Vorlesungsnotizen

Version 2.2

Zahlentheorie

Mathematik für Sekundarlehrer/innen

Franz Müller

Frühling 2017

Inhaltsverzeichnis

Einführung

Gemeinhin versteht man unter *Zahlentheorie* das Teilgebiet der Mathematik, das sich speziell mit Eigenschaften natürlicher Zahlen beschäftigt. Ein grundlegendes Resultat dieser Theorie, das man ansatzweise schon in *Euklids Elementen* ($\sigma\tau o\iota\chi\epsilon\tilde{\iota}\alpha$) findet, besagt, dass jede natürliche Zahl

$$n \in \mathbb{N}_0 = \{0, 1, 2, 3, \dots\} \text{ mit } n > 1$$

auf eine und nur eine Art als Produkt

$$n = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_k \quad \text{mit } 1 < p_1 \leq p_2 \leq \cdots \leq p_k$$

von Faktoren $p_1, \dots, p_k \in \mathbb{N}$ geschrieben werden kann, wobei die Zahlen $p_j > 1$ sich nicht ihrerseits als Produkt von mehreren Faktoren > 1 schreiben lassen, also sog. *Primzahlen* sind. Ausformuliert findet man bei Euklid bereits einen Beweis, dass die Menge der Primzahlen

$$\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, \dots\}$$

nicht endlich sein kann. Denn keine Primzahl aus einer endlichen Liste ist ein Faktor in der obigen Dastellung derjenigen Zahl, die um 1 grösser ist als das Produkt aller Zahlen in der endlichen Liste. Zum Beispiel ist $2{\cdot}3{+}1 = 7$ (Primzahl), $2{\cdot}3{\cdot}7{+}1 = 43$ (Primzahl), $2{\cdot}3{\cdot}7{\cdot}43{+}1 = 13{\cdot}139$ (beides Primzahlen), $2{\cdot}3{\cdot}7{\cdot}43{\cdot}13{\cdot}139{+}1 = 3263443$ (Primzahl), $2 \cdot 3 \cdot 7 \cdot 43 \cdot 13 \cdot 139 \cdot 3263443 + 1 = 547 \cdot 607 \cdot 1033 \cdot 31051$ (vier weitere Primzahlen), usw. usf.
Da diese Resultate schon so alt sind, denkt man vielleicht, heute wüsste man bedeutend mehr über das Wesen der natürlichen Zahlen. Zum Beispiel fanden
Fermat [1]: Eine Primzahl $p \neq 2$ ist Summe zweier Quadrate $\Leftrightarrow p = 4 \cdot n + 1$, z.B.

$$13 = 2^2 + 3^2, \quad 19 \neq n^2 + m^2 \quad \text{für alle } m, n \in \mathbb{N}_0 \ .$$

Euler [2]: $a^3 + b^3 \neq c^3$ für alle $a, b, c \in \mathbb{N}$.
Hadamard und *de la Vallée Poussin* (1896): Strebt $n \longrightarrow \infty$, so strebt

$$q(n) = \frac{\pi(n)}{n/\ln(n)} \longrightarrow 1 \ ,$$

wobei $\pi(n)$ die Anzahl Primzahlen $\leq n$ ist. Beispiel: $q(66) = 18/[66/\ln(66)] \approx 1.14$.
Wiles (1994): $a^n + b^n \neq c^n$ für alle $a, b, c, n \in \mathbb{N}$ mit $n > 2$.
Mihailescu (2002): $a^n - b^m = 1$ mit $1 < a, b, m, n \in \mathbb{N} \Leftrightarrow a = 3 = m \wedge b = 2 = n$.
Zhang (2013): Es gibt beliebig viele Primzahlen, die sich um genau k unterscheiden (für ein $0 < k \leq 70'000'000$).

[1] Brief an *Marin Mersenne* vom 25. Dezember 1640. Beweis durch Euler um 1750.
[2] Beweis publiziert 1770. „*Grosser Satz von Fermat*“ für $n = 3$.

Gerade das letzte Resultat, das inzwischen allerdings bereits zu $0 < k \leq 246$ verschärft wurde, zeigt jedoch, wie zum Teil unglaublich schwierig wohl diese Tatsachen nachzuweisen sind. Seit Jahrtausenden vermutet man nämlich, dass es beliebig viele Primzahlen gibt, die sich um $k = 2$ unterscheiden (sog. *Primzahlzwillinge*). In der Zahlentheorie zeigt sich exemplarisch, wie menschliche Erkenntnis manchmal nur durch Jahrhunderte langes Bemühen entsteht, jedoch auch, wie gross die verbleibende Unkenntnis ist.
In dieser Veranstaltung wollen wir uns dessen zwar bewusst sein, jedoch uns auf leichter zugängliche Dinge konzentrieren. Auch die sind es wert, dass man sich mit ihnen beschäftigt.

PS:

Die vorliegenden Notizen werden evtl. ab und zu gemäss Vorlesungsverlauf ergänzt. Die Versions–Nummer 2.n auf dem Titelblatt gibt Aufschluss über ein allfälliges Update.

Kapitel 1

Zahlensysteme

Wir wollen uns nicht nur mit den natürlichen, sondern auch mit ganzen, rationalen, reellen, vielleicht sogar komplexen Zahlen oder auch mit endlichen Zahlenmengen beschäftigen.

1.1 Die natürlichen Zahlen

Dennoch beginnen wir hier zunächst mit den natürlichen Zahlen [1]

$$\mathbb{N}_0 = \{0, 1, 2, 3, \dots\}$$

mit denen wir schon recht gut vertraut sind.

1.1.1 Grundoperationen, Ordnung, Induktionsprinzip

Wir haben auf diesen Zahlen bekanntlich die Addition „+“ mit Neutralelement 0,

$$\begin{aligned} + \quad &: \mathbb{N}_0 \times \mathbb{N}_0 \quad \longrightarrow \mathbb{N}_0 \\ &\quad (m, n) \quad \mapsto m + n \end{aligned}$$

und die Multiplikation „$\cdot$“mit Neutralelement 1,

$$\begin{aligned} \cdot \quad &: \mathbb{N}_0 \times \mathbb{N}_0 \quad \longrightarrow \mathbb{N}_0 \\ &\quad (m, n) \quad \mapsto m \cdot n \end{aligned}$$

mit den bekannten Rechengesetzen: *Kommutativität* ($m+n = n+m, m \cdot n = n \cdot m$), *Assoziativität* ($a + (b + c) = (a + b) + c, a \cdot (b \cdot c) = (a \cdot b) \cdot c$) und *Distributivität* der Multiplikation über die Addition ($a \cdot (b + c) = a \cdot b + a \cdot c$), die für alle $a, b, c \in \mathbb{N}_0$ (und natürlich auch in $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, ...) gelten.
Wichtig ist ferner die totale Ordnung $<$ bzw. $\leq$ auf $\mathbb{N}_0$, die mit der Addition und Multiplikation verträglich ist. Für alle $a, b, c \in \mathbb{N}_0$ gilt nämlich

$$b < c \Leftrightarrow a + b < a + c \Leftrightarrow a \cdot b < a \cdot c \ ,$$

[1] Die positiven ganzen Zahlen $\{1, 2, 3, \dots\}$, also $\mathbb{N}_0 \setminus \{0\}$, werden mit $\mathbb{N}$ bezeichnet.

wobei die letzte Implikation nach rechts ($\ldots \Rightarrow a \cdot b < a \cdot c$) natürlich nur für $a \neq 0$ gilt.
Jede nicht–leere Teilmenge $M \subset \mathbb{N}_0$ hat ein eindeutiges kleinstes Element n_0 und es gilt das sog. *Induktionsprinzip*[2], dass nämlich die nicht–leere Teilmenge M von $\mathbb{N}_0$ gleich der Menge

$$\widetilde{M} = \{n \in \mathbb{N}_0 \,|\, n_0 \leq n\}$$

ist, genau dann wenn sie n_0 als kleinstes Element enthält und zu jedem n auch $n+1$. Eine Teilmenge mit dieser Eigenschaft ist also ganz $\mathbb{N}_0$, genau dann wenn $n_0 = 0$ ihr kleinstes Element ist. Beweise von Aussagen über (Teilmengen von) natürlichen Zahlen werden oft mit diesem *Prinzip der vollständige Induktion* (PVI) geführt.

1.1.2 Teiler

Eine natürliche Zahl $a \in \mathbb{N}$ ist defnitionsgemäss ein *Teiler* von $b \in \mathbb{N}_0$, man schreibt Teiler

$$a|b \ ,$$

(und sagt „*a teilt b*“) genau dann wenn es ein $c \in \mathbb{N}_0$ gibt, so dass $a \cdot c = b$.
Jede natürliche Zahl a ist ein Teiler von 0 (da $a \cdot c = 0$ für alle $a \in \mathbb{N}_0$ und $c = 0$) und 1 ist ein Teiler jeder natürlichen Zahl $b \in \mathbb{N}_0$ (da $1 \cdot c = b$ für $c = b \in \mathbb{N}_0$).
Für eine positive ganze Zahl $b \in \mathbb{N}$ ist die Menge ihrer Teiler, wir schreiben dafür

$$\mathbb{T}(b) \ ,$$

eine Teilmenge der natürlichen Zahlen von 1 bis b mit 1 als kleinstem und b als grösstem Element. (Ausserdem gilt $\mathbb{T}(0) = \mathbb{N}_0$.)
Aufgabe
Beweise, dass für $a, b, c \in \mathbb{N}$ mit $a \cdot c = b$ gilt

$$(a < b \wedge c < b) \vee (a = 1) \vee (c = 1) \ .$$

gemeinsame Teiler
Für $b, d \in \mathbb{N}$ nennt man die nicht–leere, endliche Menge

$$\mathbb{T}(b) \cap \mathbb{T}(d)$$

ihre *gemeinsamen Teiler*. (Ferner gilt $\mathbb{T}(b) \cap \mathbb{T}(0) = \mathbb{T}(b) \cap \mathbb{N}_0 = \mathbb{T}(b)$ etc.).
Definition ggT
Das grösste Element t in $\mathbb{T}(b) \cap \mathbb{T}(d)$ heisst *grösster gemeinsamer Teiler* von b und ggT
d, man schreibt

$$\mathrm{ggT}(b, d) \quad \text{(in der Literatur auch kurz:} \quad (b, d) \text{)} \ .$$

Mann nennt b und d *teilerfremd*, falls $t = \mathrm{ggT}(b, d) = 1$. teilerfremd

[2] nicht mit dem *Induktionsprinzip* aus der Philosophie zu verwechseln

Natürlich gilt $t \leq \min\{b, d\}$. Es gilt sogar

Satz (ggT)
$t = \mathrm{ggT}(b, d)$ — der grösste gemeinsame Teiler zweier positiver zahlen $b, d \in \mathbb{N}$ — ist die *kleinste positive* Zahl der Form $a \cdot b + c \cdot d$ mit $a, c \in \mathbb{Z}$.
Ferner ist jeder gemeinsame Teiler in $\mathbb{T}(b) \cap \mathbb{T}(d)$ ein Teiler von $\mathrm{ggT}(b, d)$ (und natürlich umgekehrt), also

$$\mathbb{T}(b) \cap \mathbb{T}(d) = \mathbb{T}(\mathrm{ggT}(b, d)) = \mathbb{T}(t) \ .$$

Beweis:
Jeder gemeinsame Teiler q von b und d ist Teiler von $a \cdot b + c \cdot d$, denn aus $\tilde{a} \cdot q = b$ und $\tilde{c} \cdot q = d$ folgt

$$(a \cdot \tilde{a} + c \cdot \tilde{c}) \cdot q = a \cdot (\tilde{a} \cdot q) + c \cdot (\tilde{c} \cdot q) = a \cdot b + c \cdot d \ .$$

Die kleinste positive Zahl der Form $a \cdot b + c \cdot d$ muss also mindestens so gross sein, wie der grösste gemeinsame Teiler t von b und d. Und wenn t als $a \cdot b + c \cdot d$ geschrieben werden kann, so wird t selber von jedem gemeinsamen Teiler von b und d geteilt. Wir beweisen nun, dass $\mathrm{ggT}(b, d) = a \cdot b + c \cdot d$ für gewisse $a, c \in \mathbb{Z}$. Dies folgt aus nachstehendem, überaus wichtigen Algorithmus. Damit ist der Satz dann bewiesen. □

1.1.3 Euklidscher Algorithmus, Lemma von Euklid

Gegeben seien zwei positive ganze Zahlen $b, d \in \mathbb{N}$.
Ist $b = d$, so ist $\mathrm{ggT}(b, d) = a \cdot b + c \cdot d$, z.B. mit $a = 1$ und $c = 0$.
Ist $b \neq d$, so nennen wir die grössere der beiden Zahlen b_0, die kleinere b_1 und $b_2 = b_0 - m_1 \cdot b_1 < b_1$, wobei $m_1 \geq 1$ die grösstmögliche natürliche Zahl ist, so dass $b_2 \geq 0$ noch gewährleistet ist[3]. Jeder gemeinsame Teiler von b_0 und b_1 ist ein gemeinsamer Teiler von b_1 und b_2 und umgekehrt. Also gilt auch für je die grössten gemeinsamen Teiler

$$\mathrm{ggT}(b_0, b_1) = \mathrm{ggT}(b_1, b_2) \ .$$

Mit $b_1 > b_2$ so fortfahrend, wie vorher mit $b_0 > b_1$ erhalten wir eine strikt fallende Folge natürlicher Zahlen, die zwangsläufig mit $b_{n+1} = 0$ enden muss,

$$b_0 > b_1 > b_2 > \cdots > b_n > b_{n+1} = 0 \ ,$$

und für die $\mathrm{ggT}(b, d) = \mathrm{ggT}(b_0, b_1) = \mathrm{ggT}(b_1, b_2) = \cdots = \mathrm{ggT}(b_n, b_{n+1}) = \mathrm{ggT}(b_n, 0) = b_n$ gilt. Ausserdem gilt für entsprechend gewählte a_k, c_k $(0 \leq k \leq n-2)$

$$\begin{aligned}
\mathrm{ggT}(b, d) = b_n &= b_{n-2} - m_{n-1} \cdot b_{n-1} = a_{n-2} \cdot b_{n-2} + c_{n-2} \cdot b_{n-1} \\
&= b_{n-2} - m_{n-1} \cdot (b_{n-3} - m_{n-2} \cdot b_{n-2}) = a_{n-3} \cdot b_{n-3} + c_{n-3} \cdot b_{n-2} \\
&= \ldots \\
&= a_0 \cdot b_0 + c_0 \cdot b_1 = a \cdot b + c \cdot d \ ,
\end{aligned}$$

[3] siehe auch Unterabschnitt 1.2.2: *Teilen mit Rest*

falls $n > 1$. (Ist bereits $b_2 = 0$, so ist $b_0 = m_1 \cdot b_1$ und $b_1 = \mathrm{ggT}(b, d)$, also die kleinere der beiden Zahlen b und d.) □

Beispiel *Euklidscher Algorithmus* Euklidscher Algorith.

Sei $b = b_0 = 1292$ und $d = b_1 = 247$. Dann ist

$$\begin{aligned} b_2 &= b_0 - 5 \cdot b_1 = 1292 - 5 \cdot 247 = 1292 - 1235 = 57 \ , \\ b_3 &= b_1 - 4 \cdot b_2 = 247 - 4 \cdot 57 = 247 - 228 = 19 \ , \\ b_4 &= b_2 - 3 \cdot b_3 = 57 - 3 \cdot 19 = 0 \ . \end{aligned}$$

Also ist $b_3 = 19 = \mathrm{ggT}(1292, 247)$ der grösste gemeinsame Teiler von 1292 und 247 und Zurückrechnen ergibt die Darstellung

$$\begin{aligned} 19 &= 247 - 4 \cdot 57 \ , \\ &= 247 - 4 \cdot (1292 - 5 \cdot 247) = -4 \cdot 1292 + 21 \cdot 247 \end{aligned}$$

als kleinste positive ganze Zahl der Form $a \cdot 1292 + c \cdot 247$ mit $a, c \in \mathbb{Z}$.

Wir fragen uns noch, inwiefern die Darstellung $\mathrm{ggT}(b, d) = a \cdot b + c \cdot d$ mit $a, c \in \mathbb{Z}$ *eindeutig* ist oder eben nicht. Dazu benötigen wir das überaus wichtige

Lemma von Euklid

Seien $b, d, e \in \mathbb{N}_0$ beliebig. Teilt b die Zahl $d \cdot e$ und ist $\mathrm{ggT}(b, d) = 1$, also b und d *teilerfremd*, so teilt b die Zahl e.

Beweis:

Es gibt $a, c \in \mathbb{Z}$ mit $a \cdot b + c \cdot d = 1$ (obiger Satz) und ebenso f mit $b \cdot f = d \cdot e$, da $b | (d \cdot e)$ nach Voraussetzung. Also gilt

$$e = 1 \cdot e = (a \cdot b + c \cdot d) \cdot e = a \cdot b \cdot e + c \cdot (d \cdot e) = a \cdot b \cdot e + c \cdot (b \cdot f) = (a \cdot e + c \cdot f) \cdot b \ ,$$

das heisst, b teilt e. □

Zurück zu unserer Frage nach der Eindeutigkeit der Darstellung

$$\mathrm{ggT}(b, d) = a \cdot b + c \cdot d = \tilde{a} \cdot b + \tilde{c} \cdot d = \ldots .$$

Wir setzen $t = \mathrm{ggT}(b, d)$ und nehmen an wir hätten zwei Darstellungen von t wie oben. Dann ist

$$(a - \tilde{a}) \cdot b = (\tilde{c} - c) \cdot d \ .$$

Damit wir das Lemma anwenden können, teilen wir auf beiden Seiten durch t,

$$(a - \tilde{a}) \cdot \tilde{b} = (\tilde{c} - c) \cdot \tilde{d} \ ,$$

wobei jetzt $\tilde{b} = b/t$ und $\tilde{d} = d/t$ teilerfremd sind (Begründung?). Nach dem Lemma oben ist also $\tilde{b}$ ein Teiler von $(\tilde{c} - c)$ oder $\tilde{c} - c = m \cdot \tilde{b}$ oder $\tilde{c} = c + m \cdot \tilde{b} = c + m \cdot b/t$. Ebenso ist $\tilde{a} = a - m \cdot d/t$ und

$$\mathrm{ggT}(b, d) = (a - m \cdot d/t) \cdot b + (c + m \cdot b/t) \cdot d \quad (m \in \mathbb{Z} \text{ beliebig})$$

sind alle Darstellungen des grössten gemeinsamen Teilers von b und d in der Form $x \cdot b + y \cdot d$ mit $x, y \in \mathbb{Z}$. Daraus folgt allgemeiner der Satz im nächsten Unterabschnitt.

1.1.4 Ganzzahlige Lösungen einer linearen Gleichung

Satz über ganzzahlige Lösungen einer linearen Gleichung [4]
Für $b, d, f \in \mathbb{N}_0$ mit $t = \text{ggT}(b, d)$ (nicht b und d beide 0) hat die Gleichung

$$b \cdot x + d \cdot y = f$$

i) — genau die ganzzahligen Lösungen $(x, y) = (a - m \cdot d/t, c + m \cdot b/t) \in \mathbb{Z}^2$ ($m \in \mathbb{Z}$ beliebig), falls $t|f$. Es existieren insbesondere sog. partikuläre Lösungen $(a, c) \in \mathbb{Z}^2$ mit $a \cdot b + c \cdot d = f$.

ii) — keine ganzzahlige Lösungen, falls $t \not| f$.

Bemerkungen:
Der Satz gilt entsprechend für $b, d, f \in \mathbb{Z}$.

Im Falle $t|f$ (Lösungen), ist es oft von Vorteil, die Gleichung durch t zu teilen.

Beweis:
Falls x und y ganze Zahlen sind, so teilt jeder gemeinsame Teiler, insbesondere der grösste, von b und d auch $b \cdot x + d \cdot y = f$. Ist $\tilde{a} \cdot b + \tilde{c} \cdot d = t = \text{ggT}(b, d)$ eine Darstellung von t, so findet man also die partikuläre Lösung $x = a = n \cdot \tilde{a}$, $y = c = n \cdot \tilde{c}$, falls $t \cdot n = f$ gilt und andernfalls gibt es keine ganzzahligen Lösungen. Die angegebene Darstellung *aller* Lösungen ergibt sich dann aus den Überlegungen, die dem Satz vorausgehen — siehe vorhergehenden Unterabschnitt. □

1.1.5 Vielfache

Sei $a \in \mathbb{N}_0$. Ist a ein Teiler von b, so heisst b ein *Vielfaches* von a. Die Menge $\mathbb{V}(a)$ der *Vielfachen* von a besteht also aus den Elementen von Vielfache

$$\mathbb{V}(a) = \{0 \cdot a\,,\ 1 \cdot a\,,\ 2 \cdot a\,,\ 3 \cdot a\,,\ \dots\} = \{0\,,\ a\,,\ 2a\,,\ 3a\,,\ \dots\}\ .$$

Sind v und w zwei Elemente aus $\mathbb{V}(a)$, so auch $v + w$ und $v \cdot w$. Die Mengen $\mathbb{V}(a)$ der Vielfachen einer natürlichen Zahl sind also abgeschlossen unter den Grundoperationen der Addition und Multiplikation. Dies ganz im Gegensatz zu den Mengen $\mathbb{T}(a)$ der Teiler einer natürlichen Zahl, die eine viel kompliziertere Struktur haben können.

gemeinsame Vielfache
Sind $a, c \in \mathbb{N}$ zwei positive ganze Zahlen, so nennt man

$$\mathbb{V}(a) \cap \mathbb{V}(c)$$

ihre *gemeinsamen Vielfachen*. (Ferner gilt $\mathbb{V}(a) \cap \mathbb{V}(0) = \mathbb{V}(0) = \{0\}$ etc.).

Definition kgV
Das kleinste Element $v > 0$ in $\mathbb{V}(a) \cap \mathbb{V}(c)$ heisst *kleinstes gemeinsames Vielfaches* von a und c, man schreibt dafür $\text{kgV}(a, c)$. kgV

[4] Vgl. mit der Darstellung aller *reellen* Lösungen, Vorlesung *Geometrie und lineare Algebra.*

Satz über kgV und ggT
Seien $a, b \in \mathbb{N}$ zwei positive ganze Zahlen. Es gilt $\mathbb{T}(a) \cap \mathbb{T}(b) = \mathbb{T}(\mathrm{ggT}(a,b))$, was in 1.1.2 bereits beweisen wurde, sowie

$$\mathbb{V}(a) \cap \mathbb{V}(b) = \mathbb{V}(\mathrm{kgV}(a,b)) \quad \text{und} \quad \mathrm{ggT}(a,b) \cdot \mathrm{kgV}(a,b) = a \cdot b \ .$$

Beispiel:
$\mathrm{ggT}(12,18) = 6$, $\mathrm{kgV}(12,18) = 36$, $\mathrm{ggT}(12,18) \cdot \mathrm{kgV}(12,18) = 6 \cdot 36 = 216 = 12 \cdot 18$.
Beweis:
Sei $s = m \cdot a = n \cdot b$ ein gemeinsames Vielfaches von a und b und sei $t = \mathrm{ggT}(a,b)$. Dann ist $s = m \cdot t \cdot \tilde{a} = n \cdot t \cdot \tilde{b}$ mit teilerfremden $\tilde{a} = a/t$ und $\tilde{b} = b/t$. Mit dem Euklidschen Lemma und $m \cdot \tilde{a} = n \cdot \tilde{b}$ folgt $\tilde{a} | n$, also $n = \tilde{a} \cdot c$ und daher $s = \tilde{a} \cdot c \cdot t \cdot \tilde{b} = c \cdot (a \cdot b/t)$. Jedes gemeinsame Vielfache $s \in \mathbb{V}(a) \cap \mathbb{V}(b)$ ist also in $\mathbb{V}(a \cdot b/t)$. Also ist $a \cdot b/t = \tilde{b} \cdot a = \tilde{a} \cdot b$ das kleinste gemeinsame Vielfache von a und b und $\mathrm{ggT}(a,b) \cdot \mathrm{kgV}(a,b) = t \cdot (a \cdot b/t) = a \cdot b$.
(Dass $\mathbb{V}(\mathrm{kgV}(a,b)) \subset \mathbb{V}(a) \cap \mathbb{V}(b)$ gilt, ist trivial, d.h. selbstverständlich.) □

1.1.6 Hauptsatz der Arithmetik und erste Folgerungen

Wir kommen nun zum Hauptsatz der Arithmetik.

Definition Primzahl
Eine positive ganze Zahl $p > 1$ heisst *prim* oder „*eine Primzahl*“ wenn sie nicht das Produkt zweier natürlichen Zahlen $a > 1$ und $b > 1$ ist. Ist $n = a \cdot b$ mit $a > 1$ und $b > 1$, so heisst n *zusammengesetzt*. Die Zahl $n = 1$ ist weder prim noch zusammengesetzt.
Zwei natürliche Zahlen $a > 0$ und $b > 0$ heissen *zueinander prim* oder *teilerfremd*, falls $\mathrm{ggT}(a,b) = 1$ gilt, siehe auch S.4.

prim

zusammengesetzt

Seien $p_1 = 2 < p_2 = 3 < p_3 = 5 < \ldots$ die Primzahlen in aufsteigender Reihenfolge. Wir haben uns bereits in der Einleitung (gemäss Euklid) überlegt, dass die Folge p_k unendlich ist.

