Skript

Diskrete Mathematik

Prof. Dr. C.P. Schnorr

http://www.mi.informatik.uni-frankfurt.de

Johann-Wolfgang-Goethe Universität
Fachbereich Informatik und Mathematik
Frankfurt am Main

2. März 2015

Einleitung

Die Diskrete Mathematik behandelt „diskrete“, insbesondere endliche Objekte und ihre Strukturen im Hinblick auf Computeranwendungen. Wichtig sind Prozeduren, die nach endlich vielen Schritten ein Ergebnis liefern, also **Algorithmen**. Effiziente Algorithmen bilden die Basis von Computeranwendungen — schwierige algorithmische Probleme diejenige von Kryptographie und Datensicherheit.

Die Vorlesung Diskrete Mathematik entwickelt auf der Grundlage von Linearer Algebra und elementarer Stochastik wichtige Bereiche der Computerwissenschaft wie Lineare Codes, Publik Key Verschlüsselung (RSA), Boolesche Funktionen und Schaltkreise. Mathematische Strukturen werden stets begleitet von Computeranwendungen. Es wird das Verständnis einfacher gegenüber schwierigen algorithmischen Problemen entwickelt. Es werden Algorithmen am Beispiel analysiert und ihre Computerrealisierung behandelt. Es wird das Zusammenspiel algorithmischer, stochastischer und algebraischer Aspekte entwickelt.

Einerseits wendet sich die Vorlesung an Studenten der Informatik vorzugsweise im vierten Semester. Andererseits bietet die Vorlesung für Mathematikstudenten einen Kurs in angewandter Algebra und gilt als praktische Mathematik im Sinne der Studienordnung zum Diplom in Mathematik. Allgemeine Literaturhinweise (siehe Anhang):

- N.L. Biggs: Discrete Mathematics (Oxford University Press 1985)
- D.E. Knuth: The Art of Computer Programming, Vol.2 Chapter 4 (Addison-Wesley 1981, second edition), Vol.1 Chapter 1 (Addison Wesley 1972)
- M. Aigner: Diskrete Mathematik, (Vieweg, 1996)
- J. von zur Gathen und J. Gerhard: Modern Computer Algebra, (Cambridge University Press 1999)
- T. Ihringer: Diskrete Mathematik, (B.G. Teubner 1994)
- G. Kersting: Vorlesungsskript Diskrete Mathematik, www.math.uni-frankfurt.de/ stoch/kersting/Skripten.html
- C.P. Schnorr: Vorlesungsskript Diskrete Mathematik, www.mi.informatik.uni-frankfurt.de/index.html#publications

Diese Ausarbeitung basiert auf den Vorlesungen „Diskrete Mathematik“ der Sommersemester 1992, 1995, 2001, 2006, 2008, 2010.

Von Marc Fischlin und Roger Fischlin 1995/96 erstmals in LaTeX2e gesetzt.

Inhaltsverzeichnis

Kapitel 1

Euklidischer Algorithmus

Der Euklidische Algorithmus ist eines der ältesten Rechenverfahren. Er war schon EUDOXUS (375 v.Chr.) bekannt und ist im Band 7 der „Elemente“ von EUKLID (300 v.Chr.) beschrieben. Dies ist die älteste überlieferte Beschreibung eines Algorithmus. Das Verfahren zum Multiplizieren natürlicher Zahlen benutzten zwar schon die Steuerbeamten im alten Agypten zur Flächenberechnung, eine Verfahrensbeschreibung hinterliessen sie aber nicht.

Der Euklidische Algorithmus bestimmt den größten gemeinsamen Teiler natürlicher Zahlen. Er kommt in vielen Rechenprozessen zur Anwendung, z.B. bei der Zerlegung von Zahlen und Polynomen und der Lösung ganzzahliger linearer Gleichungen. Wichtigste Varianten sind die Algorithmen 1 und 4. Algorithmus 3 bereitet den Algorithmus 4 vor.

Größter gemeinsamer Teiler. Wir betrachten zunächst den Ring $\mathbb{Z}$ der ganzen Zahlen. Wir schreiben $a \mid b$ für ganze Zahlen a, b, falls a *Teiler* von b ist, d.h., falls es ein ganze Zahl c gibt mit $ac = b$.

Definition 1.1
$d \in \mathbb{Z}$ *heißt* größter gemeinsamer Teiler*, kurz ggT, von* $a_1, \ldots, a_n \in \mathbb{Z} \setminus \{0\}$*, falls*

a) $d \mid a_1, \ldots, d \mid a_n$,

b) $z \mid a_1, \ldots, z \mid a_n \quad \Rightarrow \quad z \mid d \quad$ *für alle* $z \in \mathbb{Z}$.

Wir schreiben dann $d = \mathrm{ggT}(a_1, \ldots, a_n)$. Gilt $\mathrm{ggT}(a_1, \ldots, a_n) = 1$, so sagt man, $a_1, \ldots, a_n$ sind *relativ prim* oder *teilerfremd*.

Der ggT von $a_1, \ldots, a_n$ ist bis auf das Vorzeichen eindeutig bestimmt. Denn, ist d' ein weiterer ggT für $a_1, \ldots, a_n$, teilen sich d und d' gegenseitig, so daß $d' = \pm d$ folgt.

Weniger evident ist die Existenz von $\mathrm{ggT}(a,b)$. Eine Möglichkeit besteht darin, a und b in Primfaktoren zu zerlegen. Seien $p_1,\dots,p_r$ die Primzahlen, die in a oder b als Teiler enthalten sind. Dann gibt es ganze Zahlen $e_1,\dots,e_r,f_1,\dots,f_r \geq 0$ so daß $a = \pm p_1^{e_1}\dots p_r^{e_r}$ und $b = \pm p_1^{f_1}\dots p_r^{f_r}$ ($e_i = 0$ bedeutet, daß p_i kein Teiler von a ist). Die gemeinsamen Teiler von a und b sind dann von der Form $z = \pm p_1^{g_1}\dots p_r^{g_r}$ mit $g_i \in \{0,1,\dots,m_i\}$, $m_i = \min(e_i,f_i)$, und es folgt $\mathrm{ggT}(a,b) = \pm p_1^{m_1}\dots p_r^{m_r}$. Vom Standpunkt des Rechnens ist die Primfaktorzerlegung unbefriedigend, denn die Zerlegung einer Zahl in ihre Primfaktoren ist sehr rechenaufwendig.

Wir gehen hier anders vor und klären die Existenzfrage, indem wir ein Rechenverfahren angeben, das größte gemeinsame Teiler liefert. Es beruht auf einer grundlegenden Eigenschaft ganzer Zahlen, der *Division mit Rest*. Zu ganzen Zahlen $a,b \neq 0$ gibt es ganze Zahlen q,r, so daß

$$a \;=\; qb + r \quad \text{mit } 0 \leq r < |b|.$$

Dabei ist $q = \lfloor a/b \rfloor$ der ganzzahlige Quotient von a und b, d.h. die größte ganze Zahl kleiner gleich a/b. Es gilt $0 \leq a/b - \lfloor a/b \rfloor < 1$.

Berechnung des ggT. Die Idee des Euklidischen Algorithmus ist es, aus zwei Zahlen den ggT schrittweise herauszudividieren. Die Grundform des Algorithmus arbeitet mit positiven, ganzzahligen Quotienten $\lfloor a_0/a_1 \rfloor$ und erzeugt eine Folge von kleiner werdenden positiven Resten $a_0, a_1, \dots$. Das folgende Programm kommt mit zwei Speicherplätzen a_0, a_1 aus, bei zyklischem Recycling.

Algorithmus 1 Euklidischer Algorithmus

EINGABE: $m,n \in \mathbb{N}$ mit $m > n$

1. $a_0 := m$, $a_1 := n$

2. $\begin{bmatrix} a_0 \\ a_1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -\lfloor a_0/a_1 \rfloor \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \end{bmatrix}$, (in der *zentrierten* Variante wird $\lfloor a_0/a_1 \rfloor$ ersetzt durch die nächste ganze Zahl $\lceil a_0/a_1 \rfloor$ zu a_0/a_1.)

3. IF $a_1 \neq 0$ THEN GOTO 2

AUSGABE: $a_0 = \mathrm{ggT}(n,m)$

In Schritt 2 wird der Rest $a_0 - \lfloor a_0/a_1 \rfloor a_1 \in [0, a_1[$ gebildet und auf a_1 zurückgespeichert, das alte a_1 wird zu a_0. Damit gilt stets $a_0 > a_1 \geq 0$. Im zentrierten Algorithmus gilt dagegen stets $|a_0| > |a_1|$. Speichert man nicht auf a_0, a_1 zurück, lautet die Rekursion von Schritt 2

$$a_{i+1} := a_{i-1} - \lfloor a_{i-1}/a_i \rfloor\, a_i \qquad \text{für i=1,2,...}$$

Hier ist die Schrittfolge bei Eingabe von $m = 512$ und $n = 447$:

a_0	a_1	$\lfloor a_0/a_1 \rfloor$
512	447	1
447	65	6
65	57	1
57	8	7
8	1	8
1	0	

$$\begin{aligned} 512 &= 1 \cdot 447 + 65 \\ 447 &= 6 \cdot 65 + 57 \\ 65 &= 1 \cdot 57 + 8 \\ 57 &= 7 \cdot 8 + 1 \\ 8 &= 8 \cdot 1 + 0 \end{aligned}$$

Der Algorithmus liefert $\mathrm{ggT}(512, 447) = 1$, d.h. 512 und 447 sind relativ prim.

Der Euklidischen Algorithmus ist leicht übertragbar auf Polynome und 2-dimensionale Gitterbasen.

Algorithmus 2 Euklidischer Algorithmus für Polynome

EINGABE: $g, h \in K[x]$ mit $h \neq 0$ und $\mathrm{grad}(g) \geq \mathrm{grad}(h)$

1. $f_0 := g, f_1 := h$.

2. $\begin{bmatrix} f_0 \\ f_1 \end{bmatrix} := \begin{bmatrix} 0 & 1 \\ 1 & -q \end{bmatrix} \begin{bmatrix} f_0 \\ f_1 \end{bmatrix}$, dabei ist $q \in K[x]$ Quotient bei der Division f_0/f_1 derart, daß $\mathrm{grad}(f_0 - qf_1) < \mathrm{grad} f_1$

3. IF $f_1 \neq 0$ THEN GOTO 2

AUSGABE: $f_0 = \mathrm{ggT}(g, h)$

Reduktion von Polynomen. Sei K ein Körper. Zu den Polynomen $g_0, g_1 \in K[x]$ berechnet man den $\mathrm{ggT}(g_0, g_1)$ analog zu (1.1) mit der Rekursion

$$g_{i+1} = g_{i-1} - q_{i-1} g_i \qquad i = 1, 2, \ldots$$

Dabei ist q_{i-1} Quotient bei der Division von g_{i-1} durch g_i und g_{i+1} der Rest derart, daß $\mathrm{grad}(g_{i+1}) < \mathrm{grad}(g_i)$. In $K[x]$ gibt es nämlich eine eindeutige Division mit Rest.

Reduktion von Gitterbasen der Dimension 2. Seien $b_0, b_1 \in \mathbb{Z}^n$ linear unabhängige Vektoren. Dann heist

$$L(b_0, b_1) = \{ t_0 b_0 + t_1 b_1 \mid t_0, t_1 \in \mathbb{Z} \} = b_0 \mathbb{Z} + b_1 \mathbb{Z}$$

ein *Gitter* mit *Basis* b_0, b_1. Sei $\langle\ ,\ \rangle : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ das Standard-Skalarprodukt und $\|b\| = \langle b, b \rangle^{1/2}$ die *Euklidische Länge* von $b \in \mathbb{R}^n$. Das Gitter $L = L(b_0, b_1)$ hat die *Determinante*

$$\det L = \det \begin{bmatrix} \langle b_0, b_0\rangle & \langle b_0, b_1\rangle \\ \langle b_1, b_0\rangle & \langle b_1, b_1\rangle \end{bmatrix}^{1/2} = (\|b_0\|^2\|b_1\|^2 - \langle b_0, b_1\rangle^2)^{1/2}.$$

$\det L(b_0, b_1)$ ist der Flächeninhalt des von den Vektoren b_0, b_1 erzeugten Parallelogramms $b_0[0,1] + b_1[0,1]$.

Um eine Basis aus kurzen Vektoren des Gitters $L := L(b_0, b_1)$ zu konstruieren, geht man wie folgt vor. Vertausche die Vektoren b_0, b_1 so dass $\|b_0\| \geq \|b_1\|$. Iteriere mit den Zeilenvektoren b_0, b_1

$$\begin{bmatrix} b_0 \\ b_1 \end{bmatrix} := \begin{bmatrix} 0 & 1 \\ 1 & -q \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \end{bmatrix} \quad \text{mit } q := \lceil \langle b_0, b_1\rangle / \langle b_0, b_0\rangle \rfloor$$

solange wie $q \neq 0$ und vertausche am Ende gegebenenfalls b_0, b_1 so dass $\|b_0\| \leq \|b_1\|$. Die Wahl von q liefert $\|b_0 - qb_1\| = \min_{t\in Z} \|b_0 - tb_1\|$. Bei Abbruch ist b_0 der kürzeste Vektor (ungleich 0) im Gitter L und b_1 ist der kürzeste zu b_0 linear unabhängige Vektor. Ferner gilt $\|b_0\| \cdot \|b_1\| \leq \sqrt{\frac{4}{3}} \det L(b_0, b_1)$.

Korrektheit des Euklidischen Algorithmus. Für die Rekursion (1.1), bei der nicht auf a_0, a_1 zurückgespeichert wird, gilt offenbar

$$\mathrm{ggT}(a_{i-1}, a_i) = \mathrm{ggT}(a_i, a_{i+1}).$$

Wir erhalten

$$\mathrm{ggT}(a_0, a_1) = \mathrm{ggT}(a_{j-1}, a_j)$$

Für das erste j mit $a_{j+1} = 0$ gilt somit $\mathrm{ggT}(a_0, a_1) = a_j$, und damit ist $\mathrm{ggT}(a_0, a_1)$ korrekt berechnet.

Satz 1.2
Der Euklidische Algorithmus bricht bei Eingabe $m, n \in \mathbb{N}$ mit $m > n$ nach höchstens $\log_{\sqrt{2}}(m)$ Iterationen ab.

Beweis. Die Iterationszahl sei die kleinste Zahl j mit $a_{j+1} = 0$. Durch Induktion über i zeigen wir

$$a_{i+1} < \tfrac{a_{i-1}}{2} \qquad \text{für } 1 \leq i \leq j$$

Im Induktionsschritt unterscheiden wir zwei Fälle

- Falls $a_i \leq \frac{a_{i-1}}{2}$, gilt $a_{i+1} < a_i \leq \frac{a_{i-1}}{2}$.
- Falls $a_i > \frac{a_{i-1}}{2}$, gilt $a_{i-1} = a_i + a_{i+1}$ und somit $a_{i+1} < \frac{a_{i-1}}{2}$.

Mit $a_0 = m$ folgt $a_{2i} < m \cdot 2^{-i}$ und somit ist die Iterationszahl $j \leq \log_{\sqrt{2}}(m)$. □

Mit einer Worst-Case-Analyse verbessern wir die Schranke $\log_{\sqrt{2}}(m)$ zu $\log_{1,618}(m)$. Eine *Worst-Case-Eingabe* $n, m \in \mathbb{N}$ für j Iterationen liegt vor, wenn n und m minimal für die Iterationszahl j ist (die Iterationszahl ist die kleinste Zahl j mit $a_{j+1} = 0$). Dies ist der Fall, wenn

$$\begin{aligned} \lfloor a_{i-1}/a_i \rfloor &= 1 && \text{für } i = 1, 2, \ldots, j-1 \\ \lfloor a_{j-1}/a_j \rfloor &= 2 && a_{j+1} = 0 \end{aligned}$$

Beachte, dass $\lfloor a_{j-1}/a_j \rfloor = 1$ nicht möglich ist, da mit $a_{j+1} = 0$ folgen würde, dass $a_j = a_{j-1}$.
Die Fibonacci[1]-Folge wird erklärt durch $F_0 = 0, F_1 = 1, F_j := F_{j-1} + F_{j-2}$ für $j \geq 2$. Bei Eingabe von $m = F_{j+2}$ und $n = F_{j+1}$ gilt im Euklidischen Algorithmus

$$\begin{aligned} q_i = \lfloor a_{i-1}/a_i \rfloor &= 1 && \text{für } i = 1, 2, \ldots, j-1 \\ q_j = \lfloor a_{j-1}/a_j \rfloor &= 2 && a_{j+1} = 0 \end{aligned}$$

Damit sind die Fibonacci-Zahlen F_{j+2} und F_{j+1} Worst-Case-Eingaben für den Euklidischen Algorithmus mit j Iterationen. Es gilt (siehe [K73a], Abschnitt 1.2.8):

$$\phi^{j-2} < F_j < \phi^{j-1} \ , \quad F_j = \lceil \phi^j / \sqrt{5} \rfloor$$

$\phi := \frac{1+\sqrt{5}}{2} \approx 1,618$ ist die Zahl des *Goldenen Schnittes*. Damit ist die Iterationszahl des Euklidischen Algorithmus bei Eingabe von m und n mit $m > n$ höchstens $\lceil \log_\phi \left(\sqrt{5}m\right) \rceil - 2$.

Die Iterationszahl des Euklidischen Algorithmus wird weiter erniedrigt, indem man bei der Division mit Rest negative Reste zulässt und den Absolutwert des Restes minimiert. Im *zentrierten* Euklidischen Algorithmus wird der Quotient a_{i-1}/a_i durch die nächste ganze Zahl $\lceil a_{i-1}/a_i \rfloor$ approximiert, $\lceil x \rfloor =_{\text{def}} \lceil x - \frac{1}{2} \rceil$. Die Rekursion (1.1) lautet dann

$$a_{i+1} := a_{i-1} - \lceil a_{i-1}/a_i \rfloor a_i \qquad i = 1, 2, \ldots$$

Damit ist $a_{i+1} \in [-\frac{a_i}{2}, \frac{a_i}{2}[$ die Zahl in $a_{i-1} + a_i\mathbb{Z}$ mit kleinstem Absolutwert. Die Iterationszahl ist höchstens $\log_{(1+\sqrt{2})} m + \mathcal{O}(1)$ mit $1 + \sqrt{2} \approx 2,414$.

Für die Effizienz des Euklidischen Algorithmus ist jedoch weniger die Iterationszahl maßgebend als die Anzahl der Maschinenzyklen oder die Anzahl

[1] Fibonacci Leonardo, Pisa, 1175–1240, betrachtete die Fortpflanzung von Kaninchenpaaren. Jedes Kaninchenpaar bringt ein Paar der nächsten und ein Paar der übernächsten Generation zur Welt und wird dann verspeist. Die Anzahl der Paare pro Generation ist 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89. Aber warum hat das Schneeglöckchen 3 Blütenblätter, die Butterblume 5, der Rittersporn 8, die Ringelblume 13, Astern 21, Gänseblümchen 34 oder 55 oder 89?

der Bitoperationen. Hierzu löst man die Multiplikationen und Divisionen auf in Additionen/Subtraktionen und Shifts. Dies führt zu den binären Algorithmen 4 und 5, die mit Links-Shifts (Multiplikationen mit 2) bzw. Rechts-Shifts (Divisionen durch 2) arbeiten. Im Vorgriff darauf untersuchen wir *die Anzahl der Bitoperationen*, welche für einen Iterationsschritt

$$a_{i+1} := a_{i-1} - \lfloor a_{i-1}/a_i \rfloor a_i$$

von (1.1) benötigt werden. Diese hängt von der Bitlänge der Zahlen a_{i-1}, a_i ab. Sei k_i die Bitlänge von $a_i = \sum_{j=0}^{k_i-1} a_{i,j} 2^j$ mit $a_{i,j} \in \{0,1\}$. Dann geht die Berechnung von a_{i+1} mit Multiplikation/Division nach der Schulmethode mit $\mathcal{O}(k_i(k_{i-1} - k_{i+1}))$ Bitoperationen. Die Gesamtzahl der Bitoperationen ist somit $\mathcal{O}(\sum_i k_i(k_{i-1} - k_{i+1})) = \mathcal{O}(k_0 k_1)$. Bei Eingabe von k-Bit Zahlen $m = a_0, n = a_1$ fallen also nach der Schulmethode $\mathcal{O}(k)^2$ Bitoperationen an.

Die Anzahl der Bitoperationen kann weiter reduziert werden, indem man vorweg die führenden Bits der Zahlen transformiert und die Transformationsschritte auf den niedrigen Bits gebündelt nachträgt, siehe Schönhage, Proc. ISSAC 91, pp. 128–133, 1991.

Erweiterter Euklidischer Algorithmus Nach dem Satz von Bézout[2] (Satz A.25 auf Seite 115) kann der größte gemeinsame Teiler zweier Zahlen $n, m \in \mathbb{Z}$ als ganzzahlige Linearkombination von n und m darstellt werden. Es existieren also $b, c \in \mathbb{Z}$ mit

$$\mathrm{ggT}(n, m) = mb + nc.$$

Um die Koeffizienten b und c zu bestimmen, erweitern wir den Euklidischen Algorithmus.

Hier ist die Schrittfolge bei Eingabe von $m = 7247$ und $n = 3721$:

a_0	a_1	$\lfloor a_0/a_1 \rfloor$	b_0	b_1	c_0	c_1
7247	3721	1	1	0	0	1
3721	3526	1	0	1	1	−1
3529	195	18	1	−1	−1	2
195	16	12	−1	19	2	37
16	3	5	19	229	−37	446
3	1	3	−229	1164	446	−2267
1	0					

Der erweiterte Euklidische Algorithmus liefert für $m = 7247$ und $n = 3721$

$$1 = \mathrm{ggT}(m, n) = 1164 \cdot m - 2267 \cdot n.$$

[2] Bézout, Étienne, Nemours 1730–1783

Algorithmus 3 Erweiterter Euklidischer Algorithmus

EINGABE: $m, n \in \mathbb{N}$ mit $m > n$

1. $\begin{bmatrix} a_0 & b_0 & c_0 \\ a_1 & b_1 & c_1 \end{bmatrix} := \begin{bmatrix} m & 1 & 0 \\ n & 0 & 1 \end{bmatrix}$

/* stets gilt: $a_i = mb_i + nc_i$ für $i = 0, 1$ sowie $a_0 > a_1 \geq 0$ */

2. $\begin{bmatrix} a_0 & b_0 & c_0 \\ a_1 & b_1 & c_1 \end{bmatrix} := \begin{bmatrix} 0 & 1 \\ 1 & -\lfloor a_0/a_1 \rfloor \end{bmatrix} \begin{bmatrix} a_0 & b_0 & c_0 \\ a_1 & b_1 & c_1 \end{bmatrix}$

3. IF $a_1 \neq 0$ THEN GOTO 2

AUSGABE: (a_0, b_0, c_0) mit $a_0 = \mathrm{ggT}(m, n) = mb_0 + nc_0$

Erweiterter, binärer Euklidischer Algorithmus. Zu $a \in \mathbb{Z}$ sei $\ell(a)$ die Bitlänge von $|a|$. Es gilt $\ell(0) = 1$ und für $a \neq 0$

$$2^{\ell(a)-1} \leq |a| = \sum_{i=0}^{\ell(a)-1} a_i 2^i < 2^{\ell(a)}, a_i \in \{0, 1\}, a_{\ell(a)-1} = 1.$$

Für das Vorzeichen $\mathrm{sign}(a) \in \{\pm 1, 0\}$ gilt $a = \mathrm{sign}(a)\,|a|$.

Algorithmus 4 Erweiterter, binärer Euklidischer Algorithmus

EINGABE: $m, n \in \mathbb{N}$ mit $m > n$

1. $\begin{bmatrix} a_0 & b_0 & c_0 \\ a_1 & b_1 & c_1 \end{bmatrix} := \begin{bmatrix} m & 1 & 0 \\ n & 0 & 1 \end{bmatrix}$

/* stets gilt: $a_i = mb_i + nc_i$ für $i = 1, 2$ sowie $|a_0| > |a_1|$ */

2. $\begin{bmatrix} a_0 & b_0 & c_0 \\ a_1 & b_1 & c_1 \end{bmatrix} := \begin{bmatrix} 0 & 1 \\ 1 & -2^{l\ell(a_0)-\ell(a_1)} \mathrm{sign}(a_0 \cdot a_1) \end{bmatrix} \begin{bmatrix} a_0 & b_0 & c_0 \\ a_1 & b_1 & c_1 \end{bmatrix}$

3. IF $a_1 \neq 0$ THEN GOTO 2

AUSGABE: (a_0, b_0, c_0) mit $a_0 = \mathrm{ggT}(m, n) = mb_0 + nc_0$

Der Algorithmus führt nur Additionen, Subtraktionen und Links-Shifts (Multiplikationen mit 2-er Potenzen) durch. Es treten positive und negative Werte a_0, a_1 auf. Die Anzahl der Iterationen ist durch $\ell(m)$ beschränkt. Die Anzahl der Iterationen ist im Mittel für zufällige m, n nur $\frac{2}{3}\ell(m)$. Denn die binäre Länge $\ell(a_0)$ wird pro Iteration mindestens um 1, in der Hälfte der Fälle aber um 2 erniedrigt. Wichtig ist, dass Addition, Subtraktion und Shift bei geeigneter Zahlendarstellung und Rechnerarchitektur jeweils nur

einen Maschinenzyklus erfordern. Damit ist die Anzahl der Maschinenzyklen des binären Euklidischen Algorithmus durch die Bitlänge der Eingabe beschränkt.

Haben m und n höchstens die Bitlänge k dann geht die Berechnung von $\mathrm{ggT}(n,m)$ in $\mathcal{O}\left(k^2\right)$ Bitoperationen. Die Anzahl der Bitoperationen im Euklidischen Algorithmus kann weiter reduziert werden, indem man vorweg die führenden Bits der Zahlen transformiert und die Transformationsschritte auf den niedrigen Bits gebündelt nachträgt, siehe Schönhage, Proc. ISSAC 91, pp. 128–133, 1991. Beim gebündelten Nachtragen benutzt man die schnelle Multiplikation/Division mittels Fouriertransformation mit $\mathcal{O}(k \log k \log\log k)$ Bitoperationen. Auf diese Weise geht der Euklidische Algorithmus in $\mathcal{O}(k(\log k)^2 \log\log k)$ Bitoperationen. Zusammenfassend kann man sagen, dass der Rechenaufwand zur Berechnung von $\mathrm{ggT}(m,n)$ dieselbe Größenordnung hat wie der zur Berechnung des Produkts $m \cdot n$.

Euklidischer Algorithmus mit Parität.* Algorithmus 5 ist schnell, liefert aber keine explizite Darstellung $\mathrm{ggT}(m,n) = mb + nc$ mit ganzen Zahlen b, c. Algorithmus 5 ist vorteilhaft, wenn die Eingaben m, n nicht explizit gegeben sind, aber auf die Parität von m, n zugegriffen werden kann.

Algorithmus 5 Binärer Euklidischer Algorithmus

EINGABE: $m, n \in \mathbb{N}$ mit $m > n$

1. $k := 0$, $u := m$, $v := n$

2. WHILE u und v gerade DO $u := u/2$, $v := v/2$, $k := k + 1$

3. IF v gerade THEN vertausche u und v

4. WHILE u gerade DO $u := u/2$

5. IF $u < v$ THEN vertausche u und v

6. $u := u - v$

7. IF $u \neq 0$ THEN GOTO 4

AUSGABE: $2^k v = \mathrm{ggT}(m,n)$

Die Division durch 2 bedeutet Verschieben der Bits um eine Position nach rechts. Man nennt diese Operation daher Rechts-Shift. Alle Divisionen des Algorithmus 5 sind Rechts-Shifts. Das Verfahren 5 ist schnell, weil Addition, Subtraktion und Rechts-Shift bei geeigneter Zahlendarstellung und Rechnerarchitektur jeweils nur einen Maschinenzyklus erfordern.

Zur Korrektheit von Algorithmus 5 zeigt man durch Induktion, dass stets $\mathrm{ggT}(n,m) = 2^k \cdot \mathrm{ggT}(u,v)$, im einzelnen:

- es gilt stets $\mathrm{ggT}(n, m) = 2^k \cdot \mathrm{ggT}(u, v)$.
- In Schritt 4 ist u gerade und v ungerade, somit $\mathrm{ggT}(u, v) = \mathrm{ggT}(u/2, v)$.
- In Schritt 6 gilt $\mathrm{ggT}(u, v) = \mathrm{ggT}(u - v, v)$.

Bei Eintritt in Schritt 6 sind u und v ungerade; die Subtraktion $u := u - v$ erzeugt eine gerade Zahl u, so dass anschließend in Schritt 4 ein Rechts-Shift erfolgt. Die ganzen Zahlen u, v sind nicht negativ und nehmen ab. Weil auf jede Subtraktion in Schritt 6 ein Rechts-Shift folgt, gibt es nicht mehr Subtraktionen als Rechts-Shifts.

Satz 1.3
Der binäre Euklidische Algorithmus 5 benötigt bei Eingabe von $n, m \in \mathbb{N}$ mit $0 < m, n < 2^k$ höchstens $2k$ Rechts-Shifts und $2k$ Subtraktionen. Die Zahl der Bitoperationen ist $\mathcal{O}(k^2)$.

Kapitel 2

Kettenbrüche und Kontinuanten

Der Kettenbruchalgorithmus ist eine Variante des Euklidischen Algorithmus. Er liefert zu einer beliebigen reellen Zahl α mit $0 \leq \alpha < 1$ eine Folge ganzer Quotienten $q_1, q_2, \ldots, q_j, \ldots \in \mathbb{N}$ und rationale Näherungsbrüche $\langle q_1, q_2, \ldots, q_j \rangle$ zu α. Die Näherungsbrüche $\langle q_1, q_2, \ldots, q_j \rangle$ minimieren den Fehler $|\alpha - \langle q_1, \ldots, q_j \rangle|$ für rationale Näherungen mit beschränktem Nenner. Kettenbruchnäherungen sind sowohl für Irrationalzahlen als auch für rationale Zahlen nützlich, wenn mit beschränktem Nenner und kleinem Fehler gerechnet werden soll.

Neben dem Kettenbruchalgorithmus mit positiven Quotienten gibt es, analog zum zentrierten Euklidischen Algorithmus, eine zentrierte Variante. Dabei werden die Reste absolut minimiert, es treten auch negative Reste und Quotienten auf. Die Näherungsbrüche im zentrierten Kettenbruchalgorithmus konvergieren schneller.

Die Kontinuanten sind eine Folge von Polynomen, welche die Reste im Euklidischen Algorithmus als Werte der Quotienten darstellen. Sie sind durch eine Rekursion erklärt, ähnlich derjenigen der Fibonacci-Zahlen und haben 'schwache' Symmetrie-eigenschaften.

Regelmäßige Kettenbrüche. Ein regelmäßiger *Kettenbruch* hat folgende Gestalt

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

Algorithmus 6 approximiert eine reelle Zahl α durch eine Folge von Kettenbrüchen $\langle q_1, q_2, \ldots, q_i \rangle, i = 1, 2, \ldots$ mit ganzzahligen Gliedern q_i. Die Glieder $q_i \in \mathbb{N}$ entsprechen den Quotienten, die reellen $\alpha_i, 0 \leq \alpha_i < 1$ den Resten des Euklidischen Algorithmus. Es gilt für $i \geq 2$

$$\alpha = \langle q_1 + \alpha_1 \rangle = \langle q_1, q_2 + \alpha_2 \rangle = \cdots = \langle q_1, \ldots, q_{i-1}, q_i + \alpha_i \rangle \tag{2.1}$$

mit $q_i + \alpha_i = 1/\alpha_{i-1}$, also

$$\alpha = \alpha_0 = \frac{1}{q_1 + \alpha_1} = \frac{1}{q_1 + \dfrac{1}{q_2 + \alpha_2}} = \cdots$$

Algorithmus 6 Kettenbruchentwicklung einer reellen Zahl $0 \leq \alpha < 1$

EINGABE: $\alpha \in \mathbb{R}$ mit $0 \leq \alpha < 1$

1. $\alpha_0 := \alpha, \quad i := 0$

2. WHILE $\alpha_i \neq 0$ DO

$$\alpha_{i+1} := \tfrac{1}{\alpha_i} - \left\lfloor \tfrac{1}{\alpha_i} \right\rfloor, \quad \text{gib } q_{i+1} := \left\lfloor \tfrac{1}{\alpha_i} \right\rfloor \text{ aus}, \quad i := i + 1$$

Die Glieder q_i und Reste α_i im Algorithmus 6 sind nicht negativ, es gilt stets $0 \leq \alpha_i < 1$. In der *zentrierten* Variante von Algorithmus 6 werden $\lfloor \frac{1}{\alpha_i} \rfloor$ und q_{i+1} durch die nächste ganze Zahl $\lceil \frac{1}{\alpha_i} \rfloor$ ersetzt. Es treten dann auch negative α_i, q_i auf. Die zentrierte Variante liefert absolut größere Glieder q_i mit $|q_i| \geq 2$ und absolut kleinere Reste α_i. Bei Eingabe von $\alpha = \frac{n}{m}$ entspricht Verfahren 6 dem Euklidischen Algorithmus zu m, n, die zentrierte Variante entspricht dem zentrierten Euklidischen Algorithmus.

Im Spezialfall $\alpha = 0$ liefert Algorithmus 6 keine Ausgabe. Wir identifizieren den leeren Kettenbruch $\langle\ \rangle$ mit $\alpha = 0$, $0 = \langle\ \rangle$.

Satz 2.1
Die Kettenbruchentwicklung zu α bricht genau dann ab, wenn α rational ist.

Beweis. Wenn die Kettenbruchentwicklung mit $\alpha_j = 0$ abbricht, gilt

$$\alpha = \langle q_1, \ldots, q_j \rangle = \cfrac{1}{q_1 + \cfrac{1}{\ddots \cfrac{}{q_{j-1} + \cfrac{1}{q_j}}}}$$

Wegen $q_1, q_2, \ldots, q_j \in \mathbb{Z}$ gilt $\alpha \in \mathbb{Q}$.

Für rationales $\alpha = \frac{n}{m}$ mit $m > n$ sind die Glieder q_i des Kettenbruchs zu α die Quotienten im Euklidischen Algorithmus zur Eingabe m, n aus Kapitel 1.1. Es gilt daher $\alpha = \langle q_1, \ldots, q_{j+1} \rangle$ für die Iterationszahl j des Euklidischen Algorithmus. □

Kontinuanten. Wir schreiben den Kettenbruch $\langle x_1, \ldots, x_i \rangle$ als gewöhnlichen Bruch

$$\begin{aligned} \langle x_1 \rangle &= \tfrac{1}{x_1} \\ \langle x_1, x_2 \rangle &= \frac{1}{x_1 + \frac{1}{x_2}} = \frac{x_2}{x_1 x_2 + 1} \\ \langle x_1, x_2, x_3 \rangle &= \frac{1}{x_1 + \dfrac{1}{x_2 + \frac{1}{x_3}}} = \frac{1}{x_1 + \frac{x_3}{x_2 x_3 + 1}} = \frac{x_2 x_3 + 1}{x_1 x_2 x_3 + x_1 + x_3} \end{aligned}$$

Die Zähler- und Nenner-Polynome von $\langle x_1, \ldots, x_i \rangle$ heißen *Kontinuanten.*

Definition 2.2
Die Kontinuanten $Q_i \in \mathbb{Z}[x_1, \ldots, x_i]$, $i = 0, 1, \ldots$, *sind die Polynome:*

$$Q_0 = 1,\ Q_1 = x_1$$

$$Q_i(x_1, \ldots, x_i) = x_1 Q_{i-1}(x_2, \ldots, x_i) + Q_{i-2}(x_3, \ldots, x_i) \quad \textit{für } i \geq 2.$$

Die Rekursion der Kontinuanten gleicht derjenigen der Fibonacci-Zahlen, es gilt $Q_i(1, 1, \ldots, 1) = F_i$. Beispiele für Kontinuanten sind:

$$Q_2(x_1, x_2) = x_1 x_2 + 1,\ Q_3(x_1, x_2, x_3) = x_1 x_2 x_3 + x_1 + x_3$$

Lemma 2.3
Für $i = 1, 2, \ldots$ gilt $\langle x_1, \ldots, x_i \rangle = \frac{Q_{i-1}(x_2, \ldots, x_i)}{Q_i(x_1, x_2, \ldots, x_i)}$.

Beweis durch Induktion über i, Induktionsschritt $i - 1 \to i$:

$$\langle x_1, \ldots, x_i \rangle = \frac{1}{x_1 + \langle x_2, \ldots, x_i \rangle}$$

$$= \frac{1}{x_1 + \frac{Q_{i-2}(x_3, \ldots, x_i)}{Q_{i-1}(x_2, \ldots, x_i)}} = \frac{Q_{i-1}(x_2, \ldots, x_i)}{x_1 Q_{i-1}(x_2, \ldots, x_i) + Q_{i-2}(x_3, \ldots, x_i)} \qquad \square$$

Lemma 2.4
$Q_i(x_1, \ldots, x_i)$ ist die Summe der Monome, die aus $x_1 x_2 \cdots x_i$ entsteht, indem man beliebige Paare $x_j x_{j+1}$ herausnimmt.

Das Lemma 2.4 beweist man durch Induktion über i mittels der Rekursionsformel für die Q_i.

Aus Lemma 2.4 folgt $Q_i(x_1, \ldots, x_i) = Q_i(x_i, x_{i-1}, \ldots, x_1)$. Die Kontinuanten sind also schwach symmetrisch. Die Kontinuanten Q_i sind gerade für gerades i und ungerade für ungerades i, d.h. $Q_i(-x_1, \ldots, -x_i) = (-1)^i \cdot Q_i(x_1, \ldots, x_i)$. Die Transformationsmatrix zum Euklidischen Algorithmus mit Quotienten $-x_1, \ldots, -x_i$ hat folgende Form:

Lemma 2.5
Für $i = 1, 2, \ldots$ gilt

a) $$\begin{bmatrix} 0 & 1 \\ 1 & x_1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & x_2 \end{bmatrix} \cdots \begin{bmatrix} 0 & 1 \\ 1 & x_i \end{bmatrix} = \begin{bmatrix} Q_{i-2}(x_2, \ldots, x_{i-1}) & Q_{i-1}(x_2, \ldots, x_i) \\ Q_{i-1}(x_1, \ldots, x_{i-1}) & Q_i(x_1, \ldots, x_i) \end{bmatrix}$$

b) $$\det\left(\begin{bmatrix} 0 & 1 \\ 1 & x_1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & x_2 \end{bmatrix} \cdots \begin{bmatrix} 0 & 1 \\ 1 & x_i \end{bmatrix} \right) = (-1)^i.$$

Beweis. a) Beweis durch Induktion über i:

- $i = 1:$ $\begin{bmatrix} 0 & 1 \\ 1 & x_1 \end{bmatrix} = \begin{bmatrix} Q_{-1} & Q_0 \\ Q_0 & Q_1(x_1) \end{bmatrix}$
- $i \to i + 1:$

$$\begin{bmatrix} Q_{i-3}(x_2, \ldots, x_{i-2}) & Q_{i-2}(x_2, \ldots, x_{i-1}) \\ Q_{i-2}(x_1, \ldots, x_{i-2}) & Q_{i-1}(x_1, \ldots, x_{i-1}) \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & x_i \end{bmatrix}$$
$$= \begin{bmatrix} Q_{i-2}(x_2, \ldots, x_{i-1}) & Q_{i-3}(x_2, \ldots, x_{i-2}) + x_i Q_{i-2}(x_2, \ldots, x_{i-1}) \\ Q_{i-1}(x_1, \ldots, x_{i-1}) & Q_{i-2}(x_1, \ldots, x_{i-2}) + x_i Q_{i-1}(x_1, \ldots, x_{i-1}) \end{bmatrix}$$
$$= \begin{bmatrix} Q_{i-2}(x_2, \ldots, x_{i-1}) & Q_{i-1}(x_2, \ldots, x_{i-1}) \\ Q_{i-1}(x_1, \ldots, x_{i-1}) & Q_i(x_1, \ldots, x_i) \end{bmatrix}$$

b) Die Determinantenfunktion multiplikativ ist. □

Korollar 2.6
Für $q_1, \ldots, q_i \in \mathbf{Z}$ sind $Q_{i-1}(q_1, \ldots, q_i)$ und $Q_i(q_1, \ldots, q_i)$ teilerfremd.

Nach Lemma 2.5 gilt

$$1 \in Q_i(q_1, \ldots, q_i)\mathbf{Z} + Q_{i+1}(q_1, \ldots, q_{i+1})\mathbb{Z}$$

und es folgt die Behauptung des Korollars.

Näherungsgesetze. Es seien $q_1, \ldots, q_i$ die Glieder im regelmäßigen oder im zentrierten Kettenbruch $\alpha = \alpha_0 = \langle q_1, \ldots, q_i + \alpha_i \rangle = \frac{Q_{i-1}(q_2,\ldots,q_i)}{Q_{i+1}(q_1,\ldots,q_i,1/\alpha_i,)}$ zu α mit $0 < \alpha < 1$ und $\alpha = \langle q_1, \ldots, q_i + \alpha_i \rangle = \langle q_1, \ldots, q_i, 1/\alpha_i \rangle$ mit Näherungsbruch

$$\frac{a_i}{b_i} = \langle q_1, \ldots, q_i \rangle = \frac{Q_{i-1}(q_2, \ldots, q_i)}{Q_i(q_1, \ldots, q_i)}$$

Dann gilt nach Lemma 2.5

$$\det \begin{bmatrix} a_{i-1} & a_i \\ b_{i-1} & b_i \end{bmatrix} = a_{i-1}b_i - a_i b_{i-1} = (-1)^i,$$

und

$$\frac{a_i}{b_i} - \frac{a_{i-1}}{b_{i-1}} = \frac{a_i b_{i-1} - a_{i-1} b_i}{b_{i-1} b_i} = \frac{(-1)^{i-1}}{b_{i-1} b_i}.$$

Der Fehler der Näherung $\frac{a_i}{b_i}$ ist damit

$$\begin{aligned} \alpha - \frac{a_i}{b_i} &= \langle q_1, \ldots, q_i, 1/\alpha_i \rangle - \langle q_1, \ldots, q_i \rangle \\ &= \frac{(-1)^i}{b_i \cdot Q_{i+1}(q_1, \ldots, q_i, 1/\alpha_i)} \end{aligned}$$

Nun gilt stets $|Q_{i+1}(q_1, \ldots, q_i, \frac{1}{\alpha_i})| \geq |Q_i(q_1, \ldots, q_i)| = |b_i|$, denn im regelmäßigen Kettenbruch sind alle Glieder positiv und im zentrierten absolut größer gleich 2. Somit erhalten wir:

Satz 2.7 (Näherungsgesetz von Lagrange)
Im regelmäßigen wie im zentrierten Kettenbruch von α gilt für die Näherung $\frac{a_i}{b_i} := \langle q_1, \ldots, q_i \rangle$, dass $|\alpha - \frac{a_i}{b_i}| \leq |b_i|^{-2}$, somit $\alpha = \lim_{i\to\infty} \langle q_1, \ldots, q_i \rangle$.

Wir setzen $\langle q_1, \ldots, q_i, \ldots \rangle =_{def} \lim\limits_{i\to\infty} \langle q_1, \ldots, q_i \rangle$ für $q_1, q_2, \ldots \in \mathbf{N}$. Zur Irrationalzahl $\langle q_1, q_2, \ldots, q_i, \ldots \rangle$ sind die rationalen Zahlen $\langle q_1, \ldots, q_i \rangle$ *Näherungsbrüche.* Zu $\langle q_1, \ldots, q_i \rangle$ sind $\langle q_1, \ldots, q_j \rangle$, $j = 1, \ldots, i$, *Näherungsbrüche.*

Korollar 2.8
Zu jeder Folge $(q_i) \in \mathbb{Z}^{\mathbb{N}}_{\neq 0}$ gibt es eine irrationale Zahl $\alpha = \langle q_1, \ldots, q_i, \ldots \rangle$. Zu jeder irrationalen Zahl α mit $0 < \alpha < 1$ gibt es eine eindeutig bestimmte Folge $(q_i) \in \mathbb{N}^{\mathbb{N}}_{>0}$ mit $\alpha = \langle q_1, \ldots, q_i, \ldots \rangle$.

Beispiele von Kettenbruchentwicklungen. Sei $\phi = \frac{1}{2}(1 + \sqrt{5}) = \frac{A}{B} = \frac{A+B}{A}$ die Zahl des goldenen Schnitts (Übungsaufgabe B.13):

$$\phi = 1 + \langle 1, 1, 1, 1 \ldots . \rangle \qquad \textit{regelmäßig}$$

$$\phi = 2 + \langle -3, 3, -3, 3 \cdots \rangle \qquad \textit{zentriert}$$

Die Eulersche Zahl:

$$e = 2 + \langle 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, 1, 10, \ldots \rangle \qquad \textit{regelmäßig}$$

$$e = 3 + \langle -4, 2, 5, -2, 7, 2, 9, -2, 11, 2, 13, \ldots \rangle \qquad \textit{zentriert}$$

Die Entwicklung von π beginnt mit großen Gliedern:

$$\pi = 3 + \langle 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, 14, 2, 1, 1, \ldots \rangle \qquad \textit{regelmäßig}$$

$$\pi = 3 + \langle 7, 16, -294, -10, -3, \ldots \rangle \qquad \textit{zentriert}$$

Quadratische Irrationalzahlen

$$\sqrt{\tfrac{2}{3}} = \langle 1, \overline{4, 2} \rangle = \langle 1, 4, 2, 4, 2, \cdots \rangle \qquad \textit{regelmäßig}$$

$$\sqrt{\tfrac{2}{3}} = \langle -1, -5, \overline{-2, -4} \rangle \qquad \textit{zentriert}$$

Satz 2.9 (Euler, Lagrange)
Jeder periodische Kettenbruch stellt eine quadratische Irrationalzahl dar (Euler). *Die Kettenbrüche quadratischer Irrationalzahlen sind stets periodisch* (Lagrange).

Den Beweis zu Satz 2.9 findet man in [**?**, Kapitel 24-25]. Die Güte eines Näherungsbruches $\frac{a}{b}$ zu α messen wir durch den Faktor $|\alpha - \frac{a}{b}| \cdot b^2$. Besonders genaue Näherungen $\langle q_1, \ldots, q_i \rangle$ treten auf, wenn ein großes Kettenbruchglied q_{i+1} folgt. Wegen $q_{i+1} = \lfloor \frac{1}{\alpha_i} \rfloor$, bzw $q_{i+1} = \lceil \frac{1}{\alpha_i} \rfloor$ ist dann der Rest α_i und der Approximationsfehler klein. Die regelmäßige Kettenbruchentwicklung $\pi = 3 + \langle 7, 15, 1, 292, 1, \cdots \rangle$ liefert die Näherungsbrüche

$$\pi - \tfrac{22}{7} \approx -0,0049 \cdot 7^{-2}, \ \pi - \tfrac{223}{106} \approx 0,9 \cdot 106^{-2}$$

$$\pi - \tfrac{355}{113} \approx -0,0034 \cdot 113^{-2}.$$

Den vorzüglichen Näherungen $\frac{22}{7}, \frac{355}{113}$ folgen große Glieder $q_2 = 15, q_4 = 292$. Auf die wenig günstige Näherung $\frac{223}{106}$ folgt ein kleines Glied $q_3 = 1$. Alle Näherungen $\frac{a_i}{b_i}$, auf die eine Glied $q_{i+1} = 1$ folgt, werden im zentrierten Kettenbruch übersprungen. Der zentrierte Kettenbruch $\pi = 3 + \langle 7, 16, -294, -10, -3, \cdots \rangle$ liefert die Näherungen $\frac{22}{7}$, $\frac{355}{113}$ und dann $\pi - \frac{10438}{33215} \approx 0,36 \cdot 33215^{-2}$. Die Glieder q_i des zentrierten Kettenbruchs sind absolut größer gleich 2 und im Mittel doppelt so groß wie im regelmäßigen Kettenbruch. Damit liefert die zentrierte Kettenbruchentwicklung eine Auswahl von besonders günstigen Näherungen. Dagegen liefert die regelmäßige Variante eine vollständige Aufzählung aller akzeptablen Näherungen. Nach Legendre treten alle rationalen Approximationen $\frac{a}{b}$ zu α mit Fehler kleiner gleich $\frac{1}{2}b^{-2}$ als Näherungsbrüche in der Kettenbruchentwicklung von α auf, siehe [Pe54, Kapitel 13].

Optimalität der Näherung, Irrationalität von $\sqrt{2}$. Nach dem Näherungsgesetz von Lagrange hat jeder Näherungsbruch $\frac{a}{b}$ zu α die Fehlerschranke $|\alpha - \frac{a}{b}| \leq b^{-2}$. Wir zeigen, dass diese Approximationsgüte für $\alpha = \sqrt{2}$ nahezu optimal ist.

Sei a/b eine beliebige, rationale Näherung von $\sqrt{2}$ mit $|\sqrt{2} + \frac{a}{b}| < 3$. Es folgt

$$|\sqrt{2} - \tfrac{a}{b}| \cdot |\sqrt{2} + \tfrac{a}{b}| = |2 - (\tfrac{a}{b})^2| = |2b^2 - a^2| \cdot \tfrac{1}{b^2} \geq \tfrac{1}{b^2}$$

$$|\sqrt{2} - \tfrac{a}{b}| \geq 1/(|\sqrt{2} + \tfrac{a}{b}| \cdot b^2) \geq 1/(3b^2).$$

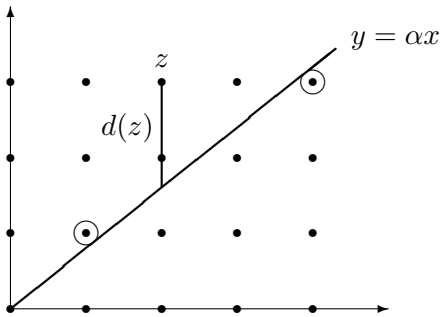
Dabei gilt $2b^2 - a^2 \neq 0$, denn $2b^2 = a^2$ steht im Widerspruch zur eindeutigen Primfaktorzerlegung der ganzen Zahlen. Die Primzahl 2 kommt in $2b^2$ mit ungerader Vielfachheit, in a^2 aber mit gerader Vielfachheit vor. Insbesondere ist $\sqrt{2}$ damit irrational.

Gute Näherung mit Nenner gegebener Größe. Um zu α eine gute Näherung $\frac{p}{q}$ zu finden mit gegebener Größenordnung von p, $q = \mathcal{O}(2^n)$, $|\alpha - \frac{p}{q}| = \mathcal{O}\left(q^{-2}\right)$ geht man wie folgt vor. Man reduziert eine Gitterbasis, bestehend aus den Vektoren $b_0 = (2^{2n}\alpha, 1)$ $b_1 = (2^{2n}, 0)$. Der Reduktionsalgorithmus ist analog zum Euklidischen Algorithmus von Kapitel 1. Das Gitter $L(b_0, b_1)$ hat die Determinante

$$|\det \begin{bmatrix} 2^{2n}\alpha & , & 2^{2n} \\ 1 & , & 0 \end{bmatrix}| = 2^{2n}.$$

Für den kürzesten Gittervektor $\bar{b} = qb_0 - pb_1 \neq 0$ mit $p, q \in \mathbf{Z}$ gilt $\|\bar{b}\|^2 = 2^{4n}(q\alpha - p)^2 + q^2 \leq \sqrt{\frac{4}{3}} \cdot 2^{2n}$ und somit $|\alpha - \frac{p}{q}| \leq (\frac{4}{3})^{1/4} \cdot 2^{-n}|q|^{-1}$ und $|q| \leq (\frac{4}{3})^{1/4} \cdot 2^n$. Insbesondere folgt $2^{-n}(\frac{3}{4})^{1/4} \leq |q|^{-1}$, und somit $|\alpha - \frac{p}{q}| \leq \sqrt{\frac{4}{3}}\, q^{-2}$. Damit liefert der kürzeste Gittervektor eine akzeptable Näherung $\frac{p}{q}$ mit $|q| \leq (\frac{4}{3})^{1/4} \cdot 2^n$. Wenn $\frac{p}{q}$ keine besonders vorzügliche Näherung ist, muss auch der zweite Basisvektor einer reduzierten Basis eine ähnlich gute Näherung liefern. Für die reduzierte Basis b_0, b_1 gilt nämlich $\|b_0\| \cdot \|b_1\| \leq \sqrt{\frac{4}{3}} 2^{2n}$.

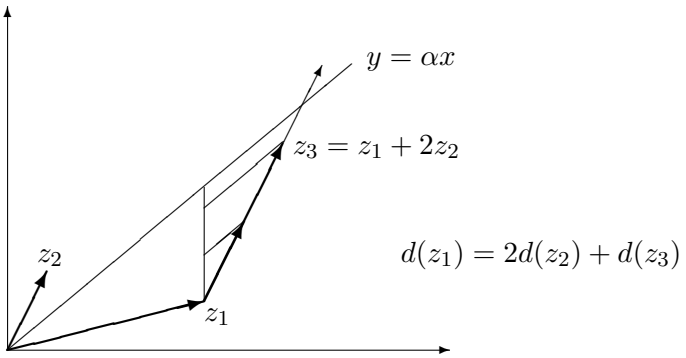
Geometrische Interpretation des Kettenbruchalgorithmus. Gute rationale Näherungen $\frac{a}{b}$ zur reellen Zahl α entsprechen ganzzahlige Punkte $(b, a) \in \mathbf{Z}^2$ in der Zahlenebene mit kleinem Abstand $d(a, b) =_{def} |a - \alpha b|$ zur Gerade $y = \alpha x$.



Zu zwei Näherungen $z_1 = (b_1, a_1), z_2 = (b_2, a_2) \in \mathbb{Z}^2$ berechnet der Kettenbruchalgorithmus die nächste Näherung $z_3 = (b_3, a_3)$ wie folgt: $z_3 := z_1 + qz_2$ für die größte ganze Zahl q so, dass z_3 noch auf derselben Seite der Gerade liegt wie z_1. Für die Abstände $d(z_i)$ von z_i zur Gerade $y = \alpha x$ gilt dann

$$d(z_1) = qd(z_2) + d(z_3),\ 0 \leq d(z_3) < d(z_2).$$

$d(z_3)$ ist also der nicht-negative Rest bei der ganzzahligen Division $d(z_1)/d(z_2)$. Wir zeigen die Situation im Bild



Durch wiederholte Anwendung der Konstruktion entsteht aus den Startwerten $z_{-1} = (1, 0)$ und $z_0 = (0, 1)$ die Folge $\langle q_1, \ldots, q_i \rangle = \frac{a_i}{b_i}$ der Näherungsbrüche zur reellen Zahl α.

Definition 2.10
Ein Bruch $\frac{p}{q}$ *ist* beste Näherung *zu* α*, wenn aus* $\left|\alpha - \frac{\tilde{p}}{\tilde{q}}\right| < \left|\alpha - \frac{p}{q}\right|$ *folgt* $\tilde{q} > q$.

Satz 2.11
Alle Näherungsbrüche zu α *sind beste Näherung zu* α.

Der Beweis findet sich in [**?**, Kapitel 15]. Umgekehrt sind alle beste Näherungen zu α entweder Näherungsbrüche oder „Nebennäherungsbrüche“.

Analogie zum Euklidischen Algorithmus. Wir vergleichen Algorithmus 1 bei Eingabe von m, n mit der Kettenbruchentwicklung von $\frac{n}{m}$. Für $m > n > 0$ liefert die Kettenbruchentwicklung

$$\alpha_0 = \frac{n}{m}, \qquad \alpha_{i+1} = \frac{1}{\alpha_i} - \left\lfloor \frac{1}{\alpha_i} \right\rfloor, \qquad q_{i+1} = \left\lfloor \frac{1}{\alpha_i} \right\rfloor$$

Es entstehen rationale Zahlen $\alpha_i = \frac{n_i}{m_i}$, deren Zähler n_i und Nenner m_i folgende Rekursion erfüllen

$$\alpha_{i+1} = \frac{1}{\alpha_i} - \left\lfloor \frac{1}{\alpha_i} \right\rfloor = \frac{m_i}{n_i} - \left\lfloor \frac{m_i}{n_i} \right\rfloor = \frac{m_i - n_i \lfloor m_i/n_i \rfloor}{n_i} = \frac{n_{i+1}}{m_{i+1}}$$

Also gilt

$$\begin{bmatrix} m_{i+1} \\ n_{i+1} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -\underbrace{\lfloor m_i/n_i \rfloor}_{=q_{i+1}} \end{bmatrix} \begin{bmatrix} m_i \\ n_i \end{bmatrix}, \qquad \begin{bmatrix} m_0 \\ n_0 \end{bmatrix} = \begin{bmatrix} m \\ n \end{bmatrix}$$

Die Rekursion für m_i, n_i liefert das

Lemma 2.12
Der Euklidische Algorithmus zur Eingabe $a_0 = m > a_1 = n$

$$\begin{bmatrix} a_i \\ a_{i+1} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -\lceil a_{i-1}/a_i \rfloor \end{bmatrix} \begin{bmatrix} a_{i-1} \\ a_i \end{bmatrix}$$

liefert $q_i = \lceil a_{i-1}/a_i \rfloor$, die Kettenbruchglieder des regelmässigen Kettenbruchs $\frac{n}{m} = \langle q_1, \ldots, q_i \rangle$. Beide Algorithmen brechen mit $a_i = 0$ ab.

Korollar 2.13
Bricht der erweiterte Euklidischen Algorithmus bei Eingabe von m, n nach j Schritten ab, dann gilt für die Quotienten q_i und die Koeffizienten b_i, c_i
a) $\frac{m}{n} = \langle q_1, \ldots, q_j \rangle = \frac{Q_{j-1}(q_2, \ldots, q_j)}{Q_j(q_1, \ldots, q_j)}$
b) $m = \mathrm{ggT}(n, m) \cdot Q_{j-1}(q_2, \ldots, q_j), \quad n = \mathrm{ggT}(n, m) \cdot Q_j(q_1, \ldots, q_j)$
c) $b_i = (-1)^{i-1} Q_{i-1}(q_2, \ldots, q_i),\ c_i = (-1)^i Q_i(q_1, \ldots, q_i)$ *für* $i \leq j$.

Beweis. a) $\frac{n}{m} = \langle q_1, \ldots, q_j \rangle$.
b) Daher sind $Q_{j-1}(q_2, \ldots, q_j)$ und $Q_j(q_1, \ldots, q_j)$ teilerfremd und a) impliziert b).

c) $$\begin{bmatrix} a_{i+1} & b_{i+1} & c_{i+1} \\ a_{i+2} & b_{i+2} & c_{i+2} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -\underbrace{\lfloor a_{i+1}/a_{i+2} \rfloor}_{q_{i+2}} \end{bmatrix} \begin{bmatrix} a_i & b_i & c_i \\ a_{i+1} & b_{i+1} & c_{i+1} \end{bmatrix}$$

Es folgt

$$\begin{bmatrix} b_i & c_i \\ b_{i+1} & c_{i+1} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -q_{i+1} \end{bmatrix} \cdots \begin{bmatrix} 0 & 1 \\ 1 & -q_1 \end{bmatrix}$$

$$\overset{\text{Lemma 2.5,1.}}{=} \begin{bmatrix} Q_{i-1}(-q_i, \ldots, -q_2) & Q_i(-q_i, \ldots, -q_1) \\ * & * \end{bmatrix}$$

$$\begin{array}{rcccl} b_i & = & Q_{i-1}(-q_2, \ldots, -q_i) & = & (-1)^{i-1} Q_{i-1}(q_2, \ldots, q_i) \\ c_i & = & Q_i(-q_1, \ldots, -q_i) & = & (-1)^i Q_i(q_1, \ldots, q_i) \end{array}$$

- Die Vorzeichen von $b_1, b_2, \ldots, b_i$ und von $c_1, c_2, \ldots, c_i$ alternieren.
- $\operatorname{sign}(b_i) = -\operatorname{sign}(c_i)$ für $i = 1, 2, \ldots$
- $|b_i|, |c_i| \leq |Q_i(q_1, \ldots, q_i)| = \dfrac{m}{\operatorname{ggT}(m,n)}$.

Damit sind alle Zwischenwerte b_i, c_i des erweiterten Euklidischen Algorithmus absolut durch $m/\operatorname{ggT}(m,n)$ beschränkt. □

Literatur

O. Perron Die Lehre von den Kettenbrüchen, Teubner, Stuttgart (1954)

A.Y. Khintchine Continued Fractions P. Nordhoff, Groningen (1963)

M.C. Irwin Geometry of Continued Fractions, Americ. Math. Monthly (1996)

Kapitel 3

Chinesischer Restsatz, Ideale und Faktorringe

Nach dem Chinesischen Restsatz (CRT) kann man die Berechnungsprobleme in kleinere Probleme aufteilen („divide et impera“). Eine spezielle Form des Satzes stammt von Sun Tsu (etwa zwischen 280 und 473 n. Chr.). Die allgemeine Form von Satz 3.1 findet sich im Buch „Shu Shu Chiu Chang“ (1247) von Ch'in Chiu Shao.

Der Chinesischer Restsatz. Für ganze Zahlen a, b, c schreiben wir $a = b \mod c$, wenn $c|(a-b)$, d.h. wenn $a-b \in c\,\mathbb{Z}$. Es bezeichne $[i, j[= \{i, ..., j-1\}$.

Satz 3.1 (CRT)
Seien $m_1, \ldots, m_r \in \mathbb{N}$ teilerfremd, $m := m_1 \cdots m_r$ und $u_1, ..., u_r \in \mathbb{Z}$. Dann hat das Gleichungssystem $x = u_i \mod m_i$ für $i = 1, ..., r$ genau eine Lösung $x \in [0, m[$.

Bem. Nach dem Satz ist $\Psi : [0, m[\to [0, m_1[\times \cdots \times [0, m_r[,\ x \mapsto (u_1, ..., u_r)$ mit $u_i := u \mod m_i$ eine Bijektion. Wegen der Eindeutigkeit der CRT-Lösung x ist Ψ injektiv und wegen der Existenz der Lösung surjektiv (auf).

Beweis. Der Vektor $(e_1, ..., e_r) \in [0, m_1[\times \cdots \times [0, m_r[$ heißt *Basissystem* von Lösungen, wenn $e_i = \delta_{i,j} \mod m_j$ für $1 \le i, j \le r$ und das Kroneckersymbol $\delta_{i,j} := \begin{cases} 1 & \text{falls } i = j \\ 0 & \text{sonst} \end{cases}$.

Das Basissystem liefert für beliebige rechte Seiten $u_1, ..., u_r$ die Lösung

$$x = \sum_{i=1}^{r} e_i u_i \mod m,$$

denn es gilt offenbar $u_i = \sum_{i=1}^{r} e_i u_i \mod m_i$ für $i = 1, ..., r$.

Konstruktion des Basissystems $e_1, \ldots, e_r$. Setze $\overline{m}_i := \prod_{\substack{j=1 \\ j \neq i}}^{r} m_j$. Die Teilerfremdheit der $m_1, ..., m_r$ sichert dass $\mathrm{ggT}(m_i, \overline{m}_i) = 1$. Der erweiterte Euklidische Algorithmus liefert $a_i, \overline{a}_i \in \mathbb{Z}$ mit

$$\mathrm{ggT}(m_i, \overline{m}_i) = 1 = m_i \cdot a_i + \overline{a}_i \cdot \overline{m}_i.$$

Dann folgt für $e_i := 1 - m_i \cdot a_i = \overline{a}_i \cdot \overline{m}_i$ die Behauptung $e_i = \delta_{i,j} \mod m_j$.

Eindeutigkeit der Lösung. Angenommen, das Gleichunggsystems im Satz habe zwei verschiedene Lösungen $x, x' \in [0, m[$. O.B.d.A. sei $x > x'$. Dann gilt $m_i \mid (x - x')$ für $i = 1, 2, \ldots, r$. Die Teilerfremdheit der $m_1, ..., m_r$ sichert $m \mid (x - x')$. Dies ist ein Widerspruch zur Annahme, da $0 < x - x' < m$. □

Betrachten wir als Beispiel die Bijektion $\{0, 1\} \times \{0, 1, 2\} \cong \{0, 1, 2, 3, 4, 5\}$. Sei $m := 2 \cdot 3$.

u	(mod 6)	0	1	2	3	4	5
u	(mod 2)	0	1	0	1	0	1
u	(mod 3)	0	1	2	0	1	2

Als Beispiel zum Chinesischen Restsatz lösen wir ein Kongruenzsystem. Sei $m = 3 \cdot 5 \cdot 7 = 105$. Gesucht ist die ganzzahlige Lösung $x \in [-52, 52]$ mit

$$x = 2 \mod 3 \qquad x = 3 \mod 5 \qquad x = 2 \mod 7.$$

Aus

$$\begin{aligned} m_1 &= 3 & \overline{m}_1 &= m_2 m_3 = 35 \\ m_2 &= 5 & \overline{m}_2 &= m_1 m_3 = 21 \\ m_3 &= 7 & \overline{m}_3 &= m_1 m_3 = 15. \end{aligned}$$

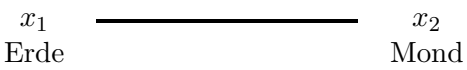
erhalten wir mit dem erweiterten Euklidischen Algorithmus

$$\begin{aligned} 1 &= \mathrm{ggT}(3, 35) = 3 \cdot 12 - 1 \cdot 35 \\ 1 &= \mathrm{ggT}(5, 21) = -5 \cdot 4 + 1 \cdot 21 \\ 1 &= \mathrm{ggT}(7, 15) = -7 \cdot 2 + 1 \cdot 15. \end{aligned}$$

Wir erhalten das Basissystem $(e_1, e_2, e_3) = (-35, 21, 15)$. Die gesuchte Lösung lautet

$$x = 2 \cdot (-35) + 3 \cdot 21 + 2 \cdot 15 = -70 + 63 + 30 = 23 \mod 105.$$

Probabilistischer Gleichheitstest An den Enden eines Kanals stehen ganze Zahlen x_1 und x_2, die auf Gleichheit zu testen sind



mit dem Ziel

- übertrage wenige Bits
- vernachlässigbar kleine Fehlerwahrscheinlichkeit des Tests

Algorithmus 7 Probabilistischer Gleichheitstest

EINGABE: $x_1, x_2 \in \mathbb{N}$ mit $0 \leq x_1, x_2 \leq 2^{10.000}$

1. Wähle zufällige Primzahl p mit $2^{100} < p < 2^{101}$.

2. Übertrage p, sowie x_1 modulo p.

3. IF $x_1 = x_2 \mod p$ THEN entscheide „gleich“
ELSE entscheide „ungleich“

Mit dem CRT wird die Fehlerwahrscheinlichkeit unabhängig von der Eingabe x_1 und x_2. Die Anzahl übertragener Bits ist maximal 202. Wenn wir dagegen an zufälligen Bitpositionen prüfen, ob x_1 und x_2 übereinstimmen, erkennen wir die Ungleichheit nicht, wenn x_1 und x_2 an fast allen Bitpositionen übereinstimmen.

Wir analysieren wir die Fehlerwahrscheinlichkeit des Verfahrens im Fall $x_1 \neq x_2$. Es gilt

$$\#\big\{p \in \big[2^{100}, 2^{101}\big] \,:\, p \text{ Primzahl und } x_1 = x_2 \mod p\big\} < 100.$$

Denn für das Produkt $P := \prod p$ dieser Primzahlen p gilt $x_1 = x_2 \mod P$, somit $P < 2^{10.000}$ und die Anzahl der p ist < 100, sonst wäre $x_1 = x_2$ wegen $0 \leq x_1, x_2 \leq 2^{10.000}$.

Anzahl Primzahlen $p \in [2^{100}, 2^{101}]$. Für die *Primzahlfunktion*

$$\pi(x) =_{\text{def}} \#\{p \,:\, p \leq x \text{ und } p \text{ Primzahl}\}$$

gilt der *Primzahlsatz* (Tschebyscheff-De la Vallée-Poisson)

$$\lim_{x\to\infty} \big[\pi(x) \cdot \tfrac{\ln x}{x}\big] = 1$$

mit Restglied $\big|\pi(x) - \int_2^x \frac{dt}{\ln t}\big| \leq x e^{-\mathcal{O}(\sqrt{\ln x})}$.

Damit gilt approximativ

$$\pi\left(2^{101}\right) - \pi\left(2^{100}\right) \approx \frac{2^{101}}{\ln(2^{101})} - \frac{2^{100}}{\ln(2^{100})} \approx \frac{1}{2} \cdot \frac{2^{101}}{101 \cdot \ln 2} \approx \frac{2^{100}}{70} > 2^{93}$$

Somit beträgt die Fehlerwahrscheinlichkeit $\approx \frac{100}{2^{93}} < 2^{-86}$.

Exakte Lösung ganzzahliger LGS. Das Gauß'sche Eliminationsverfahren zur Lösung ganzzahliger, linearer Gleichungssysteme führt zu extrem großen ganzzahligen Zwischenwerten und ist durch Arithmetik auf den verfügbaren kleinen, ganzen Zahlen i.a. nicht durchführbar. Beim Einsatz von Routinen zur Arithmetik langer ganzer Zahlen wird das Verfahren zu langsam und bei Verwendung von Gleitkomma-Arithmetik zu ungenau.

Wir reduzieren im folgenden die Arithmetik langer, ganzer Zahlen durch modulare Reduktion auf die Arithmetik kleiner ganzer Zahlen. Lediglich zum Zusammensetzen der CRT-Lösung werden einige wenige Schritte mit langen Zahlen gerechnet. Auch hierbei ist die Länge der Zahlen unter Kontrolle. Mit internen Münzwürfen werden ausgeartete Fälle wie singuläre Gleichungen vermieden. Zunächst sei $A \in \mathbb{Z}^{n\times n}$ quadratisch mit $\det A \neq 0$. Wir lösen folgende Aufgabe, dabei sind alle Vektoren in $\mathbb{R}^n$ Spaltenvektoren

Gegeben $A \in \mathbb{Z}^{n\times n}, \quad b \in \mathbb{Z}^n, \quad \det A \neq 0$

Gesucht $x \in \mathbb{Q}^n$ mit $Ax = b$.

Nach der Cramer'schen Regel gilt

$$x_j = \frac{\sum_{\nu=1}^{n} A_{\nu j} \cdot b_\nu}{\det A} \qquad j = 1, 2, \ldots, n$$

Die $A_{\nu,j}$ sind die Adjungierten von $A = [a_{i,j}]_{1\le i,j\le n}$.

$$A_{\nu j} = \det \begin{pmatrix} & & & j & & & \\ a_{1,1} & \cdots & a_{1,j-1} & 0 & a_{1,j+1} & \cdots & a_{1,n} \\ \vdots & & \vdots & 0 & \vdots & & \vdots \\ a_{\nu-1,1} & \cdots & a_{\nu-1,j-1} & 0 & a_{\nu-1,j+1} & \cdots & a_{\nu-1,n} \\ 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\ a_{\nu+1,1} & \cdots & a_{\nu+1,j-1} & 0 & a_{\nu+1,j+1} & \cdots & a_{\nu+1,n} \\ \vdots & & \vdots & 0 & \vdots & & \vdots \\ a_{n,1} & \cdots & a_{n,j-1} & 0 & a_{n,j+1} & \cdots & a_{n,n} \end{pmatrix} \nu$$

Damit genügt es, $\det A$ und $y := x \cdot \det A \in \mathbb{Z}^n$ zu bestimmen. Wir skalieren also x zu einem ganzzahligen y. Man erhält y als die eindeutig bestimmte Lösung von $Ay = b \cdot \det A$, Und wir konstruieren y mittels CRT.

Algorithmus 8 Exakte Lösung eines ganzzahligen LGS

EINGABE: $A \in \mathbb{Z}^{n\times n}$ mit $\det A \neq 0, b \in \mathbb{Z}^n$

1. Wähle zufällige Primzahlen $p_1, ..., p_k$ mit maximaler Bitlänge.

2. FOR $i = 1, 2, \ldots, k$ DO

$D_i := \det A \pmod{p_i}$

IF $D_i = 0$ THEN ersetze p_i durch ein neues p_i.

Löse $A\ y^{(i)} = b\ D_i \bmod p_i$ */es gilt* $y^{(i)} = y \mod p_i$/

3. Bestimme mittels CRT $\overline{D}, \overline{y}_j \in [-\frac{1}{2}P, \frac{1}{2}P[$, $P := p_1 \cdots p_k$ so dass $\overline{D} = D_i \mod p_i$ und $\overline{y}_j = y_j^{(i)} \mod p_i$ für alle $i = 1, ..., k$, $j = 1, ..., n$ / $A\overline{y} = b\overline{D} \mod P$/

4. *Probabilistischer Korrektheitstest.* Wähle zufällige Primzahl p_{k+1}.

IF $A \cdot \overline{y} = b \cdot \overline{D} \mod p_{k+1}$ THEN gib $x := \overline{y}/\overline{D}$ aus
ELSE erhöhe k und gehe zu Schritt **2.**

Erläuterung zum Algorithmus 8. Schritt 1. Die Primzahlen p_i wählt man maximal unter den verfügbaren Zahlen. Hat der Computer die Wortlänge 64, so wählt man die p_i zufällig im Intervall $[2^{63}, 2^{64}[$.

Schritt 2. Bestimmung von D_i und $y^{(i)}$. Mit dem Gauß'schen Eliminationsverfahren bringen wir die Matrix $[A|b]$ modulo p_i auf obere Dreiecksform. Mittels Zeilenoperationen und Spaltenvertauschungen erhalten wir

$$[A \,|\, b] \mapsto [A' \,|\, b'] = \left[\begin{array}{cccc|c} a'_{11} & a'_{12} & \cdots & a'_{1n} & b'_1 \\ 0 & a'_{22} & \cdots & a'_{2n} & b'_2 \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & \cdots & 0 & a'_{nn} & b'_n \end{array}\right].$$

Dann gilt $D_i = a'_{11} \cdots a'_{nn}$. Wir erhalten $y^{(i)} = (y_1^{(i)}, \ldots, y_n^{(i)})$ durch

$$y_n^{(i)} = b'_n/a'_{nn} \mod p_i, \ \ldots, \ y_1^{(i)} = \frac{b'_1 - \sum_{j=2}^{n} a'_{ij} y_j^{(i)}}{a'_{11}} \mod p_i$$

Mache die Vertauschungen der Variablen (Spalten) rückgängig. Es werden $\mathcal{O}(n^3)$ arithmetische Schritte modulo p_i ausgeführt.

Schritt 3. Wir setzen die Lösung mittels CRT zusammen. Konstruiere die Basislösung $(e_1, e_2, \ldots, e_k)$ mit $e_i = \delta_{i,j} \mod p_i$. für $1 \leq i, j \leq k$. Diese ist unabhängig von A, b. Setze

$$\overline{D} := \sum_{i=1}^{k} e_i D_i \mod P, \quad \overline{y} := \sum_{i=1}^{k} e_i y^{(i)} \mod P.$$

Aus $P > 2\max\{|\det A|, |y_1|, |y_2|, \ldots, |y_n|\}$ folgt $\det A, \overline{y}_j \in [-\frac{1}{2}P, \frac{1}{2}P[$ und somit $\overline{D} = \det A$, $\overline{y} = y$. Hierzu werden $\overline{D}, \overline{y}_1, \overline{y}_2, \ldots, \overline{y}_n \in [-\frac{1}{2}P, \frac{1}{2}P[$ als absolut kleinste Residuen modulo P gewählt!

Schritt 4. Für die zufälligen Primzahlen p_{k+1} gilt

$$A\overline{y} = b\overline{D} \mod p_{k+1} \mid A\overline{y} \neq b\overline{D}] = \mathcal{O}\left(\frac{\log p_{k+1} \log ||A\overline{y} - b\overline{D}||}{p_{k+1}}\right).$$

Für zufälliges $A\overline{y} - b\overline{D}$ ist diese Wahrscheinlichkeit sogar proportional zu p_{k+1}^{-n}.

Schrittzahl. Es werden $\mathcal{O}(k)$ arithmetische Schritte modulo P ausgeführt, $\mathcal{O}(n^3)$ arithmetische Schritte modulo p_i für jedes i und eine ggT Berechnung pro p_i. Im Fall $D_i = 0 \pmod{p_i}$ wird die Primzahl p_i verworfen, weil A mod p_i nicht invertierbar ist. Das Produkt aller verworfenen Primzahlen ist $\leq |\det A|$.

Die Variablen $\overline{y}$ und $\overline{D}$ werden bei Erhöhung von k wie folgt aktualisiert.

$$\begin{aligned} P_{\text{neu}} &= P \cdot p_{k+1} \\ \overline{y}_{\text{neu}} &= \left(y^{(k+1)} - \overline{y}\right)\left[P^{-1} \mod p_{k+1}\right] P + \overline{y} \mod P_{\text{neu}} \\ \overline{D}_{\text{neu}} &= \left(D_{k+1} - \overline{D}\right)\left[P^{-1} \mod p_{k+1}\right] P + \overline{D} \mod P_{\text{neu}} \end{aligned}$$

Im allgemeinen Fall ist $A \in \mathbb{Z}^{m\times n}$ und $r := \text{Rang}(A) \leq \min(m, n)$. Im Unterfall $\text{Rang}(A') = r$ für $A' := [a_{ij}]_{1\leq i,j\leq r}$ liefert jede Lösung x' von $A'x' = b'$ eine Lösung $x = (x'_1, ..., x'_r, 0, \ldots, 0) = (x', 0^{n-r})$ zu $Ax = b$.

Den allgemeinen Fall reduziert man wie folgt auf den Unterfall. Wähle zufällige Matrizen $S \in \text{GL}_m(\mathbb{Z})$, $T \in \text{GL}_n(\mathbb{Z})$, wobei die Koeffizienten von S zufällig in $[1, m]$ und die von T zufällig in $[1, n]$ gewählt werden. Für $B := SAT$ gilt $\text{Rang}(A) = \text{Rang}(B)$ und mit großer Wahrscheinlichkeit

$$\text{Rang}(B) = r = \text{Rang}\left(B'\right) \text{ für } B' = [b_{ij}]_{1\leq i,j\leq r}.$$

Löse $B'z' = (Sb)'$ nach $z' \in \mathbb{Z}^r$, setze $z := (z', 0^{n-r})$ und und $x := T^{-1}z$.

Faktorringe und Chinesischer Restsatz in Ringen. Wir drücken den Chinesischen Restsatz in eleganter Weise als Ring-Isomorphismus aus (Satz 3.4) und verallgemeinern ihn anschließend auf allgemeine Ringe (Satz 3.10).

Definition 3.2 (Ring-Homomorphimus)
Seien R, S Ringe mit 1. Die Abbildung $\varphi : R \to S$ ist ein Ring-Homomorphimus, wenn $\varphi(1_R) = 1_S$ und für alle $a, b \in R$ gilt:

$$\begin{aligned} \varphi(a + b) &= \varphi(a) + \varphi(b) \\ \varphi(a \cdot b) &= \varphi(a) \cdot \varphi(b) \end{aligned}$$

Wegen $\varphi(a) = \varphi(a + 0_R) = \varphi(a) + \varphi(0_R)$ folgt $\varphi(0_R) = 0_S$. Ohne die Forderung $\varphi(1_R) = 1_S$ wäre auch die Nullabbildung $\varphi : a \mapsto 0_S$ ein Ring-Homomorphismus. Spezielle Homomorphismen:

1. Falls φ injektiv ist, nennen wir φ einen Monomorphismus.
2. Falls φ surjektiv ist, nennen wir φ einen Epimorphismus.
3. Falls φ bijektiv ist, nennen wir φ einen Isomorphismus.
4. Falls $R = S$ ist, nennen wir φ einen Endomorphismus.
5. Falls φ bijektiv und $R = S$ ist, nennen wir φ einen Automorphismus.

Definition 3.3 (Direktes Produkt)
Das direkte Produkt zweier Ringe R_1 und R_2 ist $R_1 \times R_2$ mit komponentenweiser Addition und Multiplikation (analog zum direkten Produkt von Gruppen):

$$(r_1, r_2) + (s_1, s_2) = (r_1 + s_1, r_2 + s_2)$$
$$(r_1, r_2) \cdot (s_1, s_2) = (r_1 \cdot s_1, r_2 \cdot s_2)$$

Satz 3.4 (Chinesischer Restsatz)
Sei $m = m_1 m_2 \cdots m_r$ Produkt paarweise teilerfremder Zahlen. Dann gilt:

$$\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_r\mathbb{Z}$$

Beweis. Die Abbildung f mit

$$u \bmod m \mapsto (\ u \bmod m_1,\ u \bmod m_2,\ \ldots\ ,\ u \bmod m_r\ )$$

ist ein Ring-Homomorphismus. Nach Bemerkung **??** ist die Abbildung f bijektiv, also ein Ring-Isomorphimus. □

Es seien im folgenden alle Ringe R kommutativ mit 1.

Definition 3.5 (Ideal)
Eine Teilmenge $I \subseteq R$ ist ein Ideal von R, wenn:

a) I ist eine additive Untergruppe von R (also $0_R \in I$ und $i, j \in I \Rightarrow i \pm j \in I$).

b) $IR \subseteq I$ (also $i \in I, r \in R \Rightarrow ir \in I$)

Ideale spielen für Ringe die Rolle der Normalteiler von Gruppen.

Lemma 3.6
Sei $\varphi : R \to S$ ein Ring-Homomorphismus. Dann ist der Kern $\ker(\varphi) := \{a \in R : \varphi(a) = 0_S\}$ *Ideal von R.*

Für den Nachweis seien $a, b \in \ker(\varphi)$ und $r \in R$.

a) Wegen $\varphi(a+b) = \varphi(a) + \varphi(b) = 0_S$ gilt $a + b \in \ker(\varphi)$.

b) Wegen $\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r) \cdot 0_S = 0_S$ gilt $ra \in \ker(\varphi)$.

Lemma 3.7 (Faktorring)
Sei $I \subseteq R$ ein Ideal. Die Restklassen

$$R/I := \{x + I \mid x \in R\}$$

bilden einen Ring, den sog. Faktorring. Die Addition/Multiplikation wird über Repräsentanten erklärt. Nullelement ist I, Einselement ist $1 + I$.

Der Leser überzeuge sich, dass Addition und Multiplikation

$$(x + I) + (y + I) = (x + y) + I$$
$$(x + I) \cdot (y + I) = (x \cdot y) + I$$

wohldefiniert sind. Analog zu Satz A.19 auf Seite 112 zeigt man:

Satz 3.8 (Homomorphiesatz für Ringe)
Sei $g : R \to S$ Ring-Homomorphismus, dann gilt:

a) $\text{Bild}(g) \cong R/\ker(g)$

b) $f : R/\ker(g) \to \text{Bild}(g)$ *mit* $a+\ker(g) \mapsto g(a)$ *ist ein Ring-Isomorphimus.*

Definition 3.9 (teilerfremde Ideale)
Ideale $I_1, I_2 \subseteq R$ heißen teilerfremd, wenn:

$$I_1 + I_2 := \{i_1 + i_2 \mid i_1 \in I_1, i_2 \in I_2\} = R.$$

Es gilt $I_1 + I_2 = R$ genau dann, falls $1 \in I_1 + I_2$.

Satz 3.10
Sei R ein kommutativer Ring mit 1 und $(I_1, I_2, \ldots, I_r) \subseteq R$ paarweise teilerfremde Ideale. Dann gilt:

$$R/\bigcap_{i=1}^{r} I_i \cong R/I_1 \times R/I_2 \times \cdots \times R/I_r$$

Beweis. Es gibt den natürlichen Ring-Homomorphismus:

$$f : x + \bigcap_{i=1}^{r} I_i \quad \mapsto \quad (x + I_1, x + I_2, \ldots, x + I_r) \ \in \ \bigtimes_{i=1}^{r} R/I_i$$

Zur Konstruktion von f^{-1} geben wir ein Basissystem von Lösungen $(e_1, e_2, \ldots, e_r)$ an mit:

$$e_i = \underbrace{\delta_{i,j} \pmod{I_j}}_{\delta_{i,j}+I_j} \qquad 1 \leq i, j \leq r$$

Dann gilt:

$$f^{-1}\left(x_1 \bmod I_1, x_2 \bmod I_2, \ldots, x_r \bmod I_r\right) \ = \ \sum_{i=1}^{r} x_i \cdot e_i \ \left(\bmod \bigcap_{j=1}^{r} I_j \right)$$

wegen $(1 \leq j \leq r)$:

$$\sum_{i=1}^{r} x_i \cdot e_i = \sum_{i=1}^{r} x_i \cdot \delta_{i,j} \pmod{I_j} = x_j \pmod{I_j}$$

Exemplarisch zeigen wir die Konstruktion von e_1: Weil I_1 und I_i teilerfremd sind, gibt es $a_i \in I_1$, $b_i \in I_i$ mit $1 = a_i + b_i$ für $i = 2, 3, \ldots, r$. Setze:

$$e_i := \prod_{i=2}^{r} b_i \ \in \ (I_2 \cdot I_3 \cdots I_r)$$

Korrektheit: Es gilt:

1. $e_1 = 0 \pmod{I_i} \qquad i = 2, 3, \ldots, r$
2. $e_1 = \prod_{i=2}^{r} (1 - a_i) = 1 \pmod{I_1}$

□

Sei $p \in \mathbb{N}$ prim. $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ ist ein Körper mit p Elementen und $\left|\mathbb{Z}_p^*\right| = p - 1$. Der Ring

$$\mathbb{Z}_p[x] := \left\{ f = (f_0, f_1, \ldots, f_n) \in \mathbb{Z}_p^{n+1} \mid n \in \mathbb{N} \right\}$$

heißt Ring der formalen Polynome (Polynomvektoren). Die zugehörige Polynomfunktion ist $\sum_{i=0}^{n} f_i x^i$. Gleichheit in $\mathbb{Z}_p[x]$ ist definiert durch

$$(f_0, f_1, \ldots, f_n) = (g_0, g_1, \ldots, g_m) \qquad \text{mit } n \leq m$$

falls $f_i = g_i$ für $i = 0, 1, \ldots, n$ und $g_i = 0$ für $i > n$. Die Addition erfolgt komponentenweise, die Multiplikation über Konvolution.

$$\operatorname{grad}(f) := \begin{cases} \max\{i \mid f_i \neq 0\} & \text{falls } f \neq 0 \\ -\infty & \text{sonst.} \end{cases}$$

Fakt 3.11
Es gilt für $f, g \in \mathbb{Z}_p[x]$: $\quad \operatorname{grad}(gf) = \operatorname{grad}(f) + \operatorname{grad}(g)$.

In $\mathbb{Z}_p[x]$ gibt es Division mit Rest, d.h. zu $f, g \in \mathbb{Z}_p[x]$ mit $g \neq 0_R$ gibt es eindeutige Darstellung mit $q \in \mathbb{Z}_p[x]$:

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

Damit ist $\mathbb{Z}_p[x]$ ein *Euklidischer Ring*. Der Euklidische Algorithmus von Seite 3 berechnet zu $f, g \in \mathbb{Z}_p[x]$ den $\operatorname{ggT}(f, g)$.

Zu $g \in R$ ist $(g) := g \cdot R$ das von g *erzeugte Ideal*. Wie in Satz A.25 auf Seite 115 zeigt man:

Satz 3.12 (Satz von Bézout)
In $\mathbb{Z}_p[x]$ *ist das von* $\operatorname{ggT}(f, g)$ *erzeugte Ideal gleich* $(f) + (g)$.

Korollar 3.13
Die Ideale $(f), (g) \subseteq \mathbb{Z}_p[x]$ *sind genau dann teilerfremd, wenn* $\operatorname{ggT}(f, g) = 1$.

Korollar 3.14 (Chin. Restsatz in $\mathbb{Z}_p[x]$)
Seien $g, h \in \mathbb{Z}_p[x]$ *mit* $\operatorname{ggT}(g, h) = 1$. *Dann gilt*

$$\mathbb{Z}_p[x]/(gh) \cong \mathbb{Z}_p[x]/(g) \times \mathbb{Z}_p[x]/(h).$$

Berechnung der Euler'schen φ-Funktion. Die Euler'sche φ-Funktion ist erklärt durch $\varphi(n) = |\mathbf{Z}_n^*|$ für $n > 1$ und $\varphi(1) = 1$.

Sei $m = m_1 m_2 \cdots m_r$ das Produkt paarweise teilerfremder Zahlen. Dann gilt:

$$\begin{array}{ccccccccccc} \mathbb{Z}_m^* & \cong & \mathbb{Z}_{m_1}^* & \times & \mathbb{Z}_{m_2}^* & \times & \cdots & \times & \mathbb{Z}_{m_r}^* & & \text{Gruppen} \\ \cap & & \cap & & \cap & & & & \cap & & \\ \mathbb{Z}_m & \cong & \mathbb{Z}_{m_1} & \times & \mathbb{Z}_{m_2} & \times & \cdots & \times & \mathbb{Z}_{m_r} & & \text{Ringe} \end{array}$$

Für die koordinatenweise Multiplikation in $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r}$ gilt

$$a^{-1} \bmod m \quad \longleftrightarrow \quad \left(a^{-1} \bmod m_1, a^{-1} \bmod m_2, \ldots, a^{-1} \bmod m_r\right)$$

Das bedeutet, a hat genau dann ein Inverses modulo m, wenn es modulo $m_1, m_2, \ldots, m_r$ Inverse hat. Es folgt $\varphi(m) = \varphi(m_1) \cdots \varphi(m_r)$.

Satz 3.15
Für die Primfaktorzerlegung $n = \prod_{i=1}^{r} p_i^{e_i}$ *mit* $(e_1, e_2, \ldots, e_r) \geq 1$ *gilt*

$$\varphi(n) = \prod_{i=1}^{r} \varphi\left(p_i^{e_i}\right) = \prod_{i=1}^{r} p_i^{e_i-1}(p_i - 1) = \prod_{i=1}^{r} p_i^{e_i}(1 - p_i^{-e_i})$$

Beweis. Für eine Primzahlpotenz p^e gilt

$$\mathrm{ggT}\,(a, p^e) \in \{1, p, p^2, \ldots, p^e\}.$$

Daher ist in $1, 2, \ldots, p^e$ nur jede p-te Zahl Vielfaches von p. Wir erhalten

$$\varphi\left(p^e\right) = \#\{a \,:\, 0 < a < p^e \text{ und } p \not| \, a\} = p^e - p^{e-1} = p^{e-1}\,(p-1)$$

□

Primitve Elemente.

Satz 3.16 (Euler, Legendre)
Für jede Primzahl p *ist* $\mathbb{Z}_p^*$ *zyklisch, d.h. es existiert* $a \in \mathbb{Z}_p^*$ *mit* $\mathrm{ord}\,(a) = p - 1$. *Also gilt* $\mathbb{Z}_p = \left\{1 = a^0, a^1, a^2, \ldots, a^{p-2}\right\}$.

Wir werden folgendes Lemma später beweisen (Korollar 4.5 auf Seite 36):

Lemma 3.17
In jeder endlichen abelschen Gruppe G *gilt*

$$\begin{aligned}\mathrm{kgV}\left\{\mathrm{ord}\,(a) \mid a \in G\right\} &= \max\left\{\mathrm{ord}\,(a) \mid a \in G\right\} \\ &= \min\left\{k \in \mathbb{N} \;\middle|\; a^k = 1_G \text{ für alle } a \in G\right\}.\end{aligned}$$

Beweis (zu Satz 3.16). Betrachte die Carmichael-Funktion

$$\lambda(n) := \max\left\{\mathrm{ord}\,(a) \mid a \in \mathbb{Z}_n^*\right\}.$$

Nach dem Lemma gilt $a^{\lambda(p)} = 1$ für alle $a \in \mathbb{Z}_p^*$. Das Polynom $x^{\lambda(p)} - 1$ hat im Körper $\mathbb{Z}_p$ $p-1$ Nullstellen, nämlich alle $a \in \mathbb{Z}_p^*$. Weil $\mathbb{Z}_p$ ein Körper ist, folgt $\mathrm{grad}\left(x^{\lambda(p)} - 1\right) \geq p - 1$, also $\lambda(p) \geq p - 1$.
Wegen $\lambda(p) \mid \varphi(p) = p - 1$ folgt $\lambda(p) = p - 1$. □

Bezeichnung 3.18
Ein Element $a \in \mathbb{Z}_p^*$ *heißt* primitiv, *wenn* $\mathrm{ord}\,(a) = p - 1$.

Der Beweis zu Satz 3.16 gibt keinen Hinweis auf die Konstruktion eines primitiven Elementes in $\mathbb{Z}_p^*$. In Übungsaufgabe B.17 wird gezeigt, daß es $\varphi(p-1)$ viele primitive Elemente in $\mathbb{Z}_p^*$ gibt. Ihr Anteil ist daher:

$$\frac{\varphi(p-1)}{(p-1)} = \Omega\left(\frac{1}{\log p}\right)$$

Um primitive Elemente probabilistisch schnell zu erzeugen, genügt ein effektiver Primitivitätstest. Ist die Primfaktorzerlegung von $p-1$ bekannt, so liefert Lemma 4.7 einen solchen effektiven Test.

Kapitel 4

RSA-Chiffrierschema und die Struktur von $\mathbb{Z}_N^*$

4.1 Symmetrische Chiffrierschemata

Es sei K eine Menge von Schlüsseln und M eine Menge von Nachrichten mit zwei Abbildungen

$$E, D \ : \quad K \times M \to M$$

so daß

$$E_k D_k = D_k E_k = \mathrm{id}_M \qquad \text{für alle } k \in K.$$

Jeder Schlüssel $k \in K$ liefert also eine Permutation $E_k = E(k, \cdot)$ und $D_k = D(k, \cdot)$ auf M, die zueinander invers sind. E ist die Kodier- und D die Dekodierabbildung. Der Schlüssel k wird gleichermaßen zum Kodieren und Dekodieren benutzt.
Beispiele: DES, AES (beide von der NSA), one time pad.

4.2 Asymmetrische Chiffrierschemata

Rivest, Shamir und Adleman haben 1978 ein Chiffrierschema vorgestellt [RSA78], bei dem der Kodierschlüssel k öffentlich, der Dekodierschlüssel k' jedoch geheim ist. Die Zuordnung $k \mapsto k'$ muß „schwer“ berechenbar sein.

Der *Modul* N ist das Produkt zweier Zufallsprimzahlen P_1, P_2, die so groß sind, daß das Produkt $N = P_1 \cdot P_2$ mit bekannten Methoden und heutiger Technologie nicht zerlegt werden kann. Es muß mindestens gelten, daß $P_1, P_2 \geq 2^{1024}$. Die Zahlen $P_1 \pm 1$, $P_2 \pm 1$ müssen paarweise verschiedene Primfaktoren $\geq 2^{100}$ besitzen (vergleiche Übungsaufgabe B.30).

Die *Nachrichtenmenge* ist $\mathbb{Z}_N = \{0, 1, \ldots, N-1\}$. Nachrichten beliebiger Länge werden in Bitfolgen der Länge $\leq \log_2 N$ zerlegt und als Folgen über $\mathbb{Z}_N$ umgeschrieben. Jeder Teilnehmer hat einen ihm eigenen öffentlichen/geheimen Schlüssel (N, e, d).

Öffentlicher Schlüssel (N, e) mit $N = P_1 \cdot P_2$ für geheime Primzahlen P_1, P_2 und $1 < e < \varphi(N)$ mit $\mathrm{ggT}(e, \varphi(N)) = 1$,
so dass die Zerlegung von N schwierig ist.

Kodieren: $E : \mathbb{Z}_N \to \mathbb{Z}_N,\ E(x) = x^e \pmod N$

Geheimer Schlüssel $d = e^{-1} \bmod \varphi(N)$
(äquivalent $\varphi(N) = (P_1 - 1)(P_2 - 1)$ oder P_1, P_2).

Dekodieren: $D : \mathbb{Z}_N \mapsto \mathbb{Z}_N,\ D(y) = y^d \pmod N$

Notwendig: Die Zahl e darf klein sein, aber $d > N^{\frac{1}{4}}$ ist nach Wiener [W90] zur Sicherheit notwendig.
Wir zeigen, dass man E mittels d invertieren kann. Offen ist dagegen, ob die Invertierung auch ohne d möglich ist.

Lemma 4.1 (Legendre)
$(x^e)^d = (x^d)^e = x \bmod N$

Beweis. Nach Konstruktion von e und d gilt:

$$e \cdot d = 1 + \nu\varphi(N) \qquad \text{mit } \nu \in \mathbb{Z}.$$

Nach Legendre (Korollar A.27) gilt für alle $x \in \mathbb{Z}_N^*$:

$$x^{e \cdot d} = x^{1+\nu\varphi(N)} = x \pmod N$$

Wir erweitern dies zu

$$x^{1+\nu\varphi(N)} = x \pmod N \qquad \text{für alle } x \in \mathbb{Z}_N$$

Die Behautung folgt aus der Isomorphie

$$\begin{array}{rcl} \mathbb{Z}_N & \cong & \mathbb{Z}_{P_1} \times \mathbb{Z}_{P_2} \\ x & \longleftrightarrow & (x \bmod P_1, x \bmod P_2) \end{array}$$

und $x^{1+\nu\varphi(N)} = x \pmod{P_i}$ für alle $x \in \mathbb{Z}_{P_i}$ und $i = 1, 2$. Letztere Gleichung folgt für $x \neq 0 \bmod P_i$ aus dem Satz von Fermat (Korollar A.27) und für $x = 0 \pmod{P_i}$ gilt die Gleichung offensichtlich. □

Für beliebige quadratfreie N gilt nach obigem Beweis

$$x^{1+\nu\varphi(N)} \equiv x \pmod{N} \qquad \text{für alle } x \in \mathbb{Z}_N.$$

Kenntnis der Zerlegung P_1, P_2 von N ist äquivalent zur Kenntnis von

$$\varphi(N) = (P_1 - 1)(P_2 - 1).$$

Denn aus $\varphi(N)$ erhält man P_1, P_2 durch Auflösen der Gleichungen:

$$\begin{aligned} P_1 + P_2 &= N - \varphi(N) + 1 \\ P_1 - P_2 &= \sqrt{(P_1 + P_2)^2 - 4N}. \end{aligned}$$

RSA Signatur. Der Schlüssel sei (N, e, d).
Signatur zur Nachricht $m \in \mathbb{Z}_N$: $m^d \pmod{N_A}$
Verifikation $m = (m^d)^e \bmod N$.
Die Signatur liefert den Ursprungsnachweis zur Nachricht m. Ist die Signatur sicher (unfälschbar), dann ist der Ursprungsnachweis non repudiable.

Definition 4.2
Die Carmichael Funktion $\lambda : \mathbb{N} \to \mathbb{N}$ *sei* $\lambda(1) = 1$ *und für* $N > 1$*:*

$$\lambda(N) = \min\left\{k \in \mathbb{N} \setminus \{0\} \,:\, x^k = 1 \pmod{N} \text{ für alle } x \in \mathbb{Z}_N^*\right\}.$$

Im RSA-Schema mit öffentlichem Schlüssel (N, e) kann man dekodieren mittels $\overline{d} = e^{-1} \bmod \lambda(N)$. Es gilt nämlich für $x \in \mathbb{Z}_N^*$

$$x^{\lambda(N)} = 1 \bmod N$$

und somit $x^{e\overline{d}} = x^{1+\nu\lambda(N)} = x \pmod{N}$.

Lemma 4.3
Für alle $N \in \mathbb{N}$ *gilt* $\lambda(N) \mid \varphi(N)$.

Beweis. Division mit Rest liefert

$$\varphi(N) = s\lambda(N) + r \qquad \text{mit } 0 \le r < \lambda(N).$$

Aus $x^{\varphi(N)} = x^{\lambda(N)} = 1 \pmod{N}$ für alle $x \in \mathbb{Z}_N^*$ folgt $x^r = 1 \pmod{N}$ für alle $x \in \mathbb{Z}_N^*$. Wegen der Minimalität von $\lambda(N)$ folgt $r = 0$ und somit die Behauptung. □

Für die Sicherheit des RSA-Schemas muß $\lambda(N)$ groß sein. Wir wollen nun $\lambda(N)$ bestimmen.

Lemma 4.4
Zu jeder endlichen, abelschen Gruppe G gibt es zu $a, b \in G$ ein $c \in G$ mit

$$\operatorname{ord}(c) = \operatorname{kgV}(\operatorname{ord}(a), \operatorname{ord}(b)).$$

Beweis. Nach Übungsaufgabe B.6 angewandt auf die Gruppe $H = \langle a \rangle$ gilt

$$\operatorname{ord}\left(a^k\right) = \tfrac{\operatorname{ord}(a)}{\operatorname{ggT}(\operatorname{ord}(a),k)}$$

Für $\overline{a} = a^{\operatorname{ord}(b)}$ folgt:

$$\operatorname{ggT}(\operatorname{ord}(\overline{a}), \operatorname{ord}(b)) = \operatorname{ggT}\left(\tfrac{\operatorname{ord}(a)}{\operatorname{ggT}(\operatorname{ord}(a),\operatorname{ord}(b))}, \operatorname{ord}(b)\right) = 1$$

Es folgt $\langle \overline{a} \rangle \cap \langle b \rangle = \{1_G\}$ und $\langle \overline{a} \rangle \times \langle b \rangle \cong \langle \overline{a} b \rangle$, somit

$$\begin{aligned} \operatorname{ord}(\overline{a}b) &= \operatorname{ord}(\overline{a}) \cdot \operatorname{ord}(b) \\ &= \operatorname{kgV}(\operatorname{ord}(a), \operatorname{ord}(b)) \end{aligned}$$

□

Korollar 4.5
Für jede endliche abelsche Gruppe gilt

$$\begin{aligned} \operatorname{kgV}\{\operatorname{ord}(a) \mid a \in G\} &= \max\{\operatorname{ord}(a) \mid a \in G\} \\ &= \min\left\{k \in \mathbb{N} \;\middle|\; a^k = 1_G \text{ für alle } a \in G\right\} \end{aligned}$$

In Lemma 4.4 liegt ein direktes Produkt von Gruppen mit Isomorphismus f vor:

$$\begin{aligned} <\overline{a}b> &\cong <\overline{a}> \times <b> \\ f:\ c &\mapsto \left(c^{\operatorname{ord} b}, c^{\operatorname{ord}\overline{a}}\right) \end{aligned}$$

Iteration dieser direkten Produkt-Zerlegung führt zum

Korollar 4.6 (Hauptsatz für endliche abelsche Gruppen)
Jede endliche, zyklische, abelsche Gruppe G ist isomorph zu einem direkten Produkt $\mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{e_r}\mathbb{Z}$ von Gruppen mit Primzahlpotenz-Ordnung $p_i^{e_i}$. Für zyklisches G ist dabei $\prod_{i=1}^r p_i^{e_i} = |G|$ die Primfaktorzerlegung von $|G|$.

Zur Sicherheit des RSA-Scheams müssen $P_1 - 1$ und $P_2 - 1$ „grobkörnig“ sein, d.h. $q_i \mid (P_i - 1),\ \ i = 1, 2$ für verschiedene große Primzahlen q_i. Im speziellen Fall $\operatorname{ggT}(\ (P_1 - 1)/2, (P_2 - 1)/2\ ) = 1$ gilt

$$\begin{aligned} \lambda(N) &= \operatorname{kgV}(\lambda(P_1), \lambda(P_2)) = \operatorname{kgV}(P_1 - 1, P_2 - 1) \\ &= \tfrac{1}{2}(P_1 - 1)(P_2 - 1) = \tfrac{1}{2}\varphi(N) \end{aligned}$$

Lemma 4.7
Es sei p prim und $p-1 = \prod_{i=1}^{r} p_i^{e_i}$ die Primfaktorzerlegung von $p-1$. Genau dann ist $a \in \mathbb{Z}_p^*$ primitiv, wenn $a^{\frac{(p-1)}{p_i}} \neq 1 \pmod{p}$ für $i = 1, \ldots, r$.

Beweis. Aus $a^{\frac{(p-1)}{p_i}} \neq 1 \pmod{p}$ folgt $p_i^{e_i} \mid \mathrm{ord}(a)$. Es folgt $\prod_i p_i^{e_i} \mid \mathrm{ord}(a)$ und somit $\mathrm{ord}(a) = p-1$. □

Wir geben die Struktur der Gruppe $\mathbb{Z}_{p^e}^*$ vollständig an. Nach dem Chinesischen Restsatz ist damit auch die Struktur der Gruppe $\mathbb{Z}_N^*$ für beliebige $N \in \mathbb{N}$ vollständig bestimmt.

Satz 4.8
1. *Für jede ungerade Primzahl p und $e \geq 1$ ist $\mathbb{Z}_{p^e}^*$ zyklisch.*
2. *$\mathbb{Z}_{2^r}^* \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{r-2}}$ für $r \geq 3$.*

Beweis. 1. Für $e = 1$ gilt die Behauptung nach Satz 3.16 auf Seite 31. Fall $e = 2$. Es bezeichne ord_p bzw. ord_{p^2} die Ordnung in $\mathbb{Z}_p^*$ bzw. $\mathbb{Z}_{p^2}^*$.

Zu $y \in \{1, 2, \ldots, p-1\}$ mit $\mathrm{ord}_p(y) = p-1$ bestimmen wir $x \in \mathbb{Z}$ mit $\mathrm{ord}_{p^2}(y + xp) = p(p-1)$. Es gilt:

$$p-1 \mid \mathrm{ord}_{p^2}(y+xp) \qquad \text{für alle } x \in \mathbb{Z}$$

Denn es folgt aus $(y+xp)^r = 1 \bmod p^2$, daß $y^r = 1 \bmod p$ und somit $p-1 \mid r$.

Nun ist $\mathrm{ord}_{p^2}(y+xp) = p(p-1)$ äquivalent zu $(y+xp)^{p-1} \neq 1 \bmod p^2$. Es gilt:

$$\begin{aligned}(y+xp)^{p-1} &= y^{p-1} + y^{p-2}xp(p-1) \pmod{p^2} \\ &= y^{p-1} + y^{p-2}xp \pmod{p^2}\end{aligned}$$

Es gibt mindestens $p-1$ viele $x \in \{0, 1, \ldots, p-1\}$ mit:

$$y^{p-1} + y^{p-2}xp \neq 1 \pmod{p^2}$$

Für diese x gilt $\mathrm{ord}_{p^2}(y+xp) = p(p-1)$.

Fall $e \geq 2$. Wir zeigen, daß $ord_{p^e}(y) = \varphi(p^e)$ bereits $\mathrm{ord}_{p^{e+1}}(y) = \varphi(p^{e+1})$ impliziert. Zur Übung beweist man die

Behauptung:

$$z = 1 \bmod p^e,\ z \neq 1 \bmod p^{e+1} \qquad \Longrightarrow \qquad z^p = 1 \bmod p^{e+1},\ z^p \neq 1 \bmod p^{e+2}$$

Sei $\mathrm{ord}_{p^e}(y) = \varphi(p^e)$ und $z = y^{\varphi(p^e)/p}$, wobei $\frac{\varphi(p^e)}{p} = \varphi(p^{e-1})$. Dann gilt $z = 1 \bmod p^{e-1}$, aber $z \neq 1 \bmod p^e$. Diese Behauptung liefert $y^{\varphi(p^e)} \neq 1 \pmod{p^{e+1}}$ und folglich $\mathrm{ord}_{p^{e+1}}(y) = \varphi(p^{e+1})$.

2. Wir zeigen für $r \geq 3$:

$$\operatorname{ord}_{2^r}(5) = 2^{r-2} \tag{4.1}$$

und

$$\mathbb{Z}_{2^r}^* = \left\{ \pm 5^j \pmod{2^r} \ : \ j = 1, 2, \ldots, 2^{r-2} \right\} \tag{4.2}$$

Gleichung (4.1) gilt wegen

$$5^{2^{r-3}} = (1+4)^{2^{r-3}} = 1+2^{r-3}\cdot 4 \pmod{2^r} = 1+2^{r-1} \pmod{2^r} \neq 1 \bmod 2^r$$

Gleichung (4.2) folgt jetzt aus

$$-1 \neq 5^j \pmod{2^r} \qquad \text{für } j = 1, 2, \ldots, 2^{r-2}$$

Diese Ungleichheiten gelten aber wegen

$$5^j = \begin{cases} 5 \bmod 8 & \text{falls } j \text{ ungerade} \\ 1 \bmod 8 & \text{falls } j \text{ gerade} \end{cases}$$

Aus (4.2) folgt unmittelbar die Isomorphie $\mathbb{Z}_{2^r}^* \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{r-2}}$. □

Korollar 4.9
Für ungerades $N = \prod_{i=1}^{r} p_i^{e_i}$ *gilt:* $\lambda(N) = \operatorname{kgV}\left\{ p_i^{e_i-1}(p_i - 1) \ : \ i = 1, 2, \ldots, r \right\}$.

Beweis. Aus der Isomorphie

$$\mathbb{Z}_N^* \cong \mathbb{Z}_{p_1^{e_1}}^* \ \times \ \cdots \ \times \ \mathbb{Z}_{p_r^{e_r}}^*$$

und Lemma 4.4 schließt man:

$$\lambda(N) = \operatorname{kgV}\left\{ \lambda(p_i^{e_i}) \ : \ i = 1, 2, \ldots, r \right\}$$

Die Behauptung folgt aus Satz 4.8. □

Man wählt den RSA-Modul $N = P_1 \cdot P_2$ so, daß $\operatorname{ggT}(P_1 - 1, P_2 - 1) = 2$. Dann gilt $\lambda(N) = \frac{1}{2}\varphi(N)$. Es gibt dann neben dem Dekodierexponenten d nur noch einen zweiten Dekodierexponenten

$$d \pm \lambda(N) \quad \in \{0, 1, \ldots, \varphi(N) - 1\}$$

4.3 $*$ Pseudoprimzahlen und Carmichael-Zahlen

Zum RSA-Schema benötigt man große zufällige Primzahlen. Weil die Primzahlen $\leq N$ etwa die Dichte $\frac{1}{\log N}$ haben, genügt ein effektiver Primheitstest.

Für jede Primzahl p gilt die *Fermat-Identität* $a^{p-1} = 1 \mod p$ für alle $a \in \mathbb{Z}_p^*$.

N heißt *Pseudoprimzahl* zur Basis a, wenn N zusammengesetzt ist mit $a^{N-1} = 1 \pmod N$. Pseudoprimzahlen treten nur selten auf. Die Aussage $a^{N-1} = 1 \mod N$ für alle $a \in \mathbb{Z}_N^*$ kann man probabilistisch einfach testen. Die $a \in \mathbb{ZZ}^*$ welche die Fermat-Identität erfüllen, bilden eine Untergruppe

$$\{a \in \mathbb{Z}_N^* \,:\, a^{N-1} = 1 \pmod N\} \quad \overset{\text{Untergruppe}}{\subseteq} \quad \mathbb{Z}_N^*.$$

Die Ordnung dieser Untergruppe ist entweder $\varphi(N)$ oder höchstens $\frac{1}{2}\varphi(N)$.

Korollar 4.10
Gibt es zu $N \in \mathbb{N}$ ein $a \in \mathbb{Z}_N^*$ mit $a^{N-1} \neq 1 \pmod N$ dann gilt für zufällige, unabhängige $a_1, \ldots, a_r \in \mathbb{Z}_N^*$

$$\mathrm{Ws}\Big[a_i^{N-1} = 1 \pmod N \quad \textit{für } i = 1, 2, \ldots, r\Big] \leq 2^{-r}.$$

Definition 4.11
Eine zusammengesetzte Zahl N mit $\lambda(N) \mid N-1$ heißt Carmichael-Zahl.

Die Zusammengesetztheit von Nicht-Carmichael-Zahlen erkennt der r-fache Fermat-Test von Korollar 4.10 mit Wahrscheinlichkeit $\geq 1 - 2^r$. Der Fermat-Test kann die Zusammengesetztheit von Carmichael-Zahlen nicht erkennen. Dennoch ist der Fermat-Test für praktische Anwendungen ausreichend sicher, Carmichael-Zahlen sind nämlich sehr selten. Pomerance (1991) beschränkt die Dichte $C(x)$ der Carmichaelzahlen kleiner gleich x durch $C(x) < x^{1-\ln\ln\ln x/\ln\ln x}$ für hinreichend grosse x. Andererseits gibt es unendlich viele Carmichael-Zahlen mit Dichte $C(x) > x^{2/7}$ für hinreichend grosse x.

Satz 4.12
1. Jede Carmichael-Zahl N ist Produkt von $r \geq 3$ verschiedenen, ungeraden Primzahlen, $N = p_1 p_2 \cdots p_r$.
2. $N = p_1 p_2 \cdots p_r$ ist genau dann Carmichael–Zahl, wenn

$$(p_j - 1) \mid (\tfrac{N}{p_j} - 1) \qquad \textit{für } j = 1, 2, \ldots, r.$$

Beweis. 1. $N = \prod_{i=1}^r p_i^{e_i}$ ist genau dann Carmichael-Zahl, wenn

$$p_i^{e_i - 1}(p_i - 1) \mid N - 1 \qquad \text{für } i = 1, 2, \ldots, r.$$

Aus $\mathrm{ggT}(p_i, N-1) = 1$ folgt $e_i = 1$, also $N = p_1 p_2 \cdots p_r$.

Im Fall $r = 2$ und $p_1 < p_2$ gilt

$$(p_2 - 1) \mid (p_1 p_2 - 1), \qquad p_1 p_2 - 1 = p_1(p_2 - 1) + (p_1 - 1),$$

und somit $(p_2 - 1) \mid (p_1 - 1)$, Widerspruch.
Ferner ist jede Carmichael-Zahl $N = p_1 p_2 \cdots p_r$ ungerade, denn gerades N schließt $p - 1 \mid N - 1$ für ungerades p aus.

2. Aus $N - 1 = \left(\frac{N}{p_j} - 1\right) p_j + p_j - 1$ folgt

$$p_j - 1 \mid N - 1 \quad \Longleftrightarrow \quad p_j - 1 \mid (\tfrac{N}{p_j} - 1). \qquad \square$$

4.4 Der Primzahltest von Miller-Rabin

Der Miller-Rabin Test erweitert den Fermattest auf Carmichaelzahlen.

Lemma 4.13
Für primes $P > 2$, $P - 1 = 2^k Q$, Q ungerade gilt für alle $a \in \mathbb{Z}_P^*$

$$a^Q = 1 \pmod P \qquad \vee \qquad \exists\, i < k \,:\, a^{Q2^i} = -1 \pmod P.$$

Beweis. Jede Restklasse $a \bmod P$ hat höchstens zwei Quadratwurzeln, denn das Polynom $x^2 - a$ hat im Körper $\mathbb{Z}_P$ höchstens zwei Nullstellen. Die Quadratwurzeln von $1 \pmod P$ sind $\pm 1 \pmod P$. $\square$

Satz 4.14
$N \in \mathbb{N}$ habe ≥ 2 Prinfaktoren, sei ungerade, $N - 1 = 2^k Q$, mit Q ungerade. Dann gilt für zufällige $a \in \mathbb{Z}_N^*$ [K81, Aufgabe 4.5.4 (22)]

$$\mathrm{Ws}\Big[a^Q = 1 \pmod N \;\vee\; \exists\, i < k \,:\, a^{2^i Q} = -1 \pmod N\Big] \leq \tfrac{1}{4}.$$

Sei $N - 1 = 2^k Q$, Q ungerade, dann nennt man $a \in \mathbb{Z}_N^*$ mit

$$a^Q \neq 1 \bmod N \;\wedge\; \forall\, i < k \,:\, a^{2^i Q} \neq -1 \bmod N$$

einen *Zeugen* für die Zusammengesetztheit von N.

Definition 4.15
Es sei $\mathcal{R}$ die Klasse der Sprachen $L \subseteq \{0,1\}^*$, für die es einen Polynomial-Zeit-Algorithmus gibt, der zu $x \in L$ mit Wahrscheinlichkeit mindestens $\frac{1}{2}$ einen Beweis für „$x \in L$“ findet.

Mit dem Miller-Rabin Test kann man die Zusammengesetztheit einer nicht primen Zahl N mit Wahrscheinlichkeit mindestens $\frac{3}{4}$ in polynomial-zeit beweisen. Die Menge der zusammengesetzten Zahlen ist damit in $\mathcal{R}$. Umgekehrt zeigen Adleman, Huang (1992) dass man zu gegebener Primzahl einen Primalitätsbeweis in polynomial-zeit erwürfeln kann. Zum Erwürfeln eines Primalitätsbeweises konstruiert man geeignete elliptische Kurven, die

Beweisskizze von Adleman, Huang ist 140 Seiten lang. Schließlich wurde ein polynomial-zeit deterministischer Primaltätstest gefunden:

Satz 4.16 (Agrawal, Kayal, Saxena 2002)
Die Menge der Primzahlen ist in polynomial-zeit entscheidbar.

Es gibt einfache, praktische Verfahren, um große Primzahlen zu erzeugen. Man baut große Primzahlen iterativ aus kleinen Primzahlen zusammen.

Lemma 4.17
Seien $p_1, \ldots, p_r$ prim und $p = 1 + \prod_{i=1}^{r} p_i^{e_i}$. Aus

$$a_i^{(p-1)/p_i} \neq 1 \pmod{p}, \qquad a_i^{p-1} = 1 \pmod{p} \qquad \text{für } i = 1, 2, \ldots, r$$

folgt, daß p prim ist.

Beweis. $a_i^{(p-1)/p_i} \neq 1 \pmod{p}$, $a_i^{p-1} = 1 \pmod{p}$ impliziert $p_i^{e_i} | \mathrm{ord}(a_i)$. Nach CRT folgt $\prod_{i=1}^{r} p_i^{e_i} | \mathrm{ord}(a_i)$, und somit $\varphi(p) = p - 1$. Damit ist p prim. □

Für prime p, $p - 1 = \prod_{i=1}^{r} p_i^{e_i}$ gilt andererseits für zufällige $a \in \mathbb{Z}_p^*$

$$\mathrm{Ws}\left[a^{(p-1)/p_i} \neq 1 \pmod{p}\right] = 1 - \tfrac{1}{p_i}.$$

Daher findet man bei Kenntnis der Primfaktorzerlegung von $p-1$ die Zeugen $a_1, a_2, \ldots, a_r$ für die Primheit von p in polynomieller Zeit.

m

Kapitel 5

Gitter

$\mathbb{R}^n$ sei der n-dimensionale reelle Vektorraum mit dem Euklidischen Skalarprodukt $\langle \cdot, \cdot \rangle : \mathbb{R}^{2n} \to \mathbb{R}$ und der Vektorlänge $\|x\| = \langle x, x \rangle^{\frac{1}{2}}$. Die Matrix $B \in \mathbb{R}^{n \times m}$ habe die Spaltenvektoren $b_1, ..., b_m \in \mathbb{R}^n$, $B = [b_1, ..., b_n]$.

Definition 5.1
Zu $B := [b_1, ..., b_m] \in \mathbb{R}^{n \times m}$ *mit linear unabhängigen Vektoren* $b_1, ..., b_m$ *ist*

$$L := L(B) := \{Bx \in \mathbb{Z}^n : x \in \mathbb{Z}^m\}$$

ein Gitter *mit* Basismatrix B *und* Rang *oder* Dimension m.

Das Gitter $L(B)$ ist ein diskretes Analogon zum linearen Vektorraum $\operatorname{span}(B) = \{Bx : x \in \mathbb{R}^m\}$. Das Gitter $L(B) \subseteq \mathbb{R}^n$ heißt *vollständig*, wenn $m := \operatorname{Rang}(B) = n$. Ein Gitter hat viele Basen. Der Rang des Gitter ist unabhängig von der Wahl der Basis.

Satz 5.2
$L(\overline{B}) = L(B)$ *gilt gdw, wenn es eine Matrix* $T \in \mathrm{GL}_m(\mathbb{Z})$ *gibt mit* $\overline{B} = B \cdot T$.

Dabei ist $\mathrm{GL}_m(\mathbb{Z})$ die multiplikative Gruppe der Matrizen in $\mathbb{Z}^{n \times n}$ mit Determinante ± 1 ist.

Beweis. „$\Rightarrow$“ Wegen $L(\overline{B}) \subset L(B)$ gibt es ein $T \in \mathbb{Z}^{n \times n}$ mit $\overline{B} = B \cdot T$. Wegen $\operatorname{Rang}(\overline{B}) = \operatorname{Rang}(B)$ gilt $\det T \neq 0$. Wegen $L(B) \subset L(\overline{B})$ ist T^{-1} ganzzahlig. Aus $\det T \cdot \det T^{-1} = 1$ folgt $|\det T| = 1$, also $T \in \mathrm{GL}_m(\mathbb{Z})$.
„$\Leftarrow$“ Aus $\overline{B} = B \cdot T$ mit $T \in \mathrm{GL}_m(\mathbb{Z})$ folgt $\operatorname{Rang}(\overline{B}) = \operatorname{Rang}(B)$ und $L(\overline{B}) \subset L(B)$. Aus $\overline{B} \cdot T^{-1} = B$ folgt $L(B) \subset L(\overline{B})$, somit $L(\overline{B}) = L(B)$.
□

Zu $A \in \mathbb{R}^{n\times n}$ ist $\{x \in \mathbb{Z}^n \mid Ax = 0\}$ ein Gitter. Eine Teilmenge $S \subseteq \mathbb{R}^n$ heißt *diskret*, wenn sie keinen Häufungspunkt hat.

Satz 5.3 (ohne Beweis)
Jede diskrete, additive Untergruppe des $\mathbb{R}^n$ ist ein Gitter, d.h. sie wird von einer Gitterbasis erzeugt.

Umgekehrt ist jedes Gitter $L = L(B) \subset \mathbb{R}^n$ diskret. Hierzu betrachten wir zu $\operatorname{span}(L) = \sum_{i=1}^m b_i\mathbb{R}$ und $\psi(\mathbb{Z}^m) = L$ den VR-Isomorphismus

$$\begin{array}{rcccl} \psi & : & \mathbb{R}^m & \to & \operatorname{span}(L) \subseteq \mathbb{R}^n \\ & & (t_1, t_2, \ldots, t_m) & \mapsto & \sum_{i=1}^m t_i b_i \end{array} .$$

Weil ψ^{-1} stetig und $\mathbb{Z}^m$ diskret ist, ist auch $L = \psi(\mathbb{Z}^m)$ diskret. Wegen der Stetigkeit von ψ^{-1} liefert nämlich jeder Häufungspunkt ζ von $L \subset \operatorname{span}(L)$ einen Häufungspunkt $\psi^{-1}(\zeta) \in \mathbb{Z}^m$.

Definition 5.4
Die Determinante $\det L$ *des Gitters $L = L(B)$ ist das m–dim. Volumen des von den Spaltenvektoren $b_1, b_2, \ldots, b_m$ aufgespannten Parallelepipeds*

$$\mathcal{P}(B) := \{\textstyle\sum_{i=1}^m z_i b_i | 0 \le z_1, ..., z_m < 1\},$$

(Grundmasche von L), $\det L := vol_m \mathcal{P}(B)$. *Die um Gitterpunkte verschobenen Grundmaschen zerlegen den $\mathbb{R}^n$, $\mathcal{B} = \sum_{b\in L(B)} b + \mathcal{P}(B)$.*

Satz 5.5
Für jedes Gitter $L = L(B)$ gilt $\det L = (\det B^T B)^{1/2}$.

Beweis. 1. Für die Basismatrix $B \in \mathbb{R}^{n\times n}$, $m = n$, eines vollständigen Gitters gilt $\det L = \det B = (\det(B^T B))^{1/2}$.

2. Im Fall$m < n$ gibt es eine isometrische Abbildung $T : \operatorname{span}(L) \to \mathbb{R}^m$, d.h. eine Abbildung die das Skalarprodukt erhält, $\langle T(u), T(v)\rangle = \langle u, v\rangle$ für alle u, v.

Wir wenden den Spezialfall an auf das vollständige Gitter $T(L) \subset \mathbb{R}^m$ und benutzen, daß T Volumina und das Skalarprodukt erhält. Dann gilt

$$\det L = \det T(L) = \Big(\det[\langle T(b_i), T(b_j)\rangle_{1\le i,j\le m}]\Big)^{1/2} = \Big(\det[\langle b_i, b_j\rangle_{1\le i,j\le m}]\Big)^{1/2} .$$

□

Die Gitterdeterminante ist von der Wahl der Basis unabhängig. Seien $B, \overline{B}$ Basen von L, dann gibt es nach Satz 5.2 ein $T \in \mathrm{GL}_m(\mathbb{Z})$ mit $\overline{B} = B\,T$. Aus $|\det T| = 1$ folgt $\det(T^T B^T B T) = \det(B B^T)$.

Algorithmische Probleme. Gegeben sei eine Basis $B \in \mathbb{Z}^{n \times m}$.

1. Finde eine Basis von $L(B)$ bestehend aus möglichst kurzen Vektoren.
2. Entscheide zu $k \in \mathbb{Z}$: $\exists b \in L(B) : \ 0 < \|b\|_\infty \leq k$.

Dabei gilt $\|(y_1, ..., y_n)\|_\infty = \max_i |y_i|$.

3. Entscheide zu $k \in \mathbb{Z}$: $\exists b \in L(B) : \ 0 < \|b\| \leq k$.

Dabei gilt $\|(y_1, ..., y_n)\| = \sqrt{\sum_{i=1}^{n} y_i^2}$.

Das Problem 2, das 'kürzeste Gittervektorproblem zur $\| \ \|_\infty$-Norm'. Dieses Problem ist NP-vollständig für variable Dimension m (van Emde Boas (1982)). Das Problem 3 ist NP-hart für variables m bezüglich probabilistischer Reduktionen Ajtai (1998), aber das Problem ist polynomial-zeit für konstantes m (Lenstra 1983).

5.2 Gitterbasenreduktion

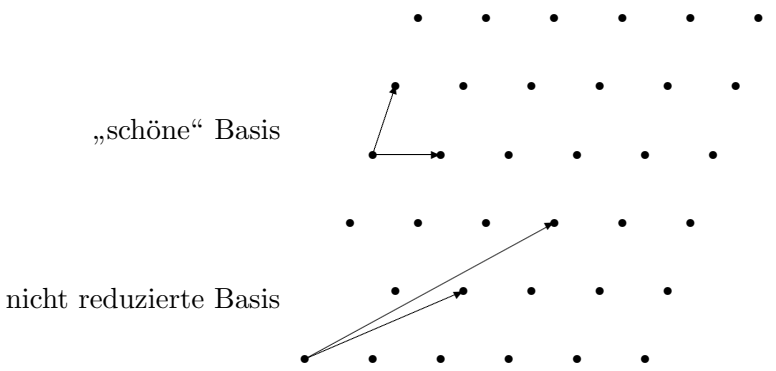


Abbildung 1: Reduktionsziel

Ziel der Gitterbasenreduktion ist es, eine Gitterbasis aus kurzen Vektoren zu erzeugen. Maßstab für die Kürze der Basis sind die sukzessiven Minima:

Definition 5.6
Die sukzessiven Minima $\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_m$ *des Gitters* $L(b_1, ..., b_m)$ *sind* $\lambda_i(L) := \min(\max\{\|\bar{b}_1\|, \ldots, \|\bar{b}_i\| \ \ \textit{für linear unabhängige} \ \ \bar{b}_1, \ldots, \bar{b}_i \in L\})$.

Leider sind Basen $b_1, b_2, \ldots, b_m$ mit $\|b_i\| = \lambda_i$ für $i = 1, 2, \ldots, m$ für $m \geq 5$ nicht immer möglich.

Definition 5.7
Die Gitterbasis $b_1, b_2 \in \mathbb{R}^n$ *heißt* reduziert, *wenn*

$$\|b_1\| \leq \|b_2\| \leq \|b_1 - b_2\| \leq \|b_1 + b_2\| .$$

Im Falle $\|b_1\| \leq \|b_2\|$ gilt für $\mu_{2,1} := \frac{\langle b_1, b_2 \rangle}{\|b_1\|^2}$:

$$| \mu_{2,1} | \leq \tfrac{1}{2} \iff \|b_2\| \leq \|b_1 \pm b_2\|.$$

Der Gram-Schmidt Koeffizient $\mu_{2,1}$ liefert einen Vektor $b_2 - \mu_{2,1} b_1$, der orthogonal zu b_1 ist, d.h. $\langle b_2 - \mu_{2,1} b_1, b_2 \rangle = 0$.

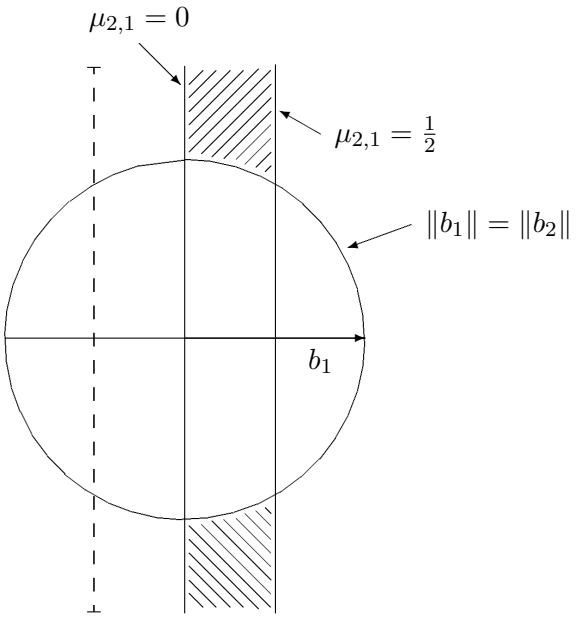


Abbildung 2: Reduzierte Basis bzgl. Euklidischer Norm

In Abbildung 2 ist der Bereich der b_2 für eine bezüglich der Euklidischen Norm reduzierten Basis b_1, b_2 schraffiert. Das rechte Halbband ist das Gebiet der Vektoren b_2 mit $0 \leq \mu_{2,1} \leq \frac{1}{2}$. Im Fall $\|b_1 + b_2\| = \|b_1 - b_2\|$ ist mit b_1, b_2 auch $-b_1, b_2$ reduziert. Im Fall $\|b_2\| = \|b_1 - b_2\|$ ist mit b_1, b_2 auch $b_1, b_1 - b_2$ reduziert. Im Fall $\|b_1\| = \|b_2\|$ ist mit b_1, b_2 auch b_2, b_1 reduziert. In den übrigen Fällen gibt es nur die reduzierten Basen b_1, b_2 bzw. $-b_1, -b_2$.

Satz 5.8
Für jede reduzierte Basis b_1, b_2 *des Gitters* L *gilt* $\|b_i\| = \lambda_i(L)$ *für* $i = 1, 2$.

Beweis. Es ist zu zeigen:

$$\|b_1\| \leq \|rb_1 + sb_2\| \qquad \text{für } (r,s) \in \mathbb{Z}^2 \setminus \{(0,0)\} \tag{5.1}$$

$$\|b_2\| \leq \|rb_1 + sb_2\| \qquad \text{für } r \in \mathbb{Z}, s \in \mathbb{Z} \setminus \{0\} \tag{5.2}$$

Ungleichung (5.1) folgt aus (5.2) wegen $\|b_1\| \leq \|b_2\|$ und $\|b_i\| \leq \|tb_i\|$ für $t \geq 1$. Es genügt also, Ungleichung (5.2) zu zeigen. Behauptung: Die Norm

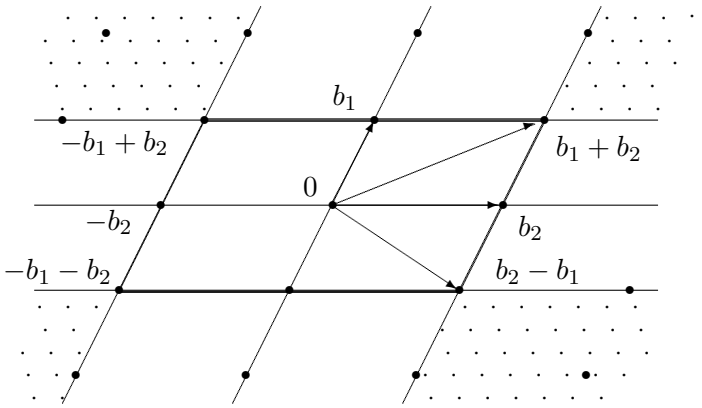


Abbildung 3: Minimalstellen der Norm

$\|\cdot\|$ nimmt ihr Minimum in den vier schraffierten Gebieten der Abbildung 3 jeweils in den Punkten $\pm b_1 \pm b_2$ an. Die Ungleichung (5.2) folgen somit aus der Reduktionsbedingung $\|b_2\| \leq \|b_1 \pm b_2\|$. □

Algorithmus 9 Reduktionsverfahren für Euklidische Norm

EINGABE: $b_1, b_2 \in \mathbb{R}^n$

1. $b_2 := b_2 - \lceil \mu_{2,1} \rfloor b_1$

2. IF $\|b_1\| > \|b_2\|$ THEN vertausche b_1 und b_2, GOTO 1
ELSE $b_2 := -b_2$ if $\mu_{2,1} < 0$

AUSGABE: reduzierte Basis b_1, b_2

Dabei bezeichnet $\lceil a \rfloor := \lceil a - \frac{1}{2} \rceil$ die zur reellen Zahl a nächste, ganze Zahl. Das Verfahren 9 transformiert eine gegebene Gitterbasis in eine reduzierte Gitterbasis. Das Verfahren bezieht sich auf die Euklidische Norm. Für beliebige Norm bestimme man in Schritt 1 $t \in \mathbb{Z}$ so, dass $\|b_1 - tb_2\|$ minimal ist und ersetze $b_2 := b_2 - tb_1$.

Der Algorithmus ist korrekt, Schritt 1 sichert $|\mu_{2,1}| \leq \frac{1}{2}$. Damit ist die Ausgabebasis reduziert. Als Iteration bezeichnen wir die einmalige Ausführung

der Schritte 1 und 2 gemäß

$$\begin{bmatrix} b_1^{\text{neu}}, & b_2^{\text{neu}} \end{bmatrix} = \begin{bmatrix} b_1, & b_2 \end{bmatrix} \cdot \begin{pmatrix} -\lceil \mu_{2,1} \rfloor & 1 \\ 1 & 0 \end{pmatrix}.$$

Das Verfahren ist eine natürliche Erweiterung des zentrierten Euklischen Algorithmus. Die Iteration beim zentrierten Euklidischen Algorithmus ist analog

$$\begin{pmatrix} a_0, & a_1 \end{pmatrix} = \begin{pmatrix} a_0, & a_1 \end{pmatrix} \cdot \begin{pmatrix} -\lceil a_0/a_1 \rfloor & 1 \\ 1 & 0 \end{pmatrix}.$$

Definition 5.9
Eine Basis b_1, b_2 heißt wohlgeordnet*, wenn die beiden folgenden, äquivalenten Bedingungen gelten*

1. $\|b_1\| \leq \|b_2\|$ *und* $\|b_1 - b_2\| \leq \|b_2\|$

2. $\|b_1\| \leq \|b_2\|$ *und* $\mu_{2,1} > \frac{1}{2}$.

Fakt 5.10
Am Ende eines jeden Durchlaufes der Schritte 1 und 2 ist die Basis b_1, b_2 entweder wohlgeordnet oder reduziert.

Das Reduktionsverfahren transformiert wohlgeordnete Basen solange auf wohlgeordnete Basen, bis eine reduzierte Basis erreicht ist. Eine Iteration heißt *eigentlich*, wenn er eine wohlgeordnete Basis auf eine wohlgeordnete Basis (am Ende von Schritt 2) transformiert. Nur der erste und der letzte Durchlauf der Schritte 1 und 2 sind möglicgerweise uneigentlich.

Lemma 5.11
Für jede wohlgeordnete Basis b_1, b_2 mit wohlgeordneter Nachfolgerbasis b_1^{neu}, b_1 gilt $b_1^{neu} = \epsilon(b_2 - \mu b_1)$ *wobei* entweder

- $\epsilon = 1$ *und* $\mu \geq 2$ oder
- $\epsilon = -1$ *und* $\mu \geq 3$.

Beweis. Sei $b_2 = \epsilon b_1^{\text{neu}} + \mu b_1$ mit *epsilon* $\in \{\pm 1\}$. Wegen $\|b_1^{\text{neu}}\| < \|b_1\|$ gilt $\langle b_1^{\text{neu}}, b_1 \rangle < \langle b_1, b_1 \rangle$.

1. Somit folgt aus $\mu < 0$ der Widerspruch

$$\langle b_1, b_2 \rangle = \pm \langle b_1^{\text{neu}}, b_1 \rangle + \mu \langle b_1, b_1 \rangle < 0.$$

2. Aus $\mu = 1$ folgt $b_2 - b_1 = \pm b_1^{\text{neu}}$, also $\|b_2 - b_1\| = \|b_1^{\text{neu}}\| < \|b_1\|$. Dies ist ein Widerspruch, da b_1, b_2 wohlgeordnet ist.

3. Aus $\epsilon = -1$ und $\mu = 2$ folgt: $b_2 - b_1 = b_1^{\text{neu}} + b_1$. Da b_1^{neu}, b_1 wohlgeordnet ist, folgt $\|b_2 - b_1\| = \|b_1^{\text{neu}} - b_1\| < \|b_1\|$. Dies ist ein Widerspruch, da b_1, b_2 wohlgeordnet ist. □

Lemma 5.12
Für die minimale, wohlgeordnete Vorgängerbasis b_1, b_2 zur wohlgeordneten Basis b_1^{neu}, b_1 gilt $b_2 = b_1^{neu} + 2b_1$.

Beweis. Zu zeigen ist $\|b_1^{\text{neu}} + 2b_1\| \leq \|-b_1^{\text{neu}} + 3b_1\|$. Wegen

$$\begin{aligned} \|b_1^{\text{neu}} + 2b_1\|^2 &= \|b_1^{\text{neu}}\|^2 + 4\|b_1\|^2 + 4\langle b_1^{\text{neu}}, b_1\rangle \\ \|-b_1^{\text{neu}} + 3b_1\|^2 &= \|b_1^{\text{neu}}\|^2 + 9\|b_1\|^2 - 6\langle b_1^{\text{neu}}, b_1\rangle \end{aligned}$$

folgt die Behauptung aus $\|b_1\|^2 \geq 2\langle b_1^{\text{neu}}, b_1\rangle$. □

Umgekehrt ist offenbar für $\epsilon = +1$ und $\mu \geq 2$ bzw. $\epsilon = -1$ und $\mu \geq 3$ die zu b_1^{neu}, b_1 zugehörige Basis b_1, b_2 wohlgeordnet.

Die minimale Vorgängerbasis zur wohlgeordneten Basis b_1, b_2 ist damit:

$$\begin{bmatrix} b_1^{(1)} & b_2^{(1)} \end{bmatrix} = \begin{bmatrix} b_1 & b_2 \end{bmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}$$

Durch Induktion über k zeigt man, die minimale Vorgängerbasis $b_1^{(k)}, b_2^{(k)}$ zur wohlgeordneten Basis b_1, b_2 gegeben ist durch:

$$\begin{bmatrix} b_1^{(k)} & b_2^{(k)} \end{bmatrix} = \begin{bmatrix} b_1 & b_2 \end{bmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}^k$$

Die Koeffizienten der Matrix:

$$\begin{pmatrix} a_{k-2} & a_{k-1} \\ a_{k-1} & a_k \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}^k$$

erfüllen die Rekursion (siehe Übungsaufgabe B.34)

$$a_0 = 1,\ a_1 = 2,\ a_2 = 5,\ a_k = 5a_{k-2} + 2a_{k-3} \text{ for } k \geq 3.$$

Durch Induktion folgt

$$\left(1+\sqrt{2}\right)^{k-1} < a_k < \left(1+\sqrt{2}\right)^k \qquad \text{für } k > 0,$$

$$\left[\left\langle b_i^{(k)}, b_j^{(k)} \right\rangle_{i,j=1,2}\right] = \begin{pmatrix} a_{k-2} & a_{k-1} \\ a_{k-1} & a_k \end{pmatrix}^k \cdot \left[\langle b_i, b_j\rangle_{i,j=1,2}\right] \cdot \begin{pmatrix} a_{k-2} & a_{k-1} \\ a_{k-1} & a_k \end{pmatrix}^k$$

Sei b_1, b_2 die letzte wohlgeordnete Basis im Reduktionsverfahren. Es gilt $\|b_1\| \geq \lambda_1$, $\|b_2\| \geq \lambda_2$, $\langle b_1, b_2\rangle \geq \frac{1}{2}\|b_1\|^2$ und somit

$$\|b_2^{(k)}\| > \lambda_2^2 a_k^2 > \lambda_2^2 \left(1+\sqrt{2}\right)^{2k-2}.$$

Es folgt

$$\log_{1+\sqrt{2}} \left(\|b_2^{(k)}\| \Big/ \lambda_2 \right) \geq k-1 \tag{5.3}$$

Satz 5.13
Die Anzahl der eigentlichen Iterationschritte (siehe Seite 48) im Reduktionsverfahren mit Eingabebasis b_1, b_2 ist höchstens

$$\left\lceil \log_{1+\sqrt{2}} \left(\max \left\{ \|b_1\|, \|b_2\| \right\} / \lambda_2 \right) \right\rceil .$$

Beweis. Sei k die Anzahl der eigentlichen Iterationen. Für die Basis $b_1^{(k)}, b_2^{(k)}$ der ersten uneigentlichen Iteration gilt einerseites $\|b_2^{(k)}\| \leq \max \{\|b_1\|, \|b_2\|\}$ und andererseits Ungleichung (5.3). □

5.2.1 LLL-Algorithmus

Der LLL-Algorithmus von Lenstra, Lenstra, Lovàsz (1982) überträgt Algorithmus 9 von Gittern der Dimension $m = 2$ auf Gitter beliebigre Dimension $m \geq 2$. Zu gegebener Basis $b_1, ..., b_m \in \mathbb{Q}^n$ von L findet der LLL-Algorithmus eine Basis von L so dass $\|b_j\| \leq 2^{n/2} \lambda_j(L)$ für $j = 1, ..., m$. Der LLL-Algorithmus ist polynomial-Zeit für beliebige $n \leq m$ und beliebig Eingabevektoren.

Mit Hilfe des LLL-Algorithmus kann man ganzzahlige, lineare Ungleichungssysteme in fester Dimension m in polynomial-Zeit lösen. Zu gegebenem $A \in \mathbb{Q}^{n \times m}$, $b \in \mathbb{Q}^n$ und festem m kann man $Ax \leq b$, $x \in \mathbb{Z}^m$ in polynomial-Zeit lösen, sofern eine Lösung existiert.

Das nächste Kapitel erklärt diesen Algorithmus der ganzzahligen, linearen Programmierung von H.W. Lenstra, Jr. (1982) für die Dimension $m = 2$.

5.3 Ganzahlige, lineare Ungleichungssysteme

Wir lösen ganzzahlige, lineare Ungleichungssysteme in zwei Variablen:

gegeben: $u_i, v_i, w_i \in \mathbb{Z} \qquad i = 1, 2, \ldots, n$

finde: $x, y \in \mathbb{Z}$ mit:

$$u_i x + v_i y \leq w_i \qquad \text{für } i = 1, 2, \ldots, n \tag{5.4}$$

Wir transformieren das Problem in ein Nächstes-Gitterpunkt-Problem in der sup–Norm $\|\cdot\|_\infty$:

$$\|(x_1, x_2, \ldots, x_n)\|_\infty := \max_{i=1,2,...,n} |x_i|$$

Wir setzen $M := \max_i \{|u_i|, |v_i|, |w_i|\}$ und $\overline{M} := 12M^3 + M$. Als Gitterbasis wählen wir:

$$\begin{aligned} b_1 &:= \tfrac{1}{\overline{M}} (u_1, u_2, \ldots, u_n) \\ b_2 &:= \tfrac{1}{\overline{M}} (v_1, v_2, \ldots, v_n) \end{aligned}$$

Der zu approximierende Punkt ist:

$$w := \tfrac{1}{M}\left(w_1 - \overline{M}, w_2 - \overline{M}, \ldots, w_n - \overline{M}\right)$$

Lemma 5.14
Es ist (5.4) *ganzzahlig lösbar genau dann, wenn*

$$\exists x, y \in \mathbb{Z}: \qquad \|xb_1 + yb_2 - w\|_\infty \leq 1$$

Beweis. Es gilt:

$$\begin{array}{lrcll}
 & \|xb_1 + yb_2 - w\|_\infty & \leq & 1 & \\
\iff & \left|xu_i + yv_i - w_i + \overline{M}\right| & \leq & \overline{M} & i = 1, 2, \ldots, n \\
\iff & +xu_i + yv_i - w_i & \leq & 0 & i = 1, 2, \ldots, n \quad \text{und} \\
 & -xu_i - yv_i + w_i - \overline{M} & \leq & \overline{M} & i = 1, 2, \ldots, n \\
\iff & +xu_i + yv_i & \leq & w_i & i = 1, 2, \ldots, n \quad \text{und} \\
 & -xu_i - yv_i + w_i & \leq & 2\overline{M} & i = 1, 2, \ldots, n
\end{array}$$

Im Fall $|x|, |y| \leq 6M^2$ gilt stets:

$$|xu_i + yv_i - w_i| \leq 12M^3 + M = \overline{M}$$

Es genügt zu zeigen: Ist (5.4) ganzzahlig lösbar, dann existiert eine Lösung x, y mit $|x|, ||| y| \leq 6M^2$. Von zur Gathen und Sieveking [GS78] haben 1978 gezeigt:

$$\exists x \in \mathbb{Z}^n: \quad Ax \leq b \qquad \iff \qquad \exists x \in \mathbb{Z}^n: \quad Ax \leq b, \quad \|x\|_\infty \leq (n+1)n^{n/2}M$$

mit $M := \max_{i,j}\{|a_{ij}|, |b_i|\}$. Für $n = 2$ erhalten wir: Aufgabe (5.4) ist genau dann ganzzahlig lösbar, wenn eine Lösung x, y mit $|x|, |y| \leq 6M^2$ existiert. □

Damit haben wir die Aufgabenstellung reduziert, einen Punkt b im Gitter $L(b_1, b_2)$ zu finden mit $\|b - w\|_\infty \leq 1$.

5.3.1 Lösen von $\|xb_1 - yb_2 - w\|_\infty \leq 1$

Idee

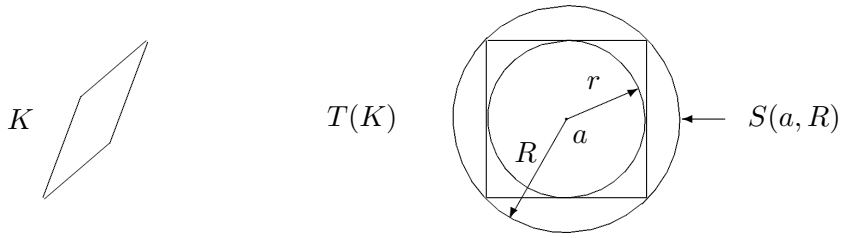
Die Schwierigkeit liegt darin, daß im allgemeinen $w \notin \operatorname{span}(b_1, b_2)$. Sei K die konvexe Menge:

$$K := \{z \in \operatorname{span}(b_1, b_2) \ : \ \|z - w\|_\infty \leq 1\}$$

1. Man verwendet eine lineare Transformation T auf b_1 und b_2 an, so daß $T(K)$ „kugelförmig“ wird in dem Sinne, daß man einen inneren Punkt $a \in T(K)$ kennt, derart, daß

$$S(a, r) \subseteq T(K) \subseteq S(a, R)$$

mit $\frac{R}{r} \leq 4$, wobei die Menge $S(a, r)$ eine Kugel mit dem Radius r um den Mittelpunkt a ist (siehe Abbildung 4). Statt die Abbildung T



r = innerer Radius zu a, K
R = äußerer Radius zu a, K

Abbildung 4: lineare Transformation T

anzuwenden, wählt man ein geschicktes Skalarprodukt $\langle \cdot, \cdot \rangle_{\text{neu}}$, unter dem K kugelförmig ist:

$$\langle x, y \rangle_{\text{neu}} := \langle Tx, Ty \rangle$$

wobei $\langle \cdot, \cdot \rangle$ das Standardskalarprodukt sei.

2. Reduziere die Basis b_1, b_2 bezüglich des Skalarproduktes $\langle \cdot, \cdot \rangle_{\text{neu}}$. Sei b_1^r, b_2^r die reduzierte Basis. Weil b_1^r, b_2^r reduziert ist, gibt es nur wenige Gitterpunkte auf der Linie $t_2 b_2^r + b_1^r \mathbb{R}$, welche $S(a, R)$ schneiden. Nur diese wenigen Linien werden auf Gitterpunkte, d.h. Punkte der Form $t_2 b_2^r + b_1^r \mathbb{Z}$, abgesucht, die in $S(a, R)$ liegen (siehe Abbildung 5).

Wahl des Skalarproduktes $\langle \cdot, \cdot \rangle$

Im Fall $K = \emptyset$ gibt es überhaupt keine Lösung zu (5.4). Falls $K \neq \emptyset$ und $\text{vol}_2(K) = 0$ liegt K auf einer Line, so daß wir diesen Fall einfach lösen können. Sei im folgenden o.B.d.A. $\text{vol}_2(K) \neq 0$.

Man bestimme $a_1, a_2, a_3 \in K$, so daß das Volumen der konvexen Hülle $\text{KH}(a_1, a_2, a_3)$ von a_1, a_2, a_3 maximal ist. Dazu halte man zwei Punkte a_i, a_j fest und wähle $a_k \in K$, so daß der Abstand von a_k zur Geraden durch a_i, a_j

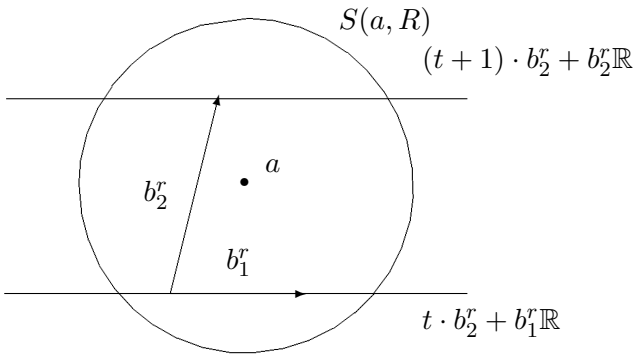


Abbildung 5: Reduzierte Basis und der Punkt a mit $S(a,R)$

maximal ist. Wiederhole den Prozeß, bis keine Vergrößerung des Volumens mehr möglich ist. Das Skalarprodukt $\langle\cdot,\cdot\rangle$ sei erklärt durch:

$$\left\langle t_1(a_1-a_2)+t_2(a_1-a_3), \bar{t}_1(a_1-a_2)+\bar{t}_2(a_1-a_3)\right\rangle := \begin{pmatrix} t_1 & t_2 \end{pmatrix} \begin{pmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 1 \end{pmatrix} \begin{pmatrix} \bar{t}_1 \\ \bar{t}_2 \end{pmatrix}$$

Es gilt $\|a_i - a_j\| = 1$ für $i \neq j$ unter diesem Skalarprodukt. Für $a_1 - a_2$ und $a_1 - a_3$ ist dies offensichtlich. Weiter gilt:

$$\begin{aligned} \langle a_2-a_3, a_2-a_3\rangle &= \langle a_2-a_1+a_1-a_3, a_2-a_1+a_1-a_3\rangle \\ &= \begin{pmatrix} -1 & +1 \end{pmatrix} \begin{pmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 1 \end{pmatrix} \begin{pmatrix} -1 \\ +1 \end{pmatrix} \\ &= 1 \end{aligned}$$

Die Punkte a_1, a_2, a_3 bilden also unter dem Skalarprodukt $\langle\cdot,\cdot\rangle$ ein gleichseitiges Dreieck mit Seitenlänge 1.

Wahl des inneren Punktes a und Radius r

Als inneren Punkt wähle $a := \frac{a_1+a_2+a_3}{3}$ und als inneren Radius $r := \frac{1}{\sqrt{12}}$. Der Inkreisradius des gleichseitigen Dreiecks ist (siehe Abbildung 6):

$$r = \frac{\sqrt{3}}{6} = \frac{1}{2\sqrt{3}} = \frac{1}{\sqrt{12}}$$

Wahl des äußeren Radius R

Es gilt:

$$\mathrm{KH}(a_1,a_2,a_3) \subseteq K \overset{(\#)}{\subseteq} \mathrm{KH}(a_1+a_2-a_3, a_2+a_3-a_1, a_3+a_1-a_3) \subseteq S\left(a, \tfrac{2}{\sqrt{3}}\right)$$

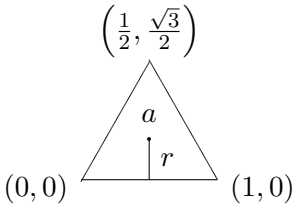


Abbildung 6: Wahl des Inkreisradius'

Die Inklusion (#) gilt, weil nach Voraussetzung $\text{vol}_2\text{KH}(a_1, a_2, a_3)$ maximal ist. Jeder Punkt x außerhalb von

$$\text{KH}(a_3 + a_1 - a_2, a_3 + a_2 - a_1, a_1 + a_2 - a_3)$$

führt mit zwei Punkten a_i, a_j zu einem größeren Volumen (siehe Abbildung 7):

$$\text{vol}_2\text{KH}(a_i, a_j, x) > \text{vol}_2\text{KH}(a_1, a_2, a_3)$$

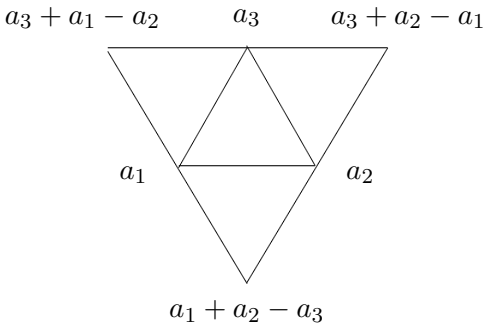


Abbildung 7: Inkreisradius r

Berechnung von R

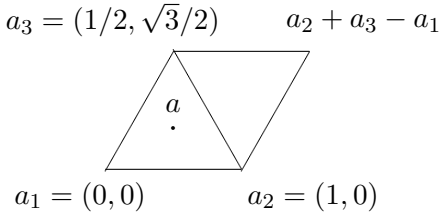


Abbildung 8: Außenkreisradius R

Es gilt (siehe Abbildung 8):

$$\begin{aligned} a &= \begin{pmatrix} \frac{1}{2} & \frac{1}{\sqrt{12}} \end{pmatrix} \\ a_2 + a_3 - a_1 &= \begin{pmatrix} \frac{3}{2} & \frac{\sqrt{3}}{2} \end{pmatrix} = \begin{pmatrix} \frac{3}{2} & \frac{3}{\sqrt{12}} \end{pmatrix} \end{aligned}$$

Für den äußeren Radius erhalten wir:

$$R = \|a_3 + a_2 - a_1 - a\| = \left\| \begin{pmatrix} 1 & \frac{+2}{\sqrt{12}} \end{pmatrix} \right\| = \sqrt{\tfrac{4}{3}} = \tfrac{2}{\sqrt{3}}$$

Test der Gitterpunkte in $S(a, R)$ auf Lösung

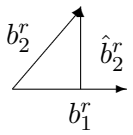


Abbildung 9: Orthogonale Projektion

Sei b_1^r, b_2^r die reduzierte Basis bezüglich des gewählten Skalarprodukts. Setze:

$$\hat{b}_2^r := b_2^r - \underbrace{\frac{\langle b_1^r, b_2^r \rangle}{\|b_1^r\|^2}}_{:=\mu_{2,1}} b_1^r$$

Es gilt: $\left\langle \hat{b}_2^r, b_1^r \right\rangle = 0$, wobei $\hat{b}_2^r$ die orthogonale Projektion von b_2^r in $\operatorname{span}(b_1^r)^\perp$ ist (siehe Abbildung 9). Setze:

$$s_1 := \frac{\langle a, b_1^r \rangle}{\|b_1^r\|^2} \qquad\qquad s_2 := \frac{\langle a, \hat{b}_2^r \rangle}{\|\hat{b}_2^r\|^2}$$

Es gilt $a = s_1 b_1^r + s_2 \hat{b}_2^r$. Gesucht ist $t_1 b_1^r + t_2 b_2^r \in K \subset S(a, R)$. Fallunterscheidung:

- $\|b_1^r\|^2 + \|\hat{b}_2^r\|^2 \leq \frac{1}{3}$

  Wir wählen $t_1, t_2 \in \mathbb{Z}$ so, daß:

  $$\begin{aligned} |s_1 - t_1 - \mu_{2,1} t_2| &\leq \tfrac{1}{2} \\ |s_2 - t_2| &\leq \tfrac{1}{2} \end{aligned}$$

  Dann gilt:

  $$t_1 b_1^r + t_2 b_2^r \in S(a, R) \subseteq K$$

  Denn:

  $$\begin{aligned} \|t_1 b_1^r + t_2 b_2^r - a\|^2 &= |s_1 - t_1 - \mu_{2,1} t_2|^2 \cdot \|b_1^r\|^2 + |s_2 - t_2|^2 \cdot \|\hat{b}_2^r\|^2 \\ &\leq \tfrac{1}{4} \|b_1^r\|^2 + \tfrac{1}{4} \|\hat{b}_2^r\|^2 \leq \tfrac{1}{4} \cdot \tfrac{1}{3} = \tfrac{1}{12} = r^2 \end{aligned}$$

- $\|b_1^r\|^2 + \left\|\hat{b}_2^r\right\|^2 > \frac{1}{3}$

  Weil b_1^r, b_2^r reduziert ist, gilt:

  $$\tfrac{3}{4}\,\|\hat{b}_2^r\|^2 \geq \|b_1^r\|^2$$

  Wir erhalten $\|\hat{b}_2^r\|^2 \left(\frac{3}{4}+1\right) > \frac{1}{3}$ und somit $\|\hat{b}_2^r\|^2 > \frac{1}{7}$. Wegen $K \subseteq S\left(a, \frac{2}{\sqrt{3}}\right)$ gilt für alle Gitterpunkte $t_1 b_1^r + t_2 b_2^r \in K$:

  $$|t_2 - s_2| \cdot \|\hat{b}_2^r\| \leq \tfrac{2}{\sqrt{3}}$$

  Es folgt:

  $$|t_2 - s_2| \leq \tfrac{2}{\sqrt{3}}\,\|\hat{b}_2^r\|^{-1} < 2 \cdot \sqrt{\tfrac{7}{3}} < 3,1$$

  Damit kommen für t_2 höchstens 7 Werte in Frage. Für jeden dieser 7 Werte berechnet man

  $$\min\left\{\|t_1 b_1^r + t_2 b_2^r - a\|_\infty \;:\; t_1 \in \mathbb{Z}\right\}$$

  Dies ist einfach. Falls diese Minima aller echt größer als 1 sind, gibt es keine Lösung. Sonst wähle $t_1, t_2 \in \mathbb{Z}$ mit:

  $$\|t_1 b_1^r + t_2 b_2^r - a\|_\infty \leq 1$$

Konstruktion der Lösung

Mit den $t_1, t_2 \in \mathbb{Z}$ aus Fall 1 bzw. Fall 2 bestimme $x, y \in \mathbb{Z}$ mit:

$$t_1 b_1^r + t_2 b_2^r = x b_1 + y b_2$$

Kapitel 6

Fehlererkennende und fehlerkorrigierende Codes

6.1 Einleitung

In ständig wachsendem Umfang werden alle Arten von Daten auf elektronischem Wege übertragen. Damit werden Fragen der Datensicherheit immer wichtiger. Wir betrachten die Sicherung von Daten gegen zufällige Störungen wie z.B. Überlagerung von mehreren Nachrichten, Leitungsrauschen oder Blitzeinschlag. Einfache Methoden zur Kodierung sind zum Beispiel:

- Die Nachricht „Meine Telefonnummer ist 22642“ wird gesendet. Der Empfänger erhält „Mexde Delifonnummer its 23641“. Der Empfänger weiß dennoch, was die ersten drei Worte bedeuten, denn die Sprache ist im allgemeinen redundant, d.h. sie enthält mehr Informationen als zum Verständnis nötig. Anders verhält es sich mit der Nummer: Hier kann der Empfänger nicht erkennen, ob überhaupt ein Fehler aufgetreten ist.

- Die Nachricht „Meine Telefonnummer ist 22642“ wird codiert, indem jedes Zeichen doppelt gesendet wird:

  „MMeeiinnee TTeelleeffoonnnnuummmmeerr iisstt 2222664422“

  Der Empfänger kann jetzt auch bei der Telefonnummer in vielen Fällen erkennen, ob ein Fehler aufgetreten ist. Wir untersuchen, „wie man Nachrichten redundant machen kann, ohne die Länge der Nachricht zu sehr zu erhöhen“.

6.2 Prüfzeichenverfahren

Prüfzeichen tauchen im alltäglichen Leben ständig auf. Betrachten wir einige Beispiele:

- Jede Warenpackung ist mit einer Artikelnummer versehen, die mit einem Lesegerät als Strichcode EAN (Europäische Artikelnummer) verarbeitet wird. Zur Vermeidung von Lesefehlern wird der gelesene Code auf bestimmte Eigenschaften geprüft:

$$a_{13} \stackrel{!}{\equiv} -(a_1 + 3a_2 + a_3 + 3a_4 + \cdots + a_{11} + 3a_{12}) \pmod{10}$$

- Die internationale Standard-Buchnummer ISBN ist eine 10-stellige Codierung: w-x-y-z. Dabei entspricht w dem Land, x dem Verlag, y dem Titel und z ist eine Prüfnummer.

Ein weiteres Beispiel ist die Numerierung der deutschen Geldscheine. Auf dieses möchten wir genauer eingehen.

Definition 6.1 (Diedergruppe)
Eine Diedergruppe D_n (der Ordnung $2n$) ist eine Gruppe mit

$$D_n = \left\{1, a, a^2, a^n, \ldots, a^{n-1}, b, ab, a^2b, \ldots, a^{n-1}b\right\}$$

wobei a, b zwei erzeugende Elemente sind, die den folgenden Relationen genügen:

a) $a^n = 1$

b) $b^2 = 1$

c) $ba = a^{n-1}b$

Wir betrachten speziell D_5. Wir können diese Gruppe auch geometrisch interpretieren als Symmetriegruppe des regelmäßigen Fünfecks. a entspricht der Drehung des Fünfecks um 72°, b eine Klappung des Fünfecks auf sich (siehe Abbildung 10). Die Potenzen a^j $(j = 0, 1, 2, 3, 4)$ sind die fünf möglichen Drehungen (inklusive der Identität) und a^jb die fünf möglichen Klappungen an den Symmetrieachsen. Die Elemente von D_5 können mit den Ziffern 0 bis 9 kodiert werden, z.B. durch:

$$a^j \mapsto j \qquad \text{und} \qquad a^jb \mapsto j + 5 \qquad j = 0, 1, 2, 3, 4$$

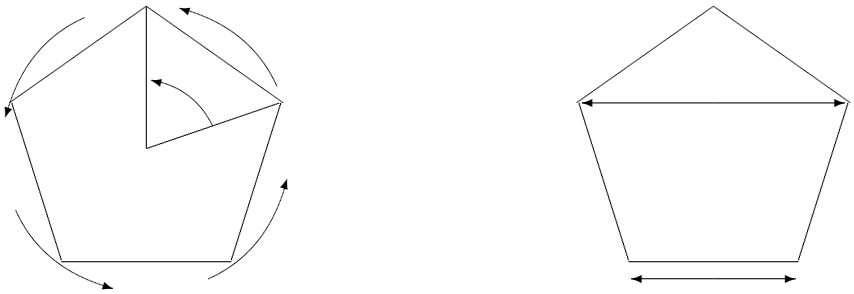


Abbildung 10: Drehungen und Klappungen des Fünfecks um 72°

Damit ergibt sich folgende Multiplikationstafel (ausführliche Multiplikationstabelle siehe Abbildung 11):

$i \cdot j$	$0 \leq j \leq 4$	$5 \leq j \leq 9$
$0 \leq j \leq 4$	$(i+j) \bmod 5$	$5 + [(i+j) \bmod 5]$
$5 \leq j \leq 9$	$5 + [(i-j) \bmod 5]$	$(i-j) \bmod 5$

		j									
	$i \cdot j$	0	1	2	3	4	5	6	7	8	9
	0	0	1	2	3	4	5	6	7	8	9
	1	1	2	3	4	0	6	7	8	9	5
	2	2	3	4	0	1	7	8	9	5	6
	3	3	4	0	1	2	8	9	5	6	7
i	4	4	0	1	2	3	9	5	6	7	8
	5	5	9	8	7	6	0	4	3	4	1
	6	6	5	9	8	7	1	0	4	0	2
	7	7	6	5	9	8	2	1	0	1	3
	8	8	7	6	5	9	3	2	1	2	4
	9	9	8	7	6	5	4	3	2	3	0

Abbildung 11: ausführliche Multiplikationstabelle

Jede Nummer eines deutschen Geldscheines besteht aus einer Folge von 11 Buchstaben und Ziffern. Die Buchstaben werden bei der Prüfung zunächst durch Ziffern ersetzt (andere Buchstaben kommen nicht vor):

A	D	G	K	L	N	S	U	Y	Z
0	1	2	3	4	5	6	7	8	9

Die so entstandene Geldscheinnummer $a_1 a_2 \dots a_{11}$ muß die folgende Prüfgleichung erfüllen:

$$T(a_1) \cdot T^2(a_2) \cdot \dots \cdot T^{10}(a_{10}) \cdot a_{11} \stackrel{!}{=} 0$$

Wobei T^i die i-te Potenz der folgenden Permutation ist:

$$T := \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 5 & 7 & 6 & 2 & 8 & 3 & 0 & 9 & 4 \end{pmatrix}$$

Diese Schreibweise bedeutet:

$$0 \mapsto 1, \quad 1 \mapsto 5, \quad 2 \mapsto 7, \quad \dots, \quad 9 \mapsto 4$$

Die Potenzen der Permutation T sind (nachrechnen !):

$$T^2 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 8 & 0 & 3 & 7 & 9 & 6 & 1 & 4 & 2 \end{pmatrix} \qquad T^3 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 9 & 1 & 6 & 0 & 4 & 3 & 5 & 2 & 7 \end{pmatrix}$$

$$T^4 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 4 & 5 & 3 & 1 & 2 & 6 & 8 & 7 & 0 \end{pmatrix} \qquad T^5 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 2 & 8 & 6 & 5 & 7 & 3 & 9 & 0 & 1 \end{pmatrix}$$

$$T^6 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 7 & 9 & 3 & 8 & 0 & 6 & 4 & 1 & 5 \end{pmatrix} \qquad T^7 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 0 & 4 & 6 & 9 & 1 & 3 & 2 & 5 & 8 \end{pmatrix}$$

$$T^8 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{pmatrix} \qquad T^9 = T$$

$$T^{10} = T^2$$

Satz 6.2
Es gilt:

1. *Für alle $x, y \in \{0, 1, \dots, 9\}$ mit $x \neq y$ gilt: $x \cdot T(y) \neq y \cdot T(x)$.*
2. *Die Prüfzeichen-Codierung der deutschen Geldscheine erlaubt die Erkennung von Einzelfehlern und Vertauschungen von zwei benachbarten Stellen (außer eventuell der letzten beiden Stellen).*

Beweis. Die erste Aussage folgt durch direktes nachrechnen. Für den zweiten Puntk beachte, daß Einzelfehler erkannt werden wegen:

- $T^i(x) \neq T^i(y)$ für jedes i und $x \neq y$
- $x \cdot y \cdot u \neq x \cdot z \cdot u$ für jedes $y \neq z$

Vertauschungen werden erkannt wegen der ersten Behauptung des Satzes (setze $x = T^i(a_i)$ und $y = T^i(a_{i+1})$). □

Es können noch weitere Fehlertypen erkannt werden.

6.3 Lineare Codes

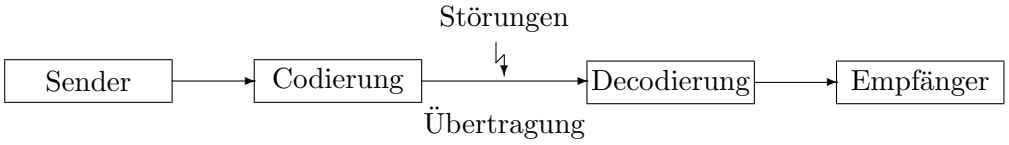


Abbildung 12: Datenübertragung

Die Datenübertragung mit Hilfe von Codes kann man sich schematisch vorstellen wie in Abbildung 12.

Definition 6.3 (Code, Blockcode)
Sei $\mathcal{A}$ ein Alphabet. Ein Code *über $\mathcal{A}$ ist eine nicht leere Teilmenge:*

$$C \subseteq \{(c_1, c_2, \ldots, c_k) \mid k \in \mathbb{N},\ c_1, ..., c_k \in \mathcal{A}\}$$

Die Elemente aus C heißen Codewörter. Falls alle Codewörter dieselbe Länge haben, d.h. $C \subseteq \mathcal{A}^n$, spricht man von einem Blockcode *der Länge n. Ein binärer Code ist ein Code über dem Alphabet $\mathbb{F}_2 = \{0, 1\}$.*

Sei $\mathbb{F}$ ein endlicher Körper, zum Beispiel:

- $\mathbb{F} = \mathbb{Z}_p$ für p prim
- $\mathbb{F} = \mathbb{Z}_p[x]/(g)$ mit p prim und $g \in \mathbb{Z}_p[x]$ irreduzibel.

Wir betrachten nur Blockcodes über endlichen Körpern $\mathbb{F}$. Zu $\mathbb{F} = \{0, 1\}$ ist $C = \{(00000), (11111)\}$ Blockcode der Länge 5.

Nachricht	→	Codewort	→	gestörtes Wort	→	vermutetes Wort	→	verm. Nachricht
0	→	(00000)	→	(01001)	→	(00000)	→	0

Die Wahrscheinlichkeit, daß die Nachricht richtig übertragen wird, ist mindestens $\frac{1}{2}$.

Definition 6.4 (Hamming-Distanz, Gewicht)
Die Hamming-Distanz *(kurz: Distanz)* $d(x, y)$ *zweier Vektoren* $x, y \in \mathbb{F}^n$ *ist die Anzahl der Stellen, an denen sich* x *und* y *unterscheiden*

$$d\left((x_1, x_2, \ldots, x_n), (y_1, y_2, \ldots, y_n)\right) := \left|\{i \,:\, x_i \neq y_i\}\right|.$$

Das Gewicht $w(x)$ *ist definiert als die Anzahl der von* 0 *verschiedenen Stellen von* x, $w\left((x_1, x_2, \ldots, x_n)\right) := |\{i \,:\, x_i \neq 0\}|$.

Es gilt $d(x, y) = w(x - y)$ und für $\mathbb{F} = \{0, 1\}$ gilt $d(x, y) = w(x + y)$ wegen $x + y = y - x$.

Definition 6.5 (Minimaldistanz)
Die Minimaldistanz $d(C)$ *des Codes* C *ist* $d(C) := \min\{d(x, y) \mid x, y \in C,\ x \neq y\}$.

Bei der *Minimal-Distanz-Dekodierung* dekodiert man das empfangene Tupel $v = (v_1, v_2, \ldots, v_n)$ als ein Codewort, dessen Distanz zu v minimal ist.

Definition 6.6 (t-Fehler-erkennender und -korrigierender Code)
Ein Code heißt t*-Fehler-erkennend, wenn die Minimaldistanz des Codes mindestens* $2t$ *ist. Ein Code heißt* t*-Fehler-korrigierend, wenn die Minimaldistanz des Codes mindestens* $2t + 1$ *ist.*

Definition 6.7 (Linearer Code)
Ein Code $C \subseteq \mathbb{F}^n$ *heißt linearer Code bzw.* $[n, k]$*-Code, wenn er ein Untervektorraum der Dimension* k *von* $\mathbb{F}^n$ *ist.*

Ein $[n, k, d]$-Code C ist ein $[n, k]$-Code mit Minimaldistanz $d := d(C)$.

Der Minimaldistanz d läßt sich für einen linearen Code C besonders leicht berechnen:

$$d = \min\{w(x) \mid x \in C,\ x \neq 0\}$$

Denn: Seien $x, y \in C$ mit $d = d(x, y)$, es gilt wegen $x \neq y$ und $x - y \in C$:

$$d(x, y) = d(x - y, y - y) = d(x, 0) = w(x)$$

Definition 6.8 (Generatormatrix)
Sei C *ein linearer* $[n, k]$*-Code. Die Codewörter*

$$\mathbf{g_i} = (g_{i1}, g_{i2}, \ldots, g_{in}) \qquad i = 1, 2, \ldots, k$$

seien eine Basis des Vektorraumes C*. Dann nennt man die* $k \times n$*-Matrix* $G := [g_{ij}]$ *Generatormatrix von* C *(die Zeilen von* G *sind die Codewörter* $\mathbf{g_1}, \mathbf{g_2}, \ldots, \mathbf{g_k}$*).*

Der Code C besteht also genau aus den Linearkombinationen:

$$c = b_1\mathbf{g_1} + b_2\mathbf{g_2} + \cdots b_k\mathbf{g_k} \qquad \text{mit } (b_1, b_2, \ldots, b_k) \in \mathbb{F}$$

Mit $\mathbf{c} := (c_1, c_2, \ldots, c_n)$ und $\mathbf{b} := (b_1, b_2, \ldots, b_k)$ gilt $\mathbf{c} = \mathbf{b} \cdot G$, d.h.:

$$\begin{bmatrix} c_1 & c_2 & \cdots & c_n \end{bmatrix} = \begin{bmatrix} b_1 & b_2 & \cdots & b_k \end{bmatrix} \cdot \begin{bmatrix} g_{11} & g_{12} & \cdots & g_{1n} \\ g_{21} & g_{22} & \cdots & g_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ g_{k1} & g_{k2} & \cdots & g_{kn} \end{bmatrix}$$

Wir bezeichnen:

$$\langle (u_1, u_2, \ldots, u_n), (c_1, c_2, \ldots, c_n) \rangle = \sum_{i=1}^{n} c_i u_i = c \cdot u^T$$

Definition 6.9 (Dualer Code)
Sei $C \subseteq \mathbb{F}^n$ ein $[n,k]$-Code. Der duale Code $C^\perp$ zu C ist:

$$C^\perp = \{ u \in \mathbb{F}^n \mid \langle u, c \rangle = 0 \quad \forall c \in C \}$$

Satz 6.10
Für einen $[n,k]$-Code $C \subseteq \mathbb{F}^n$ ist $C^\perp$ ein $[n, n-k]$-Code mit $\left(C^\perp\right)^\perp = C$.

Beweis. Sei $\mathbf{c_1}, \mathbf{c_2}, \ldots, \mathbf{c_n}$ Basis von C. Dann ist $C^\perp$ der Lösungsraum des linearen Gleichungssystems:

$$\langle \mathbf{u}, \mathbf{c_i} \rangle = 0 \qquad i = 1, 2, \ldots, k$$

Die Matrix des Gleichungssystems ist die Generatormatrix:

$$G := [c_{ij}]_{\substack{1 \le i \le k \\ 1 \le j \le n}}$$

Der Lösungsraum des Gleichungssystems (also $C^\perp$) hat die Dimension $n-k$. □

Satz 6.11
Sei C ein linearer $[n,k]$-Code, der in den ersten k Stellen systematisch ist. Dann hat C eine kanonische Generatormatrix, d.h. eine Generatormatrix der Form $G = [I_k|A]$. I_k ist die $k \times k$-Einheitsmatrix und A eine $k \times (n-k)$-Matrix.

Beweis. Zu jeder Nachricht $u = (u_1, u_2, \ldots, u_k)$ gibt es nach Voraussetzung genau ein Codewort $c = (u_1, u_2, \ldots, u_k, c_{k+1}, c_{k+2}, \ldots, c_n) \in C$. Insbesondere gibt es Codewörter

$$\begin{aligned} g_1 &= (1,0,0,\ldots,0,0,a_{11},a_{12},\ldots,a_{1,n-k-1},a_{1,n-k}) \\ g_2 &= (0,1,0,\ldots,0,0,a_{21},a_{22},\ldots,a_{2,n-k-1},a_{2,n-k}) \\ g_3 &= (0,0,1,\ldots,0,0,a_{31},a_{32},\ldots,a_{3,n-k-1},a_{3,n-k}) \\ &\vdots \\ g_k &= (0,0,0,\ldots,0,1,a_{k1},a_{k2},\ldots,a_{k,n-k-1},a_{k,n-k}) \end{aligned}$$

Es folgt die Behauptung. □

Sei $C := \{(000),(011),(101),(110)\}$, $\mathbb{F} = \{0,1\}$. Mögliche Generatormatrizen:

$$G_1 = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix} \qquad G_2 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \qquad G_3 = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$$

G_2 ist die kanonische Generatormatrix. Es ist klar, wie eine Nachricht u bei gegebener, kanonischer Generatormatrix codiert werden:

Satz 6.12
Sei C ein linearer Code mit kanonischer Generatormatrix $G = [I_k|A]$. Für das zur Nachricht $u = (u_1, u_2, \ldots, u_k)$ gehörige Codewort $c = (c_1, c_2, \ldots, c_n)$ gilt:

$$c = u \cdot G = (u_1, u_2, \ldots, u_k, c_{k+1}, c_{k+2}, \ldots, c_n)$$

Bis jetzt haben wir uns mit dem Erzeugen von linearen Codes beschäftigt. Als nächstes untersuchen wir, wie man erkennt, ob einen gegebener Vektor zum Code gehört.

Definition 6.13 (Kontrollmatrix, PCH-Matrix)
Sei C ein linearer Code der Länge n. Eine $l \times n$-Matrix $H = [h_{ij}]$ mit $h_{ij} \in \mathbb{F}$ heißt Kontrollmatrix oder Parity-Check-Matrix (PCH-Matrix) zu C, falls für alle Vektoren $v \in \mathbb{F}^n$ gilt:

$$v \in C \quad \Longleftrightarrow \quad H \cdot v^T = 0$$

Satz 6.14
Sei C ein $[n,k]$-Code mit Generatormatrix G. Eine $l \times n$-Matrix H ist genau dann Kontrollmatrix von C, wenn gilt:

$$H \cdot G^T = 0 \qquad \textit{und} \qquad \mathrm{Rang}(H) = n - k$$

Beweis. Wir zeigen beide Richtungen:

„⇒“ Nach Voraussetzung ist H Kontrollmatrix von G. Daher gilt:

$$C = \left\{ v \in \mathbb{F}^n \;\middle|\; H \cdot v^T = 0 \right\}$$

C ist der Lösungsraum des linearen Gleichungssystems $H \cdot v^T = 0$. Insbesondere gilt für alle Zeilenvektoren g_i der Generatormatrix wegen $g_i^T \in C$: $H \cdot g_i^T = 0$. Es folgt $H \cdot G^T = 0$. Aus der Dimensionsformel $\dim C = n - \mathrm{Rang}(H)$ folgt:

$$\mathrm{Rang}(H) = n - \dim C = n - k$$

„⇐“ Sei $H \cdot G^T = 0$ und $\mathrm{Rang}(H) = n - k$. Es gilt $H \cdot g_i^T = 0$ für alle Zeilenvektoren von G. Da jedes Codewort $c \in C$ Linearkombination der Zeilenvektoren von G ist, gilt:

$$H \cdot c^T = 0 \qquad \forall c \in C$$

Also ist C im Lösungsraum L des linearen Gleichungssystemes $H \cdot v^T = 0$ enthalten. Damit gilt:

$$k = \dim C \leq \dim L = n - \mathrm{Rang}(H) = n - (n-k) = k$$

Aus $\dim C = \dim L$ folgt $C = L$.

□

Mit Hilfe der kanonischen Generatormatrix läßt sich eine Kontrollmatrix besonders leicht finden:

Satz 6.15
Der lineare $[n,k]$-Code C habe die kanonische Generatormatrix $G = [I_k|A]$. Dann ist die Matrix $H = [-A^T|I_{n-k}]$ eine Kontrollmatrix zu C, die sogenannte kanonische Kontrollmatrix.

Beweis. Die $n-k$ Zeilen von H sind linear unabhängig (wegen I_{n-k}), daher gilt $\mathrm{Rang}(H) = n - k$. Zu zeigen bleibt $H \cdot G^T = 0$. Dies ist offensichtlich wegen

$$[-A^T|I_{n-k}][I_k|A] = -A^T + A^T = 0.$$

□

Betrachten wir das Beispiel $C := \{(000), (011), (110), (101)\}$, $n = 3$ und $k = 2$:

$$G = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \qquad A = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

Es gilt:

$$H = \begin{bmatrix} A^T | I_1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \end{bmatrix}$$

Definition 6.16 (Äquivalente Codes)
Zwei lineare Codes $C_1, C_2 \subseteq \mathbb{F}^n$ mit Generatormatrizen $G_1, G_2 \in M_{k,n}(\mathbb{F})$ heißen äquivalent, wenn es eine reguläre $k \times k$-Matrix T und eine $n \times n$-Permutationsmatrix P gibt mit $G_2 = T\ G_1\ P$.

Satz 6.17
Zu jedem linearen Code C_1 existiert ein äquivalenter Code C mit kanonischer Basismatrix $G = [I_k | B_{k,n-k}]$ und kanonischer Kontrollmatrix $H = \left[-B_{k,n-k}^T | I_{n-k}\right]$.

Beweis. Sei G_1 Generatormatrix zu C_1 mit Rang (k). Dann gibt es eine Permutationsmatrix P so daß die ersten k Spalten von $G_1\ P$ linear unabhängig sind. Es bezeichne S die Matrix bestehend aus den ersten k Spalten von $G_1\ P$. Dann ist die Generatormatrix $S^{-1}\ G_1\ P$ in kanonischer Form. □

6.4 Hamming-Codes

Der binärer Hamming-Code ist ein $[2^r - 1, 2^r - 1 - r]$-Code mit $\mathbb{F} = \mathbb{Z}_2$. Die PCH-Matrix hat als Spalten alle $2^r - 1$ Vektoren in $\mathbb{Z}_2^r \setminus \{0\}$. Für $r = 3$ erhalten wir den $[7, 4]$-Code mit der PCH-Matrix:

$$\begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

Die Minimaldistanz des Hamming-Codes C ist:

$$d(C) = \min \{ w(x) \mid x \in C \setminus \{0\} \}$$

Lemma 6.18
Der Hamming-Code C hat Minimaldistanz $d(C) = 3$ und ist 1-fehlerkorrigierend.

Beweis. Die Annahme $d(C) < 3$ führt offenbar zum Widerspruch:

- $d(C) = 1$: In der PCH-Matrix ist eine Spalte 0 — Widerspruch.
- $d(C) = 2$: In der PCH-Matrix tritt eine Spalte doppelt auf — Widerspruch.

Somit gilt $d(C) \geq 3$. Andererseites gibt es drei Spalten in der PCH-Matrix, die linear abhängig sind, also $d(C) \leq 3$. □

6.5 Hamming-Schranke und t-perfekte Codes

Sei $\mathbb{F}_q$ Körper mit q Elementen. Den Minimaldistanz eines Codes $C \subseteq \mathbb{F}_q^n$ haben wir definiert als:

$$d(C) = \min \{d(x,y) \mid x,y \in C,\ x \neq y\}$$

mit $d(x,y) = |\{i : x_i \neq y_i\}|$. Ziel ist es, Codes $C \subseteq \mathbb{F}_q^n$ zu finden mit:

1. $d(C)$ bei festem $|C|$ möglichst groß.
2. $|C|$ bei festem $d(C)$ möglichst groß.

Satz 6.19 (Hamming-Schranke)
Sei $M(n,d,q) := \max\left\{|C| : C \subseteq \mathbb{F}_q^n,\ d(C) \geq d\right\}$. *Für ungerades* $d = 2t+1$ *gilt:*

$$M(n,d,q) \leq \frac{q^n}{\sum_{i=0}^{t} \binom{n}{i}(q-1)^i}.$$

Beweis. Sei $C \subseteq \mathbb{F}_q^n$ Code mit $d(C) \geq 2t+1$. Sei

$$B_t(a) := \left\{b \in \mathbb{F}_q^n \;\middle|\; d(a,b) \leq t\right\}.$$

die Kugel um a mit Hamming-Radius t. Wegen $d(C) \geq 2t+1$ gilt $B_t(a) \cap B_t(b) = \emptyset$ für alle $a,b \in C$ mit $a \neq b$. Wir folgern $q^n \geq |C| \cdot |B_t(a)|$. Es gibt $\binom{n}{i}(q-1)^i$ Wörter in $B_t(a)$ mit Hamming-Abstand i zu a und somit:

$$|B_t(a)| = \sum_{i=0}^{t} \binom{n}{i}(q-1)^i.$$

Es folgt:

$$M(n,d,q) \leq \frac{q^n}{\sum_{i=0}^{t} \binom{n}{i}(q-1)^i}$$

□

Definition 6.20 (t-perfekter Code)
Eine Code $C \subseteq \mathbb{F}_q^n$ *heißt* t*-perfekt, wenn* $d(C) \geq 2t+1$ *und*

$$|C| = \frac{q^n}{\sum_{i=0}^{t} \binom{n}{i}(q-1)^i}.$$

Der Code $C \subseteq \mathbb{F}_q^n$ ist t-perfekt, wenn die Kugeln $B_t(a)$ den Raum $\mathbb{F}_q^n$ disjunkt zerlegen, d.h.:

$$\mathbb{F}_q^n = \dot{\bigcup_{a \in C}} B_t(a)$$

Korollar 6.21
Der $[2^r - 1, 2^r - 1 - r]$-Hamming-Code C ist 1-perfekt.

Beweis. Wegen $|C| = 2^{2^r-1-r}$ gilt:

$$M(2^r - 1, 1, 2) = \frac{2^{2^r-1}}{\sum_{i=0}^{1} \binom{2^r-1}{i}} = \frac{2^{2^r-1}}{2^r} = 2^{2^r-1-r}$$

□

Satz 6.22
Sei $\mathbb{F}$ ein endlicher Körper und $C \subset \mathbb{F}^n$ ein linearer $[n, k]$-Code mit PCH-Matrix $H = [u_1, \ldots, u_n] \in M_{r,n}(\mathbb{F})$ mit $r + k = n$. Dann sind folgende Aussagen äquivalent

1. *$d(C) = d$.*
2. *Je $d - 1$ der Vektoren $u_1, \ldots, u_n$ sind linear unabhängig.*

Beweis. Wir zeigen zuerst „1. ⇒ 2.“. Angenommen die Spaltenvektoren $u_{i_1}, u_{i_2}, \ldots, u_{i_{d'}}$ mit $d' < d$ sind linear abhängig: $\sum_{j=1}^{d'} u_{i_j} \cdot c'_{i_j} = 0$ mit $(c_{i_1}, \ldots, c_{i_d}) \neq 0$. Die Koordinaten c_{i_j} liefern durch Nullen ergänzt ein Codewort c mit Gewicht $\leq d' < d$. – Widerspruch zur Voraussetzung.

Für „2. ⇒ 1.“ nehmen wir an, es gebe ein Codewort $C = (c_1, \ldots, c_n)$ mit Gewicht $d' < d$. Wegen $\sum_{i=1}^{n} u_i \cdot c_i = 0$ sind die Vektoren u_i mit $c_i \neq 0$ linear abhängig. Damit gibt es im Widerspruch zur Annahme $d - 1$ linear
□

Kapitel 7

Endliche Körper und irreduzible Polynome in $\mathbb{Z}_p[x]$

7.1 Endliche Körper

Zu jedem Körper $\mathbb{K}$ gibt es einen kanonischen Ringhomomorphismus

$$\begin{array}{rcccl} f & : & \mathbb{Z} & \to & \mathbb{K} \\ & & m & \mapsto & \underbrace{1_K + \cdots + 1_K}_{m\text{-mal}} \end{array} .$$

Definition 7.1
Sei $\mathbb{K}$ *Körper. Die* Charakteristik *von* $\mathbb{K}$ *ist* $\operatorname{char}(\mathbb{K}) := p \in \mathbb{N}_{>0}$ *mit* $\ker(f) = (p) = p\mathbb{Z}$.

Der Kern des Ringhomomorphismus $\ker(f)$ ist ein Ideal in $\mathbb{Z}$. $\ker(f)$ ist Hauptideal weil $\mathbb{Z}$ Euklidischer Ring ist, also $\ker(f) = (p)$ für ein $p \in \mathbb{N}_{>0}$. Im Fall $p = 0$ gilt $\ker(f) = \{0\}$. Im Fall $p \neq 0$ ist p der ggT aller Zahlen $n \in \ker(f) - \{0\}$.

Satz 7.2
Die Charakteristik $\operatorname{char}(\mathbb{K})$ *ist entweder eine Primzahl oder* 0.

Beweis. Es gilt: $\mathbb{Z}/\ker(f) \cong f(\mathbb{Z}) \subseteq K$. Angenommen, es sei $(\ker(f)) = (n \cdot m)$ mit $n, m \in \mathbb{N} \setminus 1$. Dann gilt in $\mathbb{K}$:

$$f(n) = n + (n \cdot m) \neq 0 \qquad \text{und} \qquad f(m) = m + (n \cdot m) \neq 0$$

Aber

$$f(n \cdot m) = f(n) \cdot f(m) = (n \cdot m)$$

ist die 0 in $\mathbb{K}$. Also haben $f(n), f(m)$ keine Inversen in $\mathbb{K}$ — Widerspruch. □

Definition 7.3 (Primkörper)
Der Primkörper $\mathbb{K}_0$ zum Körper $\mathbb{K}$ ist der kleinste Unterkörper von $\mathbb{K}$.

Im Fall $\operatorname{char}(\mathbb{K}) = 0$ gilt $\mathbb{K}_0 \cong \mathbb{Q}$. Im Fall $\operatorname{char}(\mathbb{K}) = p \neq 0$ gilt $\mathbb{K}_0 \cong \mathbb{Z}/p\mathbb{Z}$.

Satz 7.4
Für jeden endlichen Körper $\mathbb{K}$ gilt $|\mathbb{K}| = \operatorname{char}(\mathbb{K})^n$ mit $n \in \mathbb{N}$.

Beweis. Sei $\mathbb{K}_0 \cong \mathbb{Z}/p\mathbb{Z}$ Primkörper von $\mathbb{K}$. $\mathbb{K}$ ist Vektorraum über $\mathbb{K}_0$. Sei $\{a_1, \ldots, a_n\} \subseteq K$ eine maximale Menge von über $\mathbb{K}_0$ linear unabhängigen Elementen. Es gilt

$$\sum_{i=1}^{n} t_i a_i \neq 0 \qquad \text{für alle } (t_1, \ldots, t_n) \in \mathbb{K}_0^n \setminus \{0^n\}$$

Dann gilt $\mathbb{K} = \left\{ \sum_{i=1}^{n} t_i a_i \;\middle|\; (t_1, \ldots, t_n) \in \mathbb{K}_0^n \right\}$ und $|\mathbb{K}| = |\mathbb{K}_0|^n$. □

Wie sehen die Körper mit p^n Elementen aus? Sei p prim, $f \in \mathbb{Z}_p[x]$ irreduzibel und normiert, dann ist $\mathbb{Z}_p[x]/(f)$ Körper mit $p^{\operatorname{grad}(f)}$ vielen Elementen.

Definition 7.5 (Division mit Rest)
Zu $f, g \in \mathbb{K}[x]$, $g \neq 0$, gibt es eindeutig bestimmte Polynome $q, r \in \mathbb{K}[x]$ mit $f = gq + r, \qquad \operatorname{grad}(r) < \operatorname{grad}(g)$.

Lemma 7.6
Der Polynomring $\mathbb{K}[x]$ zum Körper $\mathbb{K}$ ist ein Euklidischer Ring, d.h. es gibt eine eindeutige Division mit Rest und der Euklidische Algorithmus berechnet zu $f, g \in \mathbb{K}[x] \setminus \{0\}$, $g \neq 0$, den $\operatorname{ggT}(f, g)$.

Beweis. Eindeutigkeit des ggT. Sei

$$f = gq_i + r_i, \qquad \operatorname{grad}(r_i) < \operatorname{grad}(g), \quad i = 1, 2$$

Es folgt $g(q_1 - q_2) = r_1 - r_2$. Wegen $\operatorname{grad}(r_1 - r_2) < \operatorname{grad}(g)$ ist dies nur für $q_1 = q_2$ möglich. Also gilt $r_1 = r_2$.
Existenz des ggT. Sei

$$f = \sum_{i=0}^{n} a_i x^i, \qquad g = \sum_{i=0}^{m} b_i x^i$$

mit $a_n, b_m \neq 0$ und $n \geq m$. Induktion über $\operatorname{grad}(f) = n$. Aus

$$\underbrace{f - \frac{a_n}{b_m} x^{n-m} g}_{\operatorname{grad}<n} = g\overline{q} + \overline{r} \text{ folgt } f = g(\overline{q} + \tfrac{a_n}{b_m} x^{n-m}) + \overline{r}. \qquad \square$$

Korollar 7.7
Für einen $\mathbb{K}$ Körper ist jedes Ideal $I \subseteq K[x]$ von der Form $I = (g) = g \cdot K[x]$ mit $g \in \mathbb{K}[x]$, d.h. $\mathbb{K}[x]$ ist Hauptidealring.

Beweis. Falls $I = \{0\}$, ist die Behauptung klar. Sei $I \neq \{0\}$ und $g \in I - 0$ Polynom kleinsten Grades. Wir zeigen:

$$I = (g)$$

Zu $f \in I$ gibt es $q, r \in \mathbb{K}[x]$ mit

$$f = gq + r, \qquad r = 0 \text{ oder } \operatorname{grad}(r) < \operatorname{grad}(g)$$

Es folgt $r = f - gq \in I$ und nach Wahl von g gilt $r = 0$, da $r \in I$. Also $f \in (g)$. $\square$

Definition 7.8
Ein Polynom $f \in \mathbb{K}[x]$ ist irreduzibel, *wenn*

1. $f \neq 0$, $f \notin \mathbb{K}$
2. $\forall g, h \in \mathbb{K}[x] \; : \; f = gh \implies (g \in \mathbb{K} \vee h \in \mathbb{K})$

Ein Polynom $f \in \mathbb{K}[x]$, das nicht irreduzibel ist, nennt man reduzibel.

Lemma 7.9
Seien $f, g, h \in \mathbb{K}[x]$, h irreduzibel. Dann gilt: $h \mid f \cdot g \implies (h \mid f \vee h \mid g)$

Beweis. Angenommen, $h \nmid f$ und $h \nmid g$. Dann gilt $\operatorname{ggT}(h, f) = \operatorname{ggT}(h, g) = 1$ und somit $1 = ha + fb = hc + gd$ mit $a, b, c, d \in \mathbb{K}[x]$.
Es folgt $1 = (ha + fb)(hc + gd) = h^2ac + h(agd + cfh) + fgbd$
Aus $h \mid fg$ folgt $h \mid 1$, Widerspruch zu h irreduzibel. $\square$

Satz 7.10
Jedes normierte Polynom $f \in \mathbb{K}[x]$ hat bis auf Vertauschung der Faktoren, eine eindeutige Zerlegung $f = \prod_{i=1}^{r} h_i^{e_i}$ mit normierten, irreduziblen Polynomen h_i.

Der Beweis folgt aus dem vorangehenden Lemma, vergleiche Übungsaufgabe B.43. Der Satz gilt nicht nur für $f \in \mathbb{K}[x]$ sondern auch für beliebige, normierte $f \in \mathbb{Z}[x]$.

Satz 7.11
Sei $\mathbb{K}$ Körper und $f \in \mathbb{K}[x] \setminus \{0\}$. Dann ist $\mathbb{K}[x]/(f)$ genau dann Körper, wenn f irreduzibel ist.

Beweis.

„⇐“ Angenommen, f sei reduzibel. Falls $f \in \mathbb{K}^*$, ist $(f) = K[x]$ und $\mathbb{K}[x]/(f)$ kein Körper. Sei $f = gh$ mit $g, h \notin K$. Dann sind $g + (f)$ und $h + (f) \in \mathbb{K}[x]/(f)$ jeweils ungleich 0. Aber

$$(g + (f))(h + (f)) = gh + (f) = (f)$$

Somit haben $g + (f)$ und $h + (f)$ keine inversen Elemente, also ist $\mathbb{K}[x]/(f)$ kein Körper.

„⇒“ Sei f irreduzibel. Wir zeigen, daß zu jedem $g + (f) \in \mathbb{K}[x]/(f) - 0$ ein Inverses existiert. Weil $g \not| f$ und f irreduzibel ist, folgt $\mathrm{ggT}(g, f) = 1$. Also gibt es Polynome $a, b \in \mathbb{K}[x]$ mit $ag + fb = 1$, d.h. $a + (f)$ ist Inverses zu $g + (f)$. □

7.2 Zerfällungskörper

Lemma 7.12
Für jeden Körper $\mathbb{K}$ mit p^n Elementen und Primkörper $\mathbb{Z}_p$ gilt

$$x^{p^n} - x = \prod_{a \in \mathbb{K}} (x - a) \in \mathbb{Z}_p[x].$$

Beweis. Nach dem Satz von Lagrange (Satz A.11) gilt für alle $a \in \mathbb{K}^*$

$a^{p^n - 1} = 1$, und somit für alle $a \in \mathbb{K} : a^{p^n} = a$. Damit durchläuft $a \in \mathbb{K}$ die p^n Nullstellen von $x^{p^n} - x$. Nullstellen. □

Damit ist $\mathbb{K}$ der kleinste Körper über dem $x^{p^n} - x \in \mathbb{Z}_p[x]$ in Linearfaktoren zerfällt. Dies ist der *Zerfällungskörper* von $x^{p^n} - x$. Nach Satz 7.15 ist der Zerfällungskörper bis auf Isomorphie eindeutig bestimmt, im Vorgriff bezeichnen wir ihn mit $\mathbb{F}_{p^n}$, $\mathrm{GF}(p^n)$.

Korollar 7.13
1. *Folgende Aussagen sind äquivalent:*
   i) $m \mid n$, *ii)* $x^{p^m} - x \mid x^{p^n} - x$, *iii)* $x^{p^m - 1} - 1 \mid x^{p^n - 1} - 1$.
2. *Der Körper $\mathbb{F}_{p^n}$ enthält $\mathbb{F}_{p^m}$ genau dann wenn $m \mid n$.*

Beweis. 1. Wir zeigen $m \mid n$ ist äquivalent zu $p^m - 1 \mid p^n - 1$.

$$p^n - 1 \;=\; (p^m - 1)(p^{n-m} + p^{n-2m} + \cdots + \underbrace{p^{n - \frac{n}{m} m}}_{= p^0 = 1}) \quad \Leftrightarrow \quad m \mid n.$$

Die Äquivalenz von ii) und iii) ist trivial.

2. Wir zeigen: $\mathbb{K}' := \left\{ a \in \mathbb{F}_{p^n} \;\middle|\; a^{p^m} = a \right\}$ ist Körper mit p^m Elementen.

Offenbar gilt $0, 1 \in \mathbb{K}'$. Zu zeigen: $a, b \in \mathbb{K}' \quad \Longrightarrow \quad a \cdot b, a + b \in \mathbb{K}'$.

$$\begin{aligned} (a \cdot b)^{p^m} &= a^{p^m} \cdot b^{p^m} = a \cdot b \\ (a+b)^{p^m} &= \sum_{i=0}^{p^m} \binom{p^m}{i} a^{p^m - i} b^i = a^{p^m} + b^{p^m} = a + b. \end{aligned}$$

□

Satz 7.14
Sei $f \in \mathbb{Z}_p[x]$ irreduzibel vom Grad d und $\alpha \in \mathbb{F}_{p^d}$ Nullstelle von f. Dann hat f genau die Nullstellen $\alpha, \alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{d-1}}$.

Beweis. Sei $f = \sum_{i=0}^{d-1} f_i x^i$. Es gilt:

$$f(\alpha^p) = \sum_{i=0}^{d-1} f_i \alpha^{pi} = \sum_{i=0}^{d-1} f_i^p \alpha^{pi} = \left(\sum_{i=0}^{d-1} f_i \alpha^i \right)^p = f(\alpha)^p = 0$$

Induktion liefert die Nullstellen $\alpha, \alpha^p, \ldots, \alpha^{p^{d-1}}$.

Wir zeigen: $\alpha, \alpha^p, \ldots, \alpha^{p^{d-1}}$ sind paarweise verschieden.

Angenommen, $\alpha^{p^j} = \alpha^{p^i}$ mit $1 \leq i < j \leq d-1$. Dann gilt $\alpha^{p^i\left(p^{j-i}-1\right)} = 1$ und $\alpha^{p^d-1} = 1$ somit $\operatorname{ord}(\alpha) \mid p^{j-i} - 1$. Nach Korollar 7.13 ist α im Unterkörper

$$K' = \left\{ a \in \mathbb{F}_{p^d} \;\middle|\; a^{p^{j-i}-1} = a \right\}$$

von $\mathbb{F}_{p^d}$. Sei g das *Minimalpolynom* von α, d.h. das normierte Polynom kleinsten Grades $g \in \mathbb{Z}_p[x]$, so daß $g(\alpha) = 0$.

Wir zeigen: $\operatorname{grad}(g) \leq j - i < d$.

Angenommen, $\operatorname{grad}(g) = d = \operatorname{grad}(f)$. Dann ist

$$\left\{ \sum_{i=0}^{d-1} b_i \alpha^i \;\middle|\; b_i \in \mathbb{Z}_p \right\}$$

Körper der Ordnung p^d, und somit gleich $\mathbb{F}_{p^d}$. Widerspruch zu $\alpha \in \mathbb{K}'$. Aus $\operatorname{grad}(g) < d$ folgt $g \mid f$, im Widerspruch zu f irreduzibel. Also ist die Annahme $\alpha^{p^j} = \alpha^{p^i}$ falsch. □

Satz 7.15
Sei $\mathbb{K}$ Körper. Jedes Polynom $f \in \mathbb{K}[x]$ hat einen, bis auf Isomorphie eindeutig bestimmten, Zerfällungskörper.

Beweis. (Skizze) Sei $\mathbb{K}$ ein endlicher Körper mit $\text{char}(\mathbb{K}) = p$. O.B.d.A. sei

$$f = \sum_{i=0}^{d} f_i x^i$$

irreduzibel von Grad $d > 1$ und normiert.

- Existenz des Zerfällungskörpers: $\mathbb{F} := \mathbb{K}[x]/(f)$ ist Erweiterungskörper zu $\mathbb{K}$. Es gilt
$$|\mathbb{F}| = |\mathbb{K}|^d$$
und $x^0, \ldots, x^{d-1} \pmod f$ ist Basis des Vektorraums $\mathbb{F}$ über $\mathbb{K}$.
$$\mathbb{F} = \left\{ \sum_{i=0}^{d-1} b_i x^i \bmod f \;\middle|\; b_i \in \mathbb{K} \right\}$$
Das Polynom f hat die Nullstelle $\alpha := x \bmod f \in \mathbb{F}$. Nach Satz 7.14 hat f genau die Nullstellen
$$\alpha, \alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{d-1}}$$
Somit $f(x) = \prod_{i=0}^{d-1} \left(x - \alpha^{p^i}\right)$. $\mathbb{F}$ ist der Zerfällungskörper von f, denn f zerfällt über $\mathbb{F}$ und $\mathbb{F}$ ist minimal.
- Eindeutigkeit: Sei $\mathbb{K}(\beta)$ kleinster Erweiterungskörper zu $\mathbb{K}$, der die Nullstelle β von f enthält. Dann gibt es einen Isomorphismus
$$\begin{array}{rcccc} \varphi & : & \mathbb{K}[x]/(f) & \to & \mathbb{K}(\beta) \\ & & x \bmod f & \mapsto & \beta \end{array}$$

□

Satz 7.16
Sei p prim, $q = p^n$. Der Körper $\mathbb{F}_q$ mit p^n Elementen ist der Zerfällungskörper von $x^{p^n} - x$.

Beweis. Nach Lemma 7.12 zerfällt $x^{p^n} - x$ über jedem Körper mit p^n Elementen. Andererseits ist der Zerfällungskörper von $x^{p^n} - x$ bis auf Isomorphie eindeutig bestimmt. □

Korollar 7.17
Seien $f, g \in \mathbb{K}[x]$ irreduzible Polynome mit $\text{grad}(f) = \text{grad}(g)$. Dann gilt:

$$\mathbb{K}[x]/(f) \cong \mathbb{K}[x]/(g)$$

Satz 7.18 (Unterkörper-Kriterium)
Sei p prim und $q = p^n$ Primzahlpotenz. Die Unterkörper von $\mathbb{F}_q$ sind bis auf Isomorphie genau die Körper $\mathbb{F}_{p^m}$ mit $m \mid n$.

Beweis. Wir zeigen beide Richtungen:

„⇒“ Angenommen, $\mathbb{F} \subseteq \mathbb{F}_q$ ist Unterkörper von $\mathbb{F}_q$. Wegen $\mathrm{char}(\mathbb{F}) = p$ gilt $|\mathbb{F}| = p^m$. Es gilt $\mathbb{F} = \mathbb{F}_{p^m}$. $\mathbb{F}_q$ ist Vektorraum über $\mathbb{F}_{p^m}$. Also $q = (p^m)^{m'}$ mit $m' \in \mathbb{N}$. Somit: $n = m \cdot m'$.

„⇐“ Angenommen, $m \mid n$. Es folgt $p^m - 1 \mid p^n - 1$, somit $x^{p^m} - x \mid x^{p^n} - x$. Wir erhalten:

$$\begin{array}{ccc} \mathbb{F}_{p^m} & \subseteq & \mathbb{F}_{p^n} \\ (\text{Zerfällungskörper von } x^{p^m} - x) & & (\text{Zerfällungskörper von } x^{p^n} - x) \end{array}$$

□

Beispiel 7.19 (Unterkörper)
Sei $p = 2$ und $n = 30$, d.h. $q = 2^{30}$. Die Unterkörper von $\mathbb{F}_q$ sind in Abbildung 13 dargestellt.

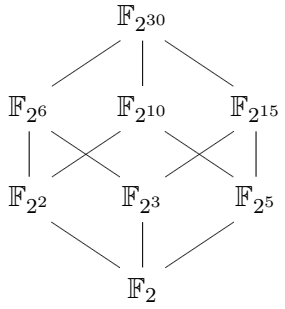


Abbildung 13: Unterkörper von $\mathbb{F}_{2^{30}}$

7.3 Normalbasen

Eine Alternative zu den Polynombasen

$$1, x, x^2, \ldots, x^{d-1} \pmod{f}$$

zu $\mathbb{F}_{p^d} \cong \mathbb{F}_p[x]/(f)$, $d = \mathrm{grad}(f)$ bilden die *Normalbasen.*

Definition 7.20 (Normalbasis)
Eine Basis der Form $a, a^p, \ldots, a^{p^{d-1}}$ von $\mathbb{F}_{p^d}$ über $\mathbb{F}_p$ heißt Normalbasis.

Satz 7.21
Jeder endliche Körper $\mathbb{F}_{p^n}$ besitzt eine Normalbasis über $\mathbb{F}_p$.

Beweis. [LN86], Theorem 2.3.5. □

Berechnung der p-ten Potenzen, p-ten Wurzeln mit Normalbasen: Sei $a, a^p, \ldots, a^{p^{d-1}}$ Normalbasis.

$$(c_0, \ldots, c_{d-1}) \in \mathbb{F}_p^d \qquad \longleftrightarrow \qquad \sum_{i=0}^{d-1} c_i a^{p^i} \in \mathbb{F}_{p^d}$$

p-te Potenz:

$$(c_0, \ldots, c_{d-1}) \quad \mapsto \quad (c_{d-1}, c_0, \ldots, c_{d-2})$$

p-te Wurzel:

$$(c_0, \ldots, c_{d-1}) \quad \mapsto \quad (c_1, \ldots, c_{d-1}, c_0)$$

In der Koordinatendarstellung bezüglich einer Normalbasis gilt:

1. Potenzieren mit p ist Rechtssshift.
2. p-te Wurzel ist Linksshift.

$$\left(\sum_{i=0}^{d-1} c_i a^{p^i}\right)^p = \sum_{i=0}^{d-1} c_i^p a^{p^{i+1}} \overset{i+1=j}{=} \sum_{j=0}^{d-1} c_{j-1} a^{p^j}$$

Wir benutzen, daß $a^{p^n} = a$.

7.4 Optimale Aufteilung von Information

M.O. Rabin hat in [R89] ein Verfahren zur Lösung der folgenden Problems vorgestellt: Teile ein File F der Länge $|F|$, $|F| = 0 \bmod m$ derart in n „Teile“ F_i $(i = 1, 2, \ldots, n)$ daß

1. $|F_i| = \frac{|F|}{m}$ für $i = 1, 2, \ldots, n$
2. Aus beliebigen m der n Teile kann man F rekonstruieren

Die Aufteilung ist *optimal* im Sinne, daß $\sum_{j=1}^{m} \left|F_{i_j}\right| = |F|$.

Wähle einen hinreichend großen endlichen Körper $\mathbb{F}$, z.B. $\mathbb{F}_{2^8}, \mathbb{F}_q$. Es gilt $|\mathbb{F}_{2^8}| = 256$. $\mathbb{F}_{2^8}$ ist Vektorraum der Dimension 8 über $\mathbb{F}_2$. $\mathbb{F}_{2^8}$ entspricht der Menge aller Bytes. In $\mathbb{F}_{2^8}$ kann man alle Buchstaben (groß und klein, mit Akzenten) und Ziffern, sowie Steuerzeichen kodieren.

Wähle $A \in M_{n,m}(\mathbb{F}_{2^8})$ so, daß von den n Zeilen je m linear unabhängig sind. Sei $|\mathbb{F}| = 8mk$. Schreibe F als $m \times k$-Matrix über $\mathbb{F}_{2^8}$:

$$F = (f_{i,j})_{1 \le i \le m,\, 1 \le j \le k}$$

Die Teile $F_1, \ldots, F_n$ seien die Zeilenvektoren der Matrix

$$C := A \cdot F \quad \in M_{n,k}(\mathbb{F}_{2^8})$$

Rekonstruktion von F aus m Zeilen $C_{i_1}, \ldots, C_{i_m}$ von C: Seien $A_{i_1}, \ldots, A_{i_m}$ die zugehörigen m Zeilen von A. Löse

$$\begin{bmatrix} C_{i_1} \\ \vdots \\ C_{i_m} \end{bmatrix} = \begin{bmatrix} A_{i_1} \\ \vdots \\ A_{i_m} \end{bmatrix} F$$

nach F auf:

$$F = \begin{bmatrix} A_{i_1} \\ \vdots \\ A_{i_m} \end{bmatrix}^{-1} \begin{bmatrix} C_{i_1} \\ \vdots \\ C_{i_m} \end{bmatrix}$$

Algorithmus 10 Konstruktion von m-fach linear unabhängigen $A_1, \ldots, A_n, \ldots \in \mathbb{Z}^m$

EINGABE: $b_1, \ldots, b_m \in \mathbb{Z}^m$ linear unabhängig

1. Setze $\nu := 1$.

2. FOR $i = 2, \ldots, m$ DO $b_i := b_i + b_{i-1}$

3. Gib $A_\nu := b_m$ aus

4. $\nu := \nu + 1$, GOTO 2

AUSGABE: $A_1, \ldots, A_n, \ldots \in \mathbb{Z}^m$

In Algorithmus 10 bezeichne $b_i^{(\nu)}$ den Vektor b_i am Ende von Runde ν. Dann gilt

$$(b_1^{(\nu)}, \ldots, b_m^{(\nu)}) = (b_1, b_2, \ldots, b_m)\, T_m^\nu$$

wobei

$$T_m = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ & 1 & \cdots & 1 \\ & & \ddots & \vdots \\ 0 & & & 1 \end{bmatrix} \quad \in M_{m,m}(\mathbb{Z})$$

wobei $(b_1^{(\nu)}, \ldots, b_m^{(\nu)})$ die $m \times m$-Matrix sei, die aus den Spaltenvektoren $b_1^{(\nu)}, \ldots, b_m^{(\nu)}$ bestehe.

Lemma 7.22
Es gibt Polynome $g_k \in \mathbb{Q}[x]$ vom Grad k, $k = 0, 1, \ldots$ mit

1. $g_0 = 1$
2. $g_k(j) = \sum_{\nu=1}^{j} g_{k-1}(\nu)$
   (a) $g_k(j) = g_k(j-1) + g_{k-1}(j)$
   (b) $g_k(j) = g_k(j-1) + g_{k-1}(j-1) + \cdots + g_0(j-1)$
3. $A_\nu = \sum_{i=1}^{m} g_{m-i}(\nu) b_i$.

Beweis (Zu 3.). Sei $T_m^\nu = (t_{i,k}^{(\nu)})_{1 \le i,k \le m}$. Wir zeigen durch Induktion über ν, daß:

$$t_{i,k}^{(\nu)} = g_{k-i}(\nu) \qquad \text{für } i \le k$$

- Sei $\nu = 0$. Für $i \le k$ gilt $t_{i,k}^{(\nu)} = 1 = g_{k-i}(0)$.
- Sei $\nu > 0$.

$$(t_{i,k}^{(\nu)})_{1 \le i,k \le m} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ & 1 & \cdots & 1 \\ & & \ddots & \vdots \\ 0 & & & 1 \end{bmatrix} (t_{i,k}^{(\nu-1)})_{1 \le i,k \le m}$$

Damit folgt:

$$t_{i,k}^{(\nu)} = \sum_{i \le j \le k} t_{j,k}^{(\nu-1)} \overset{\text{Ind.vor.}}{=} \sum_{i \le j \le k} g_{k-j}(\nu - 1) \overset{(2.b)}{=} g_{k-i}(\nu)$$

□

Satz 7.23
Je m der Vektoren $A_1, \ldots, A_n$ sind linear unabhängig.

Beweis. Sei $1 \le i_1 < i_2 < \cdots < i_m \le n$.

$$(A_{i_1}, \ldots, A_{i_m}) = (b_1, \ldots, b_m) \cdot G$$

wobei:

$$G = \begin{bmatrix} g_{m-1}(i_1) & \cdots & g_{m-1}(i_m) \\ g_{m-2}(i_1) & \cdots & g_{m-2}(i_m) \\ \vdots & \ddots & \vdots \\ g_0(i_1) & \cdots & g_0(i_m) \end{bmatrix} \in M_{m,m}(\mathbb{Z})$$

Die Determinante $\det G$ ist ein Polynom in $i_1, \ldots, i_m$ vom Grad $\sum_{i=1}^{m}(m-i) = \frac{m(m-1)}{2}$. Die Determinante verschwindet, wenn $i_\nu = i_\mu$ für $\nu \neq \mu$, d.h. Division von $\det G$ durch $i_\nu - i_\mu$ liefert den Rest 0. Somit gilt:

$$\prod_{1 \leq \nu < \mu \leq m} (i_\nu - i_\mu) \mid \det G$$

Weil $\operatorname{grad}\left(\prod_{1 \leq \nu < \mu \leq m} (i_\nu - i_\mu)\right) = \operatorname{grad}(\det G)$ folgt

$$\det G = c \cdot \prod_{1 \leq \nu < \mu \leq m} (i_\nu - i_\mu)$$

mit einer festen Konstanten c. Somit gilt für $1 \leq i_1 < i_2 < \cdots < i_m \leq n$, daß $\det G \neq 0$. Die lineare Unabhängigkeit von $A_{i_1}, \ldots, A_{i_m}$ folgt aus der linearen Unabhängigkeit von $b_1, \ldots, b_m$. □

Satz 7.24 (Van de Monde)

$$\det(\alpha_1, \ldots, \alpha_m) := \det \begin{bmatrix} \alpha_1^0 & \cdots & \alpha_m^0 \\ \vdots & \ddots & \vdots \\ \alpha_1^{m-1} & \cdots & \alpha_m^{m-1} \end{bmatrix} = \pm \prod_{1 \leq i < j \leq m} (\alpha_i - \alpha_j).$$

Beweis. Die Determinante $\det(\alpha_1, \ldots, \alpha_m) \in \mathbb{Z}[\alpha_1, \ldots, \alpha_m]$ ist ein homogenes Polynom vom Grad $\frac{m(m-1)}{2}$ in $\alpha_1, \ldots, \alpha_m$. Es gilt

$$\alpha_i - \alpha_j \mid \det(\alpha_1, \ldots, \alpha_m) \qquad \text{für alle } 1 \leq i < j \leq m,$$

denn $\det(\alpha_1, \ldots, \alpha_m) = (\alpha_i - \alpha_j)q(\alpha_1, \ldots, \alpha_m) + r(\alpha_1, \ldots, \alpha_m)$ mit $\operatorname{grad}_{\alpha_i} r(\alpha_1, \ldots, \alpha_m) = 0$, also r konstant und somit $r = 0$. Weil die $\alpha_i - \alpha_j$ irreduzibel sind, folgt $\prod_{1 \leq i < j \leq m}(\alpha_i - \alpha_j) \mid \det(\alpha_1, \ldots, \alpha_m)$, und weil beide Polynome den Grad $m(m-1)/2$ haben folgt $\det(\alpha_1, \ldots, \alpha_m) = c \cdot \prod_{1 \leq i < j \leq m}(\alpha_i - \alpha_j)$. Die Koeffizienten von $\alpha_1^0 \alpha_2^1 \cdots \alpha_m^{m-1}$ ist jeweils ± 1, also $c = \pm 1$. □

7.5 Die irreduziblen Polynome in $\mathbb{Z}_p[x]$

Satz 7.25
Sei $f \in \mathbb{F}_p[x]$ irreduzibel vom Grad d. Dann gilt $f \mid x^{p^n} - x$ genau dann, wenn $d \mid n$.

Beweis. Wir zeigen beide Richtungen:

„⇒“ Angenommen, $f \mid x^{p^n} - x$. Dann zerfällt f in $\mathbb{F}_{p^n}$ (Zerfällungskörper von $x^{p^n} - x$). Somit gilt

$$\mathbb{F}_p[x]/(f) \cong \mathbb{F}_{p^\alpha} \subseteq \mathbb{F}_{p^n}$$

Nach Satz 7.18 folgt $d \mid n$.

„⇐“ Angenommen, $d \mid n$. Nach Satz 7.15 ist $\mathbb{F}_{p^\alpha}$ isomorph zum Zerfällungskörper von f. Somit $f \mid x^{p^d} - x$. Wegen $d \mid n$ folgt $f \mid x^{p^n} - x$.

□

Satz 7.26
Sei $\mathcal{F}$ die Menge der normierten, irreduziblen Polynome in $\mathbb{F}_p[x]$. Dann gilt:

$$x^{p^n} - x = \prod_{f \in \mathcal{F},\, \mathrm{grad}(f) \mid n} f$$

Beweis. $x^{p^n} - x$ ist Produkt von irreduziblen, normierten Polynomen f. $x^{p^n} - x$ ist quadratfrei, weil

$$\mathrm{ggT}\left(\tfrac{d}{dx}\left(x^{p^n} - x\right), x^{p^n} - x\right) = \mathrm{ggT}\left(-1, x^{p^n} - x\right) = 1$$

Somit ist $x^{p^n} - x$ Produkt paarweise verschiedener irreduzibler Faktoren. Die Behauptung folgt nun aus Satz 7.25. □

Sei $q = p^n$ Primzahlpotenz. Wir bezeichnen mit $N_q(d)$ die Anzahl der irreduziblen, normierten Polynome $f \in \mathbb{F}_q[x]$ vom Grad d.

Für p prim gilt (siehe Übungsaufgabe B.44)

$$N_p(2) = \tfrac{1}{2}(p^2 - p), \qquad N_p(3) = \tfrac{1}{3}(p^3 - p).$$

Satz 7.27
Es gilt $q^n = \sum_{d \mid n,\, d>0} d N_q(d)$ für $n \in \mathbb{N}$.

Beweis. Für die Menge $\mathcal{F}$ der normierten, irreduziblen Polynome in $\mathbb{F}_p[x]$ gilt $x^{p^n} - x = \prod_{f \in \mathcal{F},\, \mathrm{grad}(f) \mid n} f$
Somit $p^n = \sum_{f \in \mathcal{F},\, \mathrm{grad}(f) \mid n} \mathrm{grad}(f) = \sum_{d \mid n,\, d>0} d N_q(d)$. □

Es gilt zum Beispiel:

$$2^6 = N_2(1) + 2 \cdot N_2(2) + 3 \cdot N_2(3) + 6 \cdot N_2(6)$$

Ziel ist die Berechnung von $N_q(d)$. Im folgenden werde bei Summen über die Teiler einer Zahl stets nur über die *positiven* Teiler summiert, d.h. statt $d \mid n$, $d > 0$ schreiben wir kurz $d \mid n$.

Definition 7.28 (Möbius-Funktion μ)
Die Möbius-Funktion $\mu : \mathbb{N} \to \{0, \pm 1\}$ ist:

$$\mu(n) = \begin{cases} 1 & \text{falls } n = 1 \\ (-1)^k & \text{falls } n \text{ ist Produkt von } k \text{ verschiedenen Primzahlen} \\ 0 & \text{falls } p^2 \mid n \text{ mit } p \text{ prim} \end{cases}$$

Lemma 7.29
Für $n \in \mathbb{N}$ gilt:

$$\sum_{d \mid n} \mu(d) = \begin{cases} 1 & \text{falls } n \geq 1 \\ 0 & \text{falls } n = 0 \end{cases}$$

Beweis. Sei $n > 1$ und $p_1, \ldots, p_k$ seien die verschiedenen Primfaktoren von n.

$$\begin{aligned} \sum_{d \mid n} \mu(d) &= \mu(1) + \sum_{i=1}^{k} \mu(p_i) \; + \sum_{1 \leq i_1 < i_2 \leq k}^{k} \mu(p_{i_1} p_{i_2}) \; + \cdots + \; \mu(p_1 p_2 \cdots p_k) \\ &= 1 + \binom{k}{1}(-1) + \binom{k}{2}(-1)^2 + \cdots + \binom{k}{k}(-1)^k \\ &= (1 + (-1))^k \\ &= 0 \end{aligned}$$

□

Satz 7.30 (Möbius-Inversions-Formel)
Sei G additive, abelsche Gruppe und $h, H : \mathbb{N} \to G$. Dann sind folgende Aussagen äquivalent:

1. $H(n) = \sum_{d \mid n} h(d)$ *für alle* $n \in \mathbb{N}$

2. $h(n) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) H(d) = \sum_{d \mid n} \mu(d) H\left(\frac{n}{d}\right)$ *für alle* $n \in \mathbb{N}$

Beweis. Wir zeigen „1 ⇒ 2“: Mit Lemma 7.29 folgt:

$$\begin{aligned}
\sum_{d \mid n} \mu\left(\frac{n}{d}\right) H(d) &= \sum_{d \mid n} \mu(d) H\left(\frac{n}{d}\right) \\
&= \sum_{d \mid n} \mu(d) \sum_{c \mid \frac{n}{d}} h(c) && (1.) \\
&= \sum_{c \mid n} \sum_{d \mid \frac{n}{c}} \mu(d) h(c) \\
&= \sum_{c \mid n} h(c) \sum_{d \mid \frac{n}{c}} \mu(d) \\
&= h(n) && \text{(Lemma 7.29)}
\end{aligned}$$

Die Implikation „2 ⇒ 1“ zeigt man analog. □

Satz 7.31
Für $n \in \mathbb{N}$ gilt:

$$N_q(n) = \frac{1}{n} \sum_{d \mid n} \mu\left(\frac{n}{d}\right) q^d = \frac{1}{n} \sum_{d \mid n} \mu(d) q^{n/d}$$

Beweis. Wende Satz 7.30 auf $G = \mathbb{Z}$, $h(n) = nN_q(n)$ und $H(n) = q^n$ an. Dann gilt 1. in Satz 7.30 und somit auch 2. in Satz 7.30. □

Beispiel 7.32 ($\mathbf{N_q(20)}$)
Aus Satz 7.31 erhalten wir:

$$\begin{aligned}
N_q(20) &= \tfrac{1}{20}\left(\mu(1)q^{20} + \mu(2)q^{10} + \mu(4)q^5 + \mu(5)q^4 + \mu(10)q^2 + \mu(20)q^1\right) \\
&= \tfrac{1}{20}\left(q^{20} - q^{10} - q^4 + q^2\right)
\end{aligned}$$

Kapitel 8

Algebraische Codes

Sei $\mathbb{F}_q$ endlicher Körper mit q Elementen. Ein $[n,k]$-Code $C \subseteq \mathbb{F}_q^n$ ist ein linearer $\mathbb{F}_q$-Vektorraum der Dimension k.

8.1 Zyklische Codes

Definition 8.1
$C \subseteq \mathbb{F}_q^n$ *heißt* zyklisch *wenn*

$$(a_0, a_1, \ldots, a_{n-2}, a_{n-1}) \in C \qquad \Longrightarrow \qquad (a_{n-1}, a_0, a_1, \ldots, a_{n-2}) \in C$$

Wir betrachten folgenden Vektorraum-Isomorphismus

$$\begin{array}{rcccl} \psi & : & \mathbb{F}_q^n & \to & \mathbb{F}_q[x]/(x^n-1) \\ & & (a_0, a_1, \ldots, a_{n-1}) & \mapsto & \underbrace{a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1} \bmod x^n - 1}_{\text{Codepolynom } a(x) \in \mathbb{F}_q[x]} \end{array}$$

Der lineare Vektorraum $\psi(C)$ ist ein Ideal genau dann, wenn $x \cdot \psi(C) \subseteq \psi(C)$. Wegen

$$x \cdot \left(a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}\right) = a_{n-1} + a_0 x + \cdots + a_{n-2} x^{n-1} \bmod (x^n - 1)$$

ist dies genau für die zyklischen Codes C erfüllt.

Lemma 8.2
Folgende Aussagen sind äquivalent:

a) $C \subseteq \mathbb{F}_q^n$ ist ein zyklischer Code.

b) $\psi(C) \subseteq \mathbb{F}_q[x]/(x^n - 1)$ *ist ein Ideal*

Lemma 8.3
Sei $h \in \mathbb{F}_q[x]$ *mit* $\operatorname{grad}(h) \geq 1$. *Zu jedem Ideal* $\overline{I} \subseteq \mathbb{F}_q[x]/(h)$ *gibt es genau ein normiertes Polynom* $g \in \mathbb{F}_q[x]$ *mit* $\overline{I} = (\overline{g})$ *und* $g \mid h$.
Dabei sei $\overline{g} = g + (h)$ *die Restklasse von* g.

Beweis. Für die kanonische Projektion $\begin{array}{rccc} \pi & : & \mathbb{F}_q[x] & \to & \mathbb{F}_q[x]/(h) \\ & & g & \mapsto & g + (h) \end{array}$ ist $I := \pi^{-1}(\overline{I}) \subseteq \mathbb{F}_q[x]$ ein Ideal. I ist ein Hauptideal, weil $\mathbb{F}_q$ ein Körper ist, $I = (g)$ mit $g \in \mathbb{F}_q[x]$. g ist das Minimalpolynom von I und somit eindeutig bestimmt. Ferner gilt $I = (g) \implies \pi(I) = (\pi(g))$. □

Satz 8.4
Zum $[n, k]$*-Code* $C \subseteq \mathbb{F}_q^n$ *sind folgende Aussagen äquivalent*

1. *C ist zyklisch.*
2. $\psi(C) \subseteq \mathbb{F}_q[x]/(x^n - 1)$ *ist ein Ideal.*
3. $\psi(C) = (\overline{g})$ *für die Restklasse* $\overline{g} = g + (h)$ *des Polynoms* g *kleinsten Grades in* $\psi(C) \setminus \{0\}$.

Die Äquivalenz der ersten beiden ersten Punkten folgt aus Lemma 8.2, die der beiden letzten aus Lemma 8.3 mit $h = x^n - 1$.

Definition 8.5 (Basis-,Code-, Generator- und Kontrollpolynom)
Sei $C \subseteq \mathbb{F}_q^n$ *ein zyklischer Code mit* $\psi(C) = (\overline{g})$. *Dann heißt* g *das Basispolynom (auch Generator- oder Codepolynom) zu* C *und* $h = (x^n - 1)/g$ *das Kontrollpolynom zu* C.

Ist $C \subseteq \mathbb{F}_q^n$ ein $[n, k]$-Code, $r = n - k$, dann gilt:

1. $\operatorname{grad}(g) = n - k = r$
2. Die Generatormatrix von C ist (sei $g =: g_0 + g_1 x + g_2 x^2 + \cdots + g_r x^r$):

$$G_g := \begin{bmatrix} g_0 & g_1 & g_2 & \cdots & g_r & 0 & \cdots & \cdots & 0 \\ 0 & g_0 & g_1 & g_2 & \cdots & g_r & 0 & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & g_0 & g_1 & g_2 & \cdots & g_r \end{bmatrix}$$

8.2 Kodierung mittels Schieberegister

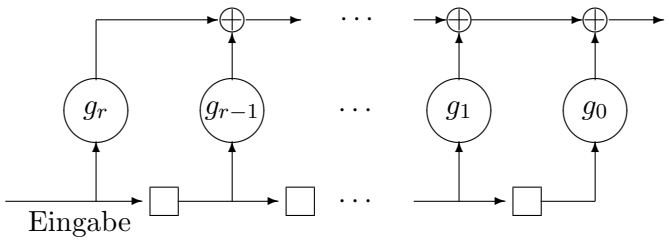


Abbildung 14: Schieberegister

Betrachte das Schiebregister in Abbildung 14, wobei:

- Eingabe: $(a_0, a_1, \ldots, a_{k-1}) \quad \sim \quad a_0 + a_1 x + \cdots + a_{k-1} x^{k-1}$
- Kodewort: $(a_0 + a_1 x + \cdots + a_{k-1} x^{k-1}) \cdot (g_0 + g_1 x + g_2 x^2 + \cdots + g_r x^r) \bmod (x^n - 1)$

Ausgabe pro Takt:

1. Takt

$a_{k-1} g_r$ ist der Koeffizient von $x^{k+r-1} = x^{n-1}$. Register:

a_{k-1}	0	0	$\cdots$	0

2. Takt

$a_{k-2} g_r + a_{k-1} g_{r-1}$ ist der Koeffizient von x^{n-2}. Register:

a_{k-2}	a_{k-1}	0	$\cdots$	0

k. Takt

$a_0 g_r + a_1 g_{r-1} + \cdots + a_{k-1} g_0$ ist der Koeffizient von x^r. Register:

a_0	a_1	a_2	$\cdots$	a_{k-1}

$k+1$. Takt

$a_0 g_{r-1} + a_1 g_{r-2} + \cdots + a_{k-2} g_0$ ist der Koeffizient von x^{r-1}. Register:

0	a_0	a_1	$\cdots$	a_{k-2}

n. Takt

$a_0 g_0$ ist der Koeffizient von x^0. Register:

0	0	$\cdots$	0	a_0

Es gilt:

Lemma 8.6
Sei $h = (x^n - 1)/g$ Kontrollpolynom zum zyklischen Code:

$$C \subseteq \mathbb{F}_q^n \cong \mathbb{F}_q[x]/(x^n - 1)$$

Dann gilt:

$$C = \{v \in \mathbb{F}_q[x] \ : \ v \cdot h = 0 \bmod (x^n - 1)\}$$

Beweis. Es gilt:

$$\begin{aligned} v \in C &\iff \exists a \in \mathbb{F}_q[x] : \ v = a \cdot g \bmod (x^n - 1) \\ &\iff v \cdot h = a \cdot g \cdot h = 0 \bmod (x^n - 1) \end{aligned}$$

□

Für die Operationen Kontrollieren und Dekodieren eines Codewortes $v \in \mathbb{F}_q^k$ bedeutet dies:

Kontrollieren: Bilde $v \cdot h \bmod (x^n - 1)$ mittles Schieberegister zum Polynom h.

Dekodieren: Berechne $v \mapsto v/g$ mittels Schieberegister mit Divisionsgatter. Bei einem Divisionrest ungleich 0, ist v kein Codewort.

8.3 Die Teiler von $x^n - 1 \in \mathbb{F}_q[x]$

Sei α primitive n-te Einheitswurzel im Zerfällungskörper von $x^n - 1$ über $\mathbb{F}_q$. Dann gilt:

$$x^n - 1 = \prod_{i=0}^{n-1} (x - \alpha^i)$$

Im Fall $\mathrm{ggT}(n, q) = 1$ (und somit $x^n - 1 \in \mathbb{F}_q[x]$ quadratfrei) ist $x^n - 1$ das Produkt aller Minimalpolynome zu α^i in $\mathbb{F}_q[x]$.

8.4 BCH-Codes (Bose, Chaudhuri, Hocquenghem)

Unser Ziel ist ein fehlerkorrigierender, zyklischer Code. Sei $\alpha \in \mathbb{F}_{q^m}$ primitive n-te Einheitswurzel, d.h. $\alpha^n = 1$ und $\operatorname{ord}(\alpha) = n$. Sei $\operatorname{ggT}(q, n) = 1$, damit ist $x^n - 1 \in \mathbb{F}_q[x]$ quadratfrei.

Definition 8.7 (BCH-Code)
Der BCH-Code $C(\alpha, n, d) \subseteq \mathbb{F}_q^n$ zu α mit Zielabstand d besteht aus den Codepolynomen $a(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$ mit $a(\alpha^i) = 0$ für $i = 1, 2, \ldots, d-1$.

Satz 8.8
Der BCH-Code $C(\alpha, n, d)$ ist ein zyklischer Code mit Distanz $d(C) \geq d$.

Beweis. Sei jeweils $m_i \in \mathbb{F}_q[x]$ das Minimalpolynom von α^i für $i = 1, 2, \ldots, d-1$. Wegen $\alpha^n = 1$ gilt $m_i \mid x^n - 1$. Setze $g := \operatorname{kgV}(m_1, m_2, \ldots, m_{d-1})$. Das Polynom g ist Basispolynom (Generatorpolynom) zu $C(\alpha, n, d)$, denn es gilt:

$$\begin{aligned} a \in C(\alpha, n, d) &\iff \left[\, a(\alpha^i) = 0 \text{ für } i = 1, 2, \ldots, d-1 \,\right] \\ &\iff \left[\, m_i \mid a \text{ für } i = 1, 2, \ldots, d-1 \,\right] \\ &\iff g \mid a \end{aligned}$$

Wegen $m_i \mid x^n - 1$ für $i = 1, 2, \ldots, d-1$ folgt $g \mid x^n - 1$. Also ist $C(\alpha, n, d)$ ein zyklischer Code. □

8.4.1 Kontrollmatrix H

Die Kontrollmatrix H zu $C(\alpha, n, d)$ über $\mathbb{F}_{q^m}$ ist:

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{d-1} & \alpha^{2(d-1)} & \ldots & \alpha^{(d-1)(n-1)} \end{bmatrix} \in \mathbb{F}_{q^m}^{(d-1)\times n}$$

Denn offenbar gilt für $a = (a_0, ..., a_{n-1}) \in \mathbb{F}_q^n$:

$$H \cdot a^T = 0 \qquad \iff \qquad \left[a(\alpha^i) = 0 \text{ für } i = 1, 2, \ldots, d-1\right]$$

$C(\alpha, n, d)$ hat die Distanz $\geq d$, weil je $d-1$ Spalten der Kontrollmatrix H linear unabhängig sind. Je $d-1$ Spalten $(i_1, i_2, \ldots, i_{d-1})$ bilden eine Vande-Monde-Matrix mit $\zeta_{i_\nu} = \alpha^{i_\nu - 1}$ (siehe Satz 7.24 auf Seite 79):

$$\begin{bmatrix} \zeta_{i_1} & \zeta_{i_2} & \cdots & \zeta_{i_{d-1}} \\ \zeta_{i_1}^2 & \zeta_{i_2}^2 & \cdots & \zeta_{i_{d-1}}^2 \\ \vdots & \vdots & \ddots & \vdots \\ \zeta_{i_1}^{d-1} & \zeta_{i_2}^{d-1} & \cdots & \zeta_{i_{d-1}}^{d-1} \end{bmatrix}$$

mit Determinate:

$$\pm \prod_{1 \le j < \mu \le d-1} \left(\zeta_{i_j} - \zeta_{i_\mu}\right) \neq 0$$

8.4.2 Zum Hamming-Code äquivalenter BCH-Code

Es gilt:

Satz 8.9
Der BCH-Code $C(\alpha, n, 3)$ der Länge $n = 2^r - 1$ mit Zieldistanz 3 über $\mathbb{F}_2$ ist äquivalent zum $[2^r - 1, 2^r - 1 - r]$-Hamming-Code.

Beweis. Das Generatorpolynom g des Codes $C(\alpha, n, 3)$ hat Grad r und nach Satz 7.14 die Nullstellen:

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

Dabei ist α primitive n-te Einheitswurzel. Wegen $n = 2^r - 1$ liegt α in $\mathbb{F}_{2^r}$. Konjugierte zu α sind $\alpha, \alpha^2, \ldots, \alpha^{2^{r-1}}$. Da α und α^2 Nullstellen des Polynoms g sind, ist g Generator-Polynom von $C(\alpha, n, 3)$. Weil g den Grad r hat, gilt $[\mathbb{F}_2(\alpha) : \mathbb{F}_2] = r$, somit $\mathbb{F}_2(\alpha) \cong \mathbb{F}_{2^r}$. Betrachten wir die PCH-Matrix zu $C(\alpha, n, 3)$:

- **die PCH-Matrix zu $C(\alpha, n, 3)$ über $\mathbb{F}_{2^r}$**

  $$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \ldots & \alpha^{2^r-2} \end{bmatrix} \in \mathbb{F}_{2^r}^{1 \times n}$$

  Die Zeile $\begin{bmatrix} 1 & \alpha^2 & \alpha^4 & \ldots & \alpha^{2(2^r-2)} \end{bmatrix}$ entfällt, weil α^2 konjugiert zu α ist.

- **die PCH-Matrix zu $C(\alpha, n, 3)$ über $\mathbb{F}_2$**

  Wir stellen die α^j bezüglich der Basis $\alpha^0, \alpha^1, \ldots, \alpha^{r-1}$ über $\mathbb{F}_2$ dar. Sei $\alpha^j = \sum_{i=0}^{r-1} c_{i,j}\alpha^i$ für $j = 0, 1, \ldots, 2^r - 2$. Die PCH-Matrix über $\mathbb{F}_2$ lautet:

  $$\begin{matrix} \alpha^0 & \alpha^1 & \cdots & \alpha^{2^r-2} \end{matrix}$$

  $$H' = \begin{bmatrix} c_{1,0} & c_{1,1} & \cdots & c_{1,2^r-2} \\ c_{2,0} & c_{2,1} & \cdots & c_{2,2^r-2} \\ \vdots & \vdots & & \vdots \\ c_{r,0} & c_{r,1} & \cdots & c_{r,2^r-2} \end{bmatrix} \begin{matrix} \alpha^0 \\ \alpha^1 \\ \vdots \\ \alpha^{r-1} \end{matrix}$$

  In der Spalte zu α^j stehen die Koordinaten von α^j bezüglich der Basis $\alpha^0, \alpha^1, \ldots, \alpha^{r-1}$. Die Spalten der Matrix H' sind paarweise verschieden, foglich ist $C(\alpha, n, 3)$ äquivalent zum $[2^r - 1, 2^r - 1 - r]$-Hamming-Code.

□

Der $[7, 4, 3]$-Hamming-Code hat die PCH-Matrix:

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \end{bmatrix}$$

Dabei ist α eine primitive $(2^3 - 1)$-te Einheitswurzel. $\alpha \in \mathbb{F}_{2^3}$ ist Nullstelle von $x^3 + x + 1$, also $\alpha^3 + \alpha + 1 = 0$. Basis von $\mathbb{F}_{2^3}$ über $\mathbb{F}_2$ ist $1, \alpha, \alpha^2$. Die PCH-Matrix H' über $\mathbb{F}_2$ ist somit:

$$H' = \begin{array}{c} \begin{array}{ccccccc} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \end{array} \\ \left[\begin{array}{ccccccc} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{array}\right] \end{array} \begin{array}{c} \alpha^0 \\ \alpha^1 \\ \alpha^2 \end{array}$$

Denn es gilt:

$$\begin{array}{lcll} \alpha^3 & = & 1 + \alpha & \\ \alpha^4 & = & \alpha + \alpha^2 & \\ \alpha^5 & = & \alpha^2 + \alpha^3 & = \quad \alpha^2 + \alpha + 1 \\ \alpha^6 & = & \alpha^3 + \alpha^2 + \alpha & = \quad \alpha^2 + 1 \end{array}$$

Das Generatorpolynom ist $g = 1 + x + x^3 \sim (1, 1, 0, 1)$. Die Generatormatrix ist:

$$G = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

Das Kontrollpolynom ist:

$$(x^n - 1)/g = (x^7 - 1)/(1 + x + x^3) = x^4 + x^2 + x + 1$$

Betrachten wir folgenden 2-Fehlerkorrigierender BCH-Code: Sei $n = 2^r - 1$ und $\alpha \in \mathbb{F}_{2^r}$ eine primitive $(2^r - 1)$-te Einheitswurzel. Die PCH-Matrix sei:

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{2^r-2} \\ 1 & \alpha^3 & \alpha^6 & \cdots & \alpha^{3(2^r-2)} \end{bmatrix}$$

Zieldistanz des Codes ist 5, beachte dass α^2, α^4 zu α konjugiert sind. Die Zeilen zu α^2 und α^4 in H entfallen. Damit ist der Code 2-fehlerkorrigierend.

Offenes Problem: Finde notwendige und hinreichende Bedinigungen dafür, daß Zieldistanz und Distanz übereinstimmen.

8.4.3 Erweiterungskörper mit primitiven n-ten Einheitswurzeln

In welchem Erweiterungskörper von $\mathbb{F}_q$ liegen die primitiven n-ten Einheitswurzeln α?

Bezeichnung 8.10 (Ordnung von q modulo n ord(q, n))
Mit $\operatorname{ord}(q,n) := \min\{m \in \mathbb{N} \,:\, q^m = 1 \bmod n\}$ *bezeichnen wir die Ordnung von* q *in* $\mathbb{Z}_n^*$.

Satz 8.11
Sei α *primitive* n*-te Einheitwurzel über* $\mathbb{F}_q$*, dann gilt:*

$$\operatorname{ord}(q,n) = \min\{m \,:\, \alpha \in \mathbb{F}_{q^m}\}$$

Beweis. Für $m = \operatorname{ord}(q,n)$ gilt $q^m = 1 \bmod n$. Somit:

$$\alpha^{q^m} = \alpha^{1 \bmod n} = \alpha$$

Weil α Nullstelle von $x^{q^m} - x$ ist, folgt $\alpha \in \mathbb{F}_{q^m}$ (Zerfällungskörper von $x^{q^m} - x$). Umgekehrt folgt aus $\alpha \in \mathbb{F}_{q^m}$, daß $\alpha^{q^m} = \alpha$. Weil α primitve n-te Einheitswurzel über $\mathbb{F}_q$ ist, folgt $q^m = 1 \bmod n$. □

Kapitel 9

Diffie-Hellman und elliptische Kurven

Sei $G = \langle g \rangle$ zyklische Gruppe der Ordnung q mit grossem Primfaktor. Öffentlich sind G, g, q. Die Teilnehmer A und B wollen einen gemeinsamen Schlüssel $k_{A,B}$ erzeugen und austauschen.

privater Schlüssel von A: $x_A \in_R \mathbb{Z}_q \cong [0, q[$.
öffentlicher Schlüssel von A: $h_A = g^{x_A} \in G$.

Das öffentliche Verzeichnis enthält: Name A, g^{x_A}.

Schlüsselaustausch von A und B

- A bildet $k_{A,B} = (g^{x_B})^{x_A} = k_B^{x_A}$
- B bildet $k_{A,B} = (g^{x_A})^{x_B} = k_A^{x_B}$

$g^{x_A \cdot x_B} = k_{A,B}$ ist der gemeinsame Schlüssel von A, B.
Zur Sicherheit ist erforderlich, dass das DL-Problem schwer ist.

DL-Problem

Gegeben $g \in G, h \in_R G$
Finde $x \in \mathbb{Z}_q : \ g^x = h$.

Lösen des DL-Problems liefert aus h_A den geheimen Schlüssel x_A.

DH-Problem

Gegeben $g \in G, g^a, g^b \in_R G$.
Berechne $g^{ab} \in_R G$.

Zur Sicherheit des DH-Schlüsselaustauschs müssen DL-Problem und DH-Problem praktisch unlösbar sein.

Benötigt werden zyklische Gruppen G mit „schwerem“ DL-Problem. Man wählt eine Gruppenordnung $|G|$ mit einem grossen Primfaktor.

Beispiele zyklischer Gruppen.
1. $\mathbb{Z}_p^*$ mit p prim ist zyklisch.
2. Sei $\mathbb{F}_{p^n}$ endlicher Körper, dann ist $\mathbb{F}_{p^n}^*$ zylisch von der Ordnung $p^n - 1$.
3. Elliptische Kurven $E_{a,b}(\mathbb{F}_{p^n})$ sind direktes Product zweier zyklischer Gruppen.

Das DL-Problem zur additiven Gruppe $\mathbb{Z}_q$ ist trivial: $gx = h$ gilt für $x = g/f \bmod q$.

BSI-Empfehlung zu Signaturalgorithmen, Juni 2001

RSA $N = p \cdot q$

DSA Digital Signature Algorithm

basiert auf dem DL-Problem einer Gruppe G, $|G| = q$ mit grossem Primfaktor,
mögliche G

1. $G = \mathbb{Z}_p^*$
2. $G = E_{a,b}(\mathbb{F}_p)$ p prim
3. $G = E_{a,b}(\mathbb{F}_{2^m})$ m prim

} EC-DSA

BSI-Empfehlung zur Bitlänge

	gültig bis	Bitlänge	
RSA	2005 / 2006	$\log_2 N$	1024 / 2048
			mind. 1280
DSA	”	$\log_2 p \geq$	1024 / 2048
			mind. 1280
		$\log_2 q \geq$ 160	160
EC-DSA	”	$\log_2 q \geq$ 160	180
	m		191

Lemma 9.1
Die Lösung des DL-Problems in einer zyklischen Gruppe G der Ordnung q geht stets *mit $O(\sqrt{q})$ Multiplikationen in G.*

Generische Methode Baby Step Giant Step.

Gegeben $g, h \in G$

Löse $g^x = h$

1. $k = \lceil \sqrt{q} \rceil$. Berechne $L_1 = \{g^1, \ldots, g^k\}$
2. Berechne $L_2 = \{h, hg^k, hg^{2k}, \ldots, hg^{k^2}\}$
3. Finde $1 \leq i, j \leq k \quad g^i = hg^{jk}$, es folgt $x = i - jk \bmod q$.
   (Sortiere L_1 und teste für die $f \in L_2$ mittels binary insertion ob $f \in L_1$, solange bis eine Kollision auftritt.)

Beh.: $L_1 \cap L_2 \neq \emptyset$

Elliptische Kurven. Seien $\mathbb{F} \subset \mathbb{K}$ Körper, $\mathbb{F}$ Koeffizientenkörper, $\mathbb{K}$ Lösungskörper,
Homogene kurze Weierstrass Gleichung zu $a, b \in \mathbb{F}$:

$$E_{a,b}(\mathbb{K}): \quad y^2z = x^3 + axz^2 + bz^3 \tag{1}$$

Weierstrass Gleichung in normierten Koordinaten

$$E_{a,b}(\mathbb{K}): \quad y^2 = x^3 + ax + b \tag{1'}$$

Diskriminante $\triangle = -16(4a^3 + 27b^2)$. Falls $\triangle \neq 0$ ist die Kurve $E_{a,b}(\mathbb{K})$ *glatt*, sonst *singulär*. Für $\mathrm{char}(\mathbb{K}) \in \{2, 3\}$ muss eine andere Form der Gleichung (1), (1') gewählt werden. $\triangle \neq 0$ schliesst Mehrfachnullstellen von $x^3 + ax + b$ aus.

Def. Zwei Lösungen $(x, y, z), (x', y', z')$ von (1) sind *äquivalent*, wenn $(x, y, z) = c \cdot (x', y', z')$ für ein $c \in \mathbb{K}^*$. Eine Äquivalenzklasse $(x : y : z)$ mit $(x, y, z) \neq (0, 0, 0)$ heisst *Punkt* von $E_{a,b}(\mathbb{K})$.

Def. Die *elliptische Kurve* $E_{a,b}(\mathbb{K})$ besteht aus den Punkten $(x : y : z)$ der Lösungen $(x, y, z) \neq (0, 0, 0)$ von (1).

Normierte Koordinaten.

1. Jeder Punkt $(x : y : z)$ mit $z \neq 0$ hat genau einen normierten Repräsentanten $(x/z, y/z, 1)$.
2. Es gibt genau einen Punkt $(x : y : z) \in E_{a,b}(\mathbb{K})$ mit $z = 0$; nämlich $O = (0 : 1 : 0)$, den unendlich fernen Punkt.
3. Die Punkte $(x : y : 1) \in E_{a,b}(\mathbb{K})$ sind die Lösungen von (1').

Die **allgemeine Weierstrass** Form für beliebige char($\mathbb{K}$)

$$E \ : \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Elliptische Kurven über $\mathbb{K} = \mathbb{R}$

Schreibweise $(x, y) = (x : y : 1)$.

Die Kurven sind symmetrisch zur x-Achse. Sie haben 1 oder 3 Punkte auf der x-Achse (Nullstellen von $x^3 + ax + b$).
Die Punkte $P = (x, 0)$ haben die Ordnung 2.

Das Additionsgesetz zu $\mathbf{E_{a,b}}(\mathbb{K})$ Betrachte die Gerade

$$G: \quad y - y_2 = \tfrac{y_1 - y_2}{x_1 - x_2}\ (x - x_2) \ = \ \lambda(x - x_2)$$

durch die Punkte $(x_1, y_1), (x_2, y_2)$ von $E_{a,b}(\mathbb{K}), x_1 \neq x_2$.

Lemma 9.2
G schneidet $E_{a,b}(\mathbb{K})$ in einem dritten Punkt (x_3, y_3).

Beweis. Der Schnitt von G und $E_{a,b}(\mathbb{K})$ führt zu

$$(\lambda(x - x_2) + y_2)^2 = x^3 + ax + b\ .$$

Für die Nullstellen x_1, x_2, x_3 gilt nach Vieta $\lambda^2 = x_1 + x_2 + x_3$. Aus $x_1, x_2 \in \mathbb{K}$, $\lambda \in \mathbb{K}$ folgt $x_3 \in \mathbb{K}$. □

Additionsgesetze.

A1. $O = (0 : 1 : 0)$ ist neutrales Element
$P + O = P\ , \quad -O = O$

A2. Für je drei Punkte $P, Q, R \in E_{a,b}(\mathbb{K})$ auf Geraden gilt

$$P + Q + R = O$$
$$P + Q = -R.$$

Gilt auch für Doppelpunkte $P = Q$ (Tangente durch P)

A3. $-(x, y) = (x, -y)$

Satz 9.3
$E_{a,b}(\mathbb{K})$ ist additive abelsche Gruppe.

Beweis. Nach A2. ist die Addition kommutativ, denn die Reihenfolge der Punkte P, Q, R geht nicht ein. Die Addition ist assoziativ. Dies folgt nach N. Koblitz [98 Chapter 6 Exercise §1.4] aus dem

Fakt. Seien G_1, G_2, G_3 und G_1', G_2', G_3' Geraden, welche $x^3 + ax + b$ jeweils in 9 Punkten (mit Multiplikation) $P_1, \ldots, P_9$ und $P_1', \ldots, P_9'$ schneiden. Aus $P_i = P_i'$ für $i = 1, \ldots, 8$ folgt $P_9 = P_9'$. □

Additionsformeln für char$(\mathbb{K}) \neq 2, 3$. $(x_1, y_1) + (x_2, y_2) + (x_3, y_3) = O$

1. Fall $x_1 \neq x_2$. Schnitt von $E_{a,b}(\mathbb{K})$ mit der Geraden G liefert

$$(\lambda(x - x_2) + y_2)^2 = x^3 + ax + b \tag{3}$$

mit $\lambda = \frac{y_1 - y_2}{x_1 - x_2}$. Nach Vieta gilt $\lambda^2 = x_1 + x_2 + x_3$, also $x_3 := \lambda^2 - x_1 - x_2$. Weiter folgt aus

$$\frac{y_3 - y_2}{x_3 - x_2} = \lambda = \frac{y_3 - y_1}{x_3 - x_1}$$

$$\begin{aligned} y_3 &= \lambda(x_3 - x_2) + y_2 \\ &= \lambda(x_3 - x_1) + y_1 \end{aligned}$$

2. Fall $x_1 = x_2,\ y_1 = y_2$ (Punktverdopplung).

Statt $\lambda = \frac{y_1 - y_2}{x_1 - x_2}$ setzt man

$$\lambda = \frac{\delta y}{\delta x} \quad |(x_1, y_1) \quad = \quad \frac{3x_1^2 + a}{2y_1} \quad \text{für } y = \sqrt{x^3 + ax + b}$$

erfordert $\text{char}\,(\mathbb{K}) \neq 2, 3 \quad x_3 := \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - x_1 - x_2$.

3. Fall $x_1 = x_2,\ y_1 = -y_2$: $(x_1, y_1) + (x_1, -y_1) = O$

Kosten der Punkte-Addition in normierten Koordinaten

Fall 1	2 Mult.	1 Div.	6 Add.
Fall 2	3 Mult.	1 Div.	5 Add.

in homogenen Koordinaten: Fall 1 16 Mult.
Fall 2 10 Mult.

Siehe Blake, Serousse, Smart (1999) chapter IV. 1.

Die Ordnung von $\mathbf{E_{a,b}}(\mathbb{F}_q)$ Sei $\mathbb{F}_q$ Körper mit $q = p^f$ Elementen.

Satz 9.4 (Hasse 1933)
$|E_{a,b}(\mathbb{F}_q)| = q + 1 - t$ *mit* $|t| \leq 2\sqrt{q}$.

$E_{a,b}(\mathbb{F}_q)$ ist *supersingulär*, wenn $t = 0(\bmod p)$ für $q = p^f$. Für supersinguläre $E_{a,b}(\mathbb{F}_q)$ gibt es einen Homomorphismus $E_{a,b}(\mathbb{F}_q) \to \mathbb{F}^*_{q^k}$ in eine Erweiterung $\mathbb{F}_{q^k}$ von $\mathbb{F}_q$. Menezes, Okamoto, Vanstone. IEEE-IT. 39 (1993), 1639–1646.

Kapitel 10

Boole'sche Algebra, $\mathcal{NP}$-Vollständigkeit

George Boole (1815 – 1864) betrieb als englischer Logiker und Mathematiker die Algebraisierung der Logik. Er wurde zum Wegbereiter der modernen Logik und der Verbandstheorie.

==========

10.1 Boole'sche Operationen

Die *Boole'sche Werte* sind $0 \sim$ falsch und $1 \sim$ wahr. *Boole'sche Variable* nehmen die Werte $0, 1$ an. Die wichtigsten *Boole'schen Operationen*:

- **Disjunktion** von x, y, Bezeichnung $x \vee y$ bzw. $x + y$

$x \backslash y$	0	1
0	0	1
1	1	1

- **Konjunktion** von x, y, Bezeichnung $x \wedge y$ bzw. $x \cdot y$

$x \backslash y$	0	1
0	0	0
1	0	1

- **Negation** von x, Bezeichnung $\neg\, x$ bzw. $\overline{x}$

x	0	1
$\overline{x}$	1	0

- **Exclusive OR, Addition** mod 2 von x, y, Bezeichnung $x \oplus y := x\overline{y} + \overline{x}y$

$x \backslash y$	0	1
0	0	1
1	1	0

Regeln: „+" und „·" sind assoziativ, kommutativ und distributiv mit Neutralelement 0 für „+" und 1 für „·". Die Negation ist *selbstinvolutorisch*, d.h. $\neg \neg x = x$.

10.2 Boole'sche Algebren

Definition 10.1 (Boole'sche Algebra)
Eine Boole'sche Algebra $\mathrm{BA} = (S, +, \cdot, \neg)$ *besteht aus einer Menge* S *mit Operationen*

$$+ : S^2 \to S, \qquad \cdot : S^2 \to S, \qquad \neg : S \to S,$$

so daß gilt:

1. *„+" und „·" sind assoziativ, kommutativ, distributiv mit neutralem Element* 0 *für „+" und* 1 *für „·".*
2. $\neg \neg x = x$
3. *Boole'sche Kongruenzen:* $x + x = x, \quad x \cdot x = x$
4. *Absorptionsgesetze:* $x(x + y) = x, \quad x + (x \cdot y) = x$
5. *De Morgan'sche Regeln:* $\overline{x + y} = \overline{x} \cdot \overline{y}, \quad \overline{x \cdot y} = \overline{x} + \overline{y}$

Es gibt zu „+" bzw. „·" keine inverse Elemente. Die Operationen „+" und „·" sind symmetrisch.

Beispiel 10.2 (Boole'sche Algebren)
Boole'sche Algebren sind zum Beispiel:

1. Die Mengenalgebra $(\mathrm{pot}(S), \cup, \cap, \text{Komplement})$.
   Dabei ist $S \neq \emptyset$ beliebige Menge. $\emptyset$ bzw. S ist das Neutralelement zu $\cup$ bzw. $\cap$.
2. Die Algebra der Boole'schen Vektoren $(\{0,1\}^n, +, \cdot, \neg)$.
   Die Operationen $+, \cdot, \neg$ werden koordinatenweise durch die Boole'schen Operationen erklärt:

$$\begin{aligned}(x_1, x_2, \ldots, x_n) \cdot (y_1, y_2, \ldots, y_n) &:= (x_1 \cdot y_1, \ldots, x_n \cdot y_n)\\ (x_1, x_2, \ldots, x_n) + (y_1, y_2, \ldots, y_n) &:= (x_1 + y_1, \ldots, x_n + y_n)\end{aligned}$$

Die allgemeine Form der De Morgan'schen Regeln lautet:

$$\overline{\sum x_i} = \prod \overline{x_i}, \qquad \overline{\prod x_i} = \sum \overline{x_i}$$

10.3 Boole'scher Verband

Definition 10.3 (Partielle Ordnung zu einer Boole'schen Algebra)
Es sei $(S, +, \cdot, \neg)$ eine Boole'sche Algebra. Die zugehörige partielle Ordnung $\leq$ auf S ist

$$x \leq y \qquad :\Longleftrightarrow \qquad \exists z \,:\, y = x + z$$

Bezüglich $\leq$ gilt:

$$\begin{aligned} \max(x, y) &= x + y \\ \min(x, y) &= x \cdot y \\ 0 &= \inf\{s \in S\} \\ 1 &= \sup\{s \in S\} \end{aligned}$$

Definition 10.4 (Boole'scher Verband)
Ein Boole'scher Verband mit Negation ist eine Struktur $(S, \leq, \neg)$, so daß:

1. *$\leq$ ist partielle Ordnung auf S*
2. *$\neg : S \to S$ ist involutorisch, d.h. $x \leq y \iff \neg\, y \leq \neg\, x$*
3. *$\max(x, y), \min(x, y)$ existieren stets*
4. *$0 = \inf\{s \in S\}, \quad 1 = \sup\{s \in S\}$*

Lemma 10.5
Jede Boole'sche Algebra $(S, +, \cdot, \neg)$ bildet bezüglich $\leq$ einen Boole'schen Verband mit Negation und umgekehrt.

Beweis. „$\Leftarrow$" Setze $x + y := \max(x, y)$ und $x \cdot y := \min(x, y)$. □

10.4 Der Ring der Boole'schen Funktionen

Definition 10.6 (Boole'sche Funktion)
Eine Funktion $f : \{0, 1\}^n \to \{0, 1\}$ heißt n-stellige Boole'sche Funktion.

Sei

$$B_n = \{0,1\}^{\{0,1\}^n} = \{f \mid f : \{0,1\}^n \to \{0,1\}\}$$

die Menge der n-stelligen Boole'schen Funktionen. Es gilt $|B_n| = 2^{2^n}$. Im folgenden bezeichne $\oplus$ die Addition in $\mathbb{Z}_2$, im Unterschied zu $+ = \vee$.

Satz 10.7
B_n bildet mit den Operationen $\vee, \wedge, \neg$

$$(f \wedge g)(x) := f(x) \wedge g(x), \qquad (f \vee g)(x) := f(x) \vee g(x), \qquad (\neg f)(x) = \neg f(x)$$

eine Boole'sche Algebra. Diese ist isomorph zur Mengenalgebra $\mathrm{pot}(\{0,1\}^n)$.

Beweis. Der zugehörige Isomorphismus lautet:

$$\begin{array}{rcccl} \psi & : & B_n & \to & \mathrm{pot}(\{0,1\}^n) \\ & & f & \mapsto & f^{-1}(1) \end{array}$$

□

Satz 10.8
B_n bildet bezüglich $\oplus$ und $\cdot$ einen Ring, den Ring der n-stelligen Boole'schen Funktionen.

$$(f \oplus g)(x) := f(x) \oplus g(x)$$

10.5 Der Ring der Boole'schen Polynome

Definition 10.9 (Ring der Boole'schen Polynome)
Den Ring der Boole'schen Polynome in den Boole'schen Variablen $x_1, x_2, \ldots, x_n$ bezeichnen wir mit:

$$\mathrm{BP}_n := \mathbb{Z}_2[x_1, x_2, \ldots, x_n / (x_1 \oplus x_1^2, \ldots, x_n \oplus x_n^2)$$

Das Ideal $(x_1 \oplus x_1^2, \ldots, x_n \oplus x_n^2) \subseteq \mathbb{Z}_2[x_1, \ldots, x_n]$ enthält genau die Polynome, die modulo der Boole'schen Kongruenzen 0 sind. Es gibt einen natürlichen Ringhomomorphismus

$$\begin{array}{rcccl} \pi & : & \mathrm{BP}_n & \to & B_n \\ & & f & \mapsto & \pi(f) \quad \text{(werte das Polynom } f(x_1, \ldots, x_n) \text{ aus)} \end{array}$$

Satz 10.10
$\mathrm{BP}_n \cong B_n$ *und jede Boole'sche Funktion in B_n hat eine eindeutige Darstellung als Boole'sches Polynom.*

Beweis. Die Existenz der Darstellung folgt aus $x \vee y = xy \oplus x \oplus y$. Zu zeigen bleibt, daß $\ker(\pi) = \{0\}$. Der Vektorraum (Modul) der homogenen Boole'schen Polynome vom Grad k:

$$\mathrm{BP}_{n,k} := \left\{ \bigoplus_{1 \le i_1 < i_2 < \cdots < i_k \le n} a_{i_1,i_2,\ldots,i_k} x_{i_1} x_{i_2} \cdots x_{i_k} \;\middle|\; a_{i_1,i_2,\ldots,i_k} \in \mathbb{Z}_2 \right\}$$

Somit ist BP_n die direkte Summe der $\mathrm{BP}_{n,k}$:

$$\mathrm{BP}_n = \bigoplus_{k=0}^{n} \mathrm{BP}_{n,k}$$

Direkte Summe von Vektorräumen:

$$\ker(\pi) = \bigoplus_{k=0}^{n} (\ker(\pi) \cap \mathrm{BP}_{n,k})$$

Zu zeigen: $\ker(\pi) \cap \mathrm{BP}_{n,k} = \{0\}$, wobei 0 Nullpolynom. Angenommen, $f \in \mathrm{BP}_{n,k}$, $f \neq 0$. Also

$$f = \bigoplus_{1 \le i_1 < i_2 < \cdots < i_k \le n} a_{i_1,i_2,\ldots,i_k} x_{i_1} x_{i_2} \cdots x_{i_k}$$

und es existiert ein $a_{i_1,i_2,\ldots,i_k} = 1$. Setze:

$$x_j := \begin{cases} 1 & \text{falls } j \in \{i_1, i_2, \ldots, i_k\} \\ 0 & \text{sonst} \end{cases}$$

Somit ist $f(x_1, x_2, \ldots, x_n) = 1$, folglich $\pi(f) \neq 0$, d.h. $f \notin \ker(\pi)$. □

Die Eindeutigkeit der Darstellung impliziert, daß diese Darstellung unflexibel und unpraktisch ist.

$$\begin{aligned} B_n &\cong \bigoplus_{k=0}^{n} \mathrm{BP}_{n,k} \\ |\mathrm{BP}_{n,k}| &= 2^{\binom{n}{k}} \\ 2^{2^n} &= 2^{\sum_{k=0}^{n} \binom{n}{k}} = \prod_{k=0}^{n} 2^{\binom{n}{k}} \end{aligned}$$

10.6 Normalformen und $\mathcal{NP}$-Vollständigkeit

Wir führen folgende Bezeichnungen ein:

Bezeichnung 10.11 (Boole'sches Literal und Boole'sche Klausel)
Ein Boole'sches Literal ist ein Ausdruck der Gestalt x_i oder $\neg\, x_i$. Setze $x_i^0 := x_i$, $x_i^1 := \neg\, x_i$. B eachte, daß $\overline{i}^i = 1$. Eine Boole'sche Klausel ist eine Disjunktion von Literalen: $x_{i_1}^{j_1} \vee x_{i_2}^{j_2} \vee \cdots \vee x_{i_k}^{j_k}$.

Definition 10.12 (Konjunktive Normalform)
*Konjunktive Normalform (*KNF*):*

$$\bigwedge_{\nu=1}^{m} \bigvee_{\mu=1}^{k_\nu} x_{i_{\nu,\mu}}^{j_{\nu,\mu}} \qquad = \qquad \prod_{\nu=1}^{m} \sum_{\mu=1}^{k_\nu} x_{i_{\nu,\mu}}^{j_{\nu,\mu}}$$

Definition 10.13 (Disjunktive Normalform)
*Disjunktive Normalform (*DNF*):* $\bigvee_{\nu=1}^{m} \bigwedge_{\mu=1}^{k_\nu} x_{i_{\nu,\mu}}^{j_{\nu,\mu}}$

Satz 10.14
Jede Boole'sche Funktion ist als KNF *bzw.* DNF *darstellbar.*

Beweis. $f \in B_n$ ist als DNF darstellbar gemäß

$$f(x_1, \ldots, x_n) = \bigvee_{f(i_1,\ldots,i_n)=1} \overline{x}_1^{i_1} \cdot \ldots \cdot \overline{x}_n^{i_n}$$

Beachte, daß $\overline{i}_1^{i_1} \cdot \ldots \cdot \overline{i}_n^{i_n} = 1$.

Aus der DNF–Darstellung erhält man eine KNF–Darstellung von $\neg\, f$ durch Anwendung der Morgan'schen Regeln

$$\neg\, f = \bigwedge_{f(i_1,\ldots,i_n)=1} (x_1^{i_1} \vee x_1^{i_2} \vee \ldots \vee x_n^{i_n}).$$

Sowohl DNF als auch die KNF–Darstellung sind nicht eindeutig bestimmt. □

Definition 10.15 (Polynomialzeitsprache)
Eine Sprache $L \subseteq \{0,1\}^*$ heißt polynomialzeit (entscheidbar), wenn es eine Turingmaschine M gibt, welche L in polynomieller Zeit entscheidet, d.h.

$$\mathrm{Res}_M(x) = \begin{cases} 1 & \textit{falls } x \in L \\ 0 & \textit{falls } x \notin L \end{cases}$$

und für die Schrittzahl von M gilt $T_M(x) = |x|^{O(1)}$.

Bezeichnung 10.16
$\mathcal{P}$ ist die Klasse der Polynomialzeitsprachen $L \subseteq \{0,1\}^*$.

Definition 10.17 (nicht-det. Polynomialzeitsprache)
Eine Sprache $L \subseteq \{0,1\}^*$ heißt nicht-deterministisch polynomialzeit, wenn es eine Polynomialzeitfunktion $f(x,y)$ und ein $c \in \mathbb{N}$ gibt, so daß

$$x \in L \iff \exists\, y : |y| \leq |x|^c \wedge f(x,y) = 1.$$

Man nennt y einen Zeugen für $x \in L$, falls $|y| \leq |x|^c \wedge f(x,y) = 1$.

Bezeichnung 10.18
$\mathcal{NP}$ ist die Klasse der nicht-deterministischen Polynomialzeitsprachen $L \subseteq \{0,1\}^*$.

Definition 10.19 (polynomialzeit-reduzierbar)
Eine Sprache L heißt polynomialzeit-reduzierbar auf L', wenn es eine Polynomialzeitfunktion f gibt, so daß $x \in L \iff f(x) \in L'$. Wir schreiben $L \leq_{pol} L'$.

Offenbar gilt $L \leq_{\text{pol}} L$ und $L_1 \leq_{\text{pol}} L_2,\ L_2 \leq_{\text{pol}} L_3$ impliziert $L_1 \leq_{\text{pol}} L_3$:

Lemma 10.20
Die Relation $\leq_{pol}$ ist reflexiv und transitiv.

Definition 10.21 ($\mathcal{NP}$-vollständig)
Eine Sprache L heißt $\mathcal{NP}$–vollständig, wenn $L \in \mathcal{NP}$ und $L' \leq_{pol} L$ für alle $L' \in \mathcal{NP}$ gilt.

Das Erfüllbarkeitsproblem der Aussagenlogik lautet:

Gegeben: eine KNF-Formel $\gamma = \bigwedge_{\nu=1}^{m} \bigvee_{\mu=1}^{k_\nu} x_{i_{\nu,\mu}}^{j_{\nu,\mu}}$

Entscheide: ist γ erfüllbar?

Die zugehörige Sprache ist

$$\text{SAT} = \{\gamma \mid \text{erfüllbare KNF-Formel } \gamma\}.$$

Dabei werden KNF-Formeln in geeigneter Weise binär kodiert.

Satz 10.22
SAT ist $\mathcal{NP}$-vollständig.

Beweis (Skizze). Gegeben sei eine Polynomialzeit-Turingmaschine M mit $\mathrm{Res}_M(x,y) = f(x,y)$ und es gelte $|y| \leq |x|^c$ für ein konstantes $c \in \mathbb{N}$. Weiterhin sei $n := |x|$, $m := |y|$ und $T(n)$ die Rechenzeit von M auf Eingaben $(x,y) \in \{0,1\}^{n+m}$ für $m \leq n^c$. Gesucht ist eine Polynomialzeit-Abbildung $x \longmapsto \gamma_x$ für eine geeignete KNF-Formel γ_x, so daß genau dann ein $y \in \{0,1\}^m$ mit $f(x,y) = 1$ existiert, wenn γ_x erfüllbar ist.

In Stufe 1 simulieren wir $T(n)$ Rechenschritte der TM M durch ein Boole'sches Netzwerk $\mathcal{N}$ in den Boole'schen Variablen $z_1, \ldots, z_{c_M}$ mit $c_M = (n + T(n))^{O(1)}$ Knoten:

- Eingaben: $x_1, \ldots, x_n,\ y_1, \ldots, y_n \in \{0,1\}$ mit den zugehörigen Boole'schen Variablen $z_1, \ldots, z_n, z_{n+1}, \ldots, z_m$.
- Operationen und Gatter: $z_j := z_{i(j)} \mathrm{op}_j z_{k(j)}$ mit $1 \leq i(j), k(j) < j$ und $\mathrm{op}_j \in \{0,1\}^{\{0,1\}^2}$ für $j = n+m, \ldots, c_M$.
- Ausgabe: z_{c_M}

Die Funktionen $i(j), k(j)$ und die Boole'schen Operationen $\mathrm{op}_j : \{0,1\}^2 \to \{0,1\}$ hängen vom Programm der TM M und n, m ab.

Ist die TM *starr*, d.h. die Bewegungen der Köpfe hängen nur von n, m und dem Zeitpunkt ab, dann gelingt die Simulation durch ein Netzwerk der Größe

$$c_M \leq O(T(n) \log T(n)) \ .$$

In Stufe 2 sei $\mathcal{N} = \mathcal{N}(M,n,m)$ gegeben, so daß $\mathrm{Res}_{\mathcal{N}}(x,y) = f(x,y)$ für $(x,y) \in \{0,1\}^{n+m}$. Gesucht ist eine Polynomialzeit-Abbildung $(\mathcal{N}, x) \mapsto \gamma_x$, so daß genau dann ein y mit $f(x,y) = 1$ existiert, wenn γ_x erfüllbar ist. O.B.d.A. seien die Netzwerk-Gatter von der Form

$$\begin{aligned} z_j &= \widetilde{z}_{i(j)} \wedge \widetilde{z}_{k(j)} \\ \text{bzw. } z_j &= \widetilde{z}_{i(j)} \vee \widetilde{z}_{k(j)} \end{aligned}$$

mit $\widetilde{z} \in \{z, \neg\, z\}$.

Behauptung 1: Die Gleichheit $z_j = \widetilde{z}_{i(j)} \wedge \widetilde{z}_{k(j)}$ gilt gdw folgende drei Klauseln erfüllt sind:

$$z_j \vee \neg\, \widetilde{z}_{i(j)} \vee \neg\, \widetilde{z}_{k(j)}, \quad \neg\, z_i \vee \widetilde{z}_{i(j)}, \quad \neg\, z_i \vee \widetilde{z}_{k(j)}.$$

Beweis. Die Klauseln bedeuten $\neg\, z_j \Rightarrow (\neg\, \widetilde{z}_{i(j)} \vee \widetilde{z}_{k(j)})$, $\quad z_j \Rightarrow (\neg\, \widetilde{z}_{i(j)})$, $z_j \Rightarrow (\neg\, \widetilde{z}_{k(j)})$.

Damit kann man $\exists\, y : \mathrm{Res}_{\mathcal{N}}(x,y) = 1$ ausdrücken durch eine KNF-Formel γ_x in $n + m + c_M$ Boole'schen Variablen mit $\leq 3c_M$ Klauseln, so daßgenau dann ein y mit $\mathrm{Res}_{\mathcal{N}}(x,y) = 1$ existiert, wenn γ_x erfüllbar ist. □

Damit ist der Satz vollständig bewiesen. □

10.6.1 Das Problem $\{0,1\}$–ganzzahlige Gleichungen

Gegeben: $\mathbf{A} \in \mathbb{Z}^{m\times n})$, $\mathbf{b} \in \mathbb{Z}^n$, $m, n \in \mathbb{N}$.

Entscheide: $\exists\, \mathbf{x} \in \{0,1\}^n : \mathbf{Ax} = \mathbf{b}$.

Die zugehörige Sprache ist

$$\{0,1\} - GL = \left\{ (\mathbf{A}, \mathbf{b}) \in \mathbb{Z}^{m\times(n+1)} \,\middle|\, \exists\, \mathbf{x} \in \{0,1\}^n : \mathbf{Ax} = \mathbf{b} \right\} .$$

Satz 10.23
$\{0,1\}$–GL ist $\mathcal{NP}$–vollständig.

Beweis. Wir zeigen 3–SAT $\leq_{\text{pol}} \{0,1\} - GL$.
Wir transformieren eine KNF

$$\gamma = \bigwedge_{1\leq\nu\leq m} \bigvee_{1\leq\mu\leq 3} x_{i_{\nu,\mu}}^{j_{\nu,\mu}}$$

in n B. Variablen $x_1, \ldots, x_n$ in ein Gleichungssystem. Wir drücken die ν–te Klausel $\bigvee\limits_{1\leq\mu\leq 3} x_{i_{\nu,\mu}}^{j_{\nu,\mu}}$ aus durch folgende Gleichung

$$(*) \qquad \sum_{1\leq\mu\leq 3} \begin{cases} x_{i_{\nu,\mu}} & \text{falls} \quad j_{\nu,\mu} = 0 \\ 1 - x_{i_{\nu,\mu}} & \text{falls} \quad j_{\nu,\mu} = 1 \end{cases} + x_{n+2\nu-1} + x_{n+2\nu} = 3$$

Die Schlupfvariablen $x_{n+2\nu-1}, x_{n+2\nu}$ kommen nur in der ν–ten Gleichung vor und sind somit frei wählbar. Das γ zugeordnete Gleichungssystem hat Koeffizienten $0, +1, -1$, Variablen $x_1, \ldots, x_n, \ldots, x_{n+2m}$.

Mit den linearen Funktionen in $\mathbb{Z}[x_1, \ldots, x_{n+2m}]$

$$f_{\nu,\mu} := \begin{cases} x_{i_{\nu,\mu}} & j_{\nu,\mu} = 0 \\ 1 - x_{i_{\nu,\mu}} & j_{\nu,\mu} = 1 \end{cases}$$

ist das Gleichungssystem $(*)$ über $\{0,1\}$ lösbar gdw $\sum\limits_{\mu=1}^{3} f_{\nu,\mu} \geq 1$ für $\nu = 1, \ldots, n$ über $\{0,1\}$ lösbar ist. Weiter gilt für jede $\{0,1\}$–Belegung von $x_1, \ldots, x_{n+2m}$:

$$\nu\text{-te Gleichung erfüllt} \iff \sum_{\mu=1}^{3} f_{\nu,\mu} \geq 1 \iff \bigvee_{1\leq\mu\leq 3} x_{i_{\nu,\mu}}^{j_{\nu,\mu}} = 1$$

Damit ist $(*)$ über $\{0,1\}$–lösbar gdw γ erfüllbar ist. □

10.6.2 Das Rucksackproblem (Knapsack, Subset Sum)

Gegeben: $n, a_1, \ldots, a_n, s \in \mathbb{N}$

Entscheide: $\exists\, x_1, \ldots, x_n \in \{0,1\} : \sum_{i=1}^{n} a_i x_i = s.$

Die zugehörige Sprache ist

$$KP = \left\{ (n, a_1, \ldots, a_n, s) \in \mathbb{N}^{n+2} \,\middle|\, \begin{array}{l} \exists\, x_1, \ldots, x_n \in \{0,1\} \\ \sum_{i=1}^{n} a_i x_i = s \end{array} \right\})$$

Satz 10.24
KP ist $\mathcal{NP}$–vollständig.

Beweis. Wir zeigen $\{0,1\} - GL \leq_{\text{pol}} KP$. Die Dimension n von KP sei gerade. Zur Beweisvereinfachung lassen wir nur Lösungen $(x_1, ..., x_n)$ von KP zu mit $\sum_{i=1}^{n} x_i = n/2$.

1. Stufe: Wir transformieren $(\mathbf{A}, \mathbf{b}) \mