3.2.1. Die Menge $\mathbb{Z}[i] = \{a + b \cdot i \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ heißt Menge der *Gauß'schen Zahlen*. Hier ist wieder $i^2 = -1$.

Abbildung 3.1: Der deutsche Mathematiker *Carl Friedrich Gauß* (1777 - 1855) lieferte in vielen Gebieten der Mathematik und Astronomie bedeutende Arbeit. Angeblich korrigierte er mit drei Jahren die Rechnungen seines Vaters. Mit 24 hatte er schon einige fundamentale Sätze bewiesen. Auch wenn er schon zu Lebzeiten ein gefeierter Mathematiker war, wurde sein ganzes Schaffen erst 1898 mit dem Fund seines Tagebuchs deutlich.

Bemerkung 3.2.2. Auf den komplexen Zahlen $\mathbb{C}$ haben wir die Verknüpfungen $+$ und $\cdot$. Wir stellen fest, dass die Summe zweier Gauß'scher Zahlen und das Produkt zweier Gauß'scher Zahlen wieder Gauß'sche Zahlen sind. Denn für $a, b, c, d \in \mathbb{Z}$ gilt:

$$(a + b \cdot i) + (c + d \cdot i) = \underbrace{(a + c)}_{\in\mathbb{Z}} + \underbrace{(b + d)}_{\in\mathbb{Z}} \cdot i \in \mathbb{Z}[i]$$

und

$$(a + b \cdot i) \cdot (c + d \cdot i) = \underbrace{(ac - bd)}_{\in\mathbb{Z}} + \underbrace{(ad + bc)}_{\in\mathbb{Z}} \cdot i \in \mathbb{Z}[i]$$

Damit können wir auch auf $\mathbb{Z}[i]$ wie gewohnt rechnen. Dass die üblichen Rechengesetze der Kommutativität, Assoziativität und Distributivität gelten, folgt sofort aus den entsprechenden Eigenschaften auf $\mathbb{C}$.

Wir wissen schon was Teilbarkeit auf $\mathbb{Z}$ bedeutet, wenn Sie das nicht wissen, dann starten Sie wieder bei Definition 1.1.1. (Begib Dich direkt dorthin. Gehe nicht über Los. Ziehe keine 4000 € ein.) Teilbarkeit wollen wir auch auf den Gauß'schen Zahlen studieren. Die folgende Definition überrascht Sie hoffentlich nicht.

Definition 3.2.3. Seien α, β Gauß'sche Zahlen (kurz: seien $\alpha, \beta \in \mathbb{Z}[i]$). Dann heißt α *Teiler* von β, wenn es eine Gauß'sche Zahl γ gibt, mit $\alpha \cdot \gamma = \beta$. Wir sagen dazu auch α *teilt* β und bezeichnen dies mit $\alpha \mid \beta$.

Da Teilbarkeit auf $\mathbb{Z}[i]$ genau so definiert ist, wie Teilbarkeit auf $\mathbb{Z}$, gelten auch hier die elementaren Teilbarkeitsregeln (a)-(d) aus Lemma 1.1.5!

Bemerkung 3.2.4. Auf den komplexen Zahlen $\mathbb{C}$ wäre diese Definition ziemlich witzlos, da jedes Element ein Inverses besitzt. Sind dann $\alpha, \beta \in \mathbb{C} \setminus \{0\}$ dann gilt $\alpha \cdot (\alpha^{-1} \cdot \beta) = \beta$. Wir können also immer eine komplexe Zahl mit α multiplizieren um β zu erhalten. Um einzusehen, dass das auf den Gauß'schen Zahlen anders ist, sollten wir herausfinden welche Elemente aus $\mathbb{Z}[i]$ ein Inverses in $\mathbb{Z}[i]$ besitzen.

Definition 3.2.5. Ein Element $\alpha \in \mathbb{Z}[i]$ heißt *invertierbar in* $\mathbb{Z}[i]$, falls ein $\beta \in \mathbb{Z}[i]$ existiert, mit $\alpha \cdot \beta = 1$. Die Menge aller invertierbarer Elemente in $\mathbb{Z}[i]$ bezeichnen wir mit $\mathbb{Z}[i]^*$.

Bemerkung 3.2.6. Wir möchten alle Elemente $a + b \cdot i \in \mathbb{Z}[i]$ bestimmen für die ein $c + d \cdot i \in \mathbb{Z}[i]$ existiert mit $(a + b \cdot i) \cdot (c + d \cdot i) = 1$. Natürlich muss dafür $a + b \cdot i \neq 0$ sein. Wir nehmen die Beträge und erhalten

$$\underbrace{|a + b \cdot i|}_{=\sqrt{a^2+b^2} \geq 1} \cdot \underbrace{|c + d \cdot i|}_{\sqrt{c^2+d^2} \geq 1} = |1| = 1$$

Die Gleichung kann also nur erfüllt sein, wenn $\sqrt{a^2 + b^2} = 1$ gilt. Das ist genau dann der Fall wenn $a^2 + b^2 = 1$ ist. Da $a, b \in \mathbb{Z}$, ist somit entweder $a = 0$ und $b = \pm 1$, oder $b = 0$ und $a = \pm 1$. Die einzigen Elemente in $\mathbb{Z}[i]$, die invertierbar seien können sind also

$$1 \quad , \quad -1 \quad , \quad i \quad , \quad -i.$$

Diese Elemente besitzen aber tatsächlich alle ein Inverses in $\mathbb{Z}[i]$, denn es gilt

$$1 \cdot 1 = 1 \quad , \quad (-1) \cdot (-1) = 1 \quad , \quad i \cdot (-i) = 1.$$

Damit erhalten wir $\mathbb{Z}[i]^* = \{1, -1, i, -i\}$.

Wir haben gesehen, dass der Betrag auf $\mathbb{C}$ das entscheidende Hilfsmittel war, um $\mathbb{Z}[i]^* = \{1, -1, i, -i\}$ zu zeigen. Daher führen wir eine Definition ein, die uns erlaubt eine wichtige Eigenschaft einer Gauß'schen Zahl mit einer ganzen Zahl auszudrücken. Beachten Sie, dass der Betrag einer Gauß'schen Zahl die *Wurzel* einer natürlichen Zahl ist.

Definition 3.2.7. Für $a + b \cdot i \in \mathbb{Z}[i]$ definieren wir die *Norm* von $a + b \cdot i$ als $N(a + b \cdot i) = a^2 + b^2$.

Bemerkung 3.2.8. Der Ausdruck $a^2 + b^2$ ist uns schon ein paarmal begegnet. Insbesondere kennen wir bereits mehrere Möglichkeiten die Norm einer Gauß'schen Zahl zu beschreiben. Für $\gamma = a + b \cdot i \in \mathbb{Z}[i]$ ist:

$$N(\gamma) \overset{\text{Def.}}{=} a^2 + b^2 \overset{3.1.11}{=} |\gamma|^2 \overset{3.1.9}{=} \gamma \cdot \bar{\gamma}. \tag{3.2}$$

Lemma 3.2.9. *Seien $\alpha, \beta \in \mathbb{Z}[i]$. Dann gilt*

(i) $N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta)$

(ii) $N(\alpha) \in \mathbb{N}_0$

(iii) $N(\alpha) = 0 \iff \alpha = 0$

Beweis. Die Aussagen (ii) und (iii) sind fast offensichtlich. Aussage (i) folgt sofort aus der Multiplikativität des Betrages auf $\mathbb{C}$ (siehe Lemma 3.1.12). Denn es ist

$$N(\alpha \cdot \beta) = |\alpha \cdot \beta|^2 = (|\alpha| \cdot |\beta|)^2 = |\alpha|^2 \cdot |\beta|^2 = N(\alpha) \cdot N(\beta)$$

□

Korollar 3.2.10. *Seien $\alpha, \beta \in \mathbb{Z}[i] \setminus \{0\}$. Dann gilt*

$$\alpha \mid \beta \implies N(\alpha) \mid N(\beta).$$

D.h.: Teilt α die Gauß'sche Zahl β, dann teilt die Norm von α auch die Norm von β.

Beweis. Sei also $\alpha \mid \beta$ für Gauß'sche Zahlen α und β. Dann existiert ein $\gamma \in \mathbb{Z}[i]$ mit $\alpha \cdot \gamma = \beta$. Mit Lemma 3.2.9 erhalten wir

$$\underbrace{N(\alpha)}_{\in\mathbb{Z}} \cdot \underbrace{N(\gamma)}_{\in\mathbb{Z}} = N(\alpha \cdot \gamma) = \underbrace{N(\beta)}_{\in\mathbb{Z}}$$

Das bedeutet genau $N(\alpha) \mid N(\beta)$. □

Beispiel 3.2.11. (a) Ist $4 + 3 \cdot i$ ein Teiler von $27 - 8 \cdot i$? Wir berechnen $N(4 + 3 \cdot i) = 4^2 + 3^2 = 25$. Wenn $4 + 3i$ ein Teiler von $27 - 8i$ ist, dann wäre also $25 \mid N(27 - 8i)$. Allerdings ist

$$N(27 - 8i) = 27^2 + 8^2 \equiv 2^2 + 8^2 \equiv 68 \equiv 18 \mod 25.$$

Es ist also $25 \nmid N(27 - 8i)$ und somit ist $4 + 3i$ kein Teiler von $27 - 8i$.

(b) Es ist $N(5) = 25 = N(4+3\cdot i)$. Insbesondere ist also $N(5) \mid N(4+3\cdot i)$. Wir behaupten nun, dass 5 trotzdem KEIN Teiler von $4+3\cdot i$ ist. Falls $5 \mid 4 + 3 \cdot i$ wäre, so gäbe es ein $\gamma \in \mathbb{Z}[i]$ mit $5 \cdot \gamma = 4 + 3 \cdot i$. In den komplexen Zahlen können wir γ berechnen, nämlich $\gamma = \frac{4+3\cdot i}{5} = \frac{4}{5} + \frac{3}{5} \cdot i$. Dies ist aber offensichtlich nicht in $\mathbb{Z}[i]$. Damit kann 5 kein Teiler von $4 + 3 \cdot i$ sein.

Wir haben zwei wichtige Beobachtung gemacht, die wir festhalten wollen.

1. Um zu überprüfen ob $\alpha \mid \beta$ gilt, für $\alpha, \beta \in \mathbb{Z}[i]$, können wir in den komplexen Zahlen $\frac{\beta}{\alpha}$ berechen. Dann ist $\alpha \mid \beta$ genau dann wenn $\frac{\beta}{\alpha} \in \mathbb{Z}[i]$.

2. Eine Gauß'sche Zahl $a + b \cdot i$ ist genau dann durch $c \in \mathbb{Z}$ teilbar, wenn c ein gemeinsamer Teiler (im herkömmlichen Sinne) von a und b ist.

Das alles gilt genau so auch für die Teilbarkeit in $\mathbb{Z}$!

Das wichtigste Hilfmittel auf den ganzen Zahlen $\mathbb{Z}$ ist der Euklidische Algorithmus aus dem fast alles folgt, was wir über $\mathbb{Z}$ wissen. Der Euklidische Algorithmus ist aber selbst eine Anwendung von Division mit Rest. Wie könnte eine Version von Division mit Rest auf $\mathbb{Z}[i]$ aussehen?

Theorem 3.2.12. *Seien $\alpha, \beta \in \mathbb{Z}[i]$ mit $\beta \neq 0$. Dann existieren $\gamma, \rho \in \mathbb{Z}[i]$ mit*

(i) $\alpha = \gamma \cdot \beta + \rho$ und

(ii) $N(\rho) < N(\beta)$

Bevor wir das Theorem beweisen, rechnen wir ein Beispiel.

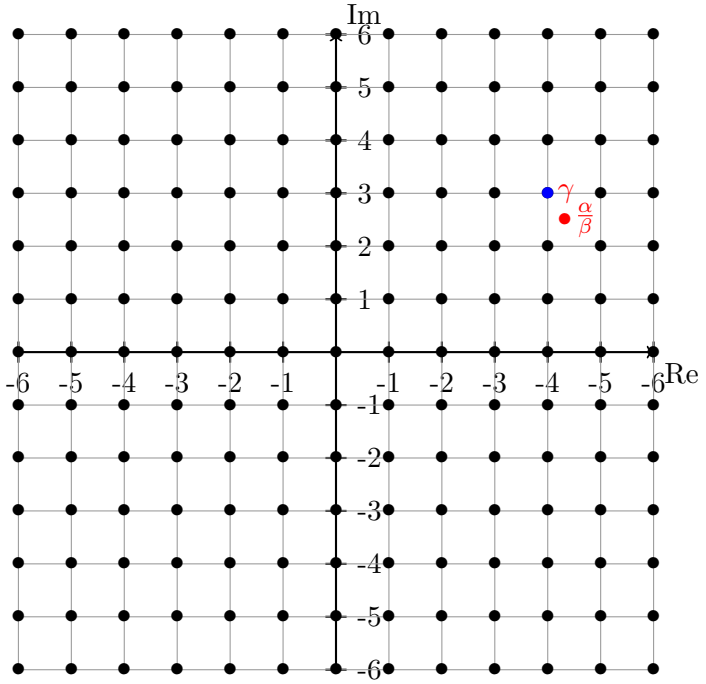
Beispiel 3.2.13. Sei $\alpha = 27 - 23 \cdot i$ und $\beta = 8 + i$. Die Norm von β ist $N(\beta) = 64 + 1 = 65$. Damit der Rest ρ eine kleine Norm besitzt, sollten wir für γ eine Gauß'sche Zahl wählen, die „nah an der komplexen Zahl $\frac{\alpha}{\beta}$ liegt". Wir rechnen daher als erstes $\frac{\alpha}{\beta} = \frac{(27-23\cdot i)\cdot(8-i)}{65} = \frac{193}{65} - \frac{211}{65} \cdot i$. Es ist $\frac{193}{65} = 2,969\ldots$ und $\frac{211}{65} = 3,246\ldots$. Damit ist $\gamma = 3 - 3 \cdot i \in \mathbb{Z}[i]$ „nah an $\frac{\alpha}{\beta}$".
Mit dieser Wahl von γ gilt dann

$$\rho \overset{(i)}{=} \alpha - \gamma \cdot \beta = (27 - 23 \cdot i) - (3 - 3 \cdot i) \cdot (8 + i) = -2 \cdot i.$$

Insbesondere ist wie gewünscht $N(\rho) = N(-2 \cdot i) = 4 < 65 = N(\beta)$.

Beweis von Theorem 3.2.12. Wir haben also $\alpha, \beta \in \mathbb{Z}[i]$ gegeben mit $\beta \neq 0$. Als erstes zeichnen wir die Gauß'schen Zahlen in die komplexe Zahlenebene ein. Da $\beta \neq 0$ existiert $\frac{\alpha}{\beta} \in \mathbb{C}$. Die komplexe Zahl $\frac{\alpha}{\beta}$ können wir auch in die Zahlenebene einzeichnen. Egal wo diese komplexe Zahl auch liegt, wir finden immer ein $\gamma \in \mathbb{Z}[i]$, so dass gilt

$$|Re(\gamma) - Re(\frac{\alpha}{\beta})| \leq \frac{1}{2} \quad \text{und} \quad |Im(\gamma) - Im(\frac{\alpha}{\beta})| \leq \frac{1}{2} \tag{3.3}$$



Wir behaupten, dass wir mit dieser Wahl von γ (beachte, dass die Wahl nicht eindeutig ist!) das Theorem beweisen können. Wir setzen daher $\rho = \alpha - \beta \cdot \gamma \in \mathbb{Z}[i]$. Dann ist ganz sicher Eigenschaft (i) erfüllt und wir müssen nur noch $N(\rho) < N(\beta)$ zeigen. Wir benutzen dafür wieder die Multiplikativität des Betrages auf den komplexen Zahlen.

$$\begin{aligned} N(\rho) < N(\beta) &\iff |\rho| < |\beta| \iff |\alpha - \beta \cdot \gamma| < |\beta| \\ &\iff |\beta \cdot (\frac{\alpha}{\beta} - \gamma)| < |\beta| \iff |\frac{\alpha}{\beta} - \gamma| < 1 \\ &\iff \sqrt{(Re(\frac{\alpha}{\beta}) - Re(\gamma))^2 + (Im(\frac{\alpha}{\beta}) - Im(\gamma))^2} < 1 \\ &\overset{(3.3)}{\iff} \sqrt{(\frac{1}{2})^2 + (\frac{1}{2})^2} < 1 \end{aligned}$$

Die letzte Aussage ist offensichtlich richtig. Damit muss auch die erste Aussage ($N(\rho) < N(\beta)$) richtig sein. Damit ist das Theorem bewiesen. □

Beispiel 3.2.14. Wir zeigen an einem Beispiel den (einzigen) Unterschied zur Division mit Rest in $\mathbb{Z}$ auf. Seien $\alpha = 5 + 3 \cdot i$ und $\beta = 1 + 2 \cdot i$. Dann ist $\frac{\alpha}{\beta} = \frac{(5+3\cdot i)\cdot(1-2\cdot i)}{1^2+2^2} = \frac{11}{5} - \frac{7}{5} \cdot i$.
Wir wählen daher $\gamma = 2 - i$. Damit $\alpha = \gamma \cdot \beta + \rho$ gilt, setzen wir

$$\rho = (5 + 3 \cdot i) - (2 - i) \cdot (1 + 2 \cdot i) = 1.$$

Dies erfüllt offensichtlich $N(\rho) < N(\beta)$. Wir können aber auch $\gamma = 2 - 2 \cdot i$ wählen. Dann ist

$$\rho = (5 + 3 \cdot i) - (2 - 2 \cdot i) \cdot (1 + 2 \cdot i) = -1 + i,$$

was ebenfalls $N(\rho) < N(\beta)$ erfüllt.
Fazit: Die Division mit Rest ist nicht eindeutig!

Bemerkung 3.2.15. Die Eindeutigkeit bei der Division mit Rest auf $\mathbb{Z}$ spielt in den meisten Beweisen der großen Theoreme über $\mathbb{Z}$ keine Rolle. Daher folgen aus der Division mit Rest auf $\mathbb{Z}[i]$ viele bekannte Theoreme:

- Es gibt den Euklidischen Algorithmus und das Lemma von Bézout auf $\mathbb{Z}[i]$!
- Je zwei Gauß'sche Zahlen α, β besitzen einen größten gemeinsamen Teiler.

- Jedes $\alpha \in \mathbb{Z}[i]$ mit $N(\alpha) > 1$ besitzt eine eindeutige Zerlegung in „Prim-Gauß'sche Zahlen".

Die letzte Aussage werden wir im nächsten Abschnitt noch weiter studieren.

3.3 Gauß'sche Primzahlen & Summe von zwei Quadraten

In diesem Abschnitt wollen wir studieren, welche (ganzen) Zahlen sich als Summe von zwei Quadratzahlen schreiben lassen. Zum Beispiel ist $0 = 0^2 + 0^2$, $1 = 1^2 + 0^2$, $2 = 1^2 + 1^2$. Allerdings ist es nicht möglich die 3 als Summe von zwei Quadratzahlen zu schreiben: Es ist $2^2 > 3$, deshalb kommen nur die Summanden 0^2 und 1^2 in Frage. Aber es ist $1^2 + 1^2 < 3$.
Dass die 3 nicht die Summe von zwei Quadratzahlen ist, können wir nutzen, um von ganz vielen Zahlen zu zeigen, dass sie nicht die Summe von zwei Quadratzahlen sind. Am schönsten wäre es natürlich wenn wir eine Aussage der Form „Wenn n gerade ist, dann dies, wenn n ungerade ist dann das." treffen könnten. Da es aber sowohl gerade als auch ungerade Summen von zwei Quadratzahlen gibt (z.B. 1 und 2), kann eine Unterscheidung zwischen geraden und ungeraden Zahlen nicht weiterhelfen. Aber was genau passiert denn bei der Unterscheidung zwischen geraden und ungeraden Zahlen? Wir rechnen modulo 2! Wenn also eine Unterscheidung modulo 2 nicht hilft, dann ist doch der nächst beste Fall, wenn uns eine Unterscheidung modulo einer anderen (hoffentlich kleinen) Zahl weiterhilft. Und genau das ist der Fall, wie das nächste Lemma zeigt.

Lemma 3.3.1. *(a) Sei $a \in \mathbb{Z}$ beliebig, dann ist entweder $a^2 \equiv 0 \mod 4$ oder $a^2 \equiv 1 \mod 4$.*

(b) Ist $n \in \mathbb{N}$ die Summe von zwei Quadratzahlen, dann ist entweder $n \equiv 0 \mod 4$, oder $n \equiv 1 \mod 4$ oder $n \equiv 2 \mod 4$. Im Umkehrschluss gilt dann, dass eine natürliche Zahl $n \in \mathbb{N}$ mit $n \equiv 3 \mod 4$ nicht die Summe von zwei Quadratzahlen ist.

BEWEIS. Der Beweis ist glücklicherweise ganz einfach.

Zu (a): Jede ganze Zahl a ist modulo 4 kongruent zu 0, 1, 2 oder 3. Damit ist a^2 modulo 4 kongruent zu $0^2 = 0$, $1^2 = 1$, $2^2 = 4$ oder $3^2 = 9$. Damit ist das Lemma bewiesen.

Alternativ können Sie das auch ganz elementar einsehen. Falls $a = 2n$ gerade ist, ist $a^2 = 4n^2$ ein Vielfaches von 4, also ist dann $a^2 \equiv 0 \mod 4$. Falls $= 2n + 1$ ungerade ist, ist $a^2 = 4n^2 + 4n + 1 = 4(n^2 + n) + 1$, also ist in diesem Fall $a^2 \equiv 1 \mod 4$.

Zu (b): Wir benutzen nur Teil (a). Sei also $n = a^2 + b^2$ die Summe von zwei Quadratzahlen. Von a^2 und b^2 wissen wir nach (a), dass sie kongruent zu 0 oder 1 modulo 4 sind. Insbesondere ist damit

$$n = a^2 + b^2 \equiv \begin{cases} 0 + 0 \equiv 0 \mod 4 & \text{oder} \\ 0 + 1 \equiv 1 \mod 4 & \text{oder} \\ 1 + 0 \equiv 1 \mod 4 & \text{oder} \\ 1 + 1 \equiv 2 \mod 4 \end{cases}$$

Wir sehen, dass n in keinem Fall kongruent zu 3 modulo 4 ist. Das war zu zeigen.

□

Damit ist die Klassifizierung von Zahlen, die sich als Summe von zwei Quadratzahlen schreiben lassen aber leider noch nicht abgeschlossen. Denn es ist zum Beispiel $21 \equiv 1 \mod 4$ aber man sieht schnell ein, dass 21 nicht die Summe von zwei Quadratzahlen ist. (Es ist $5^2 > 21$, also kommen nur $0^2, 1^2, 2^2, 3^2, 4^2$ als Summanden in Frage. Aber egal welche zwei von diesen Zahlen Sie addieren, es kommt nie 21 heraus.)
Hier kommen nun die Gauß'schen Zahlen ins Spiel! Dazu wiederholen wir nochmal was eine Gauß'sche Zahl eigentlich ist. Jede Gauß'sche Zahl α ist von der Form $\alpha = a + b \cdot i$, mit $a, b \in \mathbb{Z}$ und i erfüllt $i^2 = -1$. Das wichtigste Hilfsmittel für Gauß'sche Zahlen war die *Norm*. Diese war definiert durch

$$N(\alpha) = N(a + b \cdot i) = a^2 + b^2$$

Das ist die Summe von zwei Quadratzahlen! Also ist eine ganze Zahl n *genau dann* die Summe von zwei Quadratzahlen, *wenn* es eine Gauß'sche Zahl α

gibt, mit $N(\alpha) = n$. Wir studieren also die Frage, für welche $n \in \mathbb{N}_0$ es ein $\alpha \in \mathbb{Z}[i]$ gibt, mit $n = N(\alpha)$. Wie angekündigt werden wir dazu die Definition von Primzahlen auf die Gauß'schen Zahlen erweitern.

Eine Primzahl p in $\mathbb{Z}$ erfüllt die Bedingungen $p > 0$, $p \neq 1$ und falls a ein Teiler von p ist, ist $a \in \{\pm 1, \pm p\}$. Die letzte Bedingung lässt sich auch mit

$$a \mid p \quad \Longrightarrow \quad |a| \in \{1, |p|\}$$

beschreiben. Auf $\mathbb{Z}[i]$ können wir fast alles davon verallgemeinern. Der einzige Unterschied ist, dass wir nicht von positiven oder negativen Gauß'schen Zahlen sprechen können.

Definition 3.3.2. Ein $\pi \in \mathbb{Z}[i] \setminus \{0\}$ heißt *prim*, wenn

(i) $\pi \notin \mathbb{Z}[i]^* = \{1, -1, i, -i\}$

(ii) $\alpha \mid \pi \quad \Longrightarrow \quad N(\alpha) \in \{1, N(\pi)\}$

Beispiel 3.3.3. Wir untersuchen ob 2 und 3 prime Gauß'sche Zahlen sind.

(a) Es ist $2 = (1 + i) \cdot (1 - i)$ und $N(1 + i) = 2 \notin \{1, N(2) = 4\}$. Damit ist 2 nicht prim in $\mathbb{Z}[i]$. Allerdings ist $1 + i$ prim, denn: $1 + i \notin \mathbb{Z}[i]^*$ und die Norm jeden Teilers von $1 + i$ muss ein Teiler von $N(1 + i) = 2$ sein – also entweder 1 oder 2.

(b) Ist 3 prim in $\mathbb{Z}[i]$? Dazu nehmen wir einen beliebigen Teiler $a+b\cdot i \in \mathbb{Z}[i]$ von 3. Dann gilt

$$a^2 + b^2 = N(a + b \cdot i) \mid N(3) = 3^2 = 9.$$

Aufgrund der eindeutigen Primfaktorzerlegung in $\mathbb{Z}$ folgt $a^2 + b^2 \in \{1, 3, 9\}$. Aber $a^2 + b^2 = 3$ ist nicht möglich, wie wir gerade gesehen haben. Damit muss $N(a + b \cdot i) \in \{1, 9 = N(3)\}$ gelten. Wir haben gezeigt, dass 3 prim in $\mathbb{Z}[i]$ ist.

Bemerkung 3.3.4. Diese beiden Beispiele betrachten wir etwas genauer. Wie in Teil (a) aus dem obigen Beispiel kann man zeigen: Ist $\alpha \in \mathbb{Z}[i]$ so, dass $N(\alpha) = p$ eine Primzahl ist, dann ist α prim. Den Beweis können Sie selbst als Übung machen.
In Teil (b) haben wir folgendes gesehen: Eine Primzahl $p \in \mathbb{Z}$ hat die Norm $N(p) = p^2$. Damit sind die einzigen positiven Teiler von $N(p)$ die Zahlen 1, p und p^2. Damit gilt für die Norm eines Teilers $\alpha \in \mathbb{Z}[i]$ von p entweder $N(\alpha) = 1$ oder $N(\alpha) = p$ oder $N(\alpha) = p^2$. Wenn es nun keine Gauß'sche Zahl mit Norm p gibt, so bleiben nur noch 1 und $p^2 = N(p)$ übrig! Das heißt für eine Primzahl p gilt:

$$p \text{ ist prim in } \mathbb{Z}[i], \text{ falls es } \underline{\text{kein}} \ \alpha \in \mathbb{Z}[i] \text{ mit } N(\alpha) = p \text{ gibt.} \tag{3.4}$$

Falls es andererseits ein $\alpha \in \mathbb{Z}[i]$ mit $N(\alpha) = p$ gibt, so ist

$$p = N(\alpha) = \alpha \cdot \overline{\alpha}.$$

Also ist in diesem Falle $\alpha \mid p$ und $p = N(\alpha) \notin \{1, N(p)\} = \{1, p^2\}$. Das bedeutet:

$$p \text{ ist } \underline{\text{nicht}} \text{ prim in } \mathbb{Z}[i], \text{ falls es ein } \alpha \in \mathbb{Z}[i] \text{ mit } N(\alpha) = p \text{ gibt.} \tag{3.5}$$

Setzen wir (3.4) und (3.5) zusammen, erhalten wir eine Äquivalenz der beiden Aussagen. Also

$$p \text{ ist prim in } \mathbb{Z}[i] \iff \text{es gibt } \underline{\text{kein}} \ \alpha \in \mathbb{Z}[i] \text{ mit } N(\alpha) = p \text{ gibt.}$$

Am Anfang hatten wir festgestellt, dass eine natürliche Zahl n genau dann die Norm einer Gauß'schen Zahl ist, wenn n die Summe zweier Quadratzahlen ist. Damit erhalten wir für eine Primzahl p:

$$p \text{ ist prim in } \mathbb{Z}[i] \iff p \text{ ist nicht die Summe zweier Quadratzahlen.} \tag{3.6}$$

Wir erhalten damit sofort:

Proposition 3.3.5. *Ist $p \in \mathbb{Z}$ eine Primzahl mit $p \equiv 3 \mod 4$, dann ist p auch prim in den Gauß'schen Zahlen $\mathbb{Z}[i]$.*

Beweis. Sei also p eine Primzahl mit $p \equiv 3 \mod 4$. Dann ist p nach Lemma 3.3.1 nicht die Summe von zwei Quadratzahlen. Mit (3.6) sehen wir sofort, dass daraus folgt, dass p prim in $\mathbb{Z}[i]$ ist. □

Genau wie bei den ganzen Zahlen haben wir eine weitere wichtige Beschreibung von primen Elementen.

Lemma 3.3.6. *Seien $\alpha, \beta, \pi \in \mathbb{Z}[i]$ und sei π prim mit $\pi \mid \alpha \cdot \beta$. Dann gilt $\pi \mid \alpha$ oder $\pi \mid \beta$.*

Beweis. Wir erinnern uns, dass wir auf $\mathbb{Z}[i]$ eine Division mit Rest durchführen können. Damit gibt es auf $\mathbb{Z}[i]$ auch einen Euklidischen Algorithmus. Betrachten wir den Euklidischen Algorithmus rückwärts, erhalten wir, dass auf $\mathbb{Z}[i]$ auch das Lemma von Bézout gilt. Das wollen wir hier ausnutzen. Seien also α, β, π wie in der Voraussaetzung (insbesondere ist $\pi \mid \alpha\beta$). Falls $\pi \mid \alpha$ sind wir sofort fertig. Wir nehmen also an, dass $\pi \nmid \alpha$ ist. Da π prim ist, folgt daraus, dass π und α teilerfremd sind. Jetzt kommt das Lemma von Bézout ins Spiel. Das sagt uns nun, dass es $x, y \in \mathbb{Z}[i]$ gibt, mit $1 = \alpha x + \pi y$. Wir multiplizieren beide Seiten mit β und erhalten

$$\beta = \underbrace{\alpha\beta x}_{\text{Vor.: } \pi \mid \alpha\beta x} + \underbrace{\pi\beta y}_{\pi \mid \pi\beta y}.$$

Mit den elementaren Teilbarkeitsregeln folgt sofort $\pi \mid \beta$. Also haben wir gezeigt, dass tatsächlich $\pi \mid \alpha$ oder $\pi \mid \beta$ gilt. □

Damit haben wir alle Hilfsmittel zur Hand, die in der Vorlesung „Arithmetik“ benutzt wurden um die eindeutige Primfaktorisierung (siehe Theorem 1.1.8) auf $\mathbb{Z}$ zu beweisen. Der gleiche Beweis funktioniert also auch in unserem Setting mit den Gauß'schen Zahlen! Wir kümmern uns hier nicht um die Eindeutigkeit und begnügen uns mit der folgenden Aussage.

Theorem 3.3.7. *Sei $\alpha \in \mathbb{Z}[i]$ mit $N(\alpha) > 1$. Dann gibt es prime Gauß'sche Zahlen $\pi_1, \pi_2, \ldots, \pi_r$ mit*

$$\alpha = \pi_1 \cdot \ldots \cdot \pi_r.$$

Wir kommen zurück zur Beschreibung von primen Gauß'schen Zahlen aus (3.6).

Proposition 3.3.8. *Sei $\pi \in \mathbb{Z}[i]$ prim. Dann gibt es eine Primzahl $p \in \mathbb{Z}$ mit $\pi \mid p$.*

Beweis. Der Beweis ist glücklicherweise sehr kurz. Sei $\pi \in \mathbb{Z}[i]$ prim. Die Norm von π ist eine ganze Zahl und besitzt damit eine Primfaktorzerlegung – sagen wir $N(\pi) = p_1 \cdot \ldots \cdot p_r$ mit $p_1, \ldots, p_r$ Primzahlen. Dann ist

$$\pi \mid \pi \cdot \overline{\pi} = N(\pi) = p_1 \cdot \ldots \cdot p_r.$$

Aus Lemma 3.3.6 folgt, dass π einen der Faktoren $p_1, \ldots, p_r$ teilen muss. Das war zu zeigen. □

Bemerkung 3.3.9. Um alle primen Elemente in $\mathbb{Z}[i]$ zu finden genügt es also Teiler von Primzahlen in $\mathbb{Z}[i]$ zu finden. Wenn eine Primzahl $p \in \mathbb{Z}$ kongruent zu 3 modulo 4 ist, dann ist p prim in $\mathbb{Z}[i]$ (nach Proposition 3.3.5). Wenn eine Primzahl kongruent zu 2 modulo 4 ist, ist sie gerade und somit gleich 2. Wir haben bereits gesehen, dass $2 = (1+i)\cdot(1-i)$ nicht prim in $\mathbb{Z}[i]$ ist. Als nächstes werden wir sehen, dass Primzahlen, die kongruent zu 1 mod 4 sind, ebenfalls nicht prim in $\mathbb{Z}[i]$ sind.

Theorem 3.3.10. *Ist $p \in \mathbb{Z}$ eine Primzahl mit $p \equiv 1 \mod 4$, dann gibt es ein $\pi \in \mathbb{Z}[i]$ mit $N(\pi) = p$. Insbesondere ist p nicht prim in $\mathbb{Z}[i]$.*

Beweis. Wir geben nur die Idee des Beweises anhand eines Beispiels. Wir werden zeigen, dass es ein $\pi \in \mathbb{Z}[i]$ gibt mit $N(\pi) = 13$. Alle Schritte ließen sich auch für den allgemeinen Fall formulieren.

1. Schritt: Es gilt $13 \mid x^2 + 1$ für ein $x \in \mathbb{Z}$.

Der Beweis dieses Schrittes besteht daraus $(13-1)!$ modulo 13 zu berechnen und das auf zwei unterschiedliche Arten. Als erstes rechnen wir wie gewohnt mit Kongruenzen.

$$\begin{aligned}(13-1)! &\equiv \underbrace{12}_{\equiv -1} \cdot \underbrace{11}_{\equiv -2} \cdot \underbrace{10}_{\equiv -3} \cdot \underbrace{9}_{\equiv -4} \cdot \underbrace{8}_{\equiv -5} \cdot \underbrace{7}_{\equiv -6} \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \mod 13 \\ &\equiv (-1)^6 \cdot 6^2 \cdot 5^2 \cdot 4^2 \cdot 3^2 \cdot 2^2 \cdot 1^2 \equiv (6!)^2 \mod 13\end{aligned}$$

Als nächstes berechnen wir $(13-1)!$ modulo 13 mit Restklassen in $\mathbb{Z}/13\mathbb{Z}$. Da 13 eine Primzahl ist, besitzt jedes Element ausser der [0] in $\mathbb{Z}/13\mathbb{Z}$ ein

Inverses (siehe Korollar 1.3.22)!

$$\begin{aligned}[12!] &= [12] \cdot \underbrace{[11]}_{=[6]^{-1}} \cdot \underbrace{[10]}_{=[4]^{-1}} \cdot \underbrace{[9]}_{=[3]^{-1}} \cdot \underbrace{[8]}_{=[5]^{-1}} \cdot \underbrace{[7]}_{=[2]^{-1}} \cdot [6] \cdot [5] \cdot [4] \cdot [3] \cdot [2] \cdot [1] \\ &= [12] \cdot \left([6]^{-1} \cdot [6]\right) \cdot \left([5]^{-1} \cdot [5]\right) \cdot \left([4]^{-1} \cdot [4]\right) \cdot \left([3]^{-1} \cdot [3]\right) \cdot \left([2]^{-1} \cdot [2]\right) \cdot [1] \\ &= [12] = [-1]\end{aligned}$$

Mit Kongruenzen formuliert ergibt sich $12! \equiv -1 \mod 13$. Setzen wir diese beiden Teile zusammen erhalten wir

$$-1 \equiv 12! \equiv (6!)^2 \mod 13,$$

was nichts anderes bedeutet als $13 \mid (6!)^2 + 1$. Damit ist der erste Schritt bewiesen.
Allgemein kann man mit exakt den gleichen Argumenten zeigen, dass $p \mid \left(\frac{p-1}{2}!\right)^2 + 1$ für alle Primzahlen $p \equiv 1 \mod 4$ gilt.

2. Schritt: Es gibt ein $\pi \in \mathbb{Z}[i]$ mit $N(\pi) = 13$.

Angenommen es gäbe kein solches $\pi \in \mathbb{Z}[i]$. Dann wäre, wie in (3.4) festgestellt, 13 eine prime Gauß'sche Zahl. Aus dem ersten Schritt wissen wir $13 \mid (6!)^2 + 1$. Dieses $(6!)^2 + 1$ wollen wir nun als Produkt schreiben. In den ganzen Zahlen wäre das recht kompliziert, aber wir haben ja glücklicherweise die Gauß'schen Zahlen zur Hand. Wir können also mit einem schönen Trick die dritte binomische Formel benutzen:

$$13 \mid (6!)^2 + 1 = (6!)^2 - i^2 = (6! + i) \cdot (6! - i).$$

Da wir annehmen dass 13 prim ist, muss daraus folgen (vgl. Lemma 3.3.6), dass $13 \mid 6! + i$ oder $13 \mid 6! - i$ gilt. Dann wäre $\frac{6!}{13} + \frac{1}{13}i \in \mathbb{Z}[i]$ oder $\frac{6!}{13} - \frac{1}{13}i \in \mathbb{Z}[i]$. Da aber offensichtlich $\frac{1}{13}$ keine ganze Zahl ist, ist das nicht der Fall. Damit haben wir einen Widerspruch gefunden, was bedeutet, dass unsere Annahme falsch gewesen ist. D.h. es gibt ein $\pi \in \mathbb{Z}[i]$ mit $N(\pi) = 13$. □

Bemerkung 3.3.11. Wir fassen alles was wir über prime Gauß'sche Zahlen herausgefunden haben zusammen:

(a) Eine Primzahl $p > 2$ ist genau dann die Summe von zwei Quadratzahlen, wenn $p \equiv 1 \mod 4$ ist.

(b) Ist $\pi \in \mathbb{Z}[i]$ prim, dann gilt genau eine der folgenden Aussagen:

- $N(\pi) = 2$ oder
- $N(\pi) = p$ für eine Primzahl $p \equiv 1 \mod 4$ oder
- $N(\pi) = p^2$ für eine Primzahl $p \equiv 3 \mod 4$.

Das war bis hierhin viel Theorie. Es ist nun Zeit für eine Anwendung – also für das nächste Beispiel wieder auf volle Konzentration schalten.

Beispiel 3.3.12. Wir überprüfen ein paar Zahlen ob sie sich als Summe von zwei Quadratzahlen schreiben lassen.

(a) Was ist mit 2020? Wir zerlegen die Zahl zunächst in Primfaktoren in $\mathbb{Z}$: $2020 = 2^2 \cdot 5 \cdot 101$. Es ist $5 \equiv 101 \equiv 1 \mod 4$. Damit lassen sich 5 und 101 als Summe von zwei Quadraten schreiben. Das machen wir explizit:

$$5 = 1^2 + 2^2 \qquad 101 = 10^2 + 1^2 \qquad 2^2 = 2^2 + 0^2.$$

Mit Gauß'schen (Prim-)Zahlen erhalten wir

$$5 = N(1 + 2i) \qquad 101 = N(10 + i) \qquad 2^2 = N(2).$$

Damit erhalten wir

$$\begin{aligned} 2020 &= 2^2 \cdot 5 \cdot 101 = N(2) \cdot N(1 + 2i) \cdot N(10 + i) \\ &\overset{3.2.9}{=} N(2 \cdot (1 + 2i) \cdot (10 + i)) = N(2 \cdot (8 + 21i)) = N(16 + 42i) \\ &= 16^2 + 42^2. \end{aligned}$$

Wir wissen also nicht nur, dass 2020 die Summe von zwei Quadratzahlen ist, wir finden auch ohne Mühe (und ohne Taschenrechner) die passenden Summanden. Diese Darstellung ist natürlich nicht eindeutig. Wir könnten z.B. genau so gut mit $5 = N(2 + i)$ arbeiten. Damit erhalten wir dann

$$\begin{aligned} 2020 &= 2^2 \cdot 5 \cdot 101 = N(2) \cdot N(2 + i) \cdot N(10 + i) \\ &\overset{3.2.9}{=} N(2 \cdot (2 + i) \cdot (10 + i)) = N(2 \cdot (19 + 12i)) = N(38 + 24i) \\ &= 38^2 + 24^2. \end{aligned}$$

(b) Was ist mit 754? Wir machen genau das gleiche wie eben. PFZ: $754 = 2 \cdot 13 \cdot 29$. Jetzt müssen wir nur noch die einzelnen Faktoren als Summe von zwei Quadraten schreiben:

$$2 = 1^2 + 1^2 \qquad 13 = 2^2 + 3^2 \qquad 29 = 5^2 + 2^2.$$

Damit erhalten wir

$$\begin{aligned} 754 = 2 \cdot 13 \cdot 29 &= N(1+i) \cdot N(2+3i) \cdot N(5+2i) \\ &\overset{3.2.9}{=} N((1+i) \cdot (2+3i) \cdot (5+2i)) = N((1+i) \cdot (4+19i)) \\ &= N(-15+23i) = 15^2 + 23^2. \end{aligned}$$

(c) Was ist mit 3030? Die Primfaktorisierung ist $3030 = 2 \cdot 3 \cdot 5 \cdot 101$. Hier kommt nun die *böse* Primzahl 3 vor. Angenommen wir hätten $3030 = a^2 + b^2$. Dann wäre $3030 = N(a + bi)$. Wir wissen, dass $a + bi$ eine Faktorisierung in prime Gauß'sche Zahlen besitzt – sagen wir $a + bi = \pi_1 \cdot \ldots \cdot \pi_r$. Dann ist

$$3030 = N(\pi_1 \cdot \ldots \cdot \pi_r) = N(\pi_1) \cdot \ldots \cdot N(\pi_r).$$

Also muss eines dieser primen Elemente ein Teiler von 3 sein. Aber dann ist die Norm von diesem Element gleich 9. Damit wäre 3030 ebenfalls durch 9 teilbar! Aber das ist nicht der Fall! Damit sorgt die *böse* Primzahl 3 dafür, dass sich 3030 NICHT als Summe von zwei Quadratzahlen schreiben lässt.

(d) Was ist mit 245? PFZ: $245 = 5 \cdot 7^2$. Wieder kommt eine *böse* Primzahl 7 (d.h. $7 \equiv 3 \mod 4$) vor. Der große Unterschied besteht darin, dass diese Primzahl mit einem geraden Exponenten vorkommt! Es ist nun wie immer

$$5 = N(1+2i) \qquad 7^2 = N(7)$$

und somit $245 = N((1+2i) \cdot 7) = N(7+14i) = 7^2 + 14^2$.

(e) Was ist nun schließlich mit 2021? Die Primfaktorzerlegung erhalten wir ganz schnell wenn wir nach großen Primteilern suchen: $2021 = 43 \cdot 47$.[1]

[1] fun fact: 2021 ist das einzige Jahr, das wir erleben werden, dass das Produkt von aufeinander folgenden Primzahlen ist. Das nächste solche Jahr ist erst $2310 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$.

Beide Primzahlen 43 und 47 sind *böse* und kommen mit ungeradem Exponenten vor. Damit lässt sich 2021 nicht als Summe von zwei Quadratzahlen schreiben: Ansonsten wäre $2021 = N(a+bi)$ und $a+bi$ hätte einen Primteiler der die 43 teilt. Damit wäre aber $N(a+bi)$ durch die Norm dieses Primteilers – also durch 43^2 – teilbar. Das ist nicht der Fall!

Wenn wir die Argumente in diesen Beispielen allgemein formulieren (worauf wir hier verzichten) erhalten wir das folgende Theorem.

Theorem 3.3.13. *Eine Zahl $n \in \mathbb{N}$ ist genau dann die Summe von zwei Quadraten, wenn jeder Primteiler p von n, mit $p \equiv 3 \mod 4$, in der Primfaktorzerlegung von n mit einem geraden Exponenten vorkommt.*

Damit haben wir endlich eine Charakterisierung von natürlichen Zahlen gefunden, die die Summe von zwei Quadratzahlen sind. Die Formulierung des Theorems ist ganz elementar und hätte auch ohne viel Vorwissen formuliert werden können. Das entscheidende Hilfsmittel um dieses Theorem zu erhalten, war aber die Primfaktorzerlegung auf den Gauß'schen Zahlen!

Kapitel 4

Arithmetik und Geometrie

Ursprünglich wurde nicht mit Zahlen sondern mit geometrischen Größen wie Längen, Flächeninhalten, usw. gerechnet. Es ist daher nicht verwunderlich, dass Zahlentheorie manchmal sehr eng mit Geometrie verknüpft ist.

4.1 Pythagoräische Zahlentripel

Die Frage die wir klären wollen ist die folgende: Welche drei ganzen Zahlen a, b, c können die Seitenlängen eines rechtwinkligen Dreiecks bilden?
Ist c die Länge der Hypothenuse (der längsten Seite) eines rechtwinkligen Dreiecks, so gilt, wie wir alle wissen, $a^2 + b^2 = c^2$. Ein Beispiel ist $a = 3$, $b = 4$, $c = 5$, denn dann gilt $3^2 + 4^2 = 25 = 5^2$. Damit finden wir viele weitere Beispiel. Denn ist $d \in \mathbb{N}$ irgendeine Zahl, so gilt

$$(3 \cdot d)^2 + (4 \cdot d)^2 = (3^2 + 4^2) \cdot d^2 = 5^2 \cdot d^2 = (5 \cdot d)^2.$$

Das entspricht genau dem Strecken des Dreiecks mit den Seitenlängen 3, 4 und 5 um den Faktor d.

Abbildung 4.1: *Pythagoras* (ca. 570 – 510 v.Chr.) war Begründer einer einflussreichen mathematisch-religiösen Bewegung. Es ist umstritten, welcher dieser Teile von Pythagoras am meisten geprägt wurde. Er selbst bezeichnete sich (möglicherweise als erster überhaupt) als Philosoph, was mit „Freund der Weisheit“ übersetzt werden kann. Pythagoras war in manchen Punkten recht modern: Er gilt als einer der ersten Vegetarier und Frauen hatten in seiner Bewegung dieselben Rechte wie Männer.

Definition 4.1.1. Ein Tripel (a, b, c) aus drei natürlichen Zahlen heißt *Pythagoräisches Zahlentripel*, falls $a^2 + b^2 = c^2$ gilt.

Wir haben gerade gesehen, dass $(3, 4, 5)$ ein Pythagoräisches Zahlentripel ist, und dass damit auch $(6, 8, 10)$, $(9, 12, 15)$, $(12, 16, 20)$, ... Pythagoräische Zahlentripel sind. Es gibt aber noch viele weitere. Wir werden hier ein Verfahren kennenlernen, mit dem wir alle Pythagoräischen Zahlentripel erzeugen können.

Abbildung 4.2: Die Konstruktion von Pythagoräischen Zahlentripeln war schon lange vor Pythagoras bekannt. Auf der Tontafel *Plimpton 322* von ca. 1800 v.Chr. stehen 15 Pythagoräische Zahlentripel – unter anderem $(12709, 13500, 18541)$. Vermutlich stammt diese Tontafel aus dem heutigen Irak.

Bemerkung 4.1.2. Sei (a, b, c) ein Pythagoräisches Zahlentripel.

- Es ist dann natürlich auch (b, a, c) ein Pythagoräisches Zahlentripel. Um das zu sehen können wir entweder das zugehörige rechtwinkelige Dreieck einfach Spiegeln (Katheten vertauschen), oder wir bemerken schlicht, dass aus $a^2 + b^2 = c^2$ natürlich auch $b^2 + a^2 = c^2$ folgt.

- Falls ein $d \in \mathbb{N}$ existiert, mit $d \mid a$, $d \mid b$ und $d \mid c$, dann ist auch $(\frac{a}{d}, \frac{b}{d}, \frac{c}{d})$ ein Pythagoräisches Zahlentripel. Denn erstens sind dann nach Voraussetzung alle drei Einträge natürliche Zahlen, und zweitens gilt

$$(\frac{a}{d})^2 + (\frac{b}{d})^2 = \frac{a^2 + b^2}{d^2} \overset{\text{Def.}}{=} \frac{c^2}{d^2} = (\frac{c}{d})^2$$

Den letzten Punkt dieser Bemerkung können wir noch leicht vereinfachen.

Lemma 4.1.3. *Ist (a, b, c) ein Pythagoräisches Zahlentripel und ist $d \in \mathbb{N}$ ein gemeinsamer Teiler von a und b. Dann ist auch $(\frac{a}{d}, \frac{b}{d}, \frac{c}{d})$ ein Pythagoräisches Zahlentripel.*

Beweis. Das sieht eigentlich genau aus wie der zweite Punkt aus Bemerkung 4.1.2. Der einzige Unterschied ist, dass d nur ein gemeinsamer Teiler von a und b sein muss. Alles was wir tun müssen ist also zu zeigen, dass

dann bereits automatisch $d \mid c$ gilt. Das beweisen wir so:

$$\begin{aligned} d \mid a \text{ und } d \mid b \quad &\Longrightarrow \quad d^2 \mid a^2 \text{ und } d^2 \mid b^2 \\ &\Longrightarrow \quad d^2 \mid a^2 + b^2 \overset{(a,b,c) \text{ ist PZT}}{=} c^2 \\ &\Longrightarrow \quad d \mid c. \end{aligned}$$

Es gilt also bereits, dass d ein gemeinsamer Teiler von a, b *und* c ist, wenn wir nur voraussetzen, dass d ein geminsamer Teiler von a und b ist. Jetzt greift Bemerkung 4.1.2 und wir sind fertig. □

Durch Vertauschen von a und b sowie durch Division mit dem größten gemeinsamen Teiler von a und b können wir also stets ein Pythagoräisches Zahlentripel (a', b', c') erhalten mit

(i) $\mathrm{ggT}(a', b') = 1$, und

(ii) a' ist ungerade. (Es können nicht a' und b' beide gerade sein, da sie sonst den gemeinsamen Teiler zwei hätten, im Widerspruch zu (i). Da wir die ersten zwei Einträge vertauschen dürfen, können wir also immer dafür sorgen, dass der erste Eintrag ungerade ist.)

Definition 4.1.4. Ein Pythagoräisches Zahlentripel (a, b, c), dass die Bedingungen aus (i) und (ii) erfüllt, heißt *primitiv*. D.h.: ein Pythagoräisches Zahlentripel (a, b, c) ist *primitiv*, wenn gilt

(i) $\mathrm{ggT}(a, b) = 1$, und

(ii) a ist ungerade.

Wie oben bemerkt, kann jedes Pythagoräische Zahlentripel auf ein primitives Tripel zurückgeführt werden. Z.B. ist das Pythagoräische Zahlentripel $(4, 3, 5)$ nicht primitiv, da der erste Eintrag gerade ist und $(9, 12, 15)$ ist nicht primitiv, da die ersten beiden (und damit alle drei) Einträge den gemeinsamen Teiler 3 besitzen.

Beispiel 4.1.5. Wir betrachten das Pythagoräische Zahlentripel $(24, 10, 26)$. Dies ist datsächlich ein Pythagoräisches Zahlentripel, da die Gleichung $24^2 + 10^2 = 26^2$ mit einem Taschenrechner schnell verifiziert ist. Es ist nicht primitiv! Welches primitive Pythagoräische Zahlentripel können wir aus

$(24, 10, 26)$ generieren? Als erstes sehen wir, dass $\text{ggT}(24, 10) = 2$ ist. Wir erhalten also das Zahlentripel $(\frac{24}{2}, \frac{10}{2}, \frac{26}{2}) = (12, 5, 13)$. Das ist immer noch nicht primitiv, da der erste Eintrag gerade ist. Vertauschen der ersten beide Einträge liefert nun das primitive Pythagoräische Zahlentripel $(5, 12, 13)$.

Lemma 4.1.6. *Ist (a, b, c) ein primitives Pythagoräisches Zahlentripel, so sind a und c ungerade.*

Beweis. Wir wissen bereits (vgl. Lemma 3.3.1), dass gilt

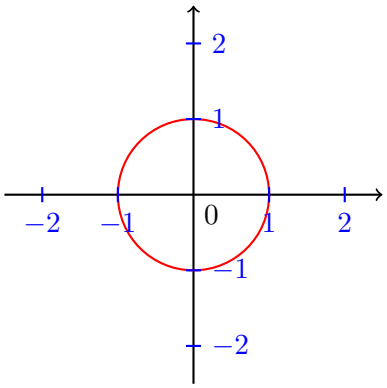
- jede gerade Quadratzahl ist kongruent zu 0 modulo 4, und
- jede ungerade Quadratzahl ist kongruent zu 1 modulo 4.

Da (a, b, c) primitiv ist, ist a ungerade. Wäre auch b ungerade, so wäre

$$c^2 \equiv a^2 + b^2 \equiv 1 + 1 \equiv 2 \mod 4,$$

was nicht sein kann. Also wissen wir, dass b gerade ist. Nun ist $c^2 = a^2 + b^2$ die Summe, von einer geraden (b^2) und einer ungeraden (a^2) Zahl – also ungerade. Damit ist natürlich auch c ungerade. Das war zu zeigen. □

Bis hier hin haben wir uns mit Dreiecken beschäftigt, auch wenn diese nur formalisiert (und nicht graphisch) aufgetaucht sind. Jetzt starten wir mit einer weiteren schönen geometrischen Figur: dem Kreis!
Genauer betrachten wir den Kreis mit Radius 1 um den Nullpunkt in einem Koordinatensystem.



Wir bezeichnen diesen Kreis mit K. Ein Punkt (x/y) mit $x, y \in \mathbb{R}$, liegt genau dann auf K, wenn der Abstand von (x/y) zum Punkt $(0/0)$ gleich 1 ist. Wie wir den Abstand berechnen, wissen wir aber alle bestens – er ist gegeben durch $\sqrt{x^2+y^2}$. Der Punkt (x/y) liegt also genau dann auf K, wenn $\sqrt{x^2+y^2} = 1$ ist. Das ist genau dann der Fall, wenn $x^2+y^2 = 1$ ist. Wir sagen auch, dass K durch die Gleichung $x^2+y^2 = 1$ beschrieben wird. Wir sehen, dass z.B. die Punkte $(-1/0)$, $(0,1)$, $(\frac{1}{\sqrt{2}}/\frac{1}{\sqrt{2}})$, $(\frac{1}{2}/\frac{\sqrt{3}}{2})$, $(\frac{3}{5}/\frac{4}{5})$ auf K liegen. Spoiler: Der Punkt $(\frac{3}{5}/\frac{4}{5})$ sollte Ihnen verdächtig bekannt vorkommen!

Definition 4.1.7. Ein Punkt (x/y) auf K heißt *rational*, wenn x und y rationale Zahlen sind.

Die Punkte $(-1,0)$ und $(\frac{3}{5}/\frac{4}{5})$ sind rationale Punkte. Die Punkte $(\frac{1}{\sqrt{2}}/\frac{1}{\sqrt{2}})$ und $(\frac{1}{2}/\frac{\sqrt{3}}{2})$ sind keine rationalen Punkte, da $\sqrt{2}$ und $\sqrt{3}$ nicht in $\mathbb{Q}$ liegen.

Satz 4.1.8. *Ist (a,b,c) ein Pythagoräisches Zahlentripel, so ist $(\frac{a}{c}/\frac{b}{c})$ ein rationaler Punkt auf K.*

Beweis. Natürlich sind $\frac{a}{c}$ und $\frac{b}{c}$ rational. Die Aussage folgt nun sofort aus der folgenden Rechnung.

$$(\frac{a}{c})^2 + (\frac{b}{c})^2 = \frac{a^2+b^2}{c^2} = \frac{c^2}{c^2} = 1.$$

□

Jedes Pythagoräische Zahlentripel liefert uns also einen rationalen Punkt auf K. Andersherum funktioniert das auch.

Satz 4.1.9. *Sind $a,b,c \in \mathbb{N}$ so, dass $(\frac{a}{c}/\frac{b}{c})$ ein rationaler Punkt auf K ist, dann ist (a,b,c) ein Pythagoräisches Zahlentripel.*

Beweis. Nach Voraussetzung sind a, b, c natürliche Zahlen. Wir müssen also nur $a^2+b^2 = c^2$ überprüfen. Das geht so:

$$a^2+b^2 = c^2 \cdot \left(\frac{a^2+b^2}{c^2}\right) = c^2 \cdot \left(\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2\right) = c^2 \cdot 1 = c^2.$$

Damit ist die Behauptung bewiesen. □

Hier haben wir den eingangs erwähnten Zusammenhang zur Geometrie. Nehmen wir die Sätze 4.1.8 uns 4.1.9 zusammen, so sehen wir, dass jedes Pythagoräische Zahlentripel einen rationalen Punkt auf K liefert, und jeder rationale Punkt auf K liefert ein Pythagoräisches Zahlentripel. Alle Pythagoräischen Zahlentripel zu bestimmen ist also im wesentlichen das gleiche wie alle rationalen Punkte auf K zu bestimmen!

Unser Ziel ist es nun alle rationalen Punkte auf K zu bestimmen!

Konstruktion 4.1.10. Es ist $P = (-1/0)$ ein rationaler Punkt auf K. Ab jetzt wird mit P immer dieser Punkt beschrieben! Sei (α/β) ein weiterer rationaler Punkt auf K, der verschieden ist von P. Die Gerade zwischen P und (α/β) hat die Steigung $\frac{\beta}{\alpha+1}$. Da $\alpha, \beta \in \mathbb{Q}$ gilt, ist diese Steigung ebenfalls in $\mathbb{Q}$!

Wieder drehen wir den Spieß um.

Konstruktion 4.1.11. Sei wie eben $P = (-1/0)$. Jetzt starten wir mit einer Geraden durch P, die eine Steigung $s \in \mathbb{Q}$ besitzt. Diese Gerade bezeichnen wir mit g_s. Dieses g_s schneidet den Kreis K in einem weiteren Punkt Q. Wir behaupten, dass dieser Punkt Q ein rationaler Punkt ist.
Um den Schnittpunkt zu berechnen brauchen wir die Geradengleichung von g_s. Wahrscheinlich erinnern Sie sich dunkel daran, dass diese von der Form

$$g_s : y = (\text{irgendwas}) \cdot x + (\text{noch irgendwas})$$

ist. Bei weiterem Herumkramen in Ihrem Schulwissen können Sie das etwas präziser als

$$g_s : y = (\text{Steigung}) \cdot x + (\text{noch irgendwas})$$

schreiben. Die Steigung von g_s kennen wir aber. Wir haben sie einfach s genannt. Damit ist die Geradengleichung gegeben durch

$$g_s : y = s \cdot x + (\text{noch irgendwas})$$

Als letztes wissen wir noch, dass der Punkt $P = (-1/0)$ auf der geraden liegt. Damit muss also gelten $0 = s \cdot (-1) + (\text{noch irgendwas})$. Diese *noch irgendwas* muss also ebenfalls gleich s sein. Wir erhalten nun endlich die Geradengleichung

$$g_s : y = s \cdot x + s$$

Die Schnittpunkte von g_s mit dem Kreis K sind also genau die Punkte (x/y), die sowohl

(I) $y = s \cdot x + s$ (der Punkt liegt auf der Geraden), als auch

(II) $x^2 + y^2 = 1$ (der Punkt liegt auf dem Kreis)

erfüllen. Um diese Punkte auszurechnen setzen wir einfach (I) in (II) ein und erhalten

$$\begin{aligned}
& x^2 + (sx + s)^2 = 1 \\
\iff \quad & (s^2+1)x^2 + 2s^2x + (s^2 - 1) = 0 \\
\iff \quad & x^2 + \frac{2s^2}{s^2+1}x + \frac{s^2-1}{s^2+1} = 0 \\
\iff \quad & (x + \frac{s^2}{s^2+1})^2 - \left(\frac{s^2}{s^2+1}\right)^2 + \frac{s^2-1}{s^2+1} = 0 \\
\iff \quad & x + \frac{s^2}{s^2+1} = \pm\sqrt{\left(\frac{s^2}{s^2+1}\right)^2 - \frac{s^2-1}{s^2+1}} = \pm\frac{1}{s^2+1} \\
\iff \quad & x = -1 \quad \text{oder} \quad x = \frac{1-s^2}{1+s^2}
\end{aligned}$$

Um nun die Schnittpunkte von g_s und K zu erhalten, müssen wir nur noch die ermittelten x-Werte in Gleichung (I) einsetzen. Wir erhalten, dass die Schnittpunkte genau die Punkte

$$P = (-1/0) \text{ (na klar!)} \qquad \text{und} \qquad Q = (\frac{1-s^2}{1+s^2}/\frac{2s}{1+s^2})$$

sind. Da $s \in \mathbb{Q}$ ist, ist der gefundene Schnittpunkt Q wie gewünscht ein rationaler Punkt!

Fazit 4.1.12. *Alle* rationalen Punkte auf K sind gegeben durch $P = (-1/0)$ und die Schnittpunkte von K mit den Geraden g_s, mit $s \in \mathbb{Q}$. Für diese Schnittpunkte haben wir eben sogar eine Formel berechnet! Wir sehen, dass alle rationalen Punkte auf K gegeben sind durch $P = (-1/0)$ und Punkte der Form $(\frac{1-s^2}{1+s^2}/\frac{2s}{1+s^2})$, mit $s \in \mathbb{Q}$.

Beispiel 4.1.13.

- Wir wählen $s = \frac{1}{2}$. Dann erhalten wir den rationalen Punkt
$$(\frac{1-(\frac{1}{2})^2}{1+(\frac{1}{2})^2}/\frac{2\cdot\frac{1}{2}}{1+(\frac{1}{2})^2}) = (\frac{3}{5}/\frac{4}{5}).$$
Das bedeutet $(\frac{3}{5})^2 + (\frac{4}{5})^2 = 1$. Multiplizieren wir beide Seiten mit 5^2 erhalten wir die Gleichung $3^2 + 4^2 = 5^2$ und somit das Pythagoräische Zahlentripel $(3, 4, 5)$.

- Für $s = \frac{1}{3}$ erhalten wir den Punkt
$$(\frac{1-(\frac{1}{3})^2}{1+(\frac{1}{3})^2}/\frac{2\cdot\frac{1}{3}}{1+(\frac{1}{3})^2}) = (\frac{4}{5}/\frac{3}{5}).$$
Daraus lesen wir das Pythagoräische Zahlentripel $(4, 3, 5)$ ab.

- Für $s = \frac{2}{3}$ erhalten wir den Punkt
$$(\frac{1-(\frac{2}{3})^2}{1+(\frac{2}{3})^2}/\frac{2\cdot\frac{2}{3}}{1+(\frac{2}{3})^2}) = (\frac{5}{13}/\frac{12}{13}),$$
also das Pythagoräische Zahlentripel $(5, 12, 13)$.

- Natürlich können wir auch etwas kompliziertere rationale Zahlen wählen. Für $s = \frac{7}{94}$ erhalten wir den Punkt
$$(\frac{1-(\frac{7}{94})^2}{1+(\frac{7}{94})^2}/\frac{2\cdot\frac{7}{94}}{1+(\frac{7}{94})^2}) = (\frac{8787}{8885}/\frac{1316}{8885}).$$
Damit haben wir das Pythagoräische Zahlentripel $(8787, 1316, 8885)$ gefunden!

Bemerkung 4.1.14. Jedes $s \in \mathbb{Q}$ können wir als gekürzten Bruch darstellen. Wir setzen daher $s = \frac{k}{n}$ mit $k, n \in \mathbb{Z}$, $n \in \mathbb{N}$ und $\mathrm{ggT}(k, n) = 1$. Es folgt, dass jeder rationale Punkt außer $P = (-1/0)$ von der Form

$$(\frac{1-(\frac{k}{n})^2}{1+(\frac{k}{n})^2}/\frac{2\cdot\frac{k}{n}}{1+(\frac{k}{n})^2}) = (\frac{n^2-k^2}{n^2+k^2}/\frac{2kn}{n^2+k^2}) \tag{4.1}$$

ist. Weiter wissen wir, dass wir alle Pythagoräischen Zahlentripel aus diesen Punkten konstruieren können. Wir haben schon eingesehen, dass wir uns dazu auf primitive Pythagoräische Zahlentripel einschränken dürfen.

Wie können wir nun aus (4.1) alle primitiven Pythagoräischen Zahlentripel herleiten? Ein erster Versuch ist genau wie in Beispiel 4.1.13 den Punkt mit $(k^2+n^2)^2$ „zu multiplizieren“. Dann erhalten wir die Gleichung

$$(n^2-k^2)^2+(2kn)^2=(n^2+k^2)^2.$$

Der Verdacht ist also, dass $(n^2-k^2, 2kn, n^2+k^2)$ ein primitives Pythagoräisches Zahlentripel liefert. Da alle Einträge natürliche Zahlen sein müssen, muss gelten $n>k\geq 1$.
Weiter muss bei einem primitiven Pythagoräischen Zahlentripel der erste Eintrag ungerade sein (siehe Lemma 4.1.6). Damit dürfen n und k nicht beide gerade oder beide ungerade sein. Es muss also $n \not\equiv k \mod 2$ gelten. Wir werden nun abschließend zeigen (zusammenfassen), dass diese notwendigen (mit rot markierten Bedingungen) schon aussreichend sind. Wir werden also das folgende Theorem beweisen.

Theorem 4.1.15. *Drei natürliche Zahlen a,b,c bilden genau dann ein primitives Pythagoräisches Zahlentripel, wenn es natürliche Zahlen k,n gibt mit den folgenden Bedingungen*

(i) $a=n^2-k^2$, $b=2kn$ *und* $c=n^2+k^2$

(ii) $\mathrm{ggT}(k,n)=1$

(iii) $n>k$

(iv) $n\not\equiv k \mod 2$.

Wir gehen jetzt den Beweis von Theorem 4.1.15 an. Wir haben hier eine „genau-dann-wenn“-Aussage. Das bedeutet, dass zwei Implikationen gezeigt werden müssen. Wir zeigen hier, dass sich jedes primitive Pythagoräische Zahlentripel (a,b,c) durch Elemente n und k der beschriebenen Form darstellen lässt. Die andere Richtung, dass für n und k, wie im Theorem tatsächlich auch (a,b,c) ein primitives Pythagoräisches Zahlentripel ist, zeigen Sie als Übung.
Wir starten mit einem Lemma.

Lemma 4.1.16. *Sind* $n, k \in \mathbb{Z}$ *mit* $n \not\equiv k \mod 2$ *und* $\mathrm{ggT}(n,k) = 1$, *dann ist* $\mathrm{ggT}(n^2-k^2, n^2+k^2) = 1$.

Beweis. Angenommen, es wäre $\mathrm{ggT}(n^2-k^2, n^2+k^2) > 1$. Dann gibt es einen gemeinsamen Teiler von n^2-k^2 und n^2+k^2 der größer als 1 ist. Insbesondere gibt es eine Primzahl p, mit$p \mid n^2-k^2$ und $p \mid n^2+k^2$. Da n^2 und k^2 nicht beide gerade oder beide ungerade sein können, ist n^2-k^2 auf jeden Fall ungerade. Wir wissen also, dass $p \neq 2$ ist! Jetzt folgern wir:

$$\begin{aligned}
& p \mid n^2-k^2 \quad \text{und} \quad p \mid n^2+k^2 \\
\Longrightarrow \quad & p \mid (n^2-k^2)+(n^2+k^2) = 2n^2 \quad \text{und} \quad p \mid (n^2+k^2)-(n^2-k^2) = 2k^2 \\
\overset{p\neq 2}{\Longrightarrow} \quad & p \mid n^2 \quad \text{und} \quad p \mid k^2 \\
\Longrightarrow \quad & p \mid n \quad \text{und} \quad p \mid k
\end{aligned}$$

Damit müsste p ein gemeinsamer Teiler von n und k sein. Da n und k aber nach Voraussetzung teilerfremd sind, ist das ein Widerspruch. Unsere Annahme $\mathrm{ggT}(n^2-k^2, n^2+k^2) > 1$ muss also falsch gewesen sein. Damit gilt wie gewünscht $\mathrm{ggT}(n^2-k^2, n^2+k^2) = 1$ und das Lemma ist bewiesen. □

Beweis von Theorem 4.1.15. Wie angekündigt starten wir mit einem primitiven Pythagoräischen Zahlentripel (a,b,c) und wollen von dort aus natürliche Zahlen n und k finden, die die Bedingungen (i), (ii), (iii) und (iv) aus Theorem 4.1.15 erfüllen.
Wir wissen bereits, dass wir mit unserem Tripel (a,b,c) einen rationalen Punkt $(\frac{a}{c}/\frac{b}{c})$ erhalten. Wir wissen, dass $b \neq 0$ ist. Damit ist dieser rationale Punkt nicht gleich $(-1/0)$. Es gibt also nach (4.1) ganze Zahlen n und k mit $n \in \mathbb{N}$, $\mathrm{ggT}(n,k) = 1$ (Bedingung (ii): ✓) und

$$(\frac{a}{c}/\frac{b}{c}) = (\frac{n^2-k^2}{n^2+k^2}/\frac{2kn}{n^2+k^2}). \tag{4.2}$$

Da $a,b,c \in \mathbb{N}$ ist, gilt $0 < \frac{b}{c} \overset{(4.2)}{=} \frac{2kn}{n^2+k^2}$. Das bedeutet gerade $0 < 2kn$. Da wir schon wissen, dass $n \in \mathbb{N}$ ist, folgt damit, dass auch $k \in \mathbb{N}$ ist. Bei n und k handelt es sich also tatsächlich um natürliche Zahlen.
Genauso impliziert $0 < \frac{a}{c} \overset{(4.2)}{=} \frac{n^2-k^2}{n^2+k^2}$ die Ungleichung $0 < n^2-k^2$. Es ist also $n^2 > k^2$ und da $n,k \in \mathbb{N}$ ist, muss damit auch $n > k$ gelten (Bedingung (iii): ✓).

Aus der Gleichung $\frac{a}{c} \overset{(4.2)}{=} \frac{n^2-k^2}{n^2+k^2}$ schließen wir $a \cdot (n^2+k^2) = c \cdot (n^2-k^2)$. Wir wissen bereits, dass n und k teilerfremd sind. Insbesondere können nicht beide Zahlen gerade sein. Angenommen beide Zahlen wären ungerade. Dann wäre mit der letzten Gleichung

$$2a \equiv a(1+1) \equiv a(n^2+k^2) \equiv c(n^2-k^2) \equiv c(1-1) \equiv 0 \mod 4.$$

Hier haben wir wieder einmal benutzt, dass das Quadrat einer ungeraden Zahl immer kongruent zu 1 modulo 4 ist. Es folgt nun, dass $4 \mid 2a$ ist – also $2 \mid a$. Das widerspricht aber der Tatsache, dass a (als erster Eintrag eines *primitiven* Pythagoräischen Zahlentripels) ungerade ist. Ein Widerspruch bedeutet, dass wir irgendwo eine falsche Annahme getroffen haben. Die einzige Annahme die wir getroffen haben war, dass n und k beide ungerade sind. Das heißt: n und k sind nicht beide ungerade! Da sie auch nicht beide gerade sind, folgt $n \not\equiv k \mod 2$ (Bedingung (iv): ✓).
Um auch den letzten Punkt zu zeigen bemerken wir, dass $\frac{a}{c}$ gekürzt ist, da a und c Einträge eines primitiven Pythagoräischen Zahlentripels sind. Weiter ist mit Lemma 4.1.16 auch $\frac{n^2-k^2}{n^2+k^2}$ gekürzt, da wir bereits wissen, dass $\mathrm{ggT}(n,k) = 1$ und $n \not\equiv k \mod 2$ ist. Aber wieviele Arten gibt es einen Bruch als gekürzten Bruch zuschreiben? Eine! D.h.: Aus der Gleichung $\frac{a}{c} \overset{(4.2)}{=} \frac{n^2-k^2}{n^2+k^2}$ folgt tatsächlich $a = n^2-k^2$ und $c = n^2+k^2$. Damit erhalten wir aber sofort

$$\frac{b}{c} \overset{(4.2)}{=} \frac{2kn}{n^2+k^2} = \frac{2nk}{c},$$

also $b = 2nk$ (Bedingung (i): ✓). Damit ist das Theorem bewiesen! □

Anhang A

Kettenbrüche

Alles Folgende ist nur für HRG-Studierende prüfungsrelevant!

In diesem abschließenden Kapitel möchten wir reelle Zahlen möglichst gut durch Brüche mit kleinem Nenner annähern. Um z.B. die Kreiszahl

$$\pi = \underbrace{3}_{\text{How}}, \underbrace{1}_{\text{I}} \underbrace{4}_{\text{want}} \underbrace{1}_{\text{a}} \underbrace{5}_{\text{drink?}} \underbrace{9}_{\text{alcoholic}} \underbrace{2}_{\text{of}} \underbrace{6}_{\text{course}} \cdots$$

durch einen Bruch anzunähern, könnte man einfach die Dezimaldarstellung an einer Stelle kappen. Sagen wir $\pi \approx 3,1415 = \frac{31415}{10000} = \frac{6813}{2000}$. Allerdings ist auch $\frac{333}{106} = 3,141509\ldots$ und somit eine leicht bessere Annäherung und das obwohl der Nenner deutlich kleiner ist als 2000.

A.1 Endliche Kettenbrüche

Beispiel A.1.1. Warum sollten uns Annäherungen – im folgenden Approximationen genannt – interessieren? Die Erde benötigt für einen vollen Umlauf um die Sonne 365 Tage, 5 Stunden, 48 Minuten und 45,261 Sekunden. Das nennen wir ein astronomisches (oder tropisches Jahr). Das astronomische Jahr besitzt also

$$365 + \frac{5}{24} + \frac{48}{60 \cdot 24} + \frac{45}{60 \cdot 60 \cdot 24} = 365,24219 \text{ Tage}$$

Wenn ein Kalenderjahr nun immer exakt 365 Tage hätte, wären die Kalenderjahre und die astronomischen Jahre bereits nach fünf (Kalender)jahren

einen ganzen Tag auseinander. Das würde bedeuten, dass nach ein paar hundert Jahren Weihnachten im Sommer läge. Es musste also eine bessere Annäherung an den Wert $365,24219 = \frac{36524219}{100000}$ gefunden werden, die immer noch leicht handhabbar ist.

Wie finden wir nun solche Approximationen? Mit Division mit Rest!

Beispiel A.1.2. Wir betrachten $\frac{45}{16}$ und führen die folgenden Rechnungen durch.

$$\begin{aligned}
(I) \qquad & 45 = \mathbf{2} \cdot 16 + 13 \\
(II) \qquad & 16 = \mathbf{1} \cdot 13 + 3 \\
(III) \qquad & 13 = \mathbf{4} \cdot 3 + 1 \\
(IV) \qquad & 3 = \mathbf{3} \cdot 1 + 0
\end{aligned}$$

Diese Rechnung ist uns zur genüge bekannt, aber die fett gedruckten Zahlen hatten bis jetzt keine sehr prominente Rolle. Das wollen wir nun ändern. Mit der obigen Rechnung erhalten wir folgende Darstellung von $\frac{45}{16}$:

$$\begin{aligned}
\frac{45}{16} &\overset{(I)}{=} \frac{2 \cdot 16 + 13}{16} = 2 + \frac{13}{16} = 2 + \frac{1}{\frac{16}{13}} \\
&\overset{(II)}{=} 2 + \frac{1}{\frac{1 \cdot 13 + 3}{13}} = 2 + \frac{1}{1 + \frac{3}{13}} = 2 + \frac{1}{1 + \frac{1}{\frac{13}{3}}} \\
&\overset{(III)}{=} 2 + \frac{1}{1 + \frac{1}{\frac{4 \cdot 3 + 1}{3}}} = \mathbf{2} + \frac{1}{\mathbf{1} + \frac{1}{\mathbf{4} + \frac{1}{\mathbf{3}}}}
\end{aligned}$$

An dieser Stelle bricht das Verfahren ab. Wir sehen, dass 2 eine sehr grobe Approximation von $\frac{45}{16} = 2,8125$ ist. Der Wert $2 + \frac{1}{\mathbf{1}} = 3$ ist schon etwas besser. Der Wert $2 + \frac{1}{1 + \frac{1}{\mathbf{4}}} = \frac{14}{5} = 2,8$ ist schon ziemlich präzise. Unsere Vermutung ist also, dass wir Approximationen von rationalen Zahlen erhalten in dem wir das obige Verfahren an irgendeiner Stelle abbrechen. Dabei soll natürlich gelten: Je länger das Verfahren läuft, desto besser wird die Approximation.

Definition A.1.3. Für $a_0 \in \mathbb{Z}$ und $a_1, \ldots, a_n \in \mathbb{N}$ setzen wir

$$\langle a_0, a_1, \ldots, a_n \rangle = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}}.$$

Einen solchen Bruch nennen wir *endlichen Kettenbruch.*

Mit dem Beispiel vom Eingang sehen wir, dass $\langle 2, 1, 4, 3 \rangle = \frac{45}{16}$ ist.

Bemerkung A.1.4. Sei wie in der Definition von Kettenbrüchen $a_0 \in \mathbb{Z}$ und $a_1, \ldots, a_n \in \mathbb{N}$. Ist $b \in \mathbb{Z}$ eine weitere ganze Zahl, so folgt sofort die Identität $\langle a_0 + b, a_1, a_2, \ldots, a_n \rangle = b + \langle a_0, a_1, \ldots, a_n \rangle$.
Benutzen wir nur die Definition von Kettenbrüchen, so sehen wir direkt die Gleichung $\langle a_0, \ldots, a_n \rangle = a_0 + \frac{1}{\langle a_1, \ldots, a_n \rangle}$. Insbesondere ist somit $\frac{1}{\langle a_1, \ldots, a_n \rangle} = \langle 0, a_1, \ldots, a_n \rangle$.

Beispiel A.1.5. Es ist $\langle 2, 1, 4, 3 \rangle = \frac{45}{16}$ und somit $\langle 0, 2, 1, 4, 3 \rangle = \frac{16}{45}$. Damit folgt auch $\langle -1, 2, 1, 4, 3 \rangle = -1 + \frac{16}{45} = -\frac{29}{45}$.

Satz A.1.6. *Jedes Element aus $\mathbb{Q}$ lässt sich als ein endlicher Kettenbruch schreiben.*

Beweis. Das Verfahren aus dem ersten Beispiel funktioniert ganz genauso für beliebige rationale Zahlen. Beachten Sie, dass „nur“ der Euklidische Algorithmus benutzt wird. □

Definition A.1.7. Sei $\langle a_0, a_1, \ldots, a_n \rangle$ ein endlicher Kettenbruch. Für $k = 0, \ldots, n$ heißt $r_k = \langle a_0, \ldots, a_k \rangle$ der *k-te Näherungsbruch.*

Es ist also $r_0 = \langle a_0 \rangle = a_0$, $r_1 = \langle a_0, a_1 \rangle = a_0 + \frac{1}{a_1}$, usw. Damit beschreibt r_k präzise, was wir zu Beginn damit gemeint haben, das Verfahren nach k Schritten abzubrechen.

Wie können wir die Näherungsbrüche nun berechnen? Dazu lassen wir für den Moment auch positive reelle Zahlen als Einträge eines Kettenbruchs zu. D.h. für $x_0 \in \mathbb{R}$ und $x_1, \ldots, x_r$ positive reelle Zahlen setzen wir

$$\langle x_0, x_1, \ldots, x_n \rangle = x_0 + \cfrac{1}{x_1 + \cfrac{1}{x_2 + \cfrac{1}{\ddots + \cfrac{1}{x_{n-1} + \cfrac{1}{x_n}}}}}.$$

Mit dieser Konvention lesen wir sofort die folgende Gleichung ab

$$\langle x_0, x_1, \ldots, x_{n-1}, x_n \rangle = \langle x_0, x_1, \ldots, x_{n-1} + \frac{1}{x_n} \rangle \tag{A.1}$$

Wir können auf diese Art also einen Kettenbruch mit $n+1$ Einträgen als Kettenbruch mit n Einträgen schreiben.

Satz A.1.8. *Sei $a_0 \in \mathbb{Z}$ und $a_1, \ldots, a_n \in \mathbb{N}$. Wir definieren rekursiv*

$$\begin{array}{llll} p_{-2} = 0 & p_{-1} = 1 & p_k = a_k \cdot p_{k-1} + p_{k-2} & \text{für alle } k \in \{0, \ldots, n\} \\ q_{-2} = 1 & q_{-1} = 0 & q_k = a_k \cdot q_{k-1} + q_{k-2} & \text{für alle } k \in \{0, \ldots, n\} \end{array}$$

Dann gilt für alle $k \in \{0, \ldots, n\}$ und alle $x > 0 \in \mathbb{R}$ die Gleichung

$$\langle a_0, \ldots, a_{k-1}, x \rangle = \frac{x \cdot p_{k-1} + p_{k-2}}{x \cdot q_{k-1} + q_{k-2}}.$$

Beweis. Wir beweisen die Aussage per Induktion über k.
Induktionsanfang: Für $k = 0$ und $x > 0 \in \mathbb{R}$ beliebig, gilt $\langle x \rangle = x = \frac{x \cdot 1 + 0}{x \cdot 0 + 1} = \frac{x \cdot p_{k-1} + p_{k-2}}{x \cdot q_{k-1} + q_{k-2}}$. Damit ist der Induktionsanfang erledigt.
Induktionsvoraussetzung: Für beliebiges aber festes $k \in \{0, \ldots, n-1\}$ gilt $\langle a_0, \ldots, a_{k-1}, x \rangle = \frac{x \cdot p_{k-1} + p_{k-2}}{x \cdot q_{k-1} + q_{k-2}}$ für alle reellen Zahlen $x > 0$.
Induktionsschritt: Sei k wie in der Induktionsvoraussetzung und sei $x > 0$ eine beliebige positive reelle Zahl. Dann gilt

$$\begin{aligned} \langle a_0, \ldots, a_k, x \rangle &\overset{(A.1)}{=} \langle a_0, \ldots, a_k + \frac{1}{x} \rangle \\ &\overset{IV}{=} \frac{(a_k + \frac{1}{x}) \cdot p_{k-1} + p_{k-2}}{(a_k + \frac{1}{x}) \cdot q_{k-1} + q_{k-2}} = \frac{a_k x p_{k-1} + x p_{k-2} + p_{k-1}}{a_k x q_{k-1} + x q_{k-2} + q_{k-1}} \\ &= \frac{x \cdot (a_k \cdot p_{k-1} + p_{k-2}) + p_{k-1}}{x \cdot (a_k \cdot q_{k-1} + q_{k-2}) + q_{k-1}} = \frac{x \cdot p_k + p_{k-1}}{x \cdot q_k + q_{k-1}} \end{aligned}$$

Das war zu zeigen. □

Korollar A.1.9. *Mit den Bezeichnungen von gerade gilt* $r_k = \frac{p_k}{q_k}$ *für alle* $k \in \{0, \ldots, n\}$.

BEWEIS. Es ist $q_0 = 1 \leq q_1 = a_1 \cdot 1 + 0 < q_2 = a_2 \cdot a_1 + 1 < \ldots$. Insbesondere ist also $q_k \neq 0$, für alle $k \in \{0, \ldots, n\}$. Damit ist $r_k = \langle a_0, a_1, \ldots, a_k \rangle \overset{A.1.8}{=} \frac{a_k \cdot p_{k-1} + p_{k-2}}{a_k \cdot q_{k-1} + q_{k-2}} = \frac{p_k}{q_k}$. □

Wir haben mit dieser rekursiven Beschreibung der Näherungsbrüche eine schnelle Methode kennengelernt, wie wir endliche Kettenbrüche samt allen Nähenrungsbrüchen berechnen können.

Beispiel A.1.10. Wir berechnen die ersten Näherungsbrüche von $\langle 0, 4, 7, 1, 3, 6, 2, 1, 170 \rangle$. Dazu benutzen wir eine Tabellenschreibweise. Diese ist immer von der Form

k	a_k	p_k	q_k	$r_k = \frac{p_k}{q_k}$
-2	–	0	1	–
-1	–	1	0	–
0				
1				
2				
3				
4				
5				
6				

Beachten Sie, dass der Index k bei -2 und nicht bei 0 oder 1 anfängt! In dieser Tabelle stecken noch keine Informationen des Kettenbruchs. Das müssen wir ändern und schreiben nun die Einträge $a_0, a_1, a_2, \ldots$ in die Tabelle. Dann haben wir:

k	a_k	p_k	q_k	$r_k = \frac{p_k}{q_k}$
-2	–	0	1	–
-1	–	1	0	–
0	0			
1	4			
2	7			
3	1			
4	3			
5	6			
6	2			

Die restlichen Einträge können wir nun nach und nach mit den Formeln $p_k = a_k p_{k-1} + p_{k-2}$ und $q_k = a_k q_{k-1} + q_{k-2}$ berechnen. Damit ist $p_0 = a_0 \cdot 1 + 0 = 0$ und $q_0 = a_0 \cdot 0 + 1 = 1$. Also können wir die nächsten Einträge in die Tabelle schreiben:

k	a_k	p_k	q_k	$r_k = \frac{p_k}{q_k}$
-2	–	0	1	–
-1	–	1	0	–
0	0	0	1	
1	4			
2	7			
3	1			
4	3			
5	6			
6	2			

Als nächstes erhalten wir dann $p_1 = a_1 \cdot 0 + 1 = 1$ und $q_1 = a_1 \cdot 1 + 0 = 4$. Und so weiter und so weiter, bis wir alle Einträge in den Spalten p_k und q_k berechnet haben. Dann sieht die Tabelle aus wie

k	a_k	p_k	q_k	$r_k = \frac{p_k}{q_k}$
-2	–	0	1	–
-1	–	1	0	–
0	0	0	1	
1	4	1	4	
2	7	7	29	
3	1	8	33	
4	3	31	128	
5	6	194	801	
6	2	419	1730	

Als letztes können wir nun ganz entspannt die Näherungsbrüche eintragen:

k	a_k	p_k	q_k	$r_k = \frac{p_k}{q_k}$
-2	–	0	1	–
-1	–	1	0	–
0	0	0	1	0
1	4	1	4	$\frac{1}{4}$
2	7	7	29	$\frac{7}{29}$
3	1	8	33	$\frac{8}{33}$
4	3	31	128	$\frac{31}{128}$
5	6	194	801	$\frac{194}{801}$
6	2	419	1730	$\frac{419}{1730}$

Der letzte Näherungsbruch – in unserem Fall $\frac{419}{1730}$ – gibt den Wert des Kettenbruchs als rationale Zahl an. Es ist also $\langle 0, 4, 7, 1, 3, 6, 2, 1, 170\rangle = \frac{419}{1730}$.
Früher war das astronomische Jahr etwa eine halbe Sekunde länger als jetzt. Es wurde mit dem Wert $\langle 365, 4, 7, 1, 3, 6, 2, 1, 170\rangle = 365 + \langle 0, 4, 7, 1, 3, 6, 2, 1, 170\rangle$ bemessen. Der 5-te Näherungsbruch $\frac{194}{801}$ bestimmt sehr gut die Länge unseres Kalenderjahres. (Es wird mit $365 + \frac{194}{800}$ Tagen angesetzt, da man mit 800 leichter rechnen kann als mit 801. Weiter ergibt sich damit sofort die zunächst willkürlich erscheinende Festlegung der Schaltjahre: In 800 Jahren müssen 194 Tage zusätzlich eingeschoben werden. Bekommt jedes vierte Jahr einen Tag dazu, haben wir 200 Tage eingeschoben; es müssen also 6 Tage abgezogen werden. Dazu wird jedem hundertsten Jahr ein Tag gestrichen, dann haben wir aber 8 Tage abgezogen. Um nun in 800 Jahren wieder

2 Tage einzufügen, wird natürlich jedem 400ten Jahr ein Tag spendiert.) Diese Regel ist ziemlich genau, da das Kalenderjahr nur um $0,00031$ Tage länger ist als das astronomische Jahr. Das heißt, dass das Kalenderjahr erst nach $\frac{1}{0.00031} = 3225.8\ldots$ Jahren um einen Tag vom astronomischen Jahr verschoben wird.

Es fehlt noch zu zeigen, dass ein Näherungsbruch tatsächlich eine Approximation des Ausgangsbruches ist.

Satz A.1.11. *Mit den Bezeichnungen aus Satz A.1.8 gilt:*

(i) $p_{k+1} \cdot q_k - q_{k+1} \cdot p_k = (-1)^k$ *für alle* $k \in \{-2, \ldots, n-1\}$

(ii) $r_{k+1} = r_k + \frac{(-1)^k}{q_k \cdot q_{k+1}}$ *für alle* $k \in \{0, \ldots, n-1\}$.

Beweis. Die erste Aussage beweisen wir per Induktion über k.
Induktionsanfang: Sei $k = -2$. Dann ist

$$p_{k+1} \cdot q_k - q_{k+1} \cdot p_k = p_{-1} \cdot q_{-2} - q_{-1} \cdot p_{-2} = 1 \cdot 1 - 0 \cdot 0 = 1 = (-1)^{-2}.$$

Damit ist der Induktionsanfang gezeigt.
Induktionsvoraussetzung: Für beliebiges aber festes $k \in \{-2, \ldots, n-2\}$ gelte $p_{k+1} \cdot q_k - q_{k+1} \cdot p_k = (-1)^k$.
Induktionsschritt: Sei k wie in der Induktionsvoraussetzung. Wir zeigen die Behauptung nun für $k+1$. Es ist

$$\begin{aligned} p_{k+2} \cdot q_{k+1} - q_{k+2} \cdot p_{k+1} &= (a_{k+2} \cdot p_{k+1} + p_k) \cdot q_{k+1} - (a_{k+2} \cdot q_{k+1} + q_k) \cdot p_{k+1} \\ &= p_k \cdot q_{k+1} - q_k \cdot p_{k+1} = (-1) \cdot (q_k \cdot p_{k+1} - p_k \cdot q_{k+1}) \\ &\overset{IV}{=} (-1) \cdot (-1)^k = (-1)^{k+1} \end{aligned}$$

Das schließt die Induktion und der erste Teil ist bewiesen.
Die zweite Aussage folgt aus der ersten durch folgende kurze Rechnung:

$$\underbrace{r_k}_{\frac{p_k}{q_k}} + \frac{(-1)^k}{q_k \cdot q_{k+1}} = \frac{p_k \cdot q_{k+1} + p_{k+1} \cdot q_k - q_{k+1} \cdot p_k}{q_k \cdot q_{k+1}} = \frac{p_{k+1} \cdot q_k}{q_k \cdot q_{k+1}} = r_{k+1}.$$

□

Bemerkung A.1.12. Wir haben bereits festgestellt, dass $q_0 \leq q_1 < q_2 < q_3 < \ldots$ gilt. Damit ist $\frac{1}{q_k \cdot q_{k+1}} > \frac{1}{q_{k+1} \cdot q_{k+2}}$ für alle $k \in \{0, \ldots, n-2\}$. Die Folge $\frac{1}{q_k \cdot q_{k+1}}$ ist also monoton fallend.
Wenden wir Satz A.1.11 zweimal an, so erhalten wir für jedes $k \in \{0, \ldots, n-2\}$:

$$r_{k+2} = r_{k+1} + \frac{(-1)^{k+1}}{q_{k+2} \cdot q_{k+1}} = r_k + \frac{(-1)^k}{q_{k+1} \cdot q_k} + \frac{(-1)^{k+1}}{q_{k+2} \cdot q_{k+1}}.$$

Da weiter $|\frac{(-1)^k}{q_{k+1} \cdot q_k}| > |\frac{(-1)^{k+1}}{q_{k+2} \cdot q_{k+1}}|$ ist, folgt

$$\begin{aligned} &r_0 < r_2 < r_4 < r_6 < \ldots \text{ ist monoton steigend und} \\ &r_1 > r_3 > r_5 > r_7 > \ldots \text{ ist monoton fallend.} \end{aligned} \tag{A.2}$$

Proposition A.1.13. *Mit den üblichen Bezeichnungen gilt für jedes $k \in \{0, \ldots, n-1\}$ die Abschätzung*

$$|r_n - r_k| \leq \frac{1}{q_k \cdot q_{k+1}}.$$

Beweis. Wir nehmen zunächst an, dass n gerade ist. Dann ist mit (A.2)

$$r_0 < \ldots < r_{n-2} < r_n \overset{A.1.11}{=} r_{n-1} - \frac{1}{q_n \cdot q_{n-1}} < r_{n-1} < r_{n-3} < \ldots < r_3 < r_1$$

Insbesondere folgt, dass $r_k \leq r_n$ für alle geraden k und $r_k \geq r_n$ für alle ungeraden k gilt. Damit liegt r_n sicher zwischen r_k und r_{k+1} für jedes $k \in \{0, \ldots, n-1\}$. Es folgt

$$|r_n - r_k| \leq |r_{k+1} - r_k| = |\frac{(-1)^k}{q_k \cdot q_{k+1}}| = \frac{1}{q_k \cdot q_{k+1}},$$

was zu zeigen war. Falls n ungerade ist, zeigt man die Aussage ganz genauso. □

Der Fehler zwischen Kalenderjahr und astronomischen Jahr ist also kleiner als $\frac{1}{801 \cdot 1730} = \frac{1}{1385730}$ Tage.

A.2 Unendliche Kettenbrüche

Bis jetzt haben wir gelernt, wie man rationale Zahlen durch Brüche mit kleinerem Nenner approximieren kann. Wir wollen als nächstes beliebige reelle Zahlen durch Brüche annähern. Das funktioniert zum Glück fast genauso.

Beispiel A.2.1. Um $\frac{45}{16}$ als Kettenbruch darzustellen, haben wir den Euklidischen Algorithmus durchgeführt. Wir haben also überlegt „wie oft 16 in die 45 passt“. Wir versuchen genau das gleiche für $\pi = 3,1415926\ldots = \frac{\pi}{1}$. Wir überlegen also „wie oft die 1 in π“ passt. Offensichtlich 3mal. Der Rest ist $\pi - 3 = 0,1415926\ldots$. Als nächstes prüfen wir, wir oft $\pi - 3$ in die 1 passt. Da $\frac{1}{\pi-3} = 7,062\ldots$, ist die Antwort 7mal. Wir können also das Verfahren des Euklidischen Algorithmus adaptieren und erhalten

$$\begin{aligned}
\pi &= \mathbf{3} \cdot 1 + (\pi - 3) \\
1 &= \mathbf{7} \cdot (\pi - 3) + \underbrace{(1 - 7 \cdot (\pi - 3))}_{=22-7\pi} \\
(\pi - 3) &= \mathbf{15} \cdot (22 - 7\pi) + \underbrace{[(\pi - 3) - 15 \cdot (22 - 7\pi)]}_{=-333+106\pi=0,0088\ldots} \\
&\vdots
\end{aligned}$$

[1] Damit können wir nun einen Kettenbruch konstruieren, der leider nicht nur ganzzahlige Einträge besitzt:

$$\begin{aligned}
\pi &= \mathbf{3} + \frac{\pi - 3}{1} = \mathbf{3} + \frac{1}{\frac{1}{\pi-3}} = \mathbf{3} + \frac{1}{\mathbf{7} + \frac{22-7\pi}{\pi-3}} = \mathbf{3} + \cfrac{1}{\mathbf{7} + \cfrac{1}{\mathbf{15} + \frac{-333+106\pi}{22-7\pi}}} \\
&= \langle 3, 7, 15 + \frac{-333 + 106\pi}{22 - 7\pi} \rangle
\end{aligned}$$

Der hier benutzte „Euklidische Algorithmus“ könnte noch weiter geführt werden, da wir keinen Rest Null erhalten haben. Wir werden gleich sehen, dass es tatsächlich nie einen Rest Null geben wird, da π keine rationale Zahl ist. Damit können wir auf diese Weise beliebig viele Stellen des Kettenbruchs von π mit natürlichen Zahlen beschreiben. Um nun π (oder jede andere irrationale Zahl) als Kettenbruch darzustellen, haben wir zwei

[1] Wir sehen, dass $-333 + 106\pi \approx 0$ und somit $\pi \approx \frac{333}{106}$ ist. Damit haben wir die Abschätzung für π aus der Einleitung hergeleitet!

Möglichkeiten: Entweder wir erlauben, dass der letzte Eintrag des Kettenbruchs keine natürliche Zahl ist, oder wir erlauben unendlich viele Einträge (die dann allesamt natürliche Zahlen sind). Da wir die natürlichen Zahlen so liebgewonnen haben, entscheiden wir uns für letzteres.

Das Ganze ziehen wir nun formal auf.

Definition A.2.2. Für $x \in \mathbb{R}$ bezeichnen wir mit $\lfloor x \rfloor$ die größte ganze Zahl, die kleiner oder gleich x ist.

Beispiel A.2.3.

- $\lfloor \pi \rfloor = 3$
- $\lfloor \sqrt{2} \rfloor = 1$
- $\lfloor 6 \rfloor = 6$
- $\lfloor -\frac{4}{3} \rfloor = -2$

Lemma A.2.4. *Sei x eine irrationale reelle Zahl; d.h. $x \in \mathbb{R} \setminus \mathbb{Q}$. Dann gilt*

(i) $x - \lfloor x \rfloor$ *ist irrational und*

(ii) $x - \lfloor x \rfloor \in (0, 1)$.

Beweis. Wir wissen, dass die Summe von zwei rationalen Zahlen wieder eine rationale Zahl ist (d.h. nichts anderes, als dass wir in $\mathbb{Q}$ Plusrechnen können). Es ist $\lfloor x \rfloor \in \mathbb{Z} \subseteq \mathbb{Q}$ eine rationale Zahl. Wäre nun $x - \lfloor x \rfloor \in \mathbb{Q}$, so wäre auch $(x - \lfloor x \rfloor) + \lfloor x \rfloor = x \in \mathbb{Q}$. Das ist aber ausgeschlossen! Damit kann $x - \lfloor x \rfloor$ nicht rational sein. Insbesondere ist also $x - \lfloor x \rfloor$ weder gleich 0 noch gleich 1. Da per Definition $\lfloor x \rfloor \leq x$, ist $0 < x - \lfloor x \rfloor$. Weiter ist der Abstand zwischen x und der nächst gelegenen ganzen Zahl, sicher kleiner gleich 1. Damit ist auch die zweite Aussage bewiesen. □

Satz A.2.5. *Sei $x \in \mathbb{R}$ eine irrationale Zahl. Wir definieren rekursiv*

$$x_0 = x \quad \text{und} \quad x_k = \frac{1}{x_{k-1} - \lfloor x_{k-1} \rfloor} \text{ für alle } k \in \mathbb{N}$$

und setzen $a_k = \lfloor x_k \rfloor$ für alle $k \in \mathbb{N}_0$. Dann gilt für alle $k \in \mathbb{N}_0$ die Gleichung $x = \langle a_0, a_1, \ldots, a_k + \frac{1}{x_{k+1}} \rangle$.

BEWEIS. Das ist die präzise Beschreibung von dem, was wir im Beispiel A.2.1 exemplarisch gesehen haben. Offensichtlich ist $a_0 \in \mathbb{Z}$ und alle weitern $a_k \in \mathbb{N}$ nach Lemma A.2.4. Formal führen wir mal wieder eine Induktion:
Induktionsanfang: Sei $k = 0$. Es ist

$$\begin{aligned} x = \langle x \rangle &= \langle \lfloor x \rfloor + (x - \lfloor x \rfloor) \rangle \\ &= \langle \lfloor x_0 \rfloor + (x_0 - \lfloor x_0 \rfloor) \rangle = \langle a_0 + (x_0 - \lfloor x_0 \rfloor) \rangle = \langle a_0 + \frac{1}{x_1} \rangle. \end{aligned}$$

Beachten Sie im letzten Schritt, dass per Definition $x_1 = \frac{1}{x_0 - \lfloor x_0 \rfloor}$ gilt. Umstellen liefert also tatsächlich $x_0 - \lfloor x_0 \rfloor = \frac{1}{x_1}$. Damit ist der Induktionsanfang gezeigt.
Induktionsvoraussetzung: Die Behauptung gelte für beliebiges aber festes $k \in \mathbb{N}$.
Induktionsschritt: Wir zeigen die Aussage nun für $k+1$, für das k aus der Induktionsvoraussetzung. Wie im Induktionsanfang benutzen wir die Gleichung $x_{k+1} - \underbrace{\lfloor x_{k+1} \rfloor}_{=a_{k+1}} = \frac{1}{x_{k+2}}$. Damit berechnen wir

$$\begin{aligned} \langle a_0, a_1, \ldots, a_k, a_{k+1} + \frac{1}{x_{k+2}} \rangle &= \langle a_0, a_1, \ldots, a_k, a_{k+1} + (x_{k+1} - a_{k+1}) \rangle \\ &= \langle a_0, a_1, \ldots, a_k, x_{k+1} \rangle \\ &\overset{(A.1)}{=} \langle a_0, a_1, \ldots, a_{k-1}, a_k + \frac{1}{x_{k+1}} \rangle \overset{\text{IV}}{=} x \end{aligned}$$

□

Bemerkung A.2.6. Wir stellen fest, dass wir ein irrationales x als Kettenbruch schreiben können mit beliebig vielen ganzzahligen Einträgen. Um nur ganzzahlige Einträge zu verwenden liegt die Idee nahe, einen unendlichen Kettenbruch

$$x = \langle a_0, a_1, a_2, \ldots \rangle$$

zu definieren. Diese Schreibweise muss natürlich erklärt und formal definiert werden. Wie so oft, wenn *unendlich viele* Elemente eine Rolle spielen, werden wir mit dem Begriff der *Konvergenz* arbeiten müssen. An dieser Stelle sollten Sie also kurz überlegen, was Sie von diesem Begriff noch alles wissen.

Satz A.2.7. *Sei $a_0 \in \mathbb{Z}$ und $a_1, a_2, a_3, \ldots$ eine Folge von natürlichen Zahlen. Setze $r_k = \langle a_0, a_1, \ldots, a_k \rangle$ für alle $k \in \mathbb{N}_0$. Die Werte r_0, r_1, r_2, r_3, $\ldots$ bilden also eine Folge von rationalen Zahlen. Diese Folge konvergiert und den Grenzwert bezeichnen wir mit $\langle a_0, a_1, a_2, \ldots \rangle$. Dieser Ausdruck heißt* unendlicher Kettenbruch.

BEWEIS. Wir schreiben wieder $r_k = \frac{p_k}{q_k}$ mit p_k und q_k aus Satz A.1.11. Wir haben bereits festgestellt, dass $1 \leq q_0 \leq q_1 < q_2 < \ldots$ gilt. Damit ist insbesondere

$$q_k \geq k \text{ für alle } k \in \mathbb{N}. \tag{A.3}$$

Wir wissen auch schon, dass die Folge $r_0, r_2, r_4, r_6, \ldots$ monoton steigt und die Folge $r_1, r_3, r_5, \ldots$ monoton fällt (siehe (A.2)). Weiter gilt für jedes $k \in \mathbb{N}$ die Ungleichung $r_0 < r_{2k} \overset{A.1.11(ii)}{<} r_{2k+1} < r_1$. Damit ist

- $r_0, r_2, r_4, r_6, \ldots$ monoton steigend und beschränkt, und
- $r_1, r_3, r_5, r_7, \ldots$ monoton fallend und beschränkt.

Beide Teilfolgen konvergieren also. Wir müssen nur noch zeigen, dass die beiden Grenzwerte gleich sind. Sei dazu G der Grenzwert der Teilfolge mit geraden Indizes und U der Grenzwert der Teilfolge mit ungeraden Indizes. Wegen $r_{2k} < r_{2k+1}$ für alle $k \in \mathbb{N}$, ist sicher $U \geq G$. Es folgt

$$\begin{aligned} 0 \leq U - G &= \lim_{k \longrightarrow \infty} r_{2k+1} - \lim_{k \longrightarrow \infty} r_{2k} = \lim_{k \longrightarrow \infty} (r_{2k+1} - r_{2k}) \\ &\overset{A.1.11}{=} \lim_{k \longrightarrow \infty} \frac{1}{q_{2k+1} \cdot q_{2k}} \overset{(A.3)}{\leq} \lim_{k \longrightarrow \infty} \frac{1}{(2k)^2} = 0 \end{aligned}$$

Zusammengenommen haben wir $U - G = 0$ – also $G = U$ – gezeigt. Da nun alle Folgenglieder r_k mit geradem und ungeradem Index gegen denselben Wert konvergieren, konvergiert die gesamte Folge $r_0, r_1, r_2, r_3, \ldots$. Das war zu zeigen. □

Theorem A.2.8. *Ist x eine irrationale Zahl und sind x_k und a_k definiert wie in Satz A.2.5, dann gilt $\langle a_0, a_1, a_2, a_3, \ldots \rangle = x$.*

BEWEIS. Mit den üblichen Bezeichnungen $r_k = \langle a_0, \ldots, a_k \rangle = \frac{p_k}{q_k}$, gilt

$$|x - r_k| \overset{A.2.5}{=} |\underbrace{\langle a_0, \ldots, a_k + \frac{1}{x_{k+1}} \rangle}_{\overset{A.1.8}{=} \frac{x_{k+1} \cdot p_k + p_{k-1}}{x_{k+1} \cdot q_k + q_{k-1}}} - \underbrace{r_k}_{= \frac{p_k}{q_k}}| = |\frac{p_{k-1} \cdot q_k - p_k \cdot q_{k-1}}{q_k \cdot (x_{k+1} \cdot q_k + q_{k-1})}|$$

$$\overset{A.1.8}{=} |\frac{1}{q_k \cdot (x_{k+1} \cdot q_k + q_{k-1})}| \overset{x_{k+1} > \lfloor x_{k+1} \rfloor = a_{k+1}}{\leq} \frac{1}{q_{k+1} \cdot q_k} \overset{(A.3)}{\leq} \frac{1}{k^2}$$

Damit ist $\lim_{k \longrightarrow \infty} |x - r_k| = \lim_{k \longrightarrow \infty} \frac{1}{k^2} = 0$. Der Abstand von x zu den Folgengliedern r_k, konvergiert somit gegen Null. Das ist nur möglich, wenn die Folge $r_0, r_1, r_2, \ldots$ gegen x konvergiert. Das war zu zeigen. □

Definition A.2.9. Ist $\langle a_0, a_1, \ldots \rangle$ ein unendlicher Kettenbruch, dann heißt $r_k = \langle a_0, \ldots, a_k \rangle$ der $k$te Näherungsbruch von $\langle a_0, a_1, \ldots \rangle$.

Beispiel A.2.10. Warum ist ein DIN A4 Blatt so groß wie es ist? Ein A4 Blatt ist die Hälfte eines A3 Blattes, das ist die Hälfte eines A2 Blattes, das ist die Hälfte eines A1 Blattes, das ist die Hälfte eines A0 Blattes. Genauso ist das A5 Blatt die Hälfte des A4 Blattes. Das A0 Format sollte – als Basis – einen schönen Flächeninhalt haben, sagen wir einen Quadratmeter, und die Seitenverhältnisse zwischen allen diesen Formaten sollten nach Möglichkeit gleich sein (d.h. ein A5 Blatt soll so aussehen, wie ein kleines A4 Blatt). Bezeichnen wir mit H die Höhe und mit B die Breite, sollte also gelten

$$\begin{aligned} \frac{H(A4)}{B(A4)} = \frac{H(A5)}{B(A5)} = \frac{B(A4)}{\frac{1}{2}H(A4)} \quad &\Longleftrightarrow \quad \left(\frac{H(A4)}{B(A4)}\right)^2 = 2 \\ &\Longleftrightarrow \quad \frac{H(A4)}{B(A4)} = \sqrt{2} \end{aligned}$$

In Worten: Das Seitenverhältnis sollte $\sqrt{2}$ betragen. Allerdings hätte man auch gerne, dass man die Breite und die Höhe mit ganzen Millimetern abmessen kann. Dafür müsste das Seitenverhältnis eine rationale Zahl sein. Wir brauchen also Approximationen von $\sqrt{2}$!
Wir berechnen die ersten Näherungsbrüche für $x = \sqrt{2}$. Dazu müssen wir zunächst die Werte x_k und $a_k = \lfloor x_k \rfloor$ berechnen:

- $x_0 = \sqrt{2}$ und somit $a_0 = \lfloor x_0 \rfloor = 1$. Das sehen wir ganz einfach, denn $1^2 = 1 < 2 < 4 = 2^2$. Damit muss $\sqrt{2}$ genau zwischen 1 und 2 liegen.

- $x_1 = \frac{1}{\sqrt{2}-1} \underbrace{=}_{\text{kommt Ihnen dieser Trick bekannt vor?}} \frac{1\cdot(\sqrt{2}+1)}{(\sqrt{2}-1)\cdot(\sqrt{2}+1)} = \sqrt{2}+1$ und $a_1 = \lfloor\sqrt{2}+1\rfloor = 2$. (Wenn $\sqrt{2}$ zwischen 1 und 2 liegt, dann muss $\sqrt{2}+1$ zwischen 2 und 3 liegen.)

- $x_2 = \frac{1}{\sqrt{2}+1-2} = \frac{1}{\sqrt{2}-1} = x_1$ und damit auch $a_2 = a_1 = 2$.

Es ist also $x_2 = x_1$! Wie berechnen wir nun x_3? Es ist doch $x_3 = \frac{1}{x_2-a_2} = \frac{1}{x_1-a_1} = x_2$. Jetzt sind wir also in einer Endlosschleife gefangen und gilt $x_1 = x_2 = x_3 = x_4 = \ldots$. Damit folgt $a_0 = 1, a_1 = 2, a_2 = 2, a_3 = 2, \ldots$. Mit unserer Notation gilt also

$$\sqrt{2} = \langle 1, 2, 2, 2, 2, 2, 2, 2, 2, \ldots\rangle$$

Die Näherungsbrüche berechnen wir nun genau wie im Fall von endlichen Kettenbrüchen:

k	a_k	p_k	q_k	$r_k = \frac{p_k}{q_k}$
-2	–	0	1	–
-1	–	1	0	–
0	1	1	1	1
1	2	3	2	$\frac{3}{2}$
2	2	7	5	$\frac{7}{5}$
3	2	17	12	$\frac{17}{12}$
4	2	41	29	$\frac{41}{29}$
5	2	99	70	$\frac{99}{70}$
6	2	239	169	$\frac{239}{169}$

Der 4te Näherungsbruch $\frac{41}{29} = \frac{1189\text{ mm}}{841\text{ mm}}$ ist genau das Seitenverhältnis eines A0 Blattes und der 5te Näherungsbruch $\frac{99}{70}$ ist exakt das Seitenverhältnis eines DIN A4 Blattes. Es ist $|\sqrt{2} - \frac{99}{70}| \leq \frac{1}{70\cdot 169} = \frac{1}{11830}$ eine wirklich gute Approximation.

Wir stellen fest, dass auch das Ziel, dass das A0 Format genau 1 m^2 betragen soll, nur eine Approximation ist. Denn $1189\text{ mm} \cdot 841\text{ mm} = 0.999949\text{ m}^2$.

Wenn sich die Einträge eines unendlichen Kettenbruchs immer gleichmässig wiederholen, nennen wir den Kettenbruch *periodisch*. Genau wie bei periodischen Dezimalentwicklungen, kennzeichnen wir das mit einem Querbalken. Z.B. ist $\sqrt{2} = \langle 1, 2, 2, 2, 2, \ldots \rangle = \langle 1, \overline{2} \rangle$.

Beispiel A.2.11. Wir berechnen den unendlichen Kettenbruch von $2+\sqrt{3}$. Dazu berechnen wir wieder sukzessive $x_0, x_1, x_2, \ldots$.

- $x_0 = 2+\sqrt{3}$. Da wieder $1^2 < 3 < 2^2$, liegt $\sqrt{3}$ zwischen 1 und 2. Damit liegt $2+\sqrt{3}$ zwischen 3 und 4. Es folgt $a_0 = \lfloor 2+\sqrt{3} \rfloor = 3$.
- $x_1 = \frac{1}{(2+\sqrt{3})-3} = \frac{\sqrt{3}+1}{(\sqrt{3}-1)\cdot(\sqrt{3}+1)} = \frac{\sqrt{3}+1}{2}$. Damit ist $a_1 = \lfloor x_1 \rfloor = 1$.
- $x_2 = \frac{1}{\frac{\sqrt{3}+1}{2}-1} = \frac{1}{\frac{\sqrt{3}-1}{2}} = \frac{2}{\sqrt{3}-1} = \frac{2(\sqrt{3}+1)}{3-1} = \sqrt{3}+1$. Damit ist $a_2 = \lfloor \sqrt{3}+1 \rfloor = 2$.
- Wir könnten jetzt genervt aufhören, aber lassen Sie uns noch einen weiteren Wert berechnen: $x_3 = \frac{1}{(\sqrt{3}+1)-2}$ Das ist ja x_1! Damit muss $a_3 = a_1$ sein.

Ab jetzt muss sich wieder alles wiederholen, denn wir haben $x_4 = \frac{1}{x_3 - a_3} = \frac{1}{x_1 - a_1} = x_2$. Damit ist $2+\sqrt{3} = \langle 3, 1, 2, 1, 2, 1, 2, 1, 2, \ldots \rangle = \langle 3, \overline{1, 2} \rangle$.

Als letztes wollen wir lernen, wie man aus einem gegebenen periodischen Kettenbruch die zugehörige reelle Zahl findet.

Beispiel A.2.12. Im ersten der folgenden Beispiele werden wir es uns ein bisschen zu einfach machen und das obige Beispiel benutzen.

(a) Welche Zahl wird durch den Kettenbruch $\langle \overline{2, 1} \rangle$ dargestellt? Oben hatten wir einen Kettenbruch in dem $\overline{1, 2}$ vorkam. Es wäre doch schön, wenn wir das irgendwie benutzen könnten... Dazu überlegen wir uns

$$\langle \overline{2, 1} \rangle = \langle 2, 1, 2, 1, 2, 1, 2, 1, 2, \ldots \rangle = \langle 2, \overline{1, 2} \rangle = \langle 3 - 1, \overline{1, 2} \rangle = \langle 3, \overline{1, 2} \rangle - 1.$$

Jetzt können wir einfach unser Wissen $\langle 3, \overline{1, 2} \rangle = 2 + \sqrt{3}$ benutzen und $\langle \overline{1, 2} \rangle = 2 + \sqrt{3} - 1 = 1 + \sqrt{3}$ ablesen.

(b) Welche Zahl wird durch den Kettenbruch $\langle 2, \overline{4} \rangle$ dargestellt? Gerade haben wir gesehen, dass der erste Eintrag auch hinterher noch angepasst

werden kann. Entscheidend ist daher ein besseres Verständnis des periodischen Teils. Wir betrachten also zunächst nur $\langle\overline{4}\rangle$. Es ist aber

$$\langle\overline{4}\rangle = 4 + \langle 0, \overline{4}\rangle = 4 + \frac{1}{\langle\overline{4}\rangle}.$$

Multiplizieren wir beide Seiten mit $\langle\overline{4}\rangle$ so erhalten wir, dass gilt

$$\langle\overline{4}\rangle^2 = 4 \cdot \langle\overline{4}\rangle + 1.$$

Wir lösen diese quadratische Gleichung und erhalten

$$\begin{aligned} & \langle\overline{4}\rangle^2 = 4 \cdot \langle\overline{4}\rangle + 1 \\ \iff \quad & \langle\overline{4}\rangle^2 - 4 \cdot \langle\overline{4}\rangle = 1 \\ \iff \quad & (\langle\overline{4}\rangle - 2)^2 - 2^2 = 1 \\ \iff \quad & \langle\overline{4}\rangle - 2 = \pm\sqrt{5} \\ \iff \quad & \langle\overline{4}\rangle = \pm\sqrt{5} + 2. \end{aligned}$$

Wir wissen aber, da der erste Eintrag von $\langle\overline{4}\rangle$ eine 4 ist, dass $\langle\overline{4}\rangle$ zwischen 4 und 5 liegen muss. Damit kommt nur $\langle\overline{4}\rangle = \sqrt{5} + 2$ in Frage!

Jetzt ist das schwierigste bereits getan. Wir erhalten

$$\langle 2, \overline{4}\rangle = \langle 4 - 2, \overline{4}\rangle = \langle 4, \overline{4}\rangle - 2 = \langle\overline{4}\rangle - 2 = \sqrt{5}.$$

(c) Welche Zahl wird durch den Kettenbruch $\langle 1, \overline{3, 2}\rangle$ dargestellt? Wieder betrachten wir erst nur den periodischen Teil:

$$\langle\overline{3, 2}\rangle = 3 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{2 + \ddots}}} = 3 + \cfrac{1}{2 + \cfrac{1}{\langle\overline{3, 2}\rangle}} = 3 + \frac{\langle\overline{3, 2}\rangle}{2\langle\overline{3, 2}\rangle + 1} = \frac{7\langle\overline{3, 2}\rangle + 3}{2\langle\overline{3, 2}\rangle + 1}.$$

Jetzt multiplizieren wir beide Seiten mit $2\langle\overline{3, 2}\rangle + 1$ und erhalten

$$\begin{aligned} & \langle\overline{3, 2}\rangle(2\langle\overline{3, 2}\rangle + 1) = 7\langle\overline{3, 2}\rangle + 3 \\ \iff \quad & 2\langle\overline{3, 2}\rangle^2 - 6\langle\overline{3, 2}\rangle = 3. \end{aligned}$$

Lösen der quadratischen Gleichung liefert nun

$$\langle\overline{3, 2}\rangle = \frac{\pm\sqrt{15} + 3}{2}.$$

Da $\langle\overline{3,2}\rangle$ zwischen 3 und 4 liegen muss, gilt $\langle\overline{3,2}\rangle = \frac{\sqrt{15}+3}{2}$. Damit können wir den periodischen Teil handhaben. Insgesamt erhalten wir

$$\begin{aligned}\langle 1,\overline{3,2}\rangle &= 1+\frac{1}{\langle\overline{3,2}\rangle} = 1+\frac{2}{\sqrt{15}+3} = \frac{\sqrt{15}+5}{\sqrt{15}+3}\\ &= \frac{(\sqrt{15}+5)(\sqrt{15}-3)}{(\sqrt{15}+3)(\sqrt{15}-3)} = \frac{2\sqrt{15}}{15-3^2} = \frac{\sqrt{15}}{3}.\end{aligned}$$

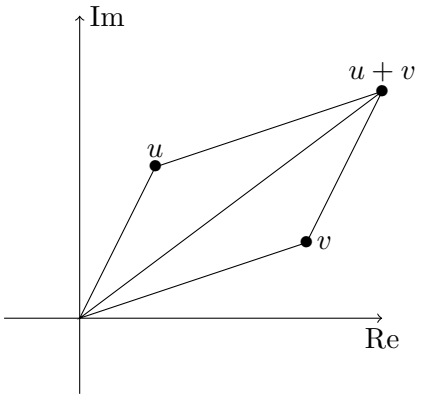
Beachten Sie, dass jede beliebige Folge von natürlichen Zahlen einen unendlichen Kettenbruch generiert. Die *meisten* unendlichen Kettenbrüche sind also nicht periodisch. Man kann zeigen, dass die periodischen Kettenbrüche genau die irrationalen reellen Zahlen darstellen, die von der Form $a+b\sqrt{c}$ sind, mit $a,b\in\mathbb{Q}$ und $c\in\mathbb{N}$. Das werden wir aber in dieser Vorlesung nicht beweisen.

Anhang B

Polarkoordinaten der komplexen Zahlen

Wir haben im Laufe der Vorlesung die komplexe Zahlenebene kennengelernt. Wenn wir komplexe Zahlen als Punkte in einem Koordinatensystem ansehen können, sollte es doch auch möglich sein, die komplexen Zahlen geometrisch zu studieren.

Die Geometrie der Addition ist recht einfach, wie das folgende Bild zeigt.



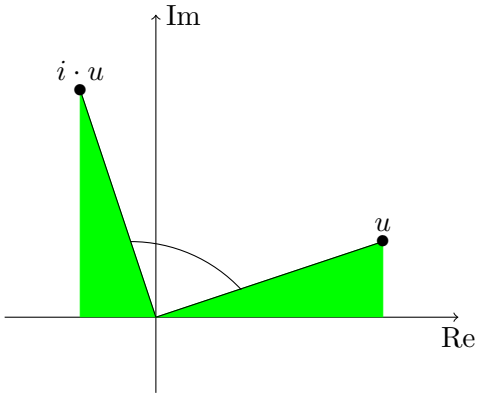
Ist $u = a+b\cdot i$ und $v = c+d\cdot i$, dann ist $u+v = (a+c)+(b+d)\cdot i$. Damit ist $u+v$ gegeben durch den Punkt mit den Koordinaten $(a+c/b+d)$. Dieser Punkt entspricht genau dem vierten Punkt des Parallelogramms mit den Punkten $(0/0), (a/b), (c/d)$. Als Nebenprodukt erhalten wir sofort $|u+v| \leq |u|+|v|$.

B.1 Geometrie der Multiplikation

Bevor wir die Multiplikation allgemein analysieren, betrachten wir drei Spezialfälle. Die Multiplikation mit einer positiven reellen Zahl r schickt eine komplexe Zahl $a+b\cdot i$ auf $ra+rb\cdot i$. Dies entspricht einer Streckung (falls $r>1$) beziehungsweise einer Stauchung (falls $r<1$). Die Multiplikation mit (-1) schickt eine komplexe Zahl $a+b\cdot i$ auf $-a-b\cdot i$. In der Zahlenebene

bedeutet dies genau eine Drehung um 180 Grad.

Multiplikation mit i schickt eine komplexe Zahl $a + b \cdot i$ auf $-b + a \cdot i$. Dies entspricht einer Drehung um 90 Grad, wie die folgende Zeichnung erklärt.

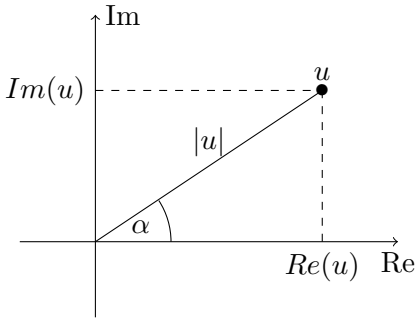


Die grünen Dreiecke sind kongruent und rechtwinklig. Die Summe der Winkel in einem der Dreiecke ist also gleich 180 Grad. Damit lesen wir sofort ab, dass der Winkel der von u und $i \cdot u$ eingeschlossen wird, ein 90 Grad Winkel ist. Da offensichtlich auch $|u| = |i \cdot u|$ gilt, entspricht Multiplikation mit i der Drehung um 90 Grad. Dies wollen wir nun verallgemeinern.

Einschub

Da -1 einer Drehung um 180 Grad entspricht, ist es nicht sehr verwunderlich, dass $i = \sqrt{-1}$ genau der Hälfte der Drehung – also einer 90 Grad Drehung – entspricht. Denn wenn wir zweimal mit i multiplizieren, haben wir nichts anderes gemacht als einmal mit -1 zu multiplizieren.

Konstruktion B.1.1. Bisher haben wir stets benutzt, dass ein Punkt im Koordinatensystem eindeutig bestimmt ist durch die beiden Koordinaten. Es gibt aber noch andere Werte mit denen wir einen solchen Punkt eindeutig beschreiben können.



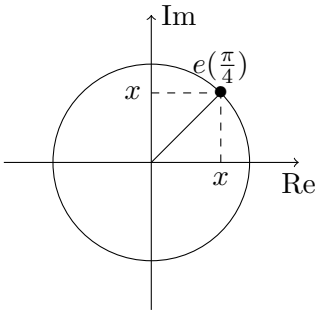
Sei $u \neq 0$ eine komplexe Zahl in der Zahlenebene und sei α der Winkel, der von u und der ersten Achse (der reellen Zahlengerade) eingeschloßen wird. Dann ist u der eindeutige Punkt, der den Winkel α einschließt und den Abstand $r = |u|$ vom Nullpunkt besitzt. Wir schreiben diesen Punkt nun als $u = r \cdot e(\alpha)$ und nennen diese Darstellung, die *Polarkoordinaten* von u.

Hier und im folgenden messen wir den Winkel α stets von der positiven reellen Achse ausgehend gegen den Uhrzeigersinn.

Bemerkung B.1.2. Es hat sich eingebürgert, dass der Winkel in den Polarkoordinaten im Bogenmaß angegeben wird. Das heißt, dass 360 Grad – also die volle Umdrehung – dem Wert 2π entspricht. Somit ist 180 Grad gegeben durch π, ... Damit folgt sofort, dass $e(\alpha) = e(\alpha + 2 \cdot \pi)$ ist, da sich der Winkel unter einer vollen Umdrehung nicht verändert.

Beispiel B.1.3. Es ist

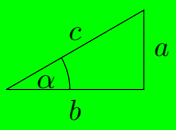
- $i = 1 \cdot e(\frac{\pi}{2})$
- $2018 = 2018 \cdot e(0) = 2018 \cdot e(2\pi)$
- $e(\pi) = -1$.
- Was ist $e(\frac{\pi}{4})$? Beachten Sie, dass diese Zahl den Betrag 1 hat und somit auf dem Kreis um den Nullpunkt mit Radius 1 liegt.



Der Winkel $\frac{\pi}{4}$ entspricht einem 45 Grad Winkel. Daher muss der Realteil gleich dem Imaginärteil sein. Es ist $1 = x^2 + x^2 = 2x^2$. Daher ist $x = \frac{1}{\sqrt{2}}$ und $e(\frac{\pi}{4}) = \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} \cdot i$.

Einschub

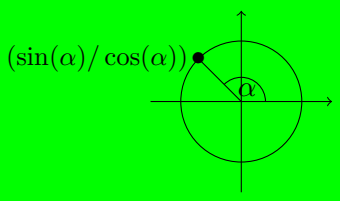
Wir wiederholen kurz die trigonometrischen Funktionen Sinus und Kosinus. Sei zunächst $0 < \alpha < \pi$ (das heißt, dass der Winkel α kleiner als ein rechter Winkel ist). Wir betrachten das rechtwinklige Dreieck



Dann ist $\sin(\alpha) = \frac{a}{c}$ und $\cos(\alpha) = \frac{b}{c}$. Allgemein haben wir die folgende Definition. Für einen Winkel α sind $\sin(\alpha)$ und $\cos(\alpha)$ die reellen Zahlen für die gilt

(i) $(\cos(\alpha)/\sin(\alpha))$ liegt auf dem Kreis um den Nullpunkt mit Radius 1.

(ii) Die Strecke zwischen $(\cos(\alpha)/\sin(\alpha))$ und $(0/0)$ schließt mit der ersten Achse den Winkel α ein.



Damit folgt erstens $\sin(\alpha)^2 + \cos(\alpha)^2 = 1$ und zweitens, $\alpha = \beta$ falls $\sin(\alpha) = \sin(\beta)$ und $\cos(\alpha) = \cos(\beta)$ gilt.

Proposition B.1.4. *Sei α ein Winkel. Dann gilt*

$$e(\alpha) = \cos(\alpha) + \sin(\alpha) \cdot i$$

Beweis. Die Definition für den Realteil und Imaginärteil von $e(\alpha)$ ist exakt die gleiche Definition für $\sin(\alpha)$ und $\cos(\alpha)$. Damit müssen die Werte gleich sein. □

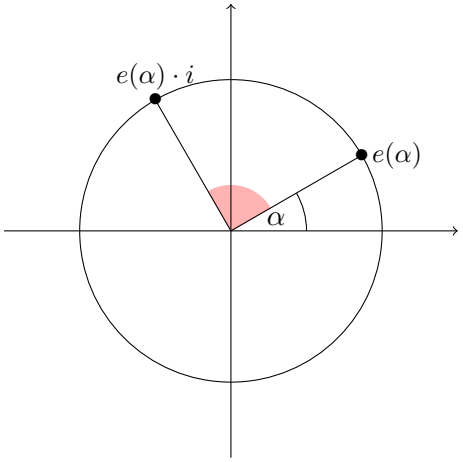
Korollar B.1.5. *Sei $r > 0$ eine reelle Zahl und α ein Winkel. Dann gilt*

$$r \cdot e(\alpha) = r \cdot \cos(\alpha) + r \cdot \sin(\alpha) \cdot i$$

Wie verhalten sich nun die Polarkoordinaten unter Multiplikation? Zum Glück sehr gutartig!

Theorem B.1.6. *Seien α, β zwei Winkel. Dann gilt $e(\alpha) \cdot e(\beta) = e(\alpha + \beta)$.*

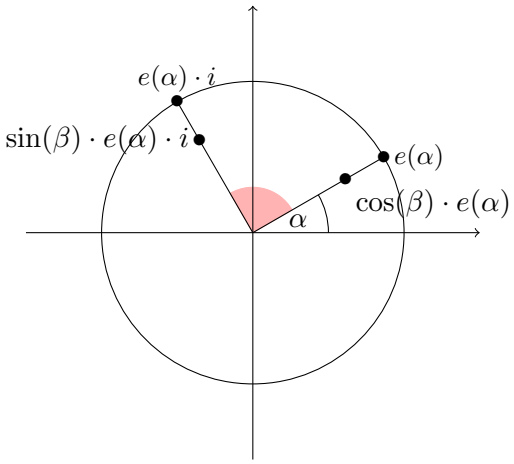
Beweis. Wir führen den Beweis geometrisch. Als erstes sehen wir, dass alle drei Elemente $e(\alpha), e(\beta), e(\alpha+\beta)$ den Betrag 1 haben, also auf dem Kreis um den Nullpunkt mit Radius 1 liegen. Weiter wissen wir, dass Multiplikation mit i einer Drehung um 90 Grad (oder π wenn wir das Bogenmaß benutzen) entspricht. Mit rot kennzeichnen wir Rechtewinkel.



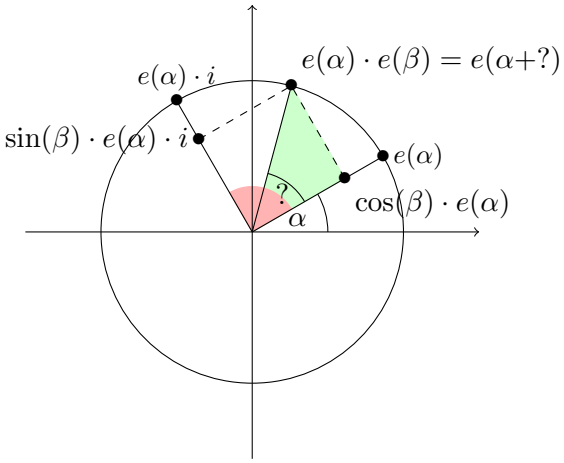
Mit Proposition B.1.4 berechnen wir

$$e(\alpha)\cdot e(\beta) = (e(\alpha))\cdot(\cos(\beta)+\sin(\beta)\cdot i) = e(\alpha)\cdot\cos(\beta)+(e(\alpha)\cdot i)\cdot\sin(\beta) \quad \text{(B.1)}$$

Die Werte $\sin(\beta)$ und $\cos(\beta)$ sind reelle Zahlen ≤ 1. Die Multiplikation mit diesen Werten entspricht daher einer Stauchung, beziehungsweise einer Drehung um 180 Grad und einer Stauchung (falls der Wert negativ ist). Wir nehmen in unseren Zeichnungen an, dass $\sin(\beta)$ und $\cos(\beta)$ positiv sind.



Die Punkte $\sin(\beta) \cdot e(\alpha) \cdot i$ und $\cos(\beta) \cdot e(\alpha)$ können wir nun addieren. Wir wissen bereits, dass die Addition dieser Werte gleich $e(\alpha) \cdot e(\beta)$ ist (siehe (B.1)). Da einer der Winkel ein rechter Winkel ist, ist das Parallelogramm, welches wir für die Addition der beiden Punkte benutzen, tatsächlich ein Rechteck.



Betrachten wir das grüne Dreieck (das einen rechten Winkel und die Seitenlängen 1, $\cos(\beta)$ und $\sin(\beta)$ hat), dann sehen wir, dass der Winkel ? die Gleichungen $\sin(?) = \sin(\beta)$ und $\cos(?) = \cos(\beta)$ erfüllt. Damit ist $?= \beta$ und insbesondere ist damit $e(\alpha + \beta) = e(\alpha) \cdot e(\beta)$. Das war zu zeigen!
Wenn $\cos(\alpha)$ und/oder $\sin(\alpha)$ negativ ist, dann funktioniert der Beweis fast genau so. □

Korollar B.1.7. *Sind $u = r \cdot e(\alpha)$ und $v = s \cdot e(\beta)$ zwei komplexe Zahlen in Polarkoordinaten, dann ist $u \cdot v = (r \cdot s) \cdot e(\alpha + \beta)$.*

Anhang C

Der große Satz von Fermat

Den kleinen Satz von Fermat haben wir bereits kennengelernt. Der große Satz von Fermat ist (nach Meinung des Autors) das spektakulärste mathematische Resultate des letzten Jahrhunderts. Wir haben gesehen, dass es unendlich viele (primitive) Pythagoräische Zahlentripel gibt. Das waren natürliche Zahlen a, b, c mit $a^2 + b^2 = c^2$. Das bedeutet, dass die Gleichung

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

unendlich viele Lösungen in den natürlichen Zahlen besitzt. Gilt das auch für die Gleichung $x^3 + y^3 = z^3$? Oder $x^4 + y^4 = z^4$? ...
Fermat schrieb dazu folgende Aussage auf einen Seitenrand des Buches mit dem er Mathematik studierte:

> *„Es ist jedoch nicht möglich, einen Kubus in 2 Kuben, oder ein Biquadrat in 2 Biquadrate und allgemein eine Potenz, höher als die zweite, in 2 Potenzen mit ebendemselben Exponenten zu zerlegen: Ich habe hierfür einen wahrhaft wunderbaren Beweis entdeckt, doch ist dieser Rand hier zu schmal, um ihn zu fassen.“*

Diese Aussage traf er ca. 1640 und in moderner Sprache behauptete er den folgenden Satz beweisen zu können.

Theorem C.0.1. *Für $n \geq 3$ besitzt die Gleichung $x^n + y^n = z^n$ keine Lösung in den natürlichen Zahlen $\mathbb{N}$.*

Den Fall $n = 4$ hatte Fermat tatsächlich bewiesen, der Fall $n = 3$ wurde erst von Euler (1770) gezeigt. Für $n = 5$ wurde Fermats Behauptung 1825

von Dirichlet und Legendre bewiesen. Es folgten immer mehr Spezialfälle. Durch Einsatz von Computern wurde die Behauptung 1952 für alle $n \leq 2000$ bestätigt. Ein voller Beweis von Theorem C.0.1 wurde allerdings erst 1994 von Andrew Wiles (*1953) und Richard Taylor (*1962) präsentiert. Dieser Beweis benutzte modernste Mathematik und neben Wiles und Taylor hatten viele weitere Mathematiker entscheidenden Anteil am Beweis (unter Anderem Gerhard Frey, der lange an der Universität Duisburg-Essen arbeitete).

Einschub

Auch wenn man es nicht mit entgültiger Sicherheit sagen kann, ist davon auszugehen, dass es Fermats „wahrhaft wunderbaren Beweis“ nicht gibt. Durch seine Notiz wurde die Vermutung rasch sehr populär. Die spannende Geschichte von Fermat bis Wiles wird sehr unterhaltsam in dem Buch *Fermats letzter Satz* von Simon Singh erzählt.

Wir werden hier den einfachsten Fall $n = 4$ studieren. Dazu beweisen wir – wie Fermat selbst – eine geometrische Aussage. Nämlich:

Satz C.0.2. *Der Flächeninhalt eines rechtwinkligen Dreiecks, dessen Seitenlängen alle ganzzahlig sind, ist keine Quadratzahl.*

Bevor wir den Satz beweisen sollten wir überlegen, was das mit dem großen Satz von Fermat zutun haben soll. Wir nehmen kurz an, der Satz wäre korrekt. Dann erhalten wir den großen Satz von Fermat für $n = 4$.

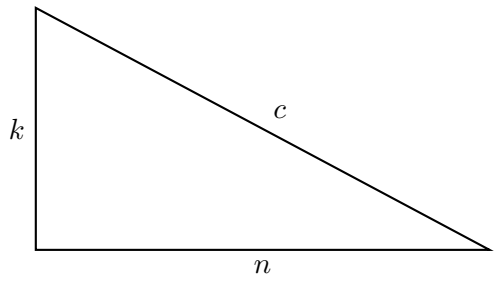
Korollar C.0.3. *Die Gleichung $x^4 + y^4 = z^4$ hat keine Lösung in den natürlichen Zahlen $\mathbb{N}$.*

Beweis. Wir führen einen Widerspruchsbeweis. Angenommen es gäbe ganze Zahlen a', b', c' mit $(a')^4 + (b')^4 = (c')^4$. Sei d der ggT von a', b', c'. Dann gilt

$$(\underbrace{\frac{a'}{d}}_{=a\in\mathbb{N}})^4 + (\underbrace{\frac{b'}{d}}_{=b\in\mathbb{N}})^4 = (\underbrace{\frac{c'}{d}}_{=c\in\mathbb{N}})^4.$$

Die Zahlen a, b, c sind nun teilerfremd und erfüllen $(a^2)^2 + (b^2)^2 = (c^2)^2$. Dann ist (a^2, b^2, c^2) ein Pythagoräisches Zahlentripel. Da wir ohne weiteres a und b vertauschen können, dürfen wir annehmen, dass a ungerade ist. Damit erhalten wir ein *primitives* Pythagoräisches Zahlentripel. Nach Theorem

4.1.15 existieren $n, k \in \mathbb{N}$ mit $a^2 = n^2 - k^2$, $b^2 = 2nk$ und $c^2 = n^2 + k^2$. Wir betrachten das rechtwinklige Dreieck



Dieses hat ganzzahlige Seitenlängen und der Flächeninhalt ist $\frac{1}{2} \cdot nk = (\frac{b}{2})^2$. Da b gerade ist, ist dies eine Quadratzahl. Nach Satz C.0.2 existiert ein solches rechtwinkliges Dreieck aber nicht. Damit muss unsere Annahme, dass die Gleichung $x^4 + y^4 = z^4$ eine Lösung besitzt, falsch gewesen sein. □

Bemerkung C.0.4. Bevor wir Satz C.0.2 beweisen, wollen wir die Struktur des Beweises erklären. Der Beweis den wir führen werden ist ein Widerspruchsbeweis. Wir werden also annehmen, dass es ein rechtwinkliges Dreieck gibt, dessen Seitenlängen a, b, c natürliche Zahlen sind und dessen Flächeninhalt $\frac{1}{2}ab$ eine Quadratzahl f_0^2 ist. Aus dieser Annahme folgern wir, dass es dann ein weiteres rechtwinkliges Dreick mit ganzzahligen Seitenlängen und Flächeninhalt $\underbrace{f_1^2}_{\in \mathbb{N}} < f_0^2$ gibt.

Warum erhalten wir damit einen Widerspruch? Das sieht man, wenn man das Argument wiederholt. Denn es gibt damit auch ein solches Dreieck mit ganzzahligen Seitenlängen und Flächeninhalt $f_2^2 < f_1^2 < f_0^2$, und so weiter und so weiter. Wir haben also eine unendliche Folge $f_0^2 > f_1^2 > f_2^2 > f_3^2 > \ldots$ von immer kleiner werdenden natürlichen (Quadrat-)Zahlen konstruiert. Das kann aber nicht möglich sein, da es nur $f_0^2 - 1$ natürliche Zahlen gibt, die kleiner als f_0^2 sind! Dieses geniale Argument wird auch *Fermat'scher Abstieg* genannt.

Wir benötigen noch ein letztes kleines Lemma.

Lemma C.0.5. *Sei $a \in \mathbb{N}$ und $a^2 = k \cdot n$ für teilerfremde natürliche Zahlen n und k. Dann sind n und k Quadratzahlen.*

Beweis. Falls $a = 1$ ist, ist die einzige mögliche Zerlegung $a^2 = 1 \cdot 1$ und somit sind $n = 1$ und $k = 1$ offensichtlich Quadratzahlen. Sei also $a \geq 2$. Dann besitzt a eine Primfaktorzerlegung

$$a = p_1^{e_1} \cdot \ldots p_r^{e_r} \quad \text{mit } p_1, \ldots, p_r \text{ Primzahlen und } e_1, \ldots, e_r \in \mathbb{N}.$$

Damit ist $a^2 = p_1^{2e_1} \cdot \ldots p_r^{2e_r}$, es kommen also alle Primfaktoren mit einem geraden Exponenten vor. Wir zerlegen nun a^2 in ein Produkt von teilerfremden Zahlen n und k – d.h. n und k haben keinen gemeinsamen Primfaktor. Dann muss p_1 eine der Zahlen n und k teilen; sagen wir $p_1 \mid n$. Da $p_1 \nmid k$, aber der Exponent von p_1 in nk gleich dem Exponent von p_1 in a^2 ist, ist $p_1^{2e_1} \mid n$. Machen wir dies für jede Primzahl $p_1, \ldots, p_r$, so sehen wir, dass jeder Primteiler von n und von k mit einem geraden Exponenten vorkommt. Damit sind n und k Quadratzahlen. □

Die Aussage ist natürlich falsch ohne die Voraussetzung $\mathrm{ggT}(n, k) = 1$. Zum Beispiel ist $4 = 2 \cdot 2$, aber 2 ist keine Quadratzahl.

Beweis von Satz C.0.2. Die Struktur des Beweises haben wir ja schon erklärt. Wir führen einen Widerspruchsbeweis und nehmen an es gäbe ein Dreieck mit Seitenlängen $a, b, c \in \mathbb{N}$ und Flächeninhalt $\frac{1}{2}ab = f^2$. Das impliziert, dass c die Länge der Hypothenuse ist und somit gilt $a^2 + b^2 = c^2$. Wir dürfen also annehmen, dass b eine gerade Zahl ist. Insbesondere ist $\frac{1}{2}ab$ tatsächlich eine natürliche Zahl. Unser Ziel ist es ein kleineres rechtwinklieges Dreieck zu konstruieren, dessen Flächeninhalt immer noch eine Quadratzahl ist.

Falls es ein $d > 1$ gibt mit $d \mid a$, $d \mid b$ und $d \mid c$, ist dies recht einfach. Dann können wir das Dreick um den Faktor d stauchen und erhalten ein rechtwinkliges Dreieck mit den Seitenlängen $\frac{a}{d}, \frac{b}{d}, \frac{c}{d} \in \mathbb{N}$ mit Flächeninhalt $\frac{1}{2}\frac{ab}{d^2} = \frac{f^2}{d^2} = (\frac{f}{d})^2 < f^2$.

Einschub

Hier muss man sich streng genommen natürlich noch überlegen, warum $\frac{f}{d} \in \mathbb{N}$ ist. Da jedoch nach Voraussetzung $(\frac{a}{d})^2 + (\frac{b}{d})^2 = (\frac{c}{d})^2$ ein Pythagoräisches Zahlentripel bildet, ist ohne Einschränkung $\frac{b}{d}$ eine gerade Zahl. Damit ist $\frac{f^2}{d^2} = \frac{1}{2} \cdot \frac{a}{d} \cdot \frac{b}{d} \in \mathbb{N}$. Das bedeutet genau $d^2 \mid f^2$, also auch $d \mid f$. Damit ist tatsächlich $\frac{f}{d} \in \mathbb{N}$ und $(\frac{f}{d})^2$ eine Quadratzahl.

Wir dürfen also ab jetzt annehmen, dass die Seitenlängen a, b, c teilerfremd sind. Dann ist aber (a, b, c) ein primitives Pythagoräisches Zahlentripel und somit existieren teilerfremde $n, k \in \mathbb{N}$, mit $n \not\equiv k \mod 2$, so dass gilt

$$a = n^2 - k^2 \qquad b = 2nk \qquad c = n^2 + k^2.$$

Den Flächeninhalt f^2 können wir nun mit Hilfe von n und k darstellen als

$$f^2 = \frac{1}{2}ab = \frac{1}{2} \cdot (n^2 - k^2) \cdot (2nk) = nk(n^2 - k^2) \tag{C.1}$$

Hieraus konstruieren wir in einigen Schritten das gesuchte Dreieck.

1. Schritt: Es ist $\mathrm{ggT}(nk, n^2 - k^2) = 1$.

Angenommen es gäbe eine Primzahl p, die nk und $n^2 - k^2$ teilt. Aus $p \mid nk$ und der Eigenschaft einer Primzahl, folgt $p \mid n$ oder $p \mid k$; sagen wir $p \mid n$. Dann folgt auch $p \mid n^2$ und nach Annahme $p \mid n^2 - k^2$. Damit teilt p auch die Differenz, also $p \mid n^2 - (n^2 - k^2) = k^2$. Es folgt (wieder da p eine Primzahl ist) $p \mid k$. Damit ist p ein gemeinsamer Teiler von n und k, aber $\mathrm{ggT}(n, k) = 1$. Damit kann eine solche Primzahl nicht existieren und der erste Schritt ist bewiesen.

2. Schritt Es existieren natürliche Zahlen r, s, t, u mit

$$n = r^2 \qquad k = s^2 \qquad n - k = t^2 \qquad n + k = u^2$$

D.h.: Die Elemente $n, k, n - k, n + k$ sind Quadratzahlen.

Nach dem 1. Schritt ist $\mathrm{ggT}(nk, n^2 - k^2) = 1$. Aus (C.1) und Lemma C.0.5 sind somit $nk = x^2$ und $(n^2 - k^2) = y^2$ Quadratzahlen. Weiter sind auch n

und k teilerfremd. Wieder mit Lemma C.0.5 sind somit $n = r^2$ und $k = s^2$ Quadratzahlen.
Es ist weiter $y^2 = n^2 - k^2 = (n-k)(n+k)$ und $n-k$ und $n+k$ sind teilerfremd (das beweist man ganz genau wie Lemma 4.1.16). Somit können wir auch hier Lemma C.0.5 anwenden und erhalten wie gewünscht, dass $n - k$ und $n + k$ Quadratzahlen sind.

3. Schritt: $(\frac{u-t}{2}, \frac{u+t}{2}, r)$ ist ein Pythagoräisches Zahlentripel.

Aus dem 2. Schritt lesen wir sofort ab, dass $u > t$ gilt. Es sind also alle drei Einträge positiv. Da eine der Zahlen n und k gerade und die andere ungerade ist, sind $n - k = t^2$ und $n + k = u^2$ ungerade. Insbesondere sind auch t und u ungerade. Es folgt, dass $u-t$ und $u+t$ gerade sind. Damit sind auch alle Einträge natürliche Zahlen. Dass es sich um ein Pythagoräisches Zahlentripel handelt zeigt die folgende Rechnung

$$\begin{aligned}(\frac{u-t}{2})^2 + (\frac{u+t}{2})^2 &= \frac{u^2 - 2ut + t^2 + u^2 + 2ut + t^2}{4} \\ &= \frac{2(u^2+t^2)}{4} \overset{\text{2. Schritt}}{=} \frac{4n}{4} = n = r^2.\end{aligned}$$

4. Schritt: Es existiert ein $s' \in \mathbb{N}$ mit $s = 2 \cdot s'$. D.h.: Die Zahl s aus dem 2. Schritt ist gerade.

Wir wissen bereits, dass u und t ungerade sind. Damit gilt $u^2 \equiv 1 \equiv t^2 \mod 4$. Es folgt

$$2s^2 = 2k = (n+k) - (n-k) = u^2 - t^2 \equiv 1 - 1 \equiv 0 \mod 4.$$

Damit ist $4 \mid 2s^2$ und somit $2 \mid s^2$. Es ist also s^2 eine gerade Zahl und somit auch s selbst. Damit ist der 4. Schritt bewiesen.

5. Schritt: Es gibt ein rechtwinkliges Dreieck mit Seitenlängen $\frac{u-t}{2}, \frac{u+t}{2}, r$ und Flächeninhalt $(s')^2$.

Aus dem 3. Schritt sehen wir sofort, dass es ein rechtwinkliges Dreieck mit den angegebenen Seitenlängen gibt. Der Flächeninhalt ist

$$\frac{1}{2} \cdot \frac{u-t}{2} \cdot \frac{u+t}{2} = \frac{1}{2} \cdot \frac{u^2-t^2}{4} \overset{\text{2. Schritt}}{=} \frac{s^2}{4} = (\frac{s}{2})^2 = (s')^2.$$

Das Dreieck aus diesem 5. Schritt ist kleiner als unser Dreieck mit Seitenlängen a, b, c und Flächeninhalt f^2, denn:

$$(s')^2 < s^2 = k \overset{(C.1)}{<} f^2.$$

Damit ist der Beweis beendent, da der Fermat'sche Abstieg (siehe Bemerkung C.0.4) einen Widerspruch liefert. □