Hauptsatz der Arithmetik
Jede positive ganze Zahl $n \in \mathbb{N}$ hat eine und nur eine Darstellung als Produkt

$$n = p_1^{\mathrm{e}_1} \cdot p_2^{\mathrm{e}_2} \cdot p_3^{\mathrm{e}_3} \cdot \ldots \cdot p_k^{\mathrm{e}_k} \cdot \ldots$$

mit eindeutig bestimmten natürlichen Exponenten $\mathrm{e}_k \in \mathbb{N}_0$, die fast alle 0 sind (d.h. alle bis auf endlich viele sind gleich 0 – das Produkt kann also immer auch als *endliches* Produkt geschrieben werden).

Beispiel
$n = 77077 = p_1^0 \cdot p_2^0 \cdot p_3^0 \cdot p_4^2 \cdot p_5^2 \cdot p_6^1 \cdot p_7^0 \cdot p_8^0 \cdot \ldots = 7^2 \cdot 11^2 \cdot 13$.
Beweis
Ist n prim, so ist $n = p_k$ für ein $k = 1, 2, 3, \ldots$. Andernfalls ist $n = a \cdot b$ mit $n > a, b > 1$ oder $n = 1$. Im zweiten Unterfall setzt man alle Exponenten $\mathrm{e}_k = 0$. Im ersten Unterfall kann man a oder b oder beide weiter zerlegen oder einer oder beide Faktoren sind prim. Da die Faktoren bei weiterer Zerlegung kleiner werden aber stets grösser

als 1 bleiben, hat man nach endlich vielen Zerlegungsschritten lauter Primfaktoren, die man noch der Grösse nach ordnen und je in der Form $p_k^{\mathrm{e}_k}$ zusammenfassen muss, um obige Darstellung zu erhalten. Weshalb ist diese Dastellung eindeutig?
Sei $n = p_1^{\mathrm{e}_1} \cdot p_2^{\mathrm{e}_2} \cdot p_3^{\mathrm{e}_3} \cdot \dots = p_1^{\tilde{\mathrm{e}}_1} \cdot p_2^{\tilde{\mathrm{e}}_2} \cdot p_3^{\tilde{\mathrm{e}}_3} \cdot \dots$. Wäre $\mathrm{e}_1 > \tilde{\mathrm{e}}_1$, so würde die natürliche Zahl $p_1^{\mathrm{e}_1 - \tilde{\mathrm{e}}_1} \geq 2$ die Zahl $m = n/p_1^{\tilde{\mathrm{e}}_1} = p_2^{\tilde{\mathrm{e}}_2} \cdot p_3^{\tilde{\mathrm{e}}_3} \cdot \dots$ teilen, die also nicht 1 sein kann. Sei $k > 1$ der kleinste Index mit $\tilde{\mathrm{e}}_k > 0$. Dann ist $m = p_2^0 \cdot p_3^0 \cdot \dots \cdot p_k^{\tilde{\mathrm{e}}_k} \cdot p_{k+1}^{\tilde{\mathrm{e}}_{k+1}} \cdot \dots = a \cdot b$ mit $a = p_k$ und $b = p_k^{\tilde{e}_k - 1} \cdot p_{k+1}^{\tilde{e}_{k+1}} \cdot \dots$. Da $p_1 = 2$ und p_k $(k > 1)$ verschiedene Primzahlen sind, sind sie teilerfremd. Nach dem Euklidschen Lemma teilt also p_1 die Zahl b, die also ihrerseits grösser als 1 sein muss. Da aber nur endliche viele Exponenten $\tilde{e}_k$ nicht 0 sind, können wir mit dem gleichen Argument weitere Faktoren p_k in der Produktdarstellung von b „abtragen“, wie wir es soeben mit m gemacht haben, und landen schliesslich bei 1, was einen Widerspruch ergibt, da 1 nicht durch $p_1 = 2$ teilbar ist. Also kann e_1 nicht grösser als $\tilde{e}_1$ sein und auch nicht kleiner, da wir das Argument ebenso mit vertauschten Rollen von e_1 und $\tilde{e}_1$ führen können. Also gilt $e_1 = \tilde{e}_1$ und daher auch $m = p_2^{\mathrm{e}_2} \cdot p_3^{\mathrm{e}_3} \cdot \dots = p_2^{\tilde{\mathrm{e}}_2} \cdot p_3^{\tilde{\mathrm{e}}_3} \cdot \dots$. Mit fortgesetzter analoger Argumentation schliessen wir $\mathrm{e}_2 = \tilde{\mathrm{e}}_2$, $\mathrm{e}_3 = \tilde{\mathrm{e}}_3$ usw. usf. □

Folgerungen aus dem Hauptsatz der Arithmetik
Aus $a = p_1^{\mathrm{e}_1} \cdot p_2^{\mathrm{e}_2} \cdot p_3^{\mathrm{e}_3} \cdot \dots > 0$ und $b = p_1^{\tilde{\mathrm{e}}_1} \cdot p_2^{\tilde{\mathrm{e}}_2} \cdot p_3^{\tilde{\mathrm{e}}_3} \cdot \dots > 0$ folgt

$$a \cdot b = p_1^{\mathrm{e}_1 + \tilde{e}_1} \cdot p_2^{\mathrm{e}_2 + \tilde{e}_2} \cdot p_3^{\mathrm{e}_3 + \tilde{e}_3} \cdot \dots \ .$$

Deshalb ist $a = p_1^{\mathrm{e}_1} \cdot p_2^{\mathrm{e}_2} \cdot p_3^{\mathrm{e}_3} \cdot \dots$ genau dann ein Teiler von $c = p_1^{\hat{\mathrm{e}}_1} \cdot p_2^{\hat{\mathrm{e}}_2} \cdot p_3^{\hat{\mathrm{e}}_3} \cdot \dots > 0$, wenn für alle $k = 1, 2, 3, \dots$ gilt $\mathrm{e}_k \leq \hat{\mathrm{e}}_k$. Es gibt $\hat{\mathrm{e}}_k + 1$ Zahlen $0, 1, \dots, \hat{\mathrm{e}}_k$, die diese letzte Bedingung erfüllen. Also gilt die

Folgerung 1
Die Zahl $c = p_1^{\hat{\mathrm{e}}_1} \cdot p_2^{\hat{\mathrm{e}}_2} \cdot p_3^{\hat{\mathrm{e}}_3} \cdot \dots > 0$ hat genau $(\hat{\mathrm{e}}_1 + 1) \cdot (\hat{\mathrm{e}}_2 + 1) \cdot (\hat{\mathrm{e}}_3 + 1) \cdot \dots$ Teiler, nämlich

$$\mathbb{T}(c) = \{p_1^{\mathrm{e}_1} \cdot p_2^{\mathrm{e}_2} \cdot p_3^{\mathrm{e}_3} \cdot \dots \mid 0 \leq \mathrm{e}_j \leq \hat{\mathrm{e}}_j \text{ für alle } j = 1, 2, 3 \dots\} \ .$$

Beispiel: Die Zahl $n = p_1^0 \cdot p_2^0 \cdot p_3^0 \cdot p_4^2 \cdot p_5^2 \cdot p_6^1 \cdot p_7^0 \cdot p_8^0 \cdot \dots = 77077$ hat genau $18 = (2+1)(2+1)(1+1)$ Teiler, nämlich

$$\mathbb{T}(77077) = \{7^0 \cdot 11^0 \cdot 13^0, 7^1 \cdot 11^0 \cdot 13^0, 7^2 \cdot 11^0 \cdot 13^0, 7^0 \cdot 11^1 \cdot 13^0, 7^1 \cdot 11^1 \cdot 13^0, \dots\}$$
$$= \{1, 7, 49, 11, 77, 539, 121, 847, 5929, 13, 91, 637, 143, 1001, 7007, 1573, 11011, 77077\}.$$

Folgerung 2
Für $a = p_1^{\mathrm{e}_1} \cdot p_2^{\mathrm{e}_2} \cdot p_3^{\mathrm{e}_3} \cdot \dots > 0$ und $b = p_1^{\tilde{\mathrm{e}}_1} \cdot p_2^{\tilde{\mathrm{e}}_2} \cdot p_3^{\tilde{\mathrm{e}}_3} \cdot \dots > 0$ folgt

$$\begin{aligned} \mathrm{ggT}(a,b) &= p_1^{\min\{\mathrm{e}_1, \tilde{\mathrm{e}}_1\}} \cdot p_2^{\min\{\mathrm{e}_2, \tilde{\mathrm{e}}_2\}} \cdot p_3^{\min\{\mathrm{e}_3, \tilde{\mathrm{e}}_3\}} \cdot \dots \ , \\ \mathrm{kgV}(a,b) &= p_1^{\max\{\mathrm{e}_1, \tilde{\mathrm{e}}_1\}} \cdot p_2^{\max\{\mathrm{e}_2, \tilde{\mathrm{e}}_2\}} \cdot p_3^{\max\{\mathrm{e}_3, \tilde{\mathrm{e}}_3\}} \cdot \dots \ , \end{aligned}$$

und natürlich $a \cdot b = \mathrm{ggT}(a,b) \cdot \mathrm{kgV}(a,b)$, da $x + y = \min\{x, y\} + \max\{x, y\}$ für alle $x, y \in \mathbb{R}$ gilt.

1.2 Die ganzen Zahlen

1.2.1 Ringstruktur

Die ganzen Zahlen $\mathbb{Z}$ haben etwas mehr Struktur als die natürlichen Zahlen $\mathbb{N}_0$. Bezüglich der Addition bilden sie eine *kommutative Gruppe*. Die (kommutative) Multiplikation ist über das Distributivgesetz mit der Addition verträglich. Man sagt:

Die ganzen Zahlen $(\mathbb{Z}, +, \cdot, 0, 1)$ bilden einen *(kommutativen) Ring mit* 1.

Allgemein erfüllt eine Menge R mit zwei binären Operationen $+\colon R \times R \longrightarrow R$ und $\cdot\colon R \times R \longrightarrow R$ als *(kommutativer) Ring* definitionsgemäss folgende Axiome: Ring

(A) $(R, +, 0)$ ist eine *kommutative Gruppe* mit 0 als *Neutralelement*.

Man nennt „+“ die *Addition* in R.

Das *additive Inverse* von $a \in R$ wird mit $-a$ bezeichnet.

(M) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ für alle $a, b, c \in R$.

Man nennt „$\cdot$“ die *Multiplikation* in R. Sie ist *assoziativ*.

(D) $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ und $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ für alle $a, b, c \in R$.

Die Multiplikation ist *links–* und *rechts–distributiv* über die Addition.

(1) Von einem Ring *„mit 1“* spricht man, falls es zusätzlich ein *multiplikatives Neutralelement* $1 \in R$ gibt mit $1 \cdot a = a = a \cdot 1$ für alle $a \in R$.

(K) Von einem *kommutativen* Ring spricht man, wenn die Multiplikation in R *kommutativ* ist: $a \cdot b = b \cdot a$ für alle $a, b \in R$.

Beispiele:

Die reellen 2×2–Matrizen mit der Nullmatrix als additives und der 2×2–Einheitsmatrix $\mathbb{I}_2$ als multiplikatives Neutralelement bilden einen (nicht–kommutativen) Ring mit 1. Man beachte, dass die Addition in jedem Fall kommutativ zu sein hat.

Ein *Körper* $(K, +, \cdot, 0, 1)$ ist ein kommutativer Ring mit $1 \neq 0$, in dem zusätzlich $(K \backslash \{0\}, \cdot, 1)$ unter der Multiplikation eine kommutative Gruppe bildet. Insbesondere hat in einem Körper jedes Element $k \neq 0$ ein *multiplikatives Inverses* „$k^{-1} = 1/k$“. Körper

Definition Einheit

Ein Element $a \in R$ in einem Ring R mit 1 heisst *Einheit*, falls $b, c \in R$ existieren mit $b \cdot a = a \cdot c = 1$. Es gilt dann notwendigerweise $b = c$, da $b = b \cdot 1 = b \cdot (a \cdot c) = (b \cdot a) \cdot c = 1 \cdot c = c$ und man schreibt $b = c = a^{-1}$. In jedem Ring R mit 1 bilden die *Einheiten* $R^\times$ eine (multiplikative) Gruppe. Insbesondere gilt $\mathbb{Z}^\times = \{1, -1\}$. Einheit $R^\times$

Aufgabe

Bestimme die Einheiten im Ring der reellen 2×2–Matrizen.

Aufgabe

Die 2×2–Matrizen mit Einträgen aus $\mathbb{Z}$ bilden einen (nicht–kommutativen) Ring R mit 1. Gib eine 2×2–Marix M in $R^\times$ mit keinem Eintrag 0. Gib M^{-1}.

Die Begriffe und Tatsachen, die wir bisher für natürliche Zahlen erörtert haben, lassen sich leicht für die ganzen Zahlen verallgemeinern. Wir definieren

$$\text{sign}(a) = \begin{cases} 1 & \text{falls } a > 0 \\ -1 & \text{falls } a < 0 \end{cases}$$

für $a \in \mathbb{Z} \setminus \{0\}$, das sog. *Signum* oder *Vorzeichen* von a. Manchmal wird noch $\text{sign}(0) = 0$ gesetzt. Dann gilt $|a| = \text{sign}(a) \cdot a \geq 0$ für alle $a \in \mathbb{Z}$. Man definiert

$$\text{ggT}(a, b) = \text{ggT}(|a|, |b|)$$

für alle $a, b \in \mathbb{Z}$ (nicht a und b beide 0). Mit $a|b$ gilt auch $-a|b$. Die Menge

$$\mathbb{T}(a) \subset \mathbb{Z}$$

aller Teiler einer ganzen Zahl $a \neq 0$ umfasst nun auch negative Zahlen und ist eine Teilmenge der ganzen Zahlen zwischen $-|a|$ und $|a|$. Für jedes $a \neq 0$ hat

$$\mathbb{V}(a) = \mathbb{Z}a = \{\ldots, -3|a|, -2|a|, -|a|, 0, |a|, 2|a|, 3|a|, \ldots\} = \{n \cdot a \,|\, n \in \mathbb{Z}\} \ ,$$

die Menge der (ganzzahligen) Vielfachen von a, die Struktur eines kommutativen Ringes (ohne 1, falls $a \neq 1$). Deshalb führt man auch $\mathbb{Z}a$ als neue Notation ein. $\mathbb{Z}a$
(Dies gilt auch für $a = 0$: $\mathbb{Z}0 = \{0\}$ ist der nicht sehr interessante *Nullring* mit nur einem Element.)
Die lineare Gleichung

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

mit ganzzahligen Koeffizienten $a, b, c \in \mathbb{Z}$ (a und b nicht beide 0) hat genau dann Lösungen $(x, y) \in \mathbb{Z}^2$, wenn $t = \text{ggT}(a, b)$ die Zahl c teilt. Die Beschreibung *aller* ganzzahliger Lösungen ist dann gleich, wie im Falle $a, b, c \in \mathbb{N}_0$, vgl. 1.1.4
Auch der Hauptsatz der Arithmetik gilt praktisch unverändert. Jede ganze Zahl $a \neq 0$ hat eine eindeutige Darstellung

$$a = \text{sign}(a) \cdot p_1^{e_1} \cdot p_2^{e_2} \cdot p_3^{e_3} \cdot \ldots$$

mit $1 < p_1 = 2 < p_2 = 3 < \ldots$ prim und natürlichen e_k, die fast alle 0 sind. Die Liste der Primzahlen besteht also unverändert aus lauter positiven Zahlen. Man sagt, $-p_k$ ist „prim bis auf Multiplikation mit einer Einheit“.

1.2.2 Teilen mit Rest

Der im Unterabschnitt 1.1.3 betrachtete Euklidsche Algorithmus kann auch als fortgesetzte *Division mit Rest* aufgefasst werden. Es gilt der folgende wichtige

Satz (Teilen mit Rest)
Für alle $a, b \in \mathbb{Z}$ mit $b \neq 0$ gibt es eindeutige $m \in \mathbb{Z}$ und $r \in \mathbb{N}$ mit $0 \leq r < |b|$ und

$$a = m \cdot b + r \ .$$

Man nennt $r \in \{0, 1, \ldots, |b| - 1\}$ den *Rest* bei der Division von a durch $b \neq 0$. Rest

Beweis:
Für $|b| \in \mathbb{N}$ gibt es zu jeder natürlichen Zahl $|a| \in \mathbb{N}_0$ genau ein $n \in \mathbb{N}_0$ mit $n \cdot |b| \leq |a| < (n+1) \cdot |b|$, also genau ein $n \in \mathbb{N}_0$ und $s \in \mathbb{N}_0$ mit $0 \leq s < |b|$ und $|a| = n \cdot |b| + s$.
Für $a = |a| \geq 0$ ist also $m = \text{sign}(b) \cdot n$ und $r = s$ zu setzen.
Für $a = -|a| < 0$ folgt $a = -n \cdot |b| - s = m \cdot b + r$ mit $m = -\text{sign}(b) \cdot (n+1)$ und $0 < r = |b| - s < |b|$, falls $0 < s < |b|$ bzw. $m = -\text{sign}(b) \cdot n$ und $r = 0$, falls $s = 0$.
(Die Eindeutigkeit von m und r lässt sich auch nachträglich nochmals durch Vergleich von $a = m \cdot b + r$ und $a = \tilde{m} \cdot b + \tilde{r}$ beweisen.) □

Beispiel: $a = -15$, $b = 7$, $a = m \cdot b + r = (-3) \cdot 7 + 6$.

1.2.3 Restklassen

Jedes $b \neq 0$ definiert eine Aequivalenzrelation auf $\mathbb{Z}$, die $\mathbb{Z}$ in $|b|$ Aequivalenzklassen aufteilt.
a und $\tilde{a}$ heissen *kongruent modulo b*, man schreibt kongruent

$$a \equiv \tilde{a} \pmod{b} ,$$

genau dann, wenn in der eindeutigen Darstellung $a = m \cdot b + r$ und $\tilde{a} = \tilde{m} \cdot b + \tilde{r}$ mit $0 \leq r, \tilde{r} < |b|$ gilt $r = \tilde{r}$, wenn also a und $\tilde{a}$ beim Teilen durch b mit Rest den gleichen Rest $r = \tilde{r}$ haben. Damit gleichbedeutend ist

$$a \equiv \tilde{a} \pmod{b} \quad \Leftrightarrow \quad b|(a - \tilde{a}) .$$

Beispiel: Die drei *Restklassen* modulo $b = 3$ in $\mathbb{Z}$ sind Restklasse

$$\begin{aligned} \text{„}0 + \mathbb{Z}3\text{“} &= \{\ldots, -12, -9, -6, -3, 0, 3, 6, 9, 12, \ldots\} , \\ \text{„}1 + \mathbb{Z}3\text{“} &= \{\ldots, -11, -8, -5, -2, 1, 4, 7, 10, 13, \ldots\} , \\ \text{„}2 + \mathbb{Z}3\text{“} &= \{\ldots, -10, -7, -4, -1, 2, 5, 8, 11, 14, \ldots\} . \end{aligned}$$

Rechnen mit Restklassen
Zu $0 \neq b \in \mathbb{Z}$ bezeichnen wir für ein $a \in \mathbb{Z}$ mit „$a + \mathbb{Z}b$“ oder mit $\pi_b(a)$ oder mit

$$\overline{a} = \{\ldots, a - 3|b|, a - 2|b|, a - |b|, a, a + |b|, a + 2|b|, a + 3|b|, \ldots\}$$

diejenige der $|b|$ Restklasse modulo b, zu der a gehört. Durchläuft r alle natürlichen Zahlen mit $0 \leq r < |b|$, so durchläuft $\overline{r}$ alle Restklassen modulo b, jede genau einmal. Wir betrachten also $r \in \mathbb{N}_0$ mit $0 \leq r < |b|$ fortan als ausgezeichnete Repräsentanten der $|b|$ Restklassen modulo b. Äusserst wichtig ist nun die Tatsache, dass für alle ganzen $b \neq 0$ die Restklassenbildung modulo b mit der Ringstruktur von $\mathbb{Z}$ verträglich ist.

Satz (Verträglichkeit der Restklassenbildung mit der Ringstruktur von $\mathbb{Z}$)
Für jedes $b \neq 0$ in $\mathbb{Z}$ und beliebige $a, \tilde{a}, c, \tilde{c} \in \mathbb{Z}$ gilt
$a \equiv \tilde{a} \pmod{b} \wedge c \equiv \tilde{c} \pmod{b} \Rightarrow a + c \equiv \tilde{a} + \tilde{c} \pmod{b} \wedge a \cdot c \equiv \tilde{a} \cdot \tilde{c} \pmod{b}$.

Beweis:
$b|(a-\tilde{a}) \wedge b|(c-\tilde{c}) \Rightarrow b|(a+c-(\tilde{a}+\tilde{c})) \wedge b|(a\cdot c-\tilde{a}\cdot\tilde{c})$.
Um einzusehen, dass $a\cdot c-\tilde{a}\cdot\tilde{c}$ unter der Voraussetzung links von b geteilt wird, schreibe man $a\cdot c-\tilde{a}\cdot\tilde{c}=(a-\tilde{a})\cdot c+\tilde{a}\cdot(c-\tilde{c})$. □

Wegen der Verträglichkeit von Restklassenbildung und Ringstruktur können wir nun mit Restklassen *rechnen*. Ja, zu jedem ganzen $b\neq 0$ bilden die Restklassen modulo b selber einen Ring mit den $|b|$ Elementen $\overline{0}$, $\overline{1}$, …, $\overline{|b|-1}$. Man schreibt

$$\mathbb{Z}/\mathbb{Z}b \quad \text{oder} \quad \mathbb{Z}_{|b|}$$

für diesen sog. *Restklassen–Ring* und definiert: Restklassen-Ring
Addition modulo b: $\overline{r}+\overline{s}=\overline{r+s}$ (unabhängig von der Wahl $r\in\overline{r}$ und $s\in\overline{s}$),
Multiplikation modulo b: $\overline{r}\cdot\overline{s}=\overline{r\cdot s}$ (unabhängig von der Wahl $r\in\overline{r}$ und $s\in\overline{s}$).
Das erste Symbol „+“ in der Definition der Addition ist also eine Operation auf Restklassen. Diese unterscheidet sich von der Addition in $\mathbb{Z}$, welche mit dem zweiten „+“ auf dieser Zeile symbolisiert wird. Entsprechendes gilt für das Symbol „·“.
Die Abbildung

$$\begin{array}{rccl} \pi_b\colon & \mathbb{Z} & \longrightarrow & \mathbb{Z}_{|b|}\ , \\ & a & \mapsto & \overline{a}\ , \end{array}$$

die jedem Element $a\in\mathbb{Z}$ seine Restklasse $\overline{a}\in\mathbb{Z}_{|b|}$ modulo b zuordnet, erfüllt also

$$\pi_b(a+c)=\pi_b(a)+\pi_b(c) \quad \text{und} \quad \pi_b(a\cdot c)=\pi_b(a)\cdot\pi_b(c)\ ,$$

wobei über die Symbole „+“ und „·“ das gleiche wie oben zu sagen ist. Zusätzlich geht die $1\in\mathbb{Z}$ auf die Restklasse $\overline{1}\neq\overline{0}$ (falls $|b|\neq 1$), die im Restklassenring $\mathbb{Z}_{|b|}$ das multiplikative Neutralelement ist. Eine solche Abbildung π von einem Ring $R_1=\mathbb{Z}$ nach einem Ring $R_2=\mathbb{Z}_{|b|}$, die mit den beiden Ringstrukturen auf R_1 und R_2 verträglich ist im Sinne der obigen Gleichungen, nennt man einen *Ringhomomorphismus*. (Genauer spricht man von einem *Epimorphismus*, da π_b zudem noch surjektiv ist.)

Folgerung Für $x,y,z,\cdots\in\mathbb{Z}$ und $0\neq b\in\mathbb{Z}$ gilt

$$\overline{f}(\overline{x},\overline{y},\overline{z}\ \ldots)=\overline{f(x,y,z,\ldots)}$$

für jeden Term $f(x,y,z,\ldots)$, der aus lauter Additionen und Multiplikationen von Koeffizienen und Variabeln x, y, … aus $\mathbb{Z}$ aufgebaut ist (sog.*Polynom in mehreren Variabeln* mit ganzen Koeffizienten). Man kann also zuerst $f(x,y,z,\ldots)$ berechnen und dann die Restklasse des Resultates $\mod b$ bestimmen oder direkt Restklassen $\overline{x}$, $\overline{y}$, … in $\overline{f}$ einsetzen und im Ring $\mathbb{Z}_{|b|}$ rechnen, wobei die Koeffizienten bzw. Operationen von f in $\overline{f}$ durch ihre Restklassen bzw. Operationen in $\mathbb{Z}_{|b|}$ ersetzt werden. Wir erhalten das gleiche Resultat bei typischerweise verschieden grossem Rechenaufwand.

Aufgabe: Berechne $\pi_3(n)$, $\pi_4(n)$ und $\pi_5(n)$ mit $n=2^{2017}$. Gilt $\pi_b(n^m)=\pi_b(n)^{\pi_b(m)}$?

1.2.4 Einheiten

Um nicht immer Betragszeichen schreiben zu müssen, nehmen wir jetzt $1 < b \in \mathbb{N}$ an. Welches sind die Einheiten in $\mathbb{Z}_b$, also die Restklassen modulo b mit multiplikativen Inversen? Es ist klar, dass die Bilder der Einheiten $\{1, -1\}$ von $\mathbb{Z}$ unter π_b wieder Einheiten sind. Zum Beispiel gilt $\pi_b(-1) \cdot \pi_b(-1) = \pi_b((-1) \cdot (-1)) = \pi_b(1) = \overline{1}$. Also ist $\pi_b(-1)$ unabhängig von b immer eine Einheit in $\mathbb{Z}_b$ mit sich selbst als multiplikatives Inverses. Ebenso klar ist, dass $\pi_b(a)$ keine Einheit sein kann, wenn $\mathrm{ggT}(a, b) \neq 1$ gilt. Andernfalls gäbe es ein $c \in \mathbb{Z}$ mit $\overline{1} = \pi_b(a) \cdot \pi_b(c) = \pi_b(a \cdot c)$, also $a \cdot c = 1 + b \cdot d$ oder $a \cdot c - b \cdot d = 1$. Die kleinste positive Zahl der Form $m \cdot a + n \cdot b$ mit $m, n \in \mathbb{Z}$ ist gemäss Annahme aber $\mathrm{ggT}(a, b) \neq 1$, ein Widerspruch.

Satz ($\mathbb{Z}_b^\times$, die Einheiten in $\mathbb{Z}_b$)
Die Einheiten $\mathbb{Z}_b^\times$ von $\mathbb{Z}_b$ sind alle Restklassen $\overline{a}$ modulo b mit $\mathrm{ggT}(a, b) = 1$.

Beweis: Es bleibt noch zu zeigen, dass $\overline{a} = \pi_b(a)$ in $\mathbb{Z}_b$ ein multiplikatives Inverses hat, wenn $\mathrm{ggT}(a, b) = 1$ gilt. Dann gibt es aber $c, d \in \mathbb{Z}$ mit $a \cdot c + b \cdot d = 1$, also $a \cdot c = 1 - b \cdot d$ und daher $\overline{a} \cdot \overline{c} = \pi_b(a) \cdot \pi_b(c) = \pi_b(a \cdot c) = \pi_b(1 - b \cdot d) = \overline{1}$. Also ist $\overline{c}$ das multiplikative Inverse von $\overline{a}$ in $\mathbb{Z}_b$.

Beispiel: $\mathbb{Z}_8^\times = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$ mit $\overline{a}^{-1} = \overline{a}$ für alle $\overline{a} \in \mathbb{Z}_8^\times$.

Die Zahlkörper $\mathbb{F}_p$
Ist $b = p$ prim, so ist jede ganze Zahl $a \in \mathbb{Z}$ entweder teilerfremd zu p oder ein Vielfaches $d \cdot p$ von p. Also ist $\overline{a} = \pi_p(a)$ eine Einheit oder $\overline{a} = \overline{0} = \pi_p(d \cdot p)$. Also ist $\mathbb{Z}_p$ ein kommutativer Ring mit 1, in dem jedes Element ausser das additive Neutralelement ein multiplikatives Inverses hat. Das heisst, $\mathbb{Z}_p$ ist ein *Körper*. Um dies zu betonen, schreibt man auch $\mathbb{F}_p$ statt $\mathbb{Z}_p$ (engl. „*field*“ für *Körper*). Körper $\mathbb{F}_p$
Achtung: Es gibt z.B. auch einen Körper mit *vier* Elementen. Dessen Struktur ist aber wesentlich verschieden vom Restklassen–Ring $\mathbb{Z}_4$ mit vier Elementen. In $\mathbb{Z}_4$ gilt nämlich $\overline{2} \cdot \overline{2} = \overline{0}$. In einem Körper ist aber ein Produkt nur dann null, wenn mindestens einer der Faktoren null ist.

1.2.5 Die Eulersche φ–Funktion

Wenn wir uns für die Struktur des Restklassenringes $\mathbb{Z}_b$ interessieren, ist es z.B. von Interesse, wieviele Reste $0 \leq r < b$ zu b teilerfremd sind, denn dies gibt einen ersten Aufschluss über $\mathbb{Z}_b^\times$, die multiplikative Gruppe der Einheiten in $\mathbb{Z}_b$.

Definition Eulersche φ–Funktion
Man definiert $\varphi(1) = 1$ und $\varphi(n) = |\mathbb{Z}_n^\times|$ für $1 < n \in \mathbb{N}$.
Die *Eulersche φ–Funktion* $\varphi(n)$ gibt also die Anzahl Reste r mit $0 \leq r < n$, die teilerfremd sind zu n. φ–Funktion

Beispiele

$\mathrm{ggT}(0, 1) = 1 \Rightarrow \varphi(1) = 1$,
$\mathrm{ggT}(0, 2) = 2$, $\mathrm{ggT}(1, 2) = 1 \Rightarrow \varphi(2) = 1$,
$\mathrm{ggT}(0, 3) = 3$, $\mathrm{ggT}(1, 3) = 1$, $\mathrm{ggT}(2, 3) = 1 \Rightarrow \varphi(3) = 2$,
$\mathrm{ggT}(0, 4) = 4$, $\mathrm{ggT}(1, 4) = 1$, $\mathrm{ggT}(2, 4) = 2$, $\mathrm{ggT}(3, 4) = 1 \Rightarrow \varphi(4) = 2$,
$\mathrm{ggT}(0, 5) = 5$, $\mathrm{ggT}(1, 5) = 1$, $\mathrm{ggT}(2, 5) = 1$, $\mathrm{ggT}(3, 5) = 1$, $\mathrm{ggT}(4, 5) = 1 \Rightarrow \varphi(5) = 4$

$\varphi(6) = 2$, $\varphi(7) = 6$, $\varphi(8) = 4$, $\varphi(9) = 6$, $\varphi(10) = 4$, $\varphi(11) = 10$, $\varphi(12) = 4$, ...

Zunächst erkennt man vielleicht keine Gesetzmässigkeit in diesen Werten. Aber es gilt $\varphi(p) = p - 1$ für p prim, denn dann ist $\mathrm{ggT}(r, p) = 1$ für alle $r = 1, 2, \ldots, p-1$. $\varphi(p)$
Mit wenig Nachdenken löst man zudem die

Aufgabe: Zeige $\varphi(p^n) = p^{n-1} \cdot (p-1) = p^n \cdot (1 - 1/p)$ für p prim und $n \in \mathbb{N}$.

Weitere Zahlenbeispiele bringen dann die Erkenntnis des folgenden

Satz Die Eulersche φ–Funktion ist eine *arithmetische Funktion*, d.h. $\varphi(a \cdot b)$

$$\forall a, b \in \mathbb{N}\colon \mathrm{ggT}(a, b) = 1 \Rightarrow \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)\ .$$

Beweis: Wir zeigen dass die Restklassen $\mod (a \cdot b)$ von

$$t \cdot a + s \cdot b \mod a \cdot b$$

für $0 \leq s < a$ und $0 \leq t < b$ mit $\mathrm{ggT}(s, a) = 1 = \mathrm{ggT}(t, b)$ alle verschieden sind und

$$r \equiv t \cdot a + s \cdot b \mod a \cdot b$$

für r mit $\mathrm{ggT}(r, a \cdot b) = 1$ und geeigneten s, t , die die obige Bedingungen erfüllen.
Aus der ersten Behauptung folgt $\varphi(a \cdot b) \geq \varphi(a) \cdot \varphi(b)$ und aus der zweiten „$\leq$“.
Ist $t \cdot a + s \cdot b \equiv \tilde{t} \cdot a + \tilde{s} \cdot b \mod a \cdot b$, so gilt $a \cdot b | (t - \tilde{t}) \cdot a + (s - \tilde{s}) \cdot b$, also $r \cdot a \cdot b = (t - \tilde{t}) \cdot a + (s - \tilde{s}) \cdot b$ oder $[r \cdot a - (s - \tilde{s})] \cdot b = (t - \tilde{t}) \cdot a$, also $b | (t - \tilde{t}) \cdot a$. Da $\mathrm{ggT}(a, b) = 1$ folgt $b | (t - \tilde{t})$ (Lemma von Euklid) und da $0 \leq t, \tilde{t} < b$ folgt $t - \tilde{t} = 0$.
Analog folgt $s - \tilde{s} = 0$ und daher $\varphi(a \cdot b) \geq \varphi(a) \cdot \varphi(b)$.
Sei nun $\mathrm{ggT}(r, a \cdot b) = 1$. Es gibt $m, n \in \mathbb{Z}$ mit $m \cdot a + n \cdot b = 1$, da $\mathrm{ggT}(a, b) = 1$.
Also gilt $r = r \cdot 1 = r \cdot (m \cdot a + n \cdot b) = (r \cdot m) \cdot a + (r \cdot n) \cdot b = \tilde{t} \cdot a + \tilde{s} \cdot b$.
Durch Addition von Vielfachen $p \cdot a$ zu $\tilde{s}$ und $q \cdot b$ zu $\tilde{t}$ ändert sich die Restklasse von $r = \tilde{t} \cdot a + \tilde{s} \cdot b \equiv (\tilde{t} + q \cdot b) \cdot a + (\tilde{s} + p \cdot a) \cdot b = t \cdot a + s \cdot b \mod a \cdot b$ nicht.
Wir wählen also $p, q \in \mathbb{Z}$ mit $0 \leq s = \tilde{s} + p \cdot a < a$ und $0 \leq t = \tilde{t} + q \cdot b < b$. Ist d ein gemeinsamer Teiler von s und a, so auch von r und $a \cdot b$, also gilt $d = 1$, da $\mathrm{ggT}(r, a \cdot b) = 1$. Es folgt $\mathrm{ggT}(s, a) = 1$ und ebenso $\mathrm{ggT}(t, b) = 1$.
Wir haben also $\varphi(a \cdot b) \leq \varphi(a) \cdot \varphi(b)$ und insgesamt $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$. □

Aufgabe: $\varphi(77077) = ?$

Mit Hilfe der Eulerschen φ–Funktion können wir nun immerhin sagen, wieviele Einheiten es im Restklassenring $\mathbb{Z}_b$ gibt, wenn wir die Primfaktorzerlegung von b kennen.

1.2.6 Primitivwurzeln

Für p prim ist $\mathbb{Z}_p = \mathbb{F}_p$ ein Körper, da jede Restklasse $\overline{0} \neq \overline{r} \in \mathbb{Z}_p$ eine multiplikative Inverse hat. Da nämlich gilt $\mathrm{ggT}(r, p) = 1$ für $0 < r < p$, gibt es $m, n \in \mathbb{Z}$ mit $m \cdot r + n \cdot p = 1$, was gleichbedeutend ist mit $m \cdot r \equiv 1 \mod p$ oder $\overline{r}^{\,-1} = \overline{m}$.

Aufgabe: Bestimme $\overline{r}^{\,-1}$ für $\overline{r} = \overline{1}, \overline{2}, \ldots, \overline{6}$ in $\mathbb{Z}_7 = \mathbb{F}_7$.

Wir wollen nun die multiplikative Gruppe $\mathbb{Z}_b^\times$ der Einheiten in $\mathbb{Z}_b$ mit $|\mathbb{Z}_b^\times| = \varphi(b)$ Elementen noch etwas genauer untersuchen. Wir schreiben M_b für diese multiplikative Gruppe der zu b teilerfremden also invertierbaren Reste $\mod b$. M_p

Zunächst formulieren wir den

Kleinen Satz von Fermat: Für alle $\overline{r} \in M_b$ gilt $\overline{r}^{\varphi(b)} = \overline{1}$.

Fermat hat diesen Satz eigentlich nur im Spezialfall von $b = p$ prim betrachtet. Er gilt aber viel allgemeiner in jeder endlichen Gruppe G mit $n = |G|$ Elementen,

$$\forall g \in G\colon\ g^n = 1 \text{ (Neutralelement) } .$$

Zudem gilt für das *kleinste* $m > 0$ mit $g^m = 1$, also für die sog. *Ordnung* $\mathrm{ord}(g)$ von $g \in G$, dass sie die Anzahl Elemente n in G teilt, $m|n$. **Beweis:***In den Übungen.* Ordnung

Aufgabe: Bestimme $\mathrm{ord}(\overline{r})$ für $\overline{r} = \overline{1}, \overline{2}, \ldots, \overline{6}$ in $\mathbb{Z}_7 = \mathbb{F}_7$.

Wir formulieren nun einen

Satz über die Ordnung der Elemente von M_p für p prim:
In M_p gibt es genau $\varphi(d)$ Elemente der Ordnung d für $d|p-1$ und keine anderen.

Beispiel: Für $p = 7$ gibt es also $\varphi(6) = 2$ Elemente der Ordnung 6, $\varphi(3) = 2$ Elemente der Ordnung 3, $\varphi(2) = 1$ Element der Ordnung 2 und, wie immer $\varphi(1) = 1$ Element der Ordnung 1. Die Lösung der vorangehenden Aufgabe bestätigt dies.

Definition Primitivwurzel
Ein Element a in M_b mit maximal möglicher Ordnung $\mathrm{ord}(a) = |M_b| = \varphi(b)$ heisst *Primitivwurzel*. Die Gruppe $M_b = \{a, a^2, \ldots, a^{\varphi(b)} = 1\}$ ist dann *zyklisch*, d.h. die Elemente $g \in M_b$ können alle als Potenzen eines einzigen Elementes a, eben einer Primitivwurzel a, erhalten werden. zyklische Gruppe

Bemerkungen

1. Aus obigem Satz folgt, dass M_p für alle p prim eine zyklische Gruppe ist. Der Satz sagt sogar, wieviele Möglichkeiten es gibt, die Elemente von M_p als Potenzen eines einzigen Elementes, eben einer Primitivwurzel zu schreiben: Es gibt $\varphi(\varphi(p)) = \varphi(p-1)$ Primitivwurzeln in M_p .

2. Aus dem Satz folgt auch, dass die Summe aller $\varphi(d)$ mit $d|p-1$ wieder $p-1$, also die Anzahl Elemente in M_p ergibt. Weiter unten werden wir sogar allgemein beweisen, dass für alle $n \in \mathbb{N}$ (also nicht nur für $n = p-1$ mit p prim) gilt

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

   Beispiel: $d|10 \Rightarrow d \in \{1, 2, 5, 10\}$. $\varphi(1)+\varphi(2)+\varphi(5)+\varphi(10) = 1+1+4+4 = 10$.

Beweis des Satzes über die Ordnung der Elemente von M_p mit p prim.
Sei a ein Element in M_p mit Ordnung d. Dann gilt $a^d = \overline{1}$ und $a^e \neq \overline{1}$ für $1 \leq e < d$. Oben haben wir erwähnt, dass in jeder endlichen Gruppe G die Ordnung jedes Elementes in G die Anzahl $|G|$ der Elemente in G teilt. Hier gilt also $d|p-1$. Jetzt benutzen wir noch, dass $\mathbb{Z}_p = \mathbb{F}_p$ ein Körper ist, falls p prim ist. Das Polynom

$$x^d - \overline{1}$$

hat in $\mathbb{F}_p = \mathbb{Z}_p$ höchstens d Nullstellen. (Aufgabe unten: In $\mathbb{Z}_n$ gilt dies i.a. nicht!) Es gibt in $M_p = \mathbb{Z}_p^\times = \mathbb{F}_p \setminus \{0\}$ also höchstens d Elemente der Ordnung d, die dann

je Nullstellen dieses Polynoms sind. Mit unserem a von Ordnung d haben wir aber bereits d verschiedene Elemente in M_p, die alle Nullstellen sind, nämlich

$$x \in \{a, a^2, \ldots, a^d = \overline{1} = a^0\} \quad \Rightarrow x^d - \overline{1} = (a^e)^d - \overline{1} = (a^d)^e - \overline{1} = \overline{1}^e - \overline{1} = \overline{0} \ .$$

Für einen Exponenten e mit $0 \leq e < d$ ist die Ordnung von a^e aber tatsächlich sogar kleiner als d, falls $\mathrm{ggT}(e, d) \neq 1$. Sei nämlich $t \cdot f = e$ und $t \cdot g = d$ mit $t > 1$, so gilt

$$(a^e)^g = (a^{t \cdot f})^g = (a^{t \cdot g})^f = (a^d)^f = \overline{1}^f = \overline{1} \ .$$

Also gilt $\mathrm{ord}(a^e) \leq g = d/t < d$ für solche Exponenten e, die zu d nicht teilerfremd sind. Tatsächlich gibt es zu jedem Teiler d von $p-1$ also höchstens $\varphi(d)$ Elemente der Ordnung d, da $\varphi(d)$ definitionsgemäss die Anzahl der Zahlen e mit $0 \leq e < d$ und $\mathrm{ggT}(e, d) = 1$ ist.
Wir schreiben nun $\psi(d)$ für die Anzahl Elemente in M_p mit Ordnung d und haben also $\psi(d) \leq \varphi(d)$ für alle $d \in \mathbb{N}$. Andererseits hat jedes der $p-1$ Elemente in M_p eine Ordnung $d \in \mathbb{N}$ mit $d | p-1$. Also gilt

$$p - 1 = \sum_{d|p-1} \psi(d) \leq \sum_{d|p-1} \varphi(d) \ .$$

Der Beweis unten für die Formel in Bemerkung 2 oben gibt nun $\psi(d) = \varphi(d)$. □

Satz Die Eulersche φ–Funktion erfüllt für alle $n \in \mathbb{N}$ die Gleichung

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

Beweis: Wieviele x mit $1 \leq x \leq n$ und $\mathrm{ggT}(x, n) = t$ gibt es? Da t ein Teiler von $n \in \mathbb{N}$ ist, gilt $1 \leq t \leq n$ und x ist ein Vielfaches von t. Also gilt

$$x \in \{1 \cdot t \, , \, 2 \cdot t \, , \, \ldots \, , (n/t) \cdot t = n\} \ ,$$

wobei $\mathrm{ggT}(x, n) = \mathrm{ggT}(k \cdot t, n) = t$ genau dann gilt, wenn $\mathrm{ggT}(k, n/t) = 1$ gilt. Also gibt es in dieser Menge genau $\varphi(n/t)$ Elemente x mit $\mathrm{ggT}(x, n) = t$. Da nun jedes Element x mit $1 \leq x \leq n$ genau einen ggT t mit n hat und mit t auch $d = n/t$ alle Teiler von n durchläuft, so gilt obige Formel.

Aufgabe: Bestimme alle Nullstellen von $x^2 - \overline{1}$ in $M_8 = \mathbb{Z}_8^\times$.

Bemerkung

Es gilt also in jedem Körper $\mathbb{F}_p = \mathbb{Z}_p$, dass die multiplikative Gruppe der Einheiten $M_p = \mathbb{F}_p \setminus \{0\} = \mathbb{Z}_p \setminus \{0\} = \mathbb{Z}_p^\times$ *zyklisch* ist, da es $\varphi(p-1) \geq 1$ Elemente maximaler Ordnung $p-1$, sog. *Primitivwurzeln* a gibt, so dass jedes Element von M_p als Potenz von a geschreiben werden kann (p prim). Entsprechendes gilt für jeden endlichen Körper. Primitivwurzel

Gauß gibt ein allgemeines Kriterium[5], wann M_n zyklisch ist und wann nicht.

Aufgabe: Untersuche, ob M_n zyklisch ist oder nicht, für $2 \leq n \leq 12$.

Aufgabe: Gib alle Primitivwurzeln von M_n, falls M_n zyklisch ist, für $1 \leq n \leq 12$.

[5] C.F.Gauß (1801) *Disquisitiones arithmeticae*, Leipzig

1.2.7 Der chinesische Restsatz

In Aufgaben zum Rechnen mit Rest wird oft, in eingekleideter oder expliziter Form, eine Zahl $n \in \mathbb{N}$ gesucht, die modulo verschiedener Zahlen $b_1, \ldots, b_k$ einen vorgeschriebenen Rest r_j hat $(1 \leq j \leq k)$. Zu erfüllen ist also etwa ein System von Kongruenzen folgender Art

$$\begin{aligned} n &\equiv r_1 && \mod b_1 \ , \\ n &\equiv r_2 && \mod b_2 \ , \\ &\ldots \\ n &\equiv r_k && \mod b_k \ . \end{aligned}$$

Eine Konstruktion möglicher Lösungen solcher Systeme erhält man aus dem sog.

Chinesischen Restsatz[6]

Sind $b_1, \ldots, b_k \in \mathbb{N}$ paarweise teilerfremd, also $\mathrm{ggT}(b_i, b_j) = 1$ für $1 \leq i < j \leq k$, so hat obiges Gleichungssystem (unendlich viele) Lösungen für beliebige r_j $(1 \leq j \leq k)$.

Beweis: Gilt $n_j \equiv 1 \mod b_j$ und $b_i | n_j$ für $1 \leq i \neq j \leq k$, so sind

$$n = r_1 \cdot n_1 + \cdots + r_k \cdot n_k + m \cdot (b_1 \cdot \ldots \cdot b_k)$$

für $m \in \mathbb{Z}$ alle Lösungen $n \in \mathbb{Z}$ des obigen Gleichungssystems. Wir konstruieren n_1. Da b_1 und $d_1 = b_2 \cdot \ldots \cdot b_k$ teilerfremd sind, gibt es a_1 und c_1 mit $a_1 \cdot b_1 + c_1 \cdot d_1 = 1$. Also gilt $n_1 = 1 - a_1 \cdot b_1 \equiv 1 \mod b_1$ und $b_i | n_1 = c_1 \cdot d_1$ für $1 < i \leq k$. Analog konstruiert man n_2 aus den teilerfremden b_2 und $d_2 = b_1 \cdot b_3 \cdot \ldots \cdot b_k$ etc.
Offensichtlich gilt $b_j | n - n'$ für alle $1 \leq j \leq k$ für zwei Lösungen n und n'. Also ist $n - n'$ ein Vielfaches von $b_1 \cdot \ldots \cdot b_k$, das kgV der teilerfremden b_j. □

Beispiel: Bestimme das kleinste $n \in \mathbb{N}$ mit

$$\begin{aligned} n &\equiv 1 && \mod 13 \ , \\ n &\equiv 2 && \mod 17 \ , \\ n &\equiv 3 && \mod 19 \ . \end{aligned}$$

Lösung: Der Euklidsche Algorithmus liefert nacheinander

$$\begin{aligned} a_1 \cdot b_1 + c_1 \cdot d_1 = -149 \cdot 13 + 6 \cdot (17 \cdot 19) = 1 \quad &\Rightarrow \quad n_1 = 1 + 149 \cdot 13 = 6 \cdot 17 \cdot 19 \ , \\ a_2 \cdot b_2 + c_2 \cdot d_2 = -29 \cdot 17 + 2 \cdot (13 \cdot 19) = 1 \quad &\Rightarrow \quad n_2 = 1 + 29 \cdot 17 = 2 \cdot 13 \cdot 19 \ , \\ a_3 \cdot b_3 + c_3 \cdot d_3 = -93 \cdot 19 + 8 \cdot (13 \cdot 17) = 1 \quad &\Rightarrow \quad n_3 = 1 + 93 \cdot 19 = 8 \cdot 13 \cdot 17 \ . \end{aligned}$$

Alle Lösungen sind also

$$\begin{aligned} n &= r_1 \cdot n_1 + r_2 \cdot n_2 + r_3 \cdot n_3 + m \cdot (b_1 \cdot b_2 \cdot b_3) \\ &= 1 \cdot (6 \cdot 17 \cdot 19) + 2 \cdot (2 \cdot 13 \cdot 19) + 3 \cdot (8 \cdot 13 \cdot 17) + m \cdot (13 \cdot 17 \cdot 19) \\ &= 8230 + m \cdot 4199 \ , \end{aligned}$$

von denen $8230 - 4199 = 4031 = 310 \cdot 13 + 1 = 237 \cdot 17 + 2 = 212 \cdot 19 + 3$ die kleinste positive ist.

[6] Sun Zi ($\approx$ 3.Jhd.) *Handbuch der Arithmetik*, wiederveröffentlicht 1247 von Qin Jiushao

1.2.8 Der diskrete Logarithmus

Wann immer p prim ist, so können die Restklassen $0 \neq \overline{a} \in \mathbb{Z}_p$ als Potenzen eines einzigen Elementes $w \in \mathbb{Z}_p$ geschrieben werden, wenn w die maximal mögliche Ordnung $p-1$ hat, also eine sog. *Primitivwurzel* in $\mathbb{Z}_p^\times$ ist, von denen es gemäss dem Satz auf S.16 genau $\varphi(p-1) \geq 1$ viele gibt.

Beispiel

$p = 7$, $\varphi(p-1) = \varphi(6) = 2$. In $M_7 = \mathbb{Z}_7^\times$ gibt es genau 2 Primitivwurzeln $w_1 = \overline{3}$ und $w_2 = \overline{5}$. Wir schreiben die Potenzen $\overline{3}^k$ und $\overline{5}^k$ mit $0 \leq k < p-1 = 6$ in einer Tabelle auf,

k	0	1	2	3	4	5
$\overline{3}^k$	$\overline{1}$	$\overline{3}$	$\overline{2}$	$\overline{6}$	$\overline{4}$	$\overline{5}$
$\overline{5}^k$	$\overline{1}$	$\overline{5}$	$\overline{4}$	$\overline{6}$	$\overline{2}$	$\overline{3}$

und stellen fest, dass tatsächliche jedes Element $\overline{a} \neq \overline{0}$ in $\mathbb{Z}_7$ sowohl als Potenz von $w_1 = \overline{3}$ als auch als Potenz von $w_2 = \overline{5}$ vorkommt.

Definiton diskreter Logarithmus

In einer endlichen zyklischen Gruppe G können definitionsgemäss alle Elemente $g \in G$ als Potenzen $g = w^k$ eines einzigen sog. *Erzeugenden* $w \in G$ (welches im allgemeinen nicht eindeutig ist) erhalten werden, mit $0 \leq k < |G|$. Man nennt erzeugend

$$k = \log_w(g)$$

den *diskreten Logarithmus* von g zur Basis w. diskreter Logarithmus

In unserem Beispiel ist also etwa $4 = \log_{\overline{5}}(\overline{2})$, da $\overline{5}^4 = \overline{2}$ und ebenso $5 = \log_{\overline{5}}(\overline{3})$.

Es gelten die üblichen

Logarithmengesetze — **Beispiel** in $\mathbb{Z}_7^\times$

I) $\log_w(g \cdot h) = \log_w(g) + \log_w(h)$, — $\log_{\overline{5}}(\overline{2} \cdot \overline{3}) = 4 + 5$.

II) $\log_w(g^k) = k \cdot \log_w(g)$, — $\log_{\overline{5}}(\overline{2}^{-1}) = (-1) \cdot 4$.

III) $\log_v(g) = \log_w(g)/\log_w(v)$ (Basiswechsel), — $\log_{\overline{3}}(\overline{2}) = \log_{\overline{5}}(\overline{2})/\log_{\overline{5}}(\overline{3}) = 4/5$.

In der Regel III) (Basiswechsel) muss natürlich v auch wieder ein Erzeuger sein.

Die Rechnungen in den Beispielen rechts müssen nun noch korrekt interpretiert werden. Da $\text{ord}(\overline{5}) = 6 = \text{ord}(\overline{3})$ gilt $\overline{5}^0 = \overline{5}^6 = \overline{5}^{12} = \cdots = \overline{1} = \overline{3}^0 = \overline{3}^6 = \ldots$ und der diskrete Logarithmus bildet also die *multiplikative* Gruppe $M_7 = \mathbb{Z}_7^\times = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$ in die *additive* Gruppe $A_6 = \mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ ab, in der $\mod 6$ gerechnet wird: $4+5 = 9 \equiv 3 \mod 6$. Im Beispiel I) gilt also $\log_{\overline{5}}(\overline{2} \cdot \overline{3}) = \log_{\overline{5}}(\overline{6}) = 3$, im Beispiel II) gilt $\log_{\overline{5}}(\overline{2}^{-1}) = \log_{\overline{5}}(\overline{4}) = -4 \equiv 2 \mod 6$ und in der additiven Gruppe A_6 gilt $5 \cdot 5 = 25 \equiv 1 \mod 6$, also $5 = 5^{-1} = 1/5$ und deshalb $\log_{\overline{3}}(\overline{2}) = 4/5 = 4 \cdot 5 \equiv 2 \mod 6$.

Im allgemeinen gibt es in einer endlichen zyklischen Gruppe G mit $n = |G|$ vielen Elemente genau $\varphi(n)$ viele Erzeuger und jeder dieser Erzeuger w liefert als Basis eines diskreten Logarithmus $\log_w$ einen sog. *Gruppenisomorphismus* von G nach der Isomorphismus

additiven Gruppe A_n mit n Elementen in der $\mod n$ gerechnet wird,

$$\begin{aligned} \log_w \colon G &\longrightarrow A_n \ , \\ g \in G &\mapsto \log_w(g) \in A_n \ . \end{aligned}$$

In unserem Spezialfall haben wir also die multiplikativen (zyklischen) Gruppen $\mathbb{Z}_p^\times = M_p$ mit $n = p-1$ vielen Elementen und $\varphi(n) = \varphi(p-1)$ möglichen Erzeugern, den Primitivwurzeln. Jede dieser Primitivwurzeln w liefert als Basis eines diskreten Logarithmus einen Isomorphismus nach der additiven Gruppe $(\mathbb{Z}_{p-1}, 0, +) = A_{p-1}$, in der $\mod p-1$ gerechnet wird,

$$\log_w \colon \mathbb{Z}_p^\times = M_p \longrightarrow \mathbb{Z}_{p-1} = A_{p-1} \ .$$

Etwas allgemeiner hat Gauß gezeigt, dass die multiplikative Gruppe der Einheiten $\mathbb{Z}_n^\times$ in $\mathbb{Z}_n$ genau dann zyklisch ist, wenn $n = 2$ oder $n = 4$ oder $n = p^k$ oder $n = 2 \cdot p^k$ für jede *ungerade* Primzahl p.
Andererseits ist uns bestens bekannt, dass jede positive Zahl $1 \neq w \in \mathbb{R}_+$ als Basis eines (kontinuierlichen) Logarithmus einen Isomorphismus der multiplikativen Gruppe $(\mathbb{R}_+, 1, \cdot)$ der positiven reellen Zahlen mit der additiven Gruppe $(\mathbb{R}, 0, +)$ aller reellen Zahlen liefert,

$$\log_w \colon \mathbb{R}_+ \longrightarrow \mathbb{R}$$

mit den Logarithmusgesetzen I), II) und III).

1.3 Rationale und reelle Zahlen

1.3.1 Körperstruktur der rationalen Zahlen

Die rationalen Zahlen $\mathbb{Q}$ können als Erweiterung der ganzen Zahlen betrachtet werden, ähnlich wie die ganzen Zahlen $\mathbb{Z}$ eine Erweiterung der natürlichen Zahlen sind.[7] Konkret kann man auf der Menge $\mathbb{Z}\times\mathbb{Z}\setminus\mathbb{Z}\times\{0\}$ eine Aequivalenzrelation definieren,

$$(a,b)\sim(c,d)\Leftrightarrow a\cdot d-b\cdot c=0\ .$$

Die Aequivalenzklasse von $(a,b)\in\mathbb{Z}\times\mathbb{Z}$ mit $b\neq 0$ wird dann als sog. *Bruch* Bruch

$$\frac{a}{b}\quad\text{oder}\quad a/b$$

notiert, wobei man, um einen eindeutigen Repräsentanten zu erhalten, zusätzlich $b\in\mathbb{N}$ und $\mathrm{ggT}(a,b)=1$ fordern kann. Man erhält so einen *gekürzten Bruch* und gekürzt schreibt a statt a/b, wenn $b=1$ ist.
Zusätzlich zur (kommutativen) additiven Gruppenstruktur $(\mathbb{Q},+,0)$ hat man nun auch eine (über die Additon distributive, kommutative) multiplikative Gruppenstruktur $(\mathbb{Q}\setminus 0,\cdot,1)$, d.h. jedes von 0 verschiedene Element in $\mathbb{Q}$ hat ein multiplikatives Inverses

$$\left(\frac{a}{b}\right)^{-1}=\frac{b}{a}\quad\text{mit}\quad\frac{a}{b}\cdot\frac{b}{a}=1\ .$$

$\mathbb{Q}$ ist also ein *Körper*. Insbesondere ist in $\mathbb{Q}$ die Division, also die Multiplikation mit Körper einem Inversen, uneingeschränkt (ausser durch 0) möglich.
Im Folgenden wird das Rechnen mit Brüchen, also das Addieren (nach vorgängigem gleichnamig machen der Nenner), Multiplizieren, Dividieren (Multiplizieren mit dem Kehrwert), Rechnen mit Doppelbrüchen usw. usf. vorausgesetzt.

1.3.2 Kettenbruchentwicklung rationaler Zahlen

Wir bestimmen den $\mathrm{ggT}(3276,1497)$ mit dem Algorithmus von Euklid,

$$\begin{aligned}
3276 &= 2\cdot 1497+282\ ,\\
1497 &= 5\cdot 282+87\ ,\\
282 &= 3\cdot 87+21\ ,\\
87 &= 4\cdot 21+3\ ,\\
21 &= 7\cdot 3+0\ .
\end{aligned}$$

Diese Rechnung benutzen wir nun, um den Bruch

$$\frac{3276}{1497}$$

[7] Man konsultiere auch die entsprechenden Abschnitte der Vorlesung „Grundbegriffe.“

folgendermassen in einen sog. *Kettenbruch* zu entwickeln (ohne uns um den ggT 3 oder vorgängiges Kürzen zu kümmern). Dabei wiederholen wir immer wieder die gleichen Schritte, Zeile um Zeile obiger Rechnung folgend,

$$\begin{aligned}
\frac{3276}{1497} &= \frac{2\cdot 1497+282}{1497} = 2+\frac{282}{1497} = 2+\frac{1}{\frac{1497}{282}} \\
&= 2+\frac{1}{\frac{5\cdot 282+87}{282}} = 2+\frac{1}{5+\frac{87}{282}} = 2+\frac{1}{5+\frac{1}{\frac{282}{87}}} \\
&= 2+\frac{1}{5+\frac{1}{\frac{3\cdot 87+21}{87}}} = 2+\frac{1}{5+\frac{1}{3+\frac{21}{87}}} = 2+\frac{1}{5+\frac{1}{3+\frac{1}{\frac{87}{21}}}} \\
&= 2+\frac{1}{5+\frac{1}{3+\frac{1}{\frac{4\cdot 21+3}{21}}}} = 2+\frac{1}{5+\frac{1}{3+\frac{1}{4+\frac{3}{21}}}} = 2+\frac{1}{5+\frac{1}{3+\frac{1}{4+\frac{1}{\frac{21}{3}}}}} \\
&= 2+\frac{1}{5+\frac{1}{3+\frac{1}{4+\frac{1}{\frac{7\cdot 3+0}{3}}}}} = 2+\frac{1}{5+\frac{1}{3+\frac{1}{4+\frac{1}{7+\frac{0}{3}}}}} = 2+\frac{1}{5+\frac{1}{3+\frac{1}{4+\frac{1}{7}}}}
\end{aligned}$$

was wir, auch um Platz zu sparen, mit Kettenbruch

$$3276/1497 = [2,5,3,4,7]$$

abkürzen. Wir betrachten nun umgekehrt die sog. *partiellen* Kettenbruchentwicklungen, die uns Näherungsbrüche liefern,

$$[2]=2\,,\ [2,5]=2+\frac{1}{5}=\frac{11}{5}\,,\ [2,5,3]=2+\frac{1}{5+\frac{1}{3}}=\frac{35}{16}\,,\ [2,5,3,4]=2+\frac{1}{5+\frac{1}{3+\frac{1}{4}}}=\frac{151}{69}$$

und schliesslich

$$[2,5,3,4,7]=\frac{1092}{499}=\frac{3276}{1497}\approx 2.18837675\ldots\ .$$

Wenn wir diese Brüche numerisch auswerten, machen wir folgende interessante Beobachtung

$$[2]<[2,5,3]<[2,5,3,4,7]<[2,5,3,4]<[2,5]\ ,$$

also

$$2<2.1875<2.18837675\cdots<2.1884\cdots<2.2\ .$$

Die durch die Kettenbruchentwicklung gefundenen Näherungsbrüche sind also abwechselnd zu klein und zu gross, geben also eine mit jedem Schritt engere „Einschachtelung“ des entwickelten Bruches. Einschachtelun
Dazu werden wir später noch Genaueres sagen. Zunächst wollen wir eine etwas effizientere Methode kennen lernen, um bei einem vorliegenden Kettenbruch

$$[b_0, b_1, \ldots, b_n]$$

die Näherungsbrüche p_i/q_i für $i = 0, 1, \ldots n$ auszurechnen. Dazu schreibt man die b_i in einer Zeile hin und trägt die p_i und q_i von links nach rechts ein.

i	-2	-1	0	1	$\ldots$	k	$\ldots$	n
b_i			b_0	b_1	$\ldots$	b_k	$\ldots$	b_n
p_i	0	1	b_0	$b_1 \cdot b_0 + 1$	$\ldots$	$b_k \cdot p_{k-1} + p_{k-2}$	$\ldots$	$b_n \cdot p_{n-1} + p_{n-2}$
q_i	1	0	1	$b_1 \cdot 1 + 0$	$\ldots$	$b_k \cdot q_{k-1} + q_{k-2}$	$\ldots$	$b_n \cdot q_{n-1} + q_{n-2}$

Da in jedem Schritt $p_k = b_k \cdot p_{k-1} + p_{k-2}$ bzw. $q_k = b_k \cdot q_{k-1} + q_{k-2}$ ausgerechnet wird, werden die p's und q's aus den zwei vorangehenden Schritten benötigt. Um mit der Rechnung beginnen zu können, initiiert man deshalb die Tabelle formal mit $p_{-1} = 1 = q_{-2}$ und $p_{-2} = 0 = q_{-1}$. Für unser Beipiel $[2, 5, 3, 4, 7]$ oben rechnet man nun nach

i	-2	-1	0	1	2	3	4
b_i			2	5	3	4	7
p_i	0	1	2	11	35	151	1092
q_i	1	0	1	5	16	69	499

.

Dies ergibt nun tatsächlich die Näherungsbrüche Näherungs-brüche

$$\frac{p_0}{q_0} = 2\ ,\ \frac{p_1}{q_1} = \frac{11}{5}\ ,\ \frac{p_2}{q_2} = \frac{35}{16}\ ,\ \frac{p_3}{q_3} = \frac{151}{69}\ ,\ \frac{p_4}{q_4} = \frac{1092}{499}\ ,$$

wie wir sie bereits oben etwas umständlicher berechnet haben. Dass die Näherungsbrüche so bereits in gekürzter Form vorliegen, dass also $\mathrm{ggT}(p_i, q_i) = 1$ gilt, folgt aus folgender

Behauptung

$$p_i \cdot q_{i+1} - p_{i+1} \cdot q_i = (-1)^{i+1} \quad \text{für } i = -2, -1, 0, 1, 2, 3, \ldots, n-1\ .$$

Denn dann gibt es offensichtlich $a = (-1)^i \cdot q_i$ und $c = (-1)^{i+1} \cdot p_i \in \mathbb{Z}$ mit

$$a \cdot p_{i+1} + c \cdot q_{i+1} = 1\ .$$

Beweis der Behauptung durch vollständige Induktion:
Verankerung bei $i = -2$: $p_{-2} \cdot q_{-1} - p_{-1} \cdot q_{-2} = 0 \cdot 0 - 1 \cdot 1 = -1 = (-1)^{-2+1}$ ✓
Schritt $i \to i+1$: $p_{i+1} \cdot q_{i+2} - p_{i+2} \cdot q_{i+1} = p_{i+1} \cdot (b_{i+2} \cdot q_{i+1} + q_i) - (b_{i+2} \cdot p_{i+1} + p_i) \cdot q_{i+1}$.
Ausmultiplizieren, Vereinfachen und Einsetzen der Induktionsvoraussetzung liefert das Gewünschte. □

Aus der Behauptung folgt nun sofort, dass die Näherungsbrüche abwechselnd zu klein und zu gross sind, da ihre Differenz

$$\frac{p_{i+1}}{q_{i+1}} - \frac{p_i}{q_i} = \frac{p_{i+1}\cdot q_i - p_i \cdot q_{i+1}}{q_{i+1}\cdot q_i} = \frac{(-1)^i}{q_{i+1}\cdot q_i}$$

bei jedem Schritt das Vorzeichen wechselt. Ausserdem wird diese Differenz ständig kleiner, da

$$q_0 = 1 \le q_1 = b_1 < q_2 = b_2 \cdot b_1 + 1 < \dots \ .$$

Da der zu entwickelnde Bruch $p/q = p_n/q_n$ immer irgendwo zwischen p_i/q_i und p_{i+1}/q_{i+1} liegt, haben also die Näherungsbrüche höchstens den Abstand

$$\left|\frac{p}{q} - \frac{p_i}{q_i}\right| \le \left|\frac{p_{i+1}}{q_{i+1}} - \frac{p_i}{q_i}\right| = \frac{1}{q_{i+1}\cdot\ q_i} \le \frac{1}{q_i^2} \quad \text{für } i = 0, 1, \dots, n-1 \ .$$

Überraschenderweise gilt sogar eine Art Umkehrung dieser Tasache, die wir weiter unten allgemeiner für reelle Zahlen x diskutieren. Brüche, die eine gegebene Zahl x relativ gut approximieren, wobei „relativ gut“ durch das Quadrat deren Nenner quantifiziert wird,[8] treten in der Kettenbruchentwicklung von x tatsächlich auch als Näherungsbrüche auf! (*Kriterium von Legendre*, 1.3.5)

Wir schulden noch eine Erklärung des Algorithmus zur obigen tabellarischen

Berechnung der Näherungsbrüche

Dies wird wieder mit vollständiger Induktion vollbracht. Offenbar sind

$$p_0/q_0 = b_0 \quad \text{und } p_1/q_1 = b_0 + 1/b_1$$

tatsächlich die ersten zwei Näherungsbrüche (Induktionsverankerung).
Für den Induktionsschritt von $[b_0, b_1, \dots, b_k]$ auf $[b_0, b_1, \dots, b_k, b_{k+1}]$ fassen wir in $[b_0, b_1, \dots, b_k, b_{k+1}]$ die letzten beiden b's zu $\tilde{b}_k = [b_k, b_{k+1}] = b_k + 1/b_{k+1}$, zusammen,

$$[b_0, b_1, \dots, b_k, b_{k+1}] = [b_0, b_1, \dots, [b_k, b_{k+1}]] = [b_0, b_1, \dots, \tilde{b}_k] \ ,$$

und bemerken, dass wir für $[b_0, b_1, \dots, \tilde{b}_k]$ die Induktionsvoraussetzung auch als nachgewiesen betrachten können, da es nicht darauf ankommt, ob die b_i ganze Zahlen sind oder allgemeiner Brüche (oder reelle Zahlen). Also ist

$$[b_0, b_1, \dots, \tilde{b}_k] = \tilde{p}_k/\tilde{q}_k \quad \text{mit} \quad \begin{cases} \tilde{p}_k & = \tilde{b}_k \cdot p_{k-1} + p_{k-2} \\ \tilde{q}_k & = \tilde{b}_k \cdot q_{k-1} + q_{k-2} \ . \end{cases}$$

Nun finden wir

$$\tilde{p}_k = (b_k + \frac{1}{b_{k+1}}) \cdot p_{k-1} + p_{k-2} = \underbrace{b_k \cdot p_{k-1} + p_{k-2}}_{p_k} + \frac{p_{k-1}}{b_{k+1}} = \frac{\overbrace{b_{k+1}\cdot p_k + p_{k-1}}^{p_{k+1}}}{b_{k+1}} \ ,$$

[8] Konkret: Nur die vier oben berechneten Näherungsbrüche erfüllen $|1092/499 - p/q| < 1/(2q^2)$!

also $\tilde{p}_k = p_{k+1}/b_{k+1}$ und ebenso $\tilde{q}_k = q_{k+1}/b_{k+1}$ und daher

$$[b_0, b_1, \ldots, b_k, b_{k+1}] = [b_0, b_1, \ldots, \tilde{b}_k] = \frac{\tilde{p}_k}{\tilde{q}_k} = \frac{p_{k+1}/b_{k+1}}{q_{k+1}/b_{k+1}} = \frac{p_{k+1}}{q_{k+1}} \qquad \square$$

Bemerkungen

1. Endete in unserem Beispiel $[2, 5, 3, 4, 7]$ die Kettenbruchentwicklung auf 1 statt auf 7, so würden wir diese als $[2, 5, 3, 5]$ schreiben. So endet also nur $[1]$ auf 1.

2. Für negative Zahlen ist $b_0 < 0$ aber $b_k > 0$ für $k > 0$. Allgemein ist $b_0 = \lfloor x \rfloor$, die sog. *Gauß–Klammer* von x, also die grösste ganze Zahl n mit $n \leq x$. Gauß–Klammer

3. Die Zuordnung von rationalen Zahlen zu sog. *normierten* Kettenbrüchen ist bijektiv. (Beachte Bemerkung 1).

4. Im folgenden betrachten wir auch Kettenbruchentwicklungen nicht–rationaler reeller Zahlen. Diese sind *unendlich*, d.h. sie brechen nicht ab.

5. Die nicht–abbrechenden *periodischen* Kettenbruchentwicklungen sind genau die irrationalen Lösungen *quadratischer* Gleichungen mit ganzzahligen Koeffizienten. (ohne Beweis) period. Kettenbruch

6. Einige der obigen Rechnungen bleiben unverändert auch für nicht–abbrechende Kettenbruchentwicklungen gültig, insbesondere die tabellarische Auswertung der Näherungsbrüche.

1.3.3 Reelle Zahlen

Bekanntlich lässt sich die Gleichung $x^2 = 3$ mit keinem Bruch aus $\mathbb{Q}$ erfüllen, wenn auch zu jeder noch so kleinen Schranke $\epsilon > 0$ natürliche Zahlen $p(\epsilon)$ und $q(\epsilon)$ angegeben werden können mit

$$\left| 3 - \left(\frac{p(\epsilon)}{q(\epsilon)} \right)^2 \right| < \epsilon \ .$$

Im Gegensatz zu den Erweiterungen $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q}$ der natürlichen über die ganzen zu den rationalen Zahlen, die die Erweiterung der Grundoperationen Addition, Subtraktion, Multiplikation und Division ermöglichen, ist die Erweiterung $\mathbb{Q} \subset \mathbb{R}$ durch eine Art „Stetigkeitsforderung," man sagt auch „Vervollständigung," bedingt: Wenn sich eine Zahl x, z.B. mit der Eigenschaft $x^2 = 3$ in $\mathbb{Q}$ beliebig gut annähern lässt, so schliesst man eigentlich nur eine Lücke in $\mathbb{Q}$, wenn man ein Objekt mit dieser Eigenschaft ($x = \sqrt{3}$) hinzunimmt. Anschaulich wird ein solches Vorgehen z.B. untermauert, indem man die Höhe in ein gleichseitiges Dreieck mit Seitenlänge 2 einzeichnet. Nach Pythagoras hat diese eine Länge mit der Eigenschaft $x^2 + 1^2 = 2^2$, also $x^2 = 3$. Vervollständigung

Man kann nun „Schachtelungen," wie wir sie bei der Kettenbruchentwicklung im vorangehenden Unterabschnitt angetroffen haben, geradezu benutzen, um Elemente aus $\mathbb{R}$ zu *definieren*. Hat man rationale Zahlen q_0, q_1, q_2, ... mit reelle Zahl

$$q_0 \le q_2 \le q_4 \le \cdots \le q_5 \le q_3 \le q_1$$

und strebt zudem $q_{2n+1} - q_{2n}$ für $n = 0, 1, 2, \ldots$ gegen 0, so werde dadurch ein eindeutiges Element $r \in \mathbb{R}$ festgelegt (das z.B. für $q_n = (-1)^{n+1}/(n+1)$ durchaus auch in $\mathbb{Q}$ liegen kann, wie in diesem Falle $r = 0$). Nach bewährter Manier ist auf den „Schachtelungen“ eine Aequivalenzrelation anzugeben, da ein Element $r \in \mathbb{R}$ natürlich auf ganz verschiedene Art und Weise in eine Schachtelung „eingesperrt“ werden kann. Mehr dazu in der Analysis, wo dieses Vorgehen eine Zentrale Rolle spielt (*Grenzwerte*). Grenzwert

Die Körperstruktur überträgt sich ohne Probleme von $\mathbb{Q}$ auf $\mathbb{R}$, da alle Grundoperationen *stetig* sind, d.h. keine Sprünge machen, d.h. Elemente, die nahe beieinander liegen, in solche abbilden, die wieder (kontrollierbar) nahe beeinander liegen. Stetigkeit

Schliesslich sei noch erwähnt, dass es eine unüberschaubare Menge weiterer Zahlkörper $\mathbb{Q} \subset \mathbb{K} \subset \mathbb{R}$ zwischen $\mathbb{Q}$ und $\mathbb{R}$ gibt. Ein wichtiges Beispiel sind die (mit Zirkel und Lineal) *konstruierbaren* Zahlen, die im Wesentlichen durch hinzunehmen zu $\mathbb{Q}$ von Quadratwurzeln (und von Quadratwurzeln von Quadratwurzeln von ...) entstehen.

1.3.4 Kettenbruchentwicklung reeller Zahlen

Für Brüche haben wir die Kettenbruchentwicklung mittels *Euklidschem Algorithmus* erhalten. Allgemeiner können wir für eine reelle Zahl, z.B. für $\sqrt{3}$ wie folgt vorgehen:

$$\sqrt{3} = \lfloor\sqrt{3}\rfloor + r_1 = 1 + \frac{1}{1/r_1} \quad \text{mit } 0 \le r_1 < 1 \ (\lfloor\ \rfloor \text{ Gaußklammer}).$$

Mit $x_1 = 1/r_1 > 1$ verfahren wir nun wie vorher mit $x_0 = \sqrt{3}$:

$$x_1 = \lfloor x_1\rfloor + r_2 = \lfloor x_1\rfloor + \frac{1}{1/r_2} \quad \text{mit } 0 \le r_2 < 1\ .$$

Nun fahren wir mit $x_2 = 1/r_2$ ebenso weiter, usw. usf. Wir erhalten einen Kettenbruch Kettenbruch

$$x_0 = \lfloor x_0\rfloor + \frac{1}{x_1} = \lfloor x_0\rfloor + \frac{1}{\lfloor x_1\rfloor + \dfrac{1}{x_2}} = \lfloor x_0\rfloor + \frac{1}{\lfloor x_1\rfloor + \dfrac{1}{\lfloor x_2\rfloor + \dfrac{1}{x_3}}} = \ldots\ ,$$

den wir mit $[b_0, b_1, b_2, \ldots]$ angeben, wobei $b_k = \lfloor x_k\rfloor \ge 1$ gilt für alle $k \in \mathbb{N}$, da im Falle von $x_0 \notin \mathbb{Q}$ der „Rest“ r_k immer $0 < r_k < 1$ erfüllt. Ebenso lässt sich z.B. der letzte Kettenbruch oben mit $[b_0, b_1, b_2, x_3]$ mit $1 < x_3 \in \mathbb{R}$ angeben.

Wir rechnen nun die Kettenbruchentwicklung für $x_0 = \sqrt{3}$ konkret aus.

$$r_1 = x_0 - \lfloor x_0\rfloor = \sqrt{3} - 1 \quad \Rightarrow \quad x_1 = \frac{1}{r_1} = \frac{1}{\sqrt{3}-1} = \frac{\sqrt{3}+1}{2}\ ,$$

$$r_2 = x_1 - \lfloor x_1\rfloor = \frac{\sqrt{3}+1}{2} - 1 \quad \Rightarrow \quad x_2 = \frac{1}{r_2} = \frac{2}{\sqrt{3}-1} = \sqrt{3}+1\ ,$$

$$r_3 = x_2 - \lfloor x_2\rfloor = (\sqrt{3}+1) - 2 \quad \Rightarrow \quad x_3 = \frac{1}{r_3} = \frac{1}{\sqrt{3}-1} = \frac{\sqrt{3}+1}{2}\ .$$

Aus $x_3 = x_1$ folgt $x_4 = x_2$, $x_5 = x_3$ usw. usf. Es ergibt sich also die *periodische* Entwicklung

$$\sqrt{3} = 1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \dots}}}}} = 1 + \cfrac{1}{1 + \cfrac{1}{2 + (\sqrt{3} - 1)}} \ ,$$

die wir abkürzend mit $[1, \overline{1, 2}]$ statt mit $[1, 1, 2, 1, 2, 1, 2, 1, 2, \dots]$ bezeichnen. period. Kettenbruch
Die tabellarische Berechnung der Näherungsbrüche p_i/q_i ergibt

i	-2	-1	0	1	2	3	4	$\dots$
b_i			1	1	2	1	2	$\dots$
p_i	0	1	1	2	5	7	19	$\dots$
q_i	1	0	1	1	3	4	11	$\dots$

.

Alle Näherungsbrüche $p_k/q_k = 1, 2, 5/3, 7/4, 19/11, \dots$ erfüllen die Abschätzung

$$\left| \sqrt{3} - \frac{p_k}{q_k} \right| \leq \frac{1}{q_k^2}$$

auf S.24. Für etwa jeden zweiten gilt sogar $|\sqrt{3} - p_k/q_k| < 1/(2q_k^2)$.

Aufgabe
Gib die Kettenbruchentwicklung von $\sqrt{2}$.

1.3.5 Kriterium von Legendre

Satz *(Kriterium von Legendre)* Legendre–Kriterium
Ist $q \in \mathbb{N}$, $p \in \mathbb{Z}$ und $x \in \mathbb{R}$ mit

$$\left| x - \frac{p}{q} \right| < \frac{1}{2 \cdot q^2} \ ,$$

so tritt p/q in der Kettenbruchentwicklung von x auf.

Ohne Einschränkung des Nenners q kann man natürliches jedes $x \in \mathbb{R}$ beliebig gut durch einen Bruch $p/q \in \mathbb{Q}$ approximieren. Dieser Satz sagt aber, dass ein *irgendwie* gefundener Näherungsbruch p/q für ein $x \in \mathbb{R}$ von der „Qualität“ $1/(2q^2)$ oder besser, automatisch auch durch die Kettenbruchentwicklung von x gefunden wird.

Beweis des Satzes
Wir betrachten den Fall, wo ein $n \in \mathbb{N}_0$ existiert mit $q_n \leq q < q_{n+1}$. Da die Nenner q_n der Näherungsbrüche in einer Kettenbruchentwicklung immer ansteigen, tritt dieser Fall immer ein, ausser es handle sich um einen abbrechenden Kettenbruch mit letztem Nenner $q_n \leq q$. In diesem Fall gilt $x = p_n/q_n = p/q \in \mathbb{Q}$ (Übung).
Im Betrachteten Fall werden wir zeigen, dass gilt

$$|q_n \cdot x - p_n| \leq |q \cdot x - p| \qquad (*)$$

und benutzen dies in folgender, mit der Dreiecksungleichung beginnender Kette von Abschätzungen:

$$\begin{aligned}
\left|\frac{p}{q}-\frac{p_n}{q_n}\right| &\leq \left|x-\frac{p}{q}\right|+\left|x-\frac{p_n}{q_n}\right| = \left|x-\frac{p}{q}\right|+\frac{1}{q_n}\cdot|q_n\cdot x-p_n| \\
&\overset{(*)}{\leq} \left|x-\frac{p}{q}\right|+\frac{1}{q_n}\cdot|q\cdot x-p| = \left|x-\frac{p}{q}\right|+\frac{q}{q_n}\cdot\left|x-\frac{p}{q}\right| \\
&= \left(1+\frac{q}{q_n}\right)\cdot\left|x-\frac{p}{q}\right| < \frac{q_n+q}{q_n}\cdot\frac{1}{2\cdot q^2} \quad \text{(nach Voraussetzung)} \\
&\leq \frac{2q}{q_n}\cdot\frac{1}{2q^2} = \frac{1}{q_n\cdot q}\ .
\end{aligned}$$

Multiplikation mit $q_n\cdot q$ ergibt schliesslich $0\leq|q_n\cdot p-q\cdot p_n|<1$, also $q_n\cdot p=q\cdot p_n$ oder $p/q=p_n/q_n$, da $z=0$ die einzige ganze Zahl mit $0\leq z<1$ ist.
Es beleibt $(*)$ nachzuweisen. Das Gleichungssystem

$$\begin{array}{rcl} p_{n+1}\cdot r+p_n\cdot s &=& p \\ q_{n+1}\cdot r+q_n\cdot s &=& q \end{array} \quad \text{hat} \quad \begin{pmatrix} r \\ s \end{pmatrix} = \frac{1}{p_{n+1}\cdot q_n-p_n\cdot q_{n+1}}\cdot\begin{pmatrix} p\cdot q_n-q\cdot p_n \\ p_{n+1}\cdot q-q_{n+1}\cdot p \end{pmatrix}$$

als eindeutige Lösung (*Cramersche Regel).* Für die Lösung gilt

1. $r,s\in\mathbb{Z}$, da nach der Behauptung auf S.23 gilt $p_{n+1}\cdot q_n-p_n\cdot q_{n+1}=(-1)^n$,
2. $s\neq 0$, sonst wäre $q=r\cdot q_{n+1}\geq q_{n+1}$ im Widerspruch zur Wahl von n,
3. $r\cdot s\leq 0$ aus dem gleichen Grund.

Ebenso haben $x-p_n/q_n$ und $x-p_{n+1}/q_{n+1}$ gemäss der Konsequenz der Behauptung auf S.23 nicht das gleiche Vorzeichen (Einschachtelung), also auch nicht $q_n\cdot x-p_n$ und $q_{n+1}\cdot x-p_{n+1}$. Mit Punkt 3. haben also $r\cdot(q_{n+1}\cdot x-p_{n+1})$ und $s\cdot(q_n\cdot x-p_n)$ nicht verschiedene Vorzeichen und wir können abschätzen

$$\begin{aligned}
|q\cdot x-p| &= |(q_{n+1}\cdot r+q_n\cdot s)\cdot x-(p_{n+1}\cdot r+p_n\cdot s)| \\
&= |r\cdot(q_{n+1}\cdot x-p_{n+1})+s\cdot(q_n\cdot x-p_n)| \\
&\overset{!}{=} |r|\cdot|q_{n+1}\cdot x+p_{n+1}|+|s|\cdot|q_n\cdot x+p_n|\geq|q_n\cdot x+p_n|\ . \qquad \square
\end{aligned}$$

1.3.6 Dezimaldarstellung

Auch durch die Dezimaldarstellung

$3\ ,\ 3.1\ ,\ 3.14\ ,\ 3.141\ ,\ 3.1415\ ,\ 3.14159\ ,\ 3.141592\ ,\ 3.1415926\ ,\ 3.14159265\ ,\ \ldots$

ergibt sich die Darstellung einer reellen Zahl $\pi\in\mathbb{R}$ als ein Einschachtelung

$$\pi\in[3,4]\ ,\ \pi\in[3.1,3.2]\ ,\ \pi\in[3.14,3.15]\ ,\ \pi\in[3.141,3.142]\ ,$$

wobei hier die „Schachtelbreite“ mit jedem Entwicklungsschritt gleichmässig um den Faktor 10 kleiner wird. Mit Hilfe der Gaußklammer lässt sich die Entwicklung der Nachkommastellen einer positiven reellen Zahl $x \in \mathbb{R}$ folgendermassen formalisieren

$$\begin{aligned} x &= \lfloor x \rfloor + x_1 \quad \text{mit } x_1 \in [0,1) \\ 10 \cdot x_1 &= \lfloor 10 \cdot x_1 \rfloor + x_2 = b_1 + x_2 \quad \text{mit } x_2 \in [0,1) \\ 10 \cdot x_2 &= \lfloor 10 \cdot x_2 \rfloor + x_3 = b_2 + x_3 \quad \text{mit } x_3 \in [0,1) \\ &\dots \end{aligned}$$

Es gilt dann $b_k \in \{0,1,2,3,4,5,6,7,8,9\}$, wobei $b_k = 9$ nur endlich oft hintereinander auftreten kann, da sich sonst ein Widerspruch zu $x_k < 1$ ergibt. Man stellt nun die positive Zahl $x \in \mathbb{R}$ dar als

Dezimal–darstellung

$$\lfloor x \rfloor . b_1 b_2 b_3 \dots$$

indem man die sog. *Nachkommastellen* b_k hintereinander nach der natürlichen Zahl $\lfloor x \rfloor \in \mathbb{N}_0$ aufreiht, abgetrennt durch ein „.“ (Komma).[9] Bricht man (wie in der Praxis unumgänglich) nach endlich vielen Schritten ab, so ist die so angegebene Zahl kleiner als x wenn nicht $b_k = 0$ für alle folgenden Stellen gilt, und zwar um weniger als 10^{-n}, wenn b_n die letzte angegebene Nachkommastelle ist. Aus mathematischer Sicht ist eine Notation

$$\pi = 3.1416$$

unzulässig (wenn mit π der halbe Umfang des Einheitskreises gemeint ist). Zulässig ist

$$\begin{aligned} \pi &\approx 3.1416 \text{ oder} \\ \pi &\doteq 3.1416 \end{aligned}$$

und bedeutet $\pi \in [3.14155, 3.14165)$ (*Rundungsregel*). Die vierte Nachkommastelle von π ist (im Dezimalsystem) jedoch $b_4 = 5$.

Rundungs-regel

Negative Zahlen $x \in \mathbb{R}$ werden mittels $\lfloor |x| \rfloor$ und Entwicklung der b_k von $|x|$ mit vorangehendem „$-$“ dargestellt. Bis auf die angesprochenen Fälle ($b_k \neq 9$ unendlich oft, Abbruch bei lauter $b_k = 0$ und $0 = -0$) ist die Zuordnung einer reellen Zahl $x \in \mathbb{R}$ zu ihrer Dezimaldarstellung $\pm \lfloor |x| \rfloor . b_1 b_2 b_3 \dots$ bijektiv. Die Umkehrabbildung von der Dezimaldarstellung zur Zahl ergibt sich durch die konvergente Reihe

$$x = \pm \left(\lfloor |x| \rfloor + \sum_{k=1}^{\infty} b_k \cdot 10^{-k} \right) .$$

[9] Wegen Verwechslungsgefahr mit „,“ in Vektorschreibweise $(3,2)$ etc. heutzutage meist „.“

1.3.7 Dezimaldarstellung rationaler Zahlen

Satz *über die Dezimaldarstellung rationaler Zahlen*
Eine reelle Zahl $x \in \mathbb{R}$ ist genau dann in $\mathbb{Q}$, wenn ihre Dezimaldarstellung schliesslich periodisch wird, also genau dann wenn es ein $r \in \mathbb{N}_0$ und ein $n \in \mathbb{N}$ gibt

$$b_{k+n} = b_k \text{ für alle } k > r \ .$$

Definitionen (Vorperiode, Periodenlänge)
Zu einem $x \in \mathbb{Q}$ und dem kleinsten $r \in \mathbb{N}_0$, zu dem es ein $n \in \mathbb{N}$ mit obiger Eigenschaft gibt, heisst

$$b_1 b_2 \dots b_r$$

die *Vorperiode* (der Länge r) von x, die auch leer sein kann. Das kleinste solche n heisst *Periodenlänge* von x und $b_{r+1} \dots b_{r+n}$ heisst die *Periode*. Vor-/Periode

Beweis des Satzes
Wir betrachten ein $0 < x = p/q \in \mathbb{Q}$ und zeigen, dass die Dezimalbruchentwicklung, wie auf S.29 formalisiert, periodisch werden muss. Aus

$$x = \frac{p}{q} = \lfloor x \rfloor + x_1 \quad \text{mit } x_1 \in [0,1) \text{ folgt } p = \lfloor x \rfloor \cdot q + x_1 \cdot q$$

mit $r_1 = x_1 \cdot q \in \mathbb{N}_0$ und $0 \le r_1 < q$. Daraus folgt, dass $r_1 = x_1 \cdot q$ der eindeutig bestimmte Rest der Division von p durch q mit Rest r_1 mit $0 \le r_1 < q$ ist. Aus

$$10 \cdot x_1 = \lfloor x_1 \rfloor + x_2 \quad \text{mit } x_2 \in [0,1) \text{ folgt } 10 \cdot x_1 \cdot q = 10 \cdot r_1 = \lfloor x_1 \rfloor \cdot q + x_2 \cdot q$$

mit $r_2 = x_2 \cdot q \in \mathbb{N}_0$ und $0 \le r_2 < q$. Daraus folgt, dass $r_2 = x_2 \cdot q$ der eindeutig bestimmte Rest der Division von $10 \cdot r_1$ durch q mit Rest r_2 mit $0 \le r_2 < q$ ist, usw. usf. Es ist also $r_1 = x_1 \cdot q$ die Restklasse von p mod q, diese wird mit 10 multipliziert und dann wieder die Restklasse $r_2 = x_2 \cdot q$ von $10 \cdot r_1$ mod q bestimmt, diese wieder mit 10 multipliziert usw. usf. Da es nur q Restklassen mod q gibt und Rest 0 zum Abbruch führt, wiederholt sich die Ausgangslage nach spätestens $q-1$ Schritten. Die Periodenlänge ist also höchstens $n = q-1$.
Hat umgekehrt x die periodische Dezimaldarstellung

$$\lfloor x \rfloor . b_1 \dots b_r b_{r+1} \dots b_{r+n} b_{r+1} \dots b_{r+n} b_{r+1} \cdots = \lfloor x \rfloor . b_1 \dots b_r \overline{b_{r+1} \dots b_{r+n}} \ ,$$

so stellt diese die rationale Zahl

$$\lfloor x \rfloor + b_1 \cdot 10^{-1} + \cdots + b_r \cdot 10^{-r} + (b_{r+1} \cdot 10^{-(r+1)} + \cdots + b_{r+n} \cdot 10^{-(r+n)}) \cdot \frac{1}{1 - 10^{-n}}$$

dar, da sich die geometrische Reihe $1 + 10^{-n} + 10^{-2n} + 10^{-3n} + \dots$ zu $1/(1-10^{-n})$ summiert. □

Wir stellen fest, dass die zuletzt im Beweis dargestellte Zahl eine ganze Zahl ergibt, wenn man sie mit $10^r \cdot (10^n - 1)$ multipliziert, da $(10^n - 1)/(1 - 10^{-n}) = 10^n$ ergibt. Davon gilt auch die Umkehrung:

Eine Zahl $z/[(10^r \cdot (10^n - 1)]$ mit $z \in \mathbb{N}$ hat eine Dezimaldarstellung der Form

$$\tilde{z}.b_1 \dots b_r \overline{b_{r+1} \dots b_{r+n}} \quad \text{mit } \tilde{z} \in \mathbb{N}_0.$$

Zunächst sieht man, dass $z/(10^n-1)$ eine solche Darstellung ohne Vorperiode ($r = 0$) haben muss, da gilt $z = 10^n \cdot z/(10^n - 1) - z/(10^n - 1)$, also

$$z = [(\underbrace{\tilde{z} \cdot 10^n + a_1 a_2 \dots a_n}_{\in \mathbb{N}_0}).a_{n+1} a_{n+2} \dots] - [\tilde{z}.a_1 a_2 \dots] \in \mathbb{N} \ .$$

Die Nachkommastellen müssen sich also wegheben: $a_{n+1} = a_1$, $a_{n+2} = a_2$, ..., d.h. es liegt eine periodische Dezimalentwicklung vor, mit Periodenlänge n. Division durch 10^r verschiebt nun diese Periode einfach um r Stellen nach rechts. (Ebenso für $z \in \mathbb{Z}$.)

Satz *über die Länge der Periode und der Vorperiode*
Sei $p/q \in \mathbb{Q}$ mit $ggT(p, q) = 1$ (gekürzter Bruch). Sei $q = q' \cdot q''$ mit[10] maximalem

$$q'' \text{ mit } \mathrm{ggT}(q'', 10) = 1 \ .$$

Sei $r \in \mathbb{N}_0$ die kleinste Zahl mit $q' | 10^r$ und $n \in \mathbb{N}$ die kleinste Zahl mit $q'' | (10^n - 1)$. Dann ist $r \geq 0$ die Länge der Vorperiode und $n > 0$ die Periodenlänge in der Dezimalentwicklung von p/q. (Für $q'' = 1$ könnte man auch von einer Periodenlänge $n = 0$ oder einer abbrechenden Dezimalbruchentwicklung sprechen.)

Beweis
Die Dezimalentwicklung von p/q ist nach dem vorausgehenden Satz periodisch, mit allenfalls einer Vorperiode der Länge r. Dann ist $10^r \cdot (10^n - 1) \cdot p/q \in \mathbb{Z}$, wie wir gesehen haben. Der Nenner q muss also ein Teiler von $10^r \cdot (10^n - 1)$ sein, da $\mathrm{ggT}(p, q) = 1$. Da $\mathrm{ggT}(10^r, 10^n - 1) = 1$ muss also 10^r ein Vielfaches von q' sein, da $\mathrm{ggT}(q'', 10) = 1$. Ebenso muss $10^n - 1$ ein Vielfaches von q'' sein. □

Beispiel $p/q = 76/325 = (4 \cdot 19)/(5^2 \cdot 13)$
Es ist $r = 2$, da $q' = 25$ und $n = 6$, da aus $q'' = 13 | (10^n - 1)$ mit $n \in \mathbb{N}$ folgt $n \geq 6$.

Bemerkung
Für eine Primzahl $p \notin \{2, 5\}$ hat also $1/p$ eine Dezimaldarstellung ohne Vorperiode mit Periodenlänge $n = \mathrm{ord}(10)$, der Ordnung von 10 in der Gruppe $\mathbb{Z}_p^\times$, ist also ein Teiler von $p - 1$. Die Periode hat also genau dann maximale Länge $p - 1$, wenn 10 eine Primitivwurzel mod p ist. Bis heute weiss man nicht, ob 10 für unendlich viele Primzahlen p eine Primitivwurzel ist. Allgemein gilt $n = \mathrm{ord}(10)$ in $\mathbb{Z}_{q''}^\times$.

Perioden–länge

1.3.8 Darstellung in beliebigen Basen

Dass wir zehn Ziffern $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ benutzen ist wohl dem Umstand zu verdanken, dass wir zehn Finger haben. Auf einem Planeten, wo intelligente Wesen an zwei Extremitäten je drei Finger haben, wird vielleicht mit sechs Ziffern gerechnet, etwa $\{0, 1, 2, 3, 4, 5\}$. Mit $z_k \in \{0, 1, 2, 3, 4, 5\}$ wäre

$$\begin{aligned} x &= \dots z_2 \cdot 6^2 + z_1 \cdot 6^1 + z_0 \cdot 6^0 + z_{-1} \cdot 6^{-1} + z_{-2} \cdot 6^{-2} + z_{-3} \cdot 6^{-3} + \dots \\ &= \dots z_2 z_1 z_0 . z_{-1} z_{-2} z_{-3} \dots \end{aligned}$$

[10] d.h. q'' enthält alle Primfaktoren von q ausser 2 und 5, die alle in q' enthalten sind

die *Hexaldarstellung* der Zahl $x \in \mathbb{R}$. Wiederum sind die rationalen Zahlen genau diejenigen, deren Hexaldarstellung schliesslich periodisch wird, z.B.

$$\begin{aligned}
[12.5\overline{43}]_6 &= 1 \cdot 6^1 + 2 \cdot 6^0 + 5 \cdot 6^{-1} + 4 \cdot 6^{-2} + 3 \cdot 6^{-3} + 4 \cdot 6^{-4} + 3 \cdot 6^{-5} + 4 \cdot 6^{-6} + \ldots \\
&= 6 + 2 + 5/6 + (4/36 + 3/216) \cdot \underbrace{(1 + 1/6^2 + 1/6^4 + 1/6^6 + \ldots)}_{=1/(1-1/36)=36/35} \\
&= 941/105 \; .
\end{aligned}$$

Wie lautet der entsprechende Satz für die Längen der Periode und der Vorperiode?

Kapitel 2

Gleichungen mit ganzzahligen Lösungen

Gleichungen über den ganzen Zahlen, bei denen man speziell nach ganzzahligen Lösungen fragt, nennt man auch *diophantische* Gleichungen nach *Diophantos*,[1] der darüber ein Buch geschrieben hat, das etwa 1500 Jahre lang auf diesem Teilgebiet der Zahlentheorie massgeblich war. *Fermat* hat dieses Buch eingehend studiert. Neben Aufgabe 8 in Band 2, wo es darum geht, ein Quadrat in zwei Quadrate zu zerlegen (Pythagoras), schreibt er an den etwas schmalen Rand seiner Bettlektüre

cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos et generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est diuidere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

Dass also ein *cubus* (dritte Potenz) in zwei *cubi* oder ein *quadratoquadratus* (vierte Potenz) in zwei *quadratoquadrati* und allgemein (*generaliter*) keine Potenz (*nulla potestas*) ab der zweiten (*ultra quadratum*) bis ins Unendliche (*in infinitum*) in zwei dieser Gleichen (*in duos eiusdem nominis*) aufzuteilen möglich ist (*diuidere fas est*) — einen wirklich wunderbaren Beweis (*sane mirabilem demonstrationem*) dieser Tatsache (*cuius rei*) habe ich entdeckt (*detexi*). Die Breite des Randes (*exiguitas marginis*) würde diesen nicht fassen (*hanc non caperet*).
Fermat liebte es, seine Mathematikerkollegen zu provozieren, indem er Sätze ankündete, die diese nicht oder nur mit grosser Mühe beweisen konnten, wobei er vorgab, keine Zeit zu haben, seine Beweise aufzuschreiben. Vielleicht brauchte er das als harmlosen Ausgleich, da ihm als Richter das Aufhängenlassen von Verbrechern nachgewiesenermassen die eine oder andere Krise bescherte (besonders, wenn sich diese nachträglich als unschuldig herausstellten oder er sich aus politischen Gründen den Intrigen und Fehlurteilen seiner Richterkollegen anschliessen musste).
Über 100 Jahre später grub *Euler* Fermats vergessenes Werk aus. Nach einigen Fehlversuchen und Aufträgen zur Sichtung Fermats Nachlasses wies er gerade mal

$$a^3 + b^3 \neq c^3$$

[1] *Diophantos von Alexandria* (zwischen 100v.Chr. und 350n.Chr.) *Arithmetica* (13 Bände, davon drei verschollen)

für natürliche Zahlen $a, b, c \in \mathbb{N}$ nach. Unter dem Pseudonym *M. LeBlanc* teilte *Sophie Germain* Gauß nach dessen Veröffentlichung der *Disquisitiones Arithmeticae* brieflich mit, weshalb

$$a^p + b^p \neq c^p$$

für zur Primzahl p teilerfremde $a, b, c \in \mathbb{N}$ gilt, wenn auch $2p + 1$ prim ist. *Kummer* verletzte französische Eitelkeiten, als er nachwies, dass sowohl die Beweisidee von *Cauchy* als auch die von *Lamé* untauglich ist, weil der Hauptsatz der Arithmetik (Eindeutigkeit der Faktorisierung) in erweiterten Zahlringen nicht immer gilt, schaffte aber immerhin

$$a^n + b^n \neq c^n$$

für $a, b, c \in \mathbb{N}$ und $100 \geq n \notin \{1, 2, 37, 59, 67, 74\}$. ... ...
Eine Reihe von drei Vorträgen in Cambridge schloss *Andrew Wiles* im Juni 1993 mit der Aussage, damit sei der grosse Satz von Fermat bewiesen um dann im Kongresshaus Zürich anlässlich des internationalen Mathematikerkongresses im August 1994 einräumen zu müssen, er könne die von *N. Katz* gefundene Lücke nicht schliessen. Dies gelang ihm nach seiner Heimreise nach Princeton im September 1994 und seither gilt die berühmteste Randnotiz der Menschheitsgeschichte (*Grosser/Letzter Satz von Fermat* oder *Satz von Wiles–Taylor*) als bestätigt und bewiesen.
Auf dem Weg dorthin haben sich durch die Jahrhunderte auch neue Probleme und Techniken daraus entwickelt. So liess sich etwa Euler 1769 vielleicht durch

$$3^3 + 4^3 + 5^3 = 6^3$$

zur (widerlegten[2]) Vermutung hinreissen, eine n–te Potenz könne nie Summe von weniger als n (und natürlich gleichzeitig von mehr als einer) n–ten Potenzen sein. Auch die (richtige) Vermutung, dass jede Zahl $n \in \mathbb{N}$ als Summe von höchstens vier Quadratzahlen geschrieben werden kann, hat Euler ein Leben lang immer wieder vergeblich zu beweisen versucht.
Heute glaubt kaum jemand, Fermat habe eine *demonstratio mirabilis* für seinen Satz gehabt, auch weil er dann später einen seiner ganz wenigen Beweise aufschreibt für

$$a^4 + b^4 \neq c^4$$

Wo, lieber Pierre, ist dann der Beweis für $n = 3$? Er ist schwieriger!
Fermat's last theorem (1997) von *Simon Singh* ist ein lesenswertes Buch zu alledem. Vor *Gödel* glaubte man noch, man könne Mathematik mit Maschinen betreiben. So phantasierte etwa *David Hilbert* (*„Wir müssen wissen, wir werden wissen“*), es könnte einen Algorithmus geben, der *im Prinzip* ganzzahlige Lösungen polynomialer Gleichungen auffindet und auf jeden Fall anhält, weil eine Lösung gefunden wurde oder nach endlicher Zeit bewiesen ist, dass keine existiert. Zeitschranken wie das Alter des Universums o.ä. würden dabei nicht akzeptiert. Durchprobieren aller Zahlen (Zahlenpaare, –tripel, ...) geht aber auch nicht, da dies nie abbrechen würde, wenn es keine ganzzahlige Lösungen gibt.
Der Satz von *Matiyasevich*[3] sagt, dass es kein solches Programm geben kann.
Sehr wohl gibt es einen solchen Algorithmus aber für

[2] Lander und Parkin (1966) $27^5 + 84^5 + 110^5 + 133^5 = 144^5$
[3] *Matiyasevich* (1970) The Diophantineness of enumerable sets

2.1 Ganzzahlige Lösungen linearer Gleichungen

2.1.1 Lineare Gleichungen mit zwei Unbekannten

Bereits auf S.7 wurde bewiesen, dass die lineare Gleichung

$$b \cdot x + d \cdot y = f$$

für $b, d, f \in \mathbb{Z}$ und $(b, d) \neq (0, 0)$ die ganzzahligen Lösungen

$$\mathbb{L} = \{(x, y) = (a, c) + m \cdot (d/t, -b/t) \,|\, m \in \mathbb{Z}\} \quad \text{oder} \quad \mathbb{L} = \{\}$$

hat, je nachdem ob $t|f$ für $t = \text{ggT}(b, d)$ gilt, oder eben $t \not| f$. Ist $f = t \cdot n$, so bestimmt man (z.B. mit dem *Euklidschen Algorithmus*) $\tilde{a}$ und $\tilde{c}$ mit

$$\tilde{a} \cdot b + \tilde{c} \cdot d = t$$

und erhält damit eine *partikuläre Lösung* $(x, y) = (a, c) = (n \cdot \tilde{a}, n \cdot \tilde{c})$, da dann gilt

$$a \cdot b + c \cdot d = n \cdot \tilde{a} \cdot b + n \cdot \tilde{c} \cdot d = n \cdot (\tilde{a} \cdot b + \tilde{c} \cdot d) = n \cdot t = f \ .$$

Sind (x, y) und (a, c) zwei ganzzahlige Lösungen von $b \cdot x + d \cdot y = f$, so gilt

$$b \cdot (x - a) + d \cdot (y - c) = 0 \ .$$

Also ist $b \cdot (x - a) = v = d \cdot (c - y)$ ein gemeinsames Vielfaches von b und d und somit ein gemeinsames Vielfaches von $\text{kgV}(b, d)$,

$$v = b \cdot (x - a) = m \cdot \text{kgV}(b, d) = m \cdot b \cdot d/t \ ,$$

also $x = a + m \cdot d/t$ (falls $b \neq 0$, andernfalls beliebig) und analog $y = c - m \cdot b/t$. Damit ist der Satz auf S.7 nochmals vollständig bewiesen.
In der linearen Algebra haben wir die Gleichung $b \cdot x + d \cdot y = f$ auch als lineare Abbildung

$$A \colon \mathbb{R}^2 \longrightarrow \mathbb{R}$$

mit zugehöriger 1×2–Matrix $(b, d) \neq (0, 0)$ vom Rang 1 interpretiert. Da für lineare Abbildungen

$$A \colon V \longrightarrow W$$

zwischen Vektorräumen V und W über dem Körper K immer der *Dimensionssatz*

$$\dim_K(\text{im}(A)) + \dim_K(\ker(A)) = \text{rk}_K(A) + \dim(\ker(A)) = \dim_K V$$

gilt[4], in unserem Fall hier also $1 + \dim_{\mathbb{R}}(\ker(A)) = 2$, so ergibt sich hier $\dim_{\mathbb{R}}(\ker(A)) = 1$ und $(d/t, -b/t)$ kann als (ganzzahliger) Basisvektor des 1–dimensionalen Kerns der Abbildung A aufgefasst werden.

[4]Skript *Lineare Algebra und Geometrie*, S.75.

Da wir hier aber einen Übergang von $\mathbb{R}$ (Körper) nach $\mathbb{Z}$ (kein Körper) bzw. von $\mathbb{R}^n$ nach $\mathbb{Z}^n$ machen, müssen wir mit den Begriffen *Bild, Kern, Rang* aus der linearen Algebra etwas vorsichtig umgehen. Zum Beispiel ist das Bild von A als linearer Abbildung über dem Körper $\mathbb{R}$ hier von der Dimension 1, also ganz $\mathbb{R}$. Jedoch gibt es möglicherweise $f \in \mathbb{Z}$, für die es keine (ganzzahligen) Lösungen gibt, eben weil wir den Definitionsbereich der Abbildung von $\mathbb{R}^2$ auf $\mathbb{Z}^2$ einschränken. Trotzdem sind diese und andere Begriffe aus der linearen Algebra hier nützlich.
Der Vollständigkeit halber betrachten wir noch ein System von *zwei* linearen Gleichungen mit *zwei* Unbekannten,

$$\begin{aligned} a \cdot x + c \cdot y &= e \ , \\ b \cdot x + d \cdot y &= f \ . \end{aligned}$$

Wir nehmen an, die entsprechende 2×2–Matrix mit $a, b, c, d \in \mathbb{Z}$ habe Rang 2, sei also invertierbar (über $\mathbb{R}$). Dann gibt es eine *eindeutige* Lösung

$$(x, y) = (e \cdot d - f \cdot c \, , \, a \cdot f - b \cdot e)/(a \cdot d - b \cdot c) \ ,$$

die sich z.B. mit der *Cramerschen Regel* bestimmen lässt und von der man einfach ablesen kann, ob sie in $\mathbb{Z}^2$ also ganzzahlig ist oder nicht.

Aufgabe
Überlege, dass die eindeutige Lösung (x, y) für $a, b, c, d, e, f \in \mathbb{Z}$ mit $a \cdot d - b \cdot c \neq 0$ im „Normalfall“ nicht in $\mathbb{Z}^2$ liegt, auch wenn für $s = \mathrm{ggT}(a, c)$ und $t = \mathrm{ggT}(b, d)$ gilt $s|e$ und $t|f$. (Diese Bedingungen sind also notwendig aber nicht hinreichend.)
Benutze geometrische Interpretation. Konstruiere ein Beispiel mit $a, b, c, d, e, f \notin \{0, \pm 1\}$, das obige notwendige Bedingungen erfüllt (z.B. weil $\mathrm{ggT}(a, c) = 1 = \mathrm{ggT}(b, d)$).

2.1.2 Lineare Gleichungen mit drei Unbekannten

Wir betrachten zunächst *eine* lineare Gleichung mit Koeffizienten $a, b, c, d \in \mathbb{Z}$,

$$a \cdot x + b \cdot y + c \cdot z = d \ ,$$

mit Rang 1, also $(a, b, c) \neq (0, 0, 0)$. Falls es Lösungen $(x, y, z) \in \mathbb{Z}^3$ gibt, so ist jeder gemeinsame Teiler von a, b und c auch ein Teiler von d. Ist also $q = \mathrm{ggT}(a, b, c)$, so ist $q|d$ eine notwendige Bedingung für ganzzahlige Lösungen. Wie im vorhergehenden Unterabschnitt sehen wir, dass diese Bedingung auch hinreichend ist, da wir

$$q = \mathrm{ggT}(a, b, c) = \mathrm{ggT}(\mathrm{ggT}(a, b), c) = r \cdot a + s \cdot b + t \cdot c$$

mit geeigneten $r, s, t \in \mathbb{Z}$ schreiben[5] können. Ist nun $d = n \cdot q$, so ist $(x, y, z) = n \cdot (r, s, t)$ eine (partikuläre) Lösung, wie man durch Einsetzen sieht,

$$a \cdot x + b \cdot y + c \cdot z = a \cdot n \cdot r + b \cdot n \cdot s + c \cdot n \cdot t = n \cdot (a \cdot r + b \cdot s + c \cdot t) = n \cdot q = d \ .$$

[5] Siehe Übung 3, Aufgabe 7.

Wiederum gilt für zwei verschiedene (ganzzahlige) Lösungen (x, y, z) und $(\tilde{x}, \tilde{y}, \tilde{z})$

$$a \cdot (x - \tilde{x}) + b \cdot (y - \tilde{y}) + c \cdot (z - \tilde{z}) = 0 \ .$$

Also ist $(x - \tilde{x}, y - \tilde{y}, z - \tilde{z})$ ein Vektor im Kern der 1×3–Matrix $A = (a, b, c)$ mit $\mathrm{rk}(A) = 1$. Aus

$$\mathrm{rk}(A) + \dim_{\mathbb{R}}(\ker(A)) = 1 + \dim_{\mathbb{R}}(\ker(A)) = 3$$

folgt, dass der Kern $\ker(A)$ von A ein 2–dimensionaler Unterraum von $\mathbb{R}^3$ ist und wir wollen eine vorwärts abgestufte ganzzahlige Basis dieses Kerns bestimmen, um damit alle (ganzzahligen) Lösungen zu beschreiben. Sei also für $(b, c) \neq (0, 0)$

$$a \cdot x + b \cdot y + c \cdot z = 0 \ .$$

Dann ist $a \cdot x = v = -b \cdot y - c \cdot z$ ein gemeinsames Vielfaches von a und $u = \mathrm{ggT}(b, c)$. Das kleinste gemeinsame Vielfache $\mathrm{kgV}(a, u)$ von a und u ist $|a| \cdot u/q$ mit

$$q = \mathrm{ggT}(a, u) = \mathrm{ggT}(a, \mathrm{ggT}(b, c)) = \mathrm{ggT}(a, b, c)$$

(vgl. mit Aufgabe 7b) von Übung 3). Somit ist also x ein Vielfaches von $u/q \in \mathbb{Z}$ und wenn wir $x = u/q$ setzen, so ist nach dem vorhergehenden Unterabschnitt

$$a \cdot x + b \cdot y + c \cdot z = (a/q) \cdot u + b \cdot y + c \cdot z$$

lösbar mit $(\tilde{y}, \tilde{z}) \in \mathbb{Z}^2$, da $(a/q) \cdot u$ von $u = \mathrm{ggT}(b, c)$ geteilt wird, da $a/q \in \mathbb{Z}$, da $q = \mathrm{ggT}(a, b, c)$. Falls also $(b, c) \neq (0, 0)$, wählen wir

$$\underline{\mathbf{k}}_1 = (u/q, \tilde{y}, \tilde{z})$$

als ersten ganzzahligen Basisvektor im Kern der Matrix (a, b, c) und für jeden ganzzahligen Vektor $\underline{\mathbf{k}} = (x, y, z)$ im Kern ist x ein Vielfaches von u/q, also $x = n \cdot (u/q)$ und daher $\underline{\mathbf{k}} - n \cdot \underline{\mathbf{k}}_1 = (0, \hat{y}, \hat{z}) \in \ker(A)$. Nach dem vorangehenden Unterabschnitt ist dann jeder ganzzahlige Vektor im Kern der Matrix (a, b, c) von der Form

$$\underline{\mathbf{k}} = n \cdot \underline{\mathbf{k}}_1 + m \cdot \underline{\mathbf{k}}_2$$

mit vorwärts abgestufter ganzzahliger Basis $\underline{\mathbf{k}}_1$, $\underline{\mathbf{k}}_2$ des Kerns, mit

$$\underline{\mathbf{k}}_2 = (0, c/u, -b/u) \ .$$

[Im Spezialfall $(b, c) = (0, 0)$ sei $\underline{\mathbf{k}}_1 = (0, 1, 0)$ und $\underline{\mathbf{k}}_2 = (0, 0, 1)$.] □
Dies beweist den

Satz *über ganzzahlige Lösungen einer linearen Gleichung in drei Variabeln*
Die ganzzahligen Lösungen der linearen Gleichung

$$a \cdot x + b \cdot y + c \cdot z = d$$

mit $a, b, c, d \in \mathbb{Z}$ *und* $(a, b, c) \neq (0, 0, 0)$ *sind*

$$\mathbb{L} = \{\underline{\mathbf{x}} + n \cdot \underline{\mathbf{k}}_1 + m \cdot \underline{\mathbf{k}}_2 \,|\, m, n \in \mathbb{Z}\} \ ,$$

falls $q|d$ *mit* $q = ggT(a, b, c)$ *und* $\mathbb{L} = \{\}$ *sonst. Die ganzzahlige partikuläre Lösung* $\underline{\mathbf{x}}$ *und die vorwärts abgestufte ganzzahlige Basis* $\underline{\mathbf{k}}_1$, $\underline{\mathbf{k}}_2$ *des Kernes von* (a, b, c) *können wie oben bestimmt werden.*

Bemerkung

Etwas einfacher findet man eine (vorwärts abgestufte) ganzahlige Basis des Kerns von

Gleichung vereinfachen

$$a \cdot x + b \cdot y + c \cdot z \ ,$$

wenn man diese Gleichung durch $q = \mathrm{ggT}(a, b, c)$ teilt, sobald man q bestimmt hat.

Aufgabe

a) Bestimme alle $(x, y, z) \in \mathbb{Z}^3$ mit $2 \cdot x + 3 \cdot y = 0$.

b) Bestimme alle $(x, y, z) \in \mathbb{Z}^3$ mit $2 \cdot x - 5 \cdot y + 4 \cdot z = 2$.

c) Zeige, dass die Lösungsmengen von a) und b) einen leeren Durchschnitt haben.

Die vorhergehende Aufgabe zeigt, dass ein Gleichungssystem aus *zwei* linearen Gleichungen mit *drei* Unbekannten,

$$\begin{aligned} a \cdot x + b \cdot y + c \cdot z &= d \ , \\ e \cdot x + f \cdot y + g \cdot z &= h \ , \end{aligned}$$

vom Rang 2 keine ganzzahligen Lösungen haben muss, auch wenn $a \cdot x + b \cdot y + c \cdot z = d$ (unendlich viele) ganzzahlige Lösungen hat und $e \cdot x + f \cdot y + g \cdot z = h$ ebenso. Gibt es jedoch ganzzahlige Lösungen des Systems, so gibt es unendlich viele, wie wir jetzt noch sehen wollen. Den Fall Rang $\neq 2$ betrachten wir nicht. Aus

$$\mathrm{rk}(A) + \dim_{\mathbb{R}}(\ker(A)) = 2 + \dim_{\mathbb{R}}(\ker(A)) = 3$$

folgt, dass der Kern $\ker(A)$ von A ein 1–dimensionaler Unterraum von $\mathbb{R}^3$ ist, wobei

$$A = \begin{pmatrix} a & b & c \\ e & f & g \end{pmatrix} \ .$$

In der Tat gilt für zwei Lösungen (x, y, z) und $(\tilde{x}, \tilde{y}, \tilde{z})$ obigen Gleichungssystems

$$\begin{aligned} a \cdot (x - \tilde{x}) + b \cdot (y - \tilde{y}) + c \cdot (z - \tilde{z}) &= 0 \ , \\ e \cdot (x - \tilde{x}) + f \cdot (y - \tilde{y}) + g \cdot (z - \tilde{z}) &= 0 \ . \end{aligned}$$

Der Vektor $(x - \tilde{x}, y - \tilde{y}, z - \tilde{z})$ steht also auf (a, b, c) wie auch auf (e, f, g) senkrecht und ist deshalb parallel zum Vektorprodukt

$$\begin{pmatrix} a \\ b \\ c \end{pmatrix} \times \begin{pmatrix} e \\ f \\ g \end{pmatrix} = \begin{pmatrix} b \cdot g - c \cdot f \\ c \cdot e - a \cdot g \\ a \cdot f - b \cdot e \end{pmatrix} = \lambda \cdot \underline{\mathbf{k}} \in \ker(A) \ .$$

Eine partikuläre (ganzzahlige) Lösung (wenn eine existiert) finden wir, indem wir z.B. das e–fache der ersten Gleichung vom a–fachen der zweiten Gleichung subtrahieren (falls $a \neq 0$), die erhaltene Gleichung

$$(a \cdot f - b \cdot e) \cdot y + (a \cdot g - c \cdot e) \cdot z = a \cdot h - d \cdot e$$

in den zwei Variabeln y und z wie im vorangehenden Unterabschnitt (ganzzahlig) lösen, diese Lösungen (mit Parameter $m \in \mathbb{Z}$, wie auf S.35 beschrieben) in die erste Gleichung einsetzen und diese nach (ganzzahligen) (x, m) lösen. Falls $a = 0$ und $e \neq 0$ vertauschen wir die Rollen der ersten und zweiten Gleichung. Falls $(a, e) = (0, 0)$ haben wir zwei Gleichungen für zwei Unbekannten y und z. Diese lösen wir, wie auf S.36 oben. $x \in \mathbb{Z}$ ist dann frei wählbar. □
Dies beweist den

Satz *über ganzzahlige Lösungen eines linearen Gleichungssystems in drei Variablen*
Die ganzzahligen Lösungen des linearen Gleichungssystems

$$\begin{aligned} a \cdot x + b \cdot y + c \cdot z &= d \ , \\ e \cdot x + f \cdot y + g \cdot z &= h \ , \end{aligned}$$

vom Rang 2 mit $a, b, c, d, e, f, g, h \in \mathbb{Z}$ *sind*

$$\mathbb{L} = \{\underline{\mathbf{x}} + n \cdot \underline{\mathbf{k}} \,|\, n \in \mathbb{Z}\} \ ,$$

falls eine (ganzzahlige) partikuläre Lösung $\underline{\mathbf{x}}$ *wie oben bestimmt werden kann und* $\mathbb{L} = \{\}$ *sonst. Dabei ist* $\underline{\mathbf{k}}$ *proportional zum Vektorprodukt* $\lambda \cdot \underline{\mathbf{k}}$ *von* (a, b, c) *und* (e, f, g) *mit*

$$\lambda = ggT(b \cdot g - c \cdot f, c \cdot e - a \cdot g, a \cdot f - b \cdot e) \ .$$

Ferner ist $ggT(a, b, c) | d \ \wedge \ ggT(e, f, g) | h$ *eine notwendige aber nicht hinreichende Bedingung für* $\mathbb{L} \neq \{\}$.

Bemerkung
Die Bedingung besagt, dass die Ebenen $a \cdot x + b \cdot y + c \cdot z = d$ und $e \cdot x + f \cdot y + g \cdot z = h$ beide (unendlich viele) Punkte mit ganzzahligen Koordinaten haben. Daraus folgt noch nicht, dass auch ihre Schnittgerade Punkte mit ganzzahligen Koordinaten hat. Falls sie aber einen solchen Punkt hat, so hat sie unendlich viele.
Der Vollständigkeit halber erwähnen wir noch, dass ein Gleichungssystem aus drei Gleichungen (mit ganzzahligen Koeffizienten) und drei Unbekannten vom Rang 3 natürlich eine eindeutige Lösung hat, von der wir ablesen können, ob sie ganzzahlig ist (z.B. wenn die Determinante der zugehörigen 3×3–Matrix eine Einheit ist).

2.2 Pythagoras

2.2.1 Eine vollständige Liste ganzzahliger Lösungen

Wir wollen *alle* ganzzahligen $(a, b, c) \in \mathbb{Z}^3$ mit

$$a^2 + b^2 = c^2 \ .$$

Gilt dies für (a, b, c), so auch für $(a \cdot d, b \cdot d, c \cdot d)$. Wir nehmen also an, $a, b, c \in \mathbb{N}$ seien teilerfremd. Dann können a und b nicht beide gerade sein. Wären a und b beide ungerade, so folgte

$$a^2 \equiv 1 \equiv b^2 \mod 4 \Rightarrow a^2 + b^2 \equiv 2 \mod 4 \Rightarrow a^2 + b^2 \not\equiv c^2 \mod 4 ,$$

da $c^2 \equiv 0 \mod 4$ für alle geraden c. Sei also a gerade, b und deshalb auch c ungerade.

Pythag. Tripel

Satz *über Pythagoräische Zahltripel*
Seien $a, b, c \in \mathbb{N}$ teilerfremd mit

$$a^2 + b^2 = c^2$$

und $2|a$. Dann gibt es eindeutig bestimmte teilerfremde $0 < u < v \in \mathbb{N}$ mit

$$a = 2 \cdot u \cdot v \ , \ b = v^2 - u^2 \ \text{ und } c = v^2 + u^2 \ .$$

Umgekehrt gibt jedes teilerfremde Zahlenpaar $u < v \in \mathbb{N}$ mittels dieser Gleichungen ein solches Tripel (a, b, c), wenn entweder nur u oder nur v gerade ist.

Liste aller Lösungen

Folgerung
Die folgende unendliche, nach der Summe $w = u + v$ geordnete Liste enthält *jedes* teilerfremde Zahlentripel $(a, b, c) \in \mathbb{N}^3$ mit $a^2 + b^2 = c^2$ und $2|a$ genau einmal:

w	3	5	5	7	7	7	9	9	9	11	11	11	11	11	13	13	...
u	1	1	2	1	2	3	1	2	4	1	2	3	4	5	1	2	...
v	2	4	3	6	5	4	8	7	5	10	9	8	7	6	12	11	...
a	4	8	12	12	20	24	16	28	40	20	36	48	56	60	24	44	...
b	3	15	5	35	21	7	63	45	9	99	77	55	33	11	143	117	...
c	5	17	13	37	29	25	65	53	41	101	85	73	65	61	145	125	...

Beweis des Satzes
Da a gerade ist und $a^2 = c^2 - b^2 = (c - b) \cdot (c + b)$ mit $2|(c - b)$ und $2|(c + b)$ gilt, haben wir

$$\left(\frac{a}{2}\right)^2 = \left(\frac{c-b}{2}\right)\left(\frac{c+b}{2}\right) \ ,$$

wo alle Klammern ganze Zahlen sind. Die zwei Klammern rechts sind teilerfremd, denn ein gemeinsamer Teiler würde die Summe c wie auch die Differenz $(-)b$ teilen. Das Produkt der beiden Klammern ist also ein Quadrat und die beiden Klammern haben keine gemeinsament Teiler. Deshalb muss jede der beiden Klammern für sich ein Quadrat sein,

$$0 < \left(\frac{c-b}{2}\right) = u^2 < v^2 = \left(\frac{c+b}{2}\right) \ ,$$

also $a = 2 \cdot u \cdot v$, $b = v^2 - u^2$ und $c = v^2 + u^2$. Die Umkehrung ist klar (Rechnung).□

Bemerkung
Für quadratische Gleichungen in mehreren Variabeln ist es gelegentlich noch möglich, sich eine vollständige Übersicht über alle ganzzahligen Lösungen zu verschaffen, wie etwa obiges Beispiel Pythagoräischer Zahltripel

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

zeigt. Polynomiale Gleichungen in zwei Variabeln x und y bei denen höchstens dritte Potenzen vorkommen bilden ein eigenes Teilgebiet der Mathematik (*elliptische Kurven* — damit sind *nicht* Ellipsen in der xy–Ebene gemeint, die durch eine *quadratische* Gleichung, z.B. $b^2 \cdot x^2 + a^2 \cdot y^2 = a^2 \cdot b^2$ beschrieben werden können.) Diesen kommt eine besondere Bedeutung zu, da ihre Punkte eine kommutative Gruppe bilden, ähnlich wie die Punkte eines Kreises die kommutative Gruppe der Drehungen in der Ebene beschreiben. Das wird etwa in der Kryptographie ausgenutzt, war aber auch zentral im Beweis (1994) des letzten Satzes von Fermat. Umso höhere Potenzen auftreten, desto nebulöser wird die Frage nach ganzzahligen Lösungen. Euler z.B. war der Meinung

$$x^4 + y^4 + z^4 = w^4$$

habe keine Lösung $(x, y, z, w) \in \mathbb{N}^4$. Jedoch 1988 fand Elkies

$$2682440^4 + 15365639^4 + 18796760^4 = 20615673^4 \ !$$

Die kleinste Lösung ist offenbar

$$95800^4 + 217519^4 + 414560^4 = 422481^4 \ .$$

Das in der Einleitung zu diesem Kapitel erwähnte sog. *10. Hilbertsche Problem*, ob es *prinzipiell* möglich sei, durch einen Algorithmus, sprich durch ein Computerprogramm entscheiden zu lassen, ob eine polynomiale Gleichung (mit ganzzahligen Koeffizienten) ganzzahlige Lösungen habe, wird durch den Satz von Matiyasevich (1970) negativ beantwortet. Das schliesst jedoch nicht aus, dass es für bestimmte Unterklassen von Gleichungen eine auf das spezifische Problem zugeschnittene Methode geben kann. Für die Klasse der Gleichungen

$$x^n + y^n = z^n \quad \text{mit } n \in \mathbb{N}$$

wurde man z.B. nach 350 Jahren intensiver Suche fündig!

2.2.2 Näherungslösungen

Es gibt kein rechtwinklig *gleichschenkliges* Dreieck mit ganzzahligen Seitenlängen, da

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

keine ganzzahligen Lösungen $(x, z) \in \mathbb{N}^2$ hat, da sonst $z^2/x^2 = 2$ mit $z/x \in \mathbb{Q}$ wäre. Man kann dann versuchen, diese Gleichung „so gut wie möglich“ mit ganzen Zahlen

$(x, z) \in \mathbb{N}^2$ zu erfüllen, wobei „so gut wie möglich“ natürlich Verschiedenes bedeuten kann. Eine erste Interpretation wäre, ganzzahlige Lösungen von

$$z^2 - 2 \cdot x^2 = \pm 1 \quad \text{statt} \quad z^2 - 2 \cdot x^2 = 0$$

zu suchen. Eine zweite Interpretation wäre, ein rechtwinkliges Dreieck mit ganzzahligen Seitenlängen und Katheten x und $y = x + 1$ zu suchen. Daraus ergäbe sich die Forderung

$$z^2 = x^2 + y^2 = x^2 + (x+1)^2 = 2 \cdot x^2 + 2 \cdot x + 1 \ ,$$

also

$$2 \cdot z^2 = 4 \cdot x^2 + 4 \cdot x + 1 + 1 = (2 \cdot x + 1)^2 + 1$$

also

$$(2 \cdot x + 1)^2 - 2 \cdot z^2 = -1 \ .$$

Aus dem nächsten Abschnitt 2.3 ergibt sich folgende vollständige Liste der Lösungen $(x, z) \in \mathbb{N}^2$ von $z^2 - 2 \cdot x^2 = \pm 1$:

Liste aller Lösungen

$$\begin{aligned} x_0 = 1 \quad &, \quad z_0 = 1 \ , \\ x_1 = 2 \quad &, \quad z_1 = 3 \ , \\ x_2 = 5 \quad &, \quad z_2 = 7 \ , \\ x_3 = 12 \quad &, \quad z_3 = 17 \ , \\ &\vdots \\ x_{n+1} = x_n + z_n \quad &, \quad z_{n+1} = 2 \cdot x_n + z_n \ . \end{aligned}$$

Wie man leicht sieht, kann man jede zweite dieser Lösungen verwenden um eine Lösung nach der zweiten Interpretation zu gewinnen, z.B. $7^2 - 2 \cdot 5^2 = -1$.
Möchte man ein *halbes gleichseitiges* Dreieck mit ganzzahligen Seiten x, y, $z = 2 \cdot x$, so wäre

$$x^2 + y^2 = z^2 = (2 \cdot x)^2 = 4 \cdot x^2 \quad \text{also} \quad y^2 - 3 \cdot x^2 = 0$$

zu erfüllen, was mit $(x, y) \in \mathbb{N}^2$ natürlich auch unmöglich ist. Fordert man stattdessen

$$y^2 - 3 \cdot x^2 = 1 \quad \text{oder} \quad y^2 - 3 \cdot x^2 = -1$$

so ist Letzteres wiederum mit $(x, y) \in \mathbb{N}^2$ unmöglich (warum?). Jedoch gilt der

Satz

Ist $N \in \mathbb{N}$ keine Quadratzahl, so kann die vollständige Liste der unendlich vielen ganzzahligen Lösungen $(x, y) \in \mathbb{N}^2$ der sog. Pell'schen Gleichung

$$y^2 - N \cdot x^2 = 1$$

angegeben werden.

Die Tatsache, dass diese Gleichung überhaupt Lösungen $(x, y) \in \mathbb{N}^2$ hat (falls $N \in \mathbb{N}$ keine Quadratzahl ist) wollen wir ohne Beweis akzeptieren. Jedoch wollen wir mittels Kriterium von Legendre plausibel machen, weshalb wir alle diese Lösungen mit einer Kettenbruchentwicklung von $\sqrt{N}$ finden können, vgl. S27. Mehr dazu im Abschnitt 2.3

2.2.3 Stereographische Projektion

Wir haben gesehen, dass die Wahl von teilerfremden $u, v \in \mathbb{N}$ verschiedener Parität (entweder u oder v gerade, nicht aber beide) zu einer teilerfremden Lösung $(x, y, z) \in \mathbb{N}^3$ führt von

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

Wenn wir diese Gleichung durch z^2 teilen, so erhalten wir gekürzte positive Brüche x/z und y/z mit

$$\left(\frac{x}{z}\right)^2 + \left(\frac{y}{z}\right)^2 = 1 \ .$$

Geometrisch kann man also sagen, der Punkt $(X|Y) = (x/z|y/z)$ liege auf dem Einheitskreis

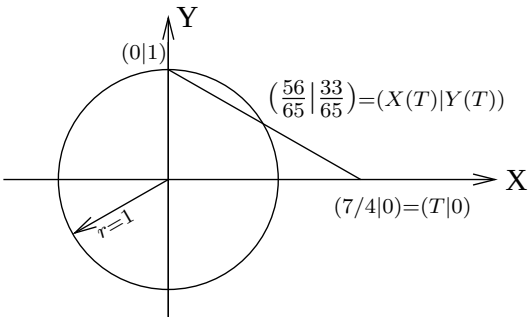
Einheitskreis

$$X^2 + Y^2 = 1$$

in der XY–Ebene und zwar auf dem Viertelkreisbogen im 1.Quadranten.
Betrachtet man nun diesen Einheitskreis zusammen mit der Geraden durch $(0|1)$ und $(T|0)$ mit $T > 1$, so schneidet diese einen weiteren Punkt

$$(X(T)|Y(T)) = \left(\frac{2 \cdot T}{T^2+1} \,\middle|\, \frac{T^2-1}{T^2+1}\right)$$

aus dem Einheitskreis heraus.



Beweise dies (z.B. mit ähnlichen Dreiecken). Man nennt $(T|0)$ die *stereographische Projektion* des Puntkes $(X(T)|Y(T))$. Setzt man nun $T = v/u \in \mathbb{Q}$ (gekürzt), so erhält man eine geometrische Interpretation der Formeln, die zur Tabelle auf S.40 führen. Beachte jedoch die folgende Aufgabe.

stereogr. Projektion

Aufgabe
Zeige, dass der gekürzte Bruch $v/u = T > 1$ das „gleiche“ Lösungstripel liefert, wie der gekürzte Bruch $\overline{v}/\overline{u} = (T+1)/(T-1) > 1$. Welcher der Parameter, (u, v) oder $(\overline{u}, \overline{v})$ kommt in der Tabelle auf S.40 *nicht* vor (in Abhängigkeit von $T \in \mathbb{Q}$)?
(Vgl. dazu auch Aufgabe 3c) von Übung 4.)

2.3 Pell

2.3.1 Eine vollständige Liste ganzzahliger Lösungen

Satz
Ist $N \in \mathbb{N}$ keine Quadratzahl, so hat die sog. *Pell'sche Gleichung*

$$x^2 - N \cdot y^2 = 1$$

unendlich viele Lösungen $(x, y) \in \mathbb{N}^2$. Ist (x_1, y_1) die kleinste Lösung, so ist die nach der Grösse n–te Lösung (x_n, y_n) gegeben durch

$$x_n + \sqrt{N} \cdot y_n = (x_1 + \sqrt{N} \cdot y_1)^n \ .$$

Bemerkung
Wir wollen diesen Satz nicht vollständig beweisen, aber plausibel machen, weshalb wir mit der Kettenbruchentwicklung von $\sqrt{N}$ alle Lösungen finden (unter der Annahme, dass es Lösungen gibt). Sei nämlich $(x, y) \in \mathbb{N}^2$ eine Lösung (zu gegebenem $N \in \mathbb{N}$, das keine Quadratzahl ist). Dann gilt

$$\frac{x^2}{y^2} = N + \frac{1}{y^2} \ , \ \text{also} \ \frac{x}{y} = \sqrt{N + \frac{1}{y^2}} \ , \ \text{also} \ \frac{x}{y} - \sqrt{N} = \sqrt{N + \frac{1}{y^2}} - \sqrt{N} \ .$$

Erweitern der rechten Seite mit $\sqrt{N + 1/y^2} + \sqrt{N}$ ergibt mit $(a-b)(a+b) = a^2 - b^2$

$$0 < \frac{x}{y} - \sqrt{N} = \frac{1}{y^2 \cdot \left(\sqrt{N + \frac{1}{y^2}} + \sqrt{N}\right)} < \frac{1}{2 \cdot y^2} \ .$$

Auf Grund des Kriteriums von Legendre auf S.27 folgt nun, dass der Näherungsbruch x/y für $\sqrt{N}$, der aus der Lösung der Pell'schen Gleichung hervorgeht, in der Kettenbruchentwicklung von $\sqrt{N}$ auftauchen muss.
Ferner wollen wir nachweisen, dass mit

$$x_1^2 - N \cdot y_1^2 = 1 \ \text{ und } \ x_n^2 - N \cdot y_n^2 = 1 \ ,$$

auch

$$x_{n+1}^2 - N \cdot y_{n+1}^2 = 1$$

gilt, wobei x_{n+1} und y_{n+1} festgelegt sind durch

$$x_{n+1} + \sqrt{N} \cdot y_{n+1} = (x_1 + \sqrt{N} \cdot y_1)^{n+1} = (x_1 + \sqrt{N} \cdot y_1)(x_n + \sqrt{N} \cdot y_n).$$

Aus der letzten Gleichung folgt rekursiv für (x_n, y_n),

$$\begin{aligned} x_{n+1} &= x_1 \cdot x_n + N \cdot y_1 \cdot y_n \ \text{und} \\ y_{n+1} &= x_1 \cdot y_n + y_1 \cdot x_n \ . \end{aligned}$$

Es ist also unter obigen Voraussetzungen an (x_1, y_1) und (x_n, y_n) nachzuweisen, dass

$$x_{n+1}^2 - N \cdot y_{n+1}^2 = (x_1 \cdot x_n + N \cdot y_1 \cdot y_n)^2 - N \cdot (x_1 \cdot y_n + y_1 \cdot x_n)^2 = 1 \ .$$

Durch Ausmultiplizieren aller Klammer sieht man aber, dass dies das Gleiche ist, wie

$$(x_1^2 - N \cdot y_1^2) \cdot (x_n^2 - N \cdot y_n^2) = 1 \cdot 1 = 1 \ .$$

Somit ist klar, dass wir mit einer Lösung automatisch unendlich viele Lösungen haben und dass diese alle in der Form x/y als Näherungsbrüche in der Kettenbruchentwicklung von $\sqrt{N}$ auftreten müssen. Wir haben aber *nicht* bewiesen, dass es *überhaupt* Lösungen gibt, und dass sie dann wie oben beschrieben *alle* aus der kleinsten Lösung konstruiert werden können, dass es also nicht noch andere geben kann.

2.3.2 Lösungen aus der Kettenbruchentwicklung

Wir erklären nun, wie man aus der Kettenbruchentwicklung von $\sqrt{N}$ (für $N \in \mathbb{N}$ keine Quadratzahl) die kleinste und damit alle Lösungen $(x_n, y_n) \in \mathbb{N}^2$ von

$$x^2 - N \cdot y^2 = 1$$

erhält. Wir benutzen dazu die Kettenbruchentwicklung reeller Zahlen wie im Unterabschnitt 1.3.4 auf S.26 beschrieben. Ebenso benutzen wir das Tabellenrechnen von S.27, wobei wir die entsprechende Tabelle noch um zwei Zeilen (a_n und c_n) erweitern. Um die Sache gerade etwas konkret zu machen, wollen wir $N = \sqrt{19}$ entwickeln. Ohne Tabelle würden wir wie folgt beginnen

$$\begin{aligned}
r_1 = x_0 - \lfloor x_0 \rfloor = \sqrt{19} - \underline{4} \quad &\Rightarrow \quad x_1 = \frac{1}{r_1} = \frac{1}{\sqrt{19} - 4} = \frac{\sqrt{19} + \underline{4}}{\underline{3}} \ , \\
r_2 = x_1 - \lfloor x_1 \rfloor = \frac{\sqrt{19} + 4}{3} - \underline{2} \quad &\Rightarrow \quad x_2 = \frac{1}{r_2} = \frac{3}{\sqrt{19} - 2} = \frac{\sqrt{19} + \underline{2}}{\underline{5}} \ , \\
r_3 = x_2 - \lfloor x_2 \rfloor = \frac{\sqrt{19} + 2}{5} - \underline{1} \quad &\Rightarrow \quad x_3 = \frac{1}{r_3} = \frac{5}{\sqrt{19} - 3} = \frac{\sqrt{19} + \underline{3}}{\underline{2}} \ , \\
&\vdots
\end{aligned}$$

Die Kettenbruchentwicklung $\sqrt{19} = [4, 2, 1, \dots] = [b_0, b_1, b_2, \dots]$ ergibt sich aus den unterstrichenen Werten links. Um die Rechnung vollständig zu formalisieren, definieren wir neben

$$b_{n+1} = \lfloor x_{n+1} \rfloor = \lfloor \frac{\sqrt{N} + a_n}{c_n} \rfloor$$

noch $(a_0, c_0) = (4, 3)$, $(a_1, c_1) = (2, 5)$, $(a_2, c_2) = (3, 2)$, ... durch die unterstrichenen Werte rechts. Neben der Rekursion für b_{n+1} und den bereits auf S.23 gegebenen

$$p_{n+1} = b_{n+1} \cdot p_n + p_{n-1} \ \text{ und } \ q_{n+1} = b_{n+1} \cdot q_n + p_{q-1}$$

ergibt sich ferner

$$\begin{aligned} a_{n+1} &= b_{n+1} \cdot c_n - a_n \quad \text{und} \\ c_{n+1} &= b_{n+1} \cdot (a_n - a_{n+1}) + c_{n-1} \ . \end{aligned}$$

Um die Rekursion zu initiieren, brauchen wir jetzt neben $p_{-2} = 0 = q_{-1}$ und $p_{-1} = 1 = q_{-2}$ noch

$$a_{-1} = 0 \ , \ c_{-1} = 1 \ \text{ und } \ c_{-2} = N \ .$$

Für $N = 19$ ergibt sich somit folgende erweiterte Tabelle für die Kettenbruchentwicklung von $\sqrt{N}$

n	-2	-1	0	1	2	3	4	5	6	7	$\dots$
b_n			4	2	1	3	1	2	8	2	$\dots$
a_n		0	4	2	3	3	2	4	4	2	$\dots$
c_n	19	1	3	5	2	5	3	1	3	5	$\dots$
p_n	0	1	4	9	13	48	61	170	1421	3012	$\dots$
q_n	1	0	1	2	3	11	14	39	326	691	$\dots$

.

Gemäss Bemerkung 5 auf S.25 wird die Kettenbruchentwicklung von $x = \sqrt{19}$ periodisch, da x eine irrationale Lösung der quadratischen Gleichung

$$x^2 - 19 = 0$$

mit ganzzahligen Koefizienten ist. In der Tat sehen wir aus der Tabelle, dass

$$(a_0, c_0) = (a_6, c_6) = \cdots = (4, 3) \ , \ (a_1, c_1) = (a_7, c_7) = \cdots = (2, 5) \ , \ \dots$$

und da mit obigen Rekursionen b_{n+1}, a_{n+1} und c_{n+1} aus a_n, b_n, c_n und c_{n-1} berechnet werden, so werden die Einträge in diesen Zeilen sich wiederholen mit Periode 6. Insbesondere haben wir

$$\sqrt{19} = [4, 2, 1, 3, 1, 2, 8, 2, \dots] = [4, \overline{2, 1, 3, 1, 2, 8}] \ .$$

Unser Augenmerk im Zusammenhang mit Lösungen der Gleichung

$$x^2 - 19 \cdot y^2 = 1$$

gilt jedoch der Tatsache

$$p_n^2 - 19 \cdot q_n^2 = (-1)^{n+1} \cdot c_n \ ,$$

die in obiger Tabelle für alle $n = -2, -1, 0, 1, 2, 3, \dots$ nachgerechnet werden kann (und die man mit vollständiger Induktion bweist, ähnlich wie z.B. die Behauptung auf S.23). Insbesondere ergibt sich mit $n = 5$ die kleinste Lösung der Pell'schen Gleichung für $N = 19$,

$$170^2 - 19 \cdot 39^2 = (-1)^{5+1} \cdot c_5 = 1 \ .$$

Aufgabe
Bestimme die zweitkleinste Lösung $(x_2, y_2) \in \mathbb{N}^2$ der Gleichung $x^2 - 19 \cdot y^2 = 1$.

Kapitel 3

Verschlüsselung

Im Zeitalter des sich gegenseitig Ausspionierens hat natürlich derjenige die Macht, der die (z.B. Fertigungs–, Industrie– oder Bank–)Geheimnisse anderer harausfinden kann, ohne seine eigenen preiszugeben. Solche werden deshalb oft in verschlüsselter Form hinterlegt und/oder übermittelt. Das Bild ist entlehnt der alltäglichen Situation, dass man etwas von Wert an einem sicheren Ort mit einem Schlüssel einschliesst und sich mit diesem Schlüssel bei Bedarf auch wieder Zugang verschafft. Dieses Bild ist für heutige Verschlüsselungsverfahren von Information aber nicht mehr ganz zutreffend, da man typischerweise Schlösser benutzt, die sozusagen alle ver– aber nur Ausgewählte entschlüsseln können. Man benutzt also sog. *asymmetrische Verschlüsselungsverfahren*, bei denen die *Ent*schlüsselung im Gegensatz zur *Ver*schlüsselung nicht ohne Zusatzinformation (in überschaubarer Zeit) möglich ist. Mathematisch gesprochen benutzt man Funktionen, deren Umkehrfunktion ungeheuer viel aufwendiger zu berechnen sind als die Funktion selber. Unser zentrales Beispiel ist

3.1 Die diskrete Exponentialfunktion

mit dem nur mit grossem Aufwand zu berechnenden *diskreten Logarithmus*[1] als Umkehrfunktion. Wir wollen z.B. 10^{131} mod 263 berechnen. Am besten entwickelt man den Exponenten zunächst im Binärsystem,

$$131 = 1 \cdot 2^7 + 0 \cdot 2^6 + 0 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^1 + 1 \cdot 2^0 \ ,$$

[1] Etwas inkonsequent spricht man meist von *modularer Exponentialfunktion* abgeleitet vom *modularen* oder *modulo*–Rechnen, wogegen die Umkehrfunktion meist als *diskreter Logarithmus* bezeichnet wird.

berechnet dann 10^e für $e = 1, 2, 4, 8, \ldots, 128$ durch *forlaufendes Quadrieren* mod 263,

$$\begin{aligned}
10^1 &= 10 \mod 263,\\
10^2 &= 100 \mod 263,\\
10^4 = (10^2)^2 = 10000 &\equiv 6 \mod 263,\\
10^8 = (10^4)^2 \equiv 6^2 &= 36 \mod 263,\\
10^{16} = (10^8)^2 \equiv 36^2 &\equiv 244 \ldots,\\
10^{32} = (10^{16})^2 \equiv 244^2 &\equiv 98 \ldots,\\
10^{64} = (10^{32})^2 \equiv 98^2 &\equiv 136 \ldots,\\
10^{128} = (10^{64})^2 \equiv 136^2 &\equiv 86 \mod 263,
\end{aligned}$$

und setzt schliesslich die gewünschte Potenz aus den berechneten Potenzen zusammen,

$$10^{131} = 10^{128} \cdot 10^2 \cdot 10^1 \equiv 86 \cdot 100 \cdot 10 \equiv 262 \equiv -1 \mod 263\ .$$

Der Rechenaufwand hier bemisst sich nach der Länge der Binärenwicklung des Exponenten e, also nach dem 2er–Logarithmus von e, der in unserem Beispiel etwas grösser als 7 ist, $\log_2(131) \approx 7.03$. Wir mussten also oben siebenmal Quadrieren, jeweils modulo 263 rechnen und am Schluss noch die entsprechenden Potenzen miteinander multiplizieren (und wieder modulo 263 rechnen).
(Nebenbei: Da die Ordnung von 10 in $\mathbb{Z}_p^\times = \mathbb{Z}_{263}^\times$ weder 1 noch 2 noch 131 ist, aber ein Teiler von $|\mathbb{Z}_{263}^\times| = \varphi(263) = 262 = 2 \cdot 131$ sein muss, mit $p = 263$ und $p' = 131$ prim, ist $\mathrm{ord}(10) = 262$. Mit anderen Worten $b = 10$ ist eine *Primitivwurzel* in $\mathbb{Z}_{263}^\times$.)
Weit schwieriger ist es, zu einer gegebenen Primitivwurzel b in $\mathbb{Z}_n^\times$ einen Exponenten e zu finden mit

$$b^e \equiv m \mod n \text{ für } m \in \mathbb{Z}_n^\times\ ,$$

mit anderen Worten, den diskreten Logarithmus $\log_b m$ von $m \in \mathbb{Z}_n^\times$ zur Basis b zu bestimmen. (In Unterabschnitt 1.2.8 haben wir $n = p$ prim angenommen, wo wir sicher sind, dass es Primitivwurzeln gibt. Wir werden in 3.4 sehen, wie sich das Problem verallgemeinert.) Man versuche etwa, $e = \log_{10}(2)$ in $\mathbb{Z}_{263}^\times$ zu finden, also e so zu bestimmen, dass gilt[2]

$$10^e \equiv 2 \mod 263\ .$$

Sehr vereinfacht gesagt, bleibt einem (nach heutigem Kenntnisstand) nicht viel anderes übrig, als alle e nacheinander auszuprobieren. Im ungünstigsten Fall müssen wir also alle Exponenten bis $e = \varphi(n)$ durchgehen. Der Rechenaufwand ist also nicht von der Grössenordnung $\log_2(n)$ sondern von der Grössenordnung von n selbst. Man sagt, *Logarithmieren* sei „*exponentiell viel aufwendiger*“ als *Exponentiieren*.

[2] $e = 156$, was man umgekehrt aber sehr schnell nachprüfen kann, $10^{156} = 10^{128} \cdot 10^{16} \cdot 10^8 \cdot 10^4$

3.2 RSA (Rivest, Shamir, Adleman)

Ist $\mathrm{ggT}(m, N) = 1$, so gilt $m \in \mathbb{Z}_N^\times$ mit $|\mathbb{Z}_N^\times| = \varphi(N)$. Ist nun

$$e \cdot d \equiv 1 \mod \varphi(N),$$

so gilt (mit dem kleinen Satz von Fermat $m^{\varphi(N)} \equiv 1 \mod N$) mit $c = m^e$,

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

Rivest, Shamir und Adleman interpretieren[3] nun RSA

$m(essage)$	als	*Nachricht*,
$c(ode)$	als	*Chiffrat*,
$e(ncryption)$	als	*Verschlüssel* und
$d(ecryption)$	als	*Entschlüssel*.

Um das Ver– und Entschlüsseln gerade an einem praktischen Beispiel vorzuführen, übersetzen wir die Nachricht „HEY“ zuerst in eine Zahl m mit Hilfe des Binärsystems

Leerschlag	$\cong$	$[00000]_2$,
A	$\cong$	$[00001]_2$,
B	$\cong$	$[00010]_2$,
C	$\cong$	$[00011]_2$,
	$\cdots$	
Z	$\cong$	$[11010]_2$,
Ä	$\cong$	$[11011]_2$,
Ö	$\cong$	$[11100]_2$,
Ü	$\cong$	$[11101]_2$,
,	$\cong$	$[11110]_2$ und
.	$\cong$	$[11111]_2$,

wobei rechts die Zahlen von 0 bis 31 stehen, in Binärdarstellung. Unser m ist also

$$[\underbrace{01000}_{\mathrm{H}}\ \underbrace{00101}_{\mathrm{E}}\ \underbrace{11001}_{\mathrm{Y}}]_2 = 1\cdot 2^0 + 0\cdot 2^1 + 0\cdot 2^2 + 1\cdot 2^3 + \cdots + 1\cdot 2^{13} = 8377.$$

(Der Handlichkeit halber haben wir m zuletzt wieder im Dezimalsystem dargestellt.) Für ihre Verehrer stellt Bärbel das Produkt $N = p \cdot q$ zweier grosser Primzahlen (in der Praxis heute mehr als 200–stellig) sowie den Verschlüssel $e = 7$ ins Netz. Für unser Beispiel nehmen wir zwei nicht ganz so grosse Primzahlen

$$N = p \cdot q = 101 \cdot 103 = 10403\ .$$

[3] R. Rivest, A. Shamir und L. Adleman (1978) A method for obtaining digital signatures and public–key cryptosystems. *Comm. ACM 21, no. 2.*

Verehrer Anton schickt Bärbel nun die romantische Nachricht m verschlüsselt

$$\text{als } c \equiv m^e = (8377)^7 \equiv \underline{339} \mod 10403 \ .$$

Da niemand ausser Bärbel $\varphi(N) = \varphi(p \cdot q) = (p-1)(q-1)$ kennt[4], kann auch niemand innert nützlicher Frist d so bestimmen, dass gilt

$$d \cdot e \equiv 1 \mod \varphi(N).$$

Bärbel jedoch kennt $\varphi(N)$ und kann d aus e z.B. mit dem *Algorithmus von Euklid* ein für allemal als ihren geheimen Entschlüssel berechnen. In unserem Beispiel gilt $d = 8743$, da

$$d \cdot e = 8743 \cdot 7 = 1 + 6 \cdot 10200 \equiv 1 \mod \varphi(N) \ .$$

Bärbel entschlüsselt also

$$m = c^d = 339^{8743} \equiv 8377 \cong \text{„HEY“} \mod 10403 \ ,$$

wie im Abschnitt 3.1 angegeben mit hilfe der 2er–Potenzen 2, 2^2, 2^3, ... 2^{13} als Exponenten,

$$\begin{aligned} 339^2 &\equiv 488 \mod 10403, \\ 488^2 \equiv 339^{2^2} &\equiv 9278 \mod 10403, \\ 339^{2^3} &\equiv 6862 \ \ldots, \\ &\vdots \\ 339^{2^{13}} &\equiv 6447 \mod 10403 \ . \end{aligned}$$

und der Binärdarstellung

$$d = 8743 = 2^{13} + 2^9 + 2^5 + 2^2 + 2^1 + 2^0 = [10001000100111]_2 \ .$$

Also gilt

$$m \equiv 339^{2^{13}+2^9+2^5+2^2+2^1+2^0} \equiv 6447 \cdot \ldots \cdot 9278 \cdot 488 \cdot 339 \equiv \underline{8377} \mod 10403 \ .$$

Bemerkungen

1. Eine längere Nachricht M wir in einzelne Stücke m_k mit $m_k < N$ zerlegt.

2. Die Wahrscheinlichkeit, dass eine Nachricht $0 \leq m < N$ nicht $\text{ggT}(m, N) = 1$ erfüllt, dass also $m \notin \mathbb{Z}_N^\times$ gilt, ist für $N = p \cdot q$ mit sehr grossen p und q verschwindend klein. In unserem Beispiel mit $N = 101 \cdot 103$ gilt $\text{ggT}(m, N) \neq 1$ für $N - \varphi(N) = 10403 - 10200 = 203$ von 10403 vielen m's, also bereits für weniger als 2%.

[4]Die Sicherheit des Verfahrens beruht also auf der Tatsache, dass man das Produkt sehr grosser Primzahlen nicht innert nützlicher Frist in Faktoren zerlegen kann. Hat man die Faktoren $N = p \cdot q$, so hat man auch $\varphi(N) = (p-1)(q-1)$ (und umgekehrt wegen: $p + q = N - \varphi(N) + 1$ und $|p - q| = \sqrt{(p+q)^2 - 4N}$).

3. Damit der Verschlüssel e ein multiplikatives Inverses d mod $\varphi(N)$ hat, muss $\mathrm{ggT}(e, \varphi(N)) = 1$ erfüllt sein. In unserem Beispiel soll e also weder die Primfaktoren 2, 3, 5 noch 17 enthalten, da dies die Primfaktoren von $\varphi(10403) = \varphi(101) \cdot \varphi(103) = 100 \cdot 102 = 2^3 \cdot 3 \cdot 5^2 \cdot 17$ sind.

4. Bärbel kann auch den *Chinesischen Restsatz* verwenden, um $m \equiv c^d \bmod N$ zu entschlüsseln. In unserem Beispiel gilt

$$\begin{aligned} c = 339 &\equiv 36 \bmod p = 101 \text{ und} \\ c = 339 &\equiv 30 \bmod q = 103 \,. \end{aligned}$$

Ferner gilt

$$\begin{aligned} d = 8743 &\equiv 43 \bmod p - 1 = 100 \text{ und} \\ d = 8743 &\equiv 73 \bmod q - 1 = 102 \,. \end{aligned}$$

Modulo $p = 101$ gilt also $m \equiv 339^{8743} \equiv 36^{87(p-1)+43} \equiv 36^{43}$, da nach dem kleinen Satz von Fermat $x^{p-1} \equiv 1$ für alle $x \in \mathbb{Z}_p^\times$. Mit $36^2 \equiv 84 \equiv 36^{32}$ und $36^8 \equiv 95$ berechnet man $m \equiv 36^{43} = 36^{32+8+2+1} \equiv 84 \cdot 95 \cdot 84 \cdot 36 \equiv 95 \bmod 101$. Ebenso berechnet man modulo $q = 103$, $m \equiv 30^{73} = 30^{64+8+1} \equiv 34$.

Nach dem chinesischen Restsatz gibt es nun ein eindeutiges $0 \leq m < N$ mit

$$\begin{aligned} m &\equiv 95 \bmod p = 101 \text{ und} \\ m &\equiv 34 \bmod q = 103 \,, \end{aligned}$$

nämlich $m = 8377$, wie sich nach der Anleitung von Unterabschnitt 1.2.7 berechnen lässt. Dieses Vorgehen ist meist effizienter bei riesigen N.

Aufgabe
Entwickle die drei Blöcke $m_1 = 1420$, $m_2 = 585$ und $m_3 = 7444$ der Nachricht M in Binärzahlen und setze sie mittels Tabelle auf S.49 zu einer (englischen) Nachricht zusammen. Berechne nun die drei Chiffrate $c_1 \equiv m_1^e$, $c_2 \equiv m_2^e$ und $c_3 \equiv m_3^e$ mod $N = 10403$ zum Verschlüssel $e = 11$. Berechne den Entschlüssel d und kontrolliere $c_k^d \equiv m_k \bmod N$ für $k = 1, 2, 3$.

3.3 Diffie, Hellman und ElGamal

3.3.1 Gemeinsamer geheimer Schlüssel

Anton und Bärbel wollen einen gemeinsamen geheimen Schlüssel erzeugen, mit dem sie sich dann verschlüsselte Nachrichten schreiben, die (innert nützlicher Frist) nur von der jeweils anderen Person wieder entschlüsselt werden können. Wir betrachten folgenden Vorschlag[5] von *Diffie* und *Hellman*.

[5] W. Diffie und M. Hellman (1976) New directions in cryptography. *IEEE Trans. Information Theory IT-22, no. 6.*

Zunächst wählen A. und B. eine grosse Primzahl p sowie eine Primitivwurzel $w \in \mathbb{Z}_p^\times$, die beide auch öffentlich gemacht werden können (weiter unten verallgemeinern wir dies). Zusätzlich wählt A. einen Exponenten $\alpha < p-1$ und B. einen Exponenten $\beta < p-1$. Weder B. noch sonst jemand kennt α. Weder A. noch sonst jemand kennt β. Nun berechnet A. seinen sog. *öffentlichen Schlüssel* $a = w^\alpha$ und B. den ihren, $b = w^\beta$. Mit ihren je geheimen Exponenten α bzw. β und den öffentlichen Schlüsseln a und b können A. bzw. B. nun beide

$$A\colon b^\alpha = (w^\beta)^\alpha = w^{\alpha\cdot\beta} \quad \text{bzw. } B\colon \ a^\beta = (w^\alpha)^\beta = w^{\alpha\cdot\beta}$$

den gleichen geheimen, den sog. *gemeinsamen Schlüssel* $w^{\alpha\cdot\beta}$ berechnen.

gemeinsamer Schlüssel

Beispiel

Anton und Bärbel einigen sich auf $p = 11$ und $w = 7$. Anton schickt Bärbel $w^\alpha = 4$. Welches α hat Anton gewählt? Der gemeinsame Schlüssel $w^{\alpha\cdot\beta}$ ist 9. Welches ist der öffentliche Schlüssel $b = w^\beta$ von Bärbel und welches ihr geheimer Exponent β ?

Lösung

Um $7^\alpha = 4$ nach α aufzulösen, müssen wir den diskreten Logarithmus von 4 zur Basis 7 in $\mathbb{Z}_{11}^\times$ berechnen, vgl. Unterabschnitt 1.2.8. Wie gesagt kennt man keinen wesentlich besseren Algorithmus, als alle Exponenten durchzuprobieren,

$$\begin{aligned} 7^2 &\equiv 5 \mod 11\ , \\ 7^3 &\equiv 2 \mod 11\ , \\ &\vdots \\ 7^6 &\equiv 4 \mod 11\ . \end{aligned}$$

Im schlimmsten Fall müssten wir alle Exponenten bis zur Grössenordnung p durchprobieren. Dies geht exponentiell viel langsamer, als mit einer Zahl, z.B. α oder β zu potenzieren, was nur etwa $\log_2(p)$ viele Operationen braucht. Ist der gemeinsame Schlüssel $w^{\alpha\cdot\beta} = 9$, so folgt

$$4^\beta \equiv 9 \mod 11\ ,$$

mit Lösungen $\beta = 3$ und $\beta = 8$ in $\{0, 1, \ldots, p-2\}$. Je nachdem ist also Bärbels öffentlicher Schlüssel $7^3 \equiv 2 \bmod 11$ oder $7^8 \equiv 9 \bmod 11$. Da b ja öffentlich gemacht werden kann, spielt diese Mehrdeutigkeit nur in dieser Aufgabe nicht aber in der Praxis eine Rolle. Anton erhält auch für beide Werte den gleichen gemeinsamen Schlüssel

$$w^{\alpha\cdot\beta} = (w^\beta)^\alpha = b^\alpha = b^6 = \begin{cases} 2^6 \\ 9^6 \end{cases} \text{ oder } \equiv 9 \mod 11\ .$$

Obiges Beispiel ist eine Rechenaufgabe und nimmt keinen Bezug auf den tatsächlichen Vorgang bei der Erzeugung eines gemeinsamen Schlüssels. Spion Charlie müsste aus p, w, $a = w^\alpha$ und $b = w^\beta$ den gemeinsamen Schlüssel $w^{\alpha\cdot\beta}$ berechnen. Man nimmt an, dass dies nur über die Berechnung der diskreten Logarithmen, also über

$$\alpha = \log_w(a) \quad \text{oder} \quad \beta = \log_w(b)$$

möglich ist. Wie erwähnt, benötigt dies eine Anzahl Rechenschritte in der Grössenordnung von p (Durchprobieren aller Exponenten bis $p-2$). Dagegen braucht es für die Berechnung von $a = w^\alpha$, $b = w^\beta$ und $w^{\alpha\cdot\beta} = a^\beta = b^\alpha$ je etwa von der Grössenordnung $\log_2(p)$ Rechenschritte. Heutzutage verwendet man Primzahlen p mit etwa $2^{10} = 1024$ Binärstellen, was etwa $300 \approx 1024 \cdot \ln(2)/\ln(10)$ Dezimalstellen entspricht, also $p \approx 2^{2^{10}} \approx 2^{1000} \approx 10^{300}$. Kann man jede Nanosekunde ns $= 10^{-9}$s einen Rechenschritt ausführen, so dauert ein Vorgang wie das Potenzieren von der Grössenordnung $\log_2(p)$ns $\approx 1000 \cdot 10^{-9}\text{s} = 10^{-6}\text{s} =$ eine Mikrosekunde. Das Berechnen des diskreten Logarithmus von der Grössenordnung p dagegen benötigt etwa $p \cdot 10^{-9}\text{s} \approx 10^{300} \cdot 10^{-9}\text{s} = 10^{291}$ Sekunden, wogegen das Alter des Universums von etwa einer halben Trillion Sekunden geradezu verschwindend kurz ist!

Verallgemeinerung

In diesem Verfahren kann statt p auch eine beliebige grosse Natürliche Zahl q gewählt werden, sowie eine beliebige Einheit $w \in \mathbb{Z}_q^\times$. In diesem Falle müssen die geheimen Exponenten α und β beide kleiner als $\varphi(q)$ gewählt werden. Wiederum sind $a = w^\alpha$ bzw. $b = w^\beta$ die öffentlichen Schlüssel von A. bzw. von B. und den gemeinsamen Schlüssel $w^{\alpha\cdot\beta}$ berechnen A. bzw. B. aus

$$A\colon\ b^\alpha = (w^\beta)^\alpha = w^{\alpha\cdot\beta} \quad \text{bzw. } B\colon\ \ a^\beta = (w^\alpha)^\beta = w^{\alpha\cdot\beta}\ .$$

Beispiel

Sei $q = 55$ mit $\varphi(q) = \varphi(5)\cdot\varphi(11) = 4\cdot 10 = 40$ und $w = 7$. Anton wählt sodann den geheimen Exponenten $\alpha = 19$ und Bärbel wählt $\beta = 13$. Um die Potenzen $a = w^\alpha$ und $b = w^\beta$ effizient berechnen zu können, berechnen wir gemäss Abschnitt 3.1

$$\begin{aligned} 7^2 &\equiv 49 \mod 55\ , \\ 49^2 \equiv 7^4 &\equiv 36 \mod 55\ , \\ 36^2 \equiv 7^8 &\equiv 31 \mod 55\ , \\ 31^2 \equiv 7^{16} &\equiv 26 \mod 55\ , \end{aligned}$$

und daraus die öffentlichen Schlüssel

$$\begin{aligned} a \equiv w^\alpha \equiv 7^{19} = 7^{1+2+16} \equiv 7\cdot 49\cdot 26 &\equiv 8 \mod 55 \text{ und} \\ b \equiv w^\beta \equiv 7^{13} = 7^{1+4+8} \equiv 7\cdot 36\cdot 31 &\equiv 2 \mod 55\ . \end{aligned}$$

Der gemeinsame Schlüssel würde nun von A. aus $w^{\alpha\cdot\beta} = b^\alpha$ und von B. aus $w^{\alpha\cdot\beta} = a^\beta$ berechnet. Da wir die geheimen Exponenten aber beide kennen, können wir unter Beachtung von $w^{\varphi(q)} = 7^{40} \equiv 1 \mod 55$ direkt berechnen

$$w^{\alpha\cdot\beta} \equiv 7^{19\cdot 13} = 7^{6\cdot 40+7} \equiv 7^7 \equiv 7^{1+2+4} \equiv 7\cdot 49\cdot 36 \equiv 28 \mod 55\ .$$

3.3.2 Verschlüsseln und Entschlüsseln nach ElGamal

Haben Anton und Bärbel einen *gemeinsamen geheimen Schlüssel* $w^{\alpha\cdot\beta}$ erzeugt, den Spion Charlie nicht in nützlicher Frist knacken kann, so können sie diesen nun benutzen, um sich verschlüsselte Nachrichten zu senden.[6]

[6] T. ElGamal (1985) A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans. Inform. Theory 31, no.4.*

Hat Anton seine Nachricht erst einmal mittels Tabelle auf S.49 in eine Zahl $0 < m < p$ verwandelt, so schickt er Bärbel das Chiffrat

$$c \equiv w^{\alpha\cdot\beta} \cdot m \mod p$$

mit $0 \leq c < p$. Mit Hilfe Antons öffentlichen Schlüssels $a = w^\alpha$ und ihres geheimen Exponenten $\beta < p-1$ kann Bärbel nun c entschlüsseln mit der Rechnung

$$m \equiv w^{-\alpha\cdot\beta} \cdot c \equiv (w^\alpha)^{-\beta} \cdot c \equiv a^{-\beta} \cdot c \equiv a^{p-1-\beta} \cdot c \mod p\ .$$

Beispiel
Wie im ersten Beispiel des letzten Unterabschnittes auf S.52 nehmen wir $p = 11$, $w = 7$, $\alpha = 6$ und $\beta = 3$ an. Die öffentlichen Schlüssel von Anton bzw. Bärbel sind dann

$$a \equiv w^\alpha \equiv 7^6 \equiv 4 \mod 11 \quad \text{bzw. } b \equiv w^\beta \equiv 7^3 \equiv 2 \mod 11\ ,$$

und der gemeinsame Schlüssel ist $w^{\alpha\cdot\beta} \equiv a^\beta \equiv b^\alpha \equiv 9 \bmod 11$.
Anton möchte die Nachricht $m = 8$ an Bärbel schicken und chiffriert

$$c \equiv w^{\alpha\cdot\beta} \cdot m \equiv 9 \cdot 8 \equiv 6 \mod 11\ .$$

Mittels öffentlichen Schlüssels $a = 4$ von Anton und ihrem geheimen Exponenten $\beta = 3$ berechnet Bärbel nun

$$m \equiv a^{-\beta} \cdot c \equiv a^{p-1-\beta} \cdot c = 4^7 \cdot 6 \equiv 8 \mod 11\ .$$

Beispiel
Wie im zweiten Beispiel des letzten Unterabschnittes auf S.53 wählen wir $q = 55$, $w = 7$, $\alpha = 19$, $\beta = 13$, so dass gilt $a = w^\alpha \equiv 8$, $b = w^\beta \equiv 2$ und $w^{\alpha\cdot\beta} = 28 \bmod 55$.
Anton möchte wiederum die Nachricht $m = 8$ an Bärbel schicken und chiffriert

$$c \equiv w^{\alpha\cdot\beta} \cdot m \equiv 28 \cdot 8 \equiv 4 \mod 55\ .$$

Mittels öffentlichen Schlüssels $a = 8$ von Anton und ihrem geheimen Exponenten $\beta = 13$ berechnet Bärbel nun

$$m \equiv a^{-\beta} \cdot c \equiv a^{\varphi(q)-\beta} \cdot c = 8^{40-13} \cdot 4 = 8^{27} \cdot 4 \equiv 2 \cdot 4 \equiv 8 \mod 55\ .$$

Wiederum liesse sich hier $8^{27} = 8^{1+2+8+16}$ nach Abschnitt 3.1 berechnen. Mit

$$x^{\varphi(q)} \equiv 1 \mod q \quad \text{für alle } x \in \mathbb{Z}_q^\times \quad \text{(kleiner Satz von Fermat)}$$

geht es aber zügiger, $8^{27} = (2^3)^{27} = 2^{81} \equiv 2^{2\cdot\varphi(55)+1} \equiv 2^1 = 2 \bmod 55$.

3.4 Verallgemeinerter diskreter Logarithmus

Wir kommen noch auf eine Tatsache zu sprechen, auf die wir schon mehrfach indirekt gestossen sind, z.B.

- bei der Gleichung $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$ falls $\text{ggT}(a, b) = 1$ auf S.15,
- beim Chinesischen Restsatz auf S.18,
- beim der Analyse von $M_{15} = \mathbb{Z}_{15}^{\times}$ in Aufgabe 4 von Übung 2,
- in der Bemerkung 4 auf S.51,

nämlich, dass die Gruppen $\mathbb{Z}_{a \cdot b}^{\times}$ mit den Gruppen $\mathbb{Z}_a^{\times}$ und $\mathbb{Z}_b^{\times}$ für teilerfremde a und b sehr eng verwandt ist. Es gilt der

Satz *über Isomorphie der Gruppen* $\mathbb{Z}_{a \cdot b}^{\times}$ *und* $\mathbb{Z}_a^{\times} \times \mathbb{Z}_b^{\times}$
Für teilerfremde $a, b \in \mathbb{N}$ *sind* $M_{a \cdot b} = \mathbb{Z}_{a \cdot b}^{\times}$ *und* $M_a \times M_b = \mathbb{Z}_a^{\times} \times \mathbb{Z}_b^{\times}$ *isomorph*,

$$\mathbb{Z}_{a \cdot b}^{\times} \cong \mathbb{Z}_a^{\times} \times \mathbb{Z}_b^{\times} \ .$$

Die beiden Gruppen links und rechts haben also nicht nur als Mengen gleich viele Elemente, $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$, sondern sie können mit einer Bijektion aufeinander abgebildet werden, die die Gruppenoperationen respektiert.

Beweis
Die Bijektion von links nanch rechts ordnet einer Restklasse $\overline{r}$ modulo $c = a \cdot b$ mit $\text{ggT}(r, c) = 1$ das Restklassenpaar $(\overline{s}, \overline{t})$ mit $\overline{s}$ Restklasse von r in $\mathbb{Z}_a^{\times}$ und $\overline{t}$ Restklasse von r in $\mathbb{Z}_b^{\times}$ zu. Dabei sind $\overline{s}$ und $\overline{t}$ gleich, auch wenn r zwei verschiedene Repräsentanten von $\overline{r}$ in $\mathbb{Z}_{a \cdot b}^{\times}$ sind, d.h. unabhängig vom Repräsentanten.
Die Umkehrabbildung liefert der Chinesische Restsatz, welcher besagt, dass es zu zwei Restklassen $\overline{s}$ modulo a und $\overline{t}$ modulo b mit $\text{ggT}(a, b) = 1$ ein eindeutiges r mit $0 \leq r < a \cdot b$ gibt, mit $r \equiv s \mod a$ und $r \equiv t \mod b$. Aus $\text{ggT}(s, a) = 1 = \text{ggT}(t, b)$ folgt zudem $\text{ggT}(r, c) = 1$.
Es zeigt sich, dass diese Bijektion und ihre Umkehrabbildung Gruppenoperationen respektieren. □

Beispiel
Sei $a = 3$ und $b = 5$. In $\mathbb{Z}_3^{\times}$ wählen wir $\overline{s}$ mit $s \equiv 2 \mod 3$ als Primitivwurzel und in $\mathbb{Z}_5^{\times}$ wählen wir $\overline{t}$ mit $t \equiv 2 \mod 5$. Dann ist jedes Element in $\mathbb{Z}_3^{\times} \times \mathbb{Z}_5^{\times}$ von der Form

$$(x, y) = (\overline{s}^i, \overline{t}^j) \quad \text{mit } 0 \leq i < 2 \quad \text{und } 0 \leq j < 4 \ .$$

Wir nennen (i, j) den *verallgemeinerten diskreten Logarithmus* von (x, y) zur Basis $(\overline{s}, \overline{t})$ in $\mathbb{Z}_a^{\times} \times \mathbb{Z}_b^{\times}$, wenn $\mathbb{Z}_a^{\times}$ und $\mathbb{Z}_b^{\times}$ beide zyklisch sind mit Primitivwurzeln $\overline{s} \in \mathbb{Z}_a^{\times}$ und $\overline{t} \in \mathbb{Z}_b^{\times}$, also wenn z.B. a und b Potenzen von ungeraden Primzahlen sind.
Mittels Chinesischem Restsatz bilden wir nun $(\overline{s}^1, \overline{t}^0) = (\overline{s}, 1) = (2, 1)$ auf r_1 mit

$$\begin{aligned} r_1 &\equiv 2 \mod 3 \text{ und} \\ r_1 &\equiv 1 \mod 5 \end{aligned}$$

und $0 \leq r_1 < a \cdot b = c = 15$ ab, also auf $r_1 = 11$. Ebenso bilden wir $(\overline{s}^0, \overline{t}^1) = (1, 2)$ auf r_2 mit $r_2 \equiv 1 \mod 3$ und $r_2 \equiv 2 \mod 5$ und $0 \leq r_2 < 15$, also auf $r_2 = 7$ ab.

Folgerung
Jedes Element in $\mathbb{Z}_{15}^{\times}$ hat eine *eindeutige Darstellung* als

$$\overline{11^i \cdot 7^j} = \overline{11}^i \cdot \overline{7}^j \quad \text{mit } 0 \leq i < 2 \quad \text{und } 0 \leq j < 4.$$

Wir nennen (i, j) den *verallgemeinerten diskreten Logarithmus* des Elemetes

$$x = \overline{11^i \cdot 7^j} \in \mathbb{Z}_{15}^{\times}$$

zur Basis $(\overline{11}, \overline{7})$.
Man beachte, dass auch eine andere Basis gewählt werden kann.

Satz *über endliche kommutative Gruppen*
Jede endliche kommutative Gruppe ist wie oben das Produkt zyklischer Gruppen.
(Aber: Die Anzahl zyklischer Gruppen ist dabei *nicht* eindeutig! Übung.)

3.5 Schlussbemerkungen

Die Sicherheit dieser weit verbreiteten Verschlüsselungsverfahren und somit unserer ganzen Informationsgesellschaft hängt von unbewiesenen Tatsachen ab.
Im Falle des RSA–Verfahrens nimmt man an, dass es praktisch unmöglich ist ein Produkt

$$N = p \cdot q$$

zweier mehrerer hundert Dezimalstellen langer Primzahlen wieder in seine zwei Faktoren zu zerlegen. Dabei ist zu beachten, dass der Nachweis, dass eine Zahl prim oder nicht prim ist, unabhängig vom Auffinden allfälliger Faktoren geschieht. Nur dann kann ein Element $x \in \mathbb{Z}_N^{\times}$ modulo N die Ordnung $N-1$ haben, wenn N prim ist, da für zusammengesetzte N stets $\text{ord}(x) \leq \varphi(N) < N-1$ gilt. Für N prim ist die Anzahl $\varphi(\varphi(N)) = \varphi(N-1)$ solcher x mit $\text{ord}(x) = N-1$ (Primitivwurzeln) doch recht gross, so dass sich Primzahlen mit Verfeinerungen des kleinen Satzes von Fermat in der Regel noch *verhältnismässig* rasch[7] als solche zu erkennen geben.
Im Falle der Erzeugung eines gemeinsamen geheimen Schlüssels nach Diffie–Hellman nimmt man an, dass es praktisch unmöglich ist, den Exponenten ϵ einer mehrerer hundert Dezimalstellen langen Zahl $e \equiv w^{\epsilon}$ modulo q zu finden, auch wenn q, w und e bekannt sind — mit anderen Worten, dass der diskrete Logarithmus nicht in nützlicher Frist berechnet werden kann. Auch das ist nicht bewiesen — ja, man weiss nicht einmal, ob die Berechnung von $w^{\alpha \cdot \beta}$ (modulo q) aus w, w^{α} und w^{β} nicht vielleicht auch ohne die Berechnung von α oder β möglich ist.
Andererseits ist es doch äusserst unwahrscheinlich, dass sich diese unbewiesenen Annahmen in nächster Zeit als widerlegt herausstellen. Es gibt jedoch zusätzliche Punkte bei den vorgestellten Verfahren, die beachtet werden müssen, weil diese *in gewissen besonderen Fällen*, z.B. bei besonders ungeschickter Wahl der Parameter, keine Sicherheit mehr gewährleisten.

[7] ... jedoch nicht so rasch wie sog. *Mersenne*—Primzahlen der Form $M(p) = 2^p - 1$ mit p prim, für die es Turbotests mittels Kettenbruchentwicklungen gibt, sog. *Lucas*–Tests.
Seit Jan. 2016 ist $M(74207281)$ die grösste bekannte Primzahl, bis heute 13. Mai 2017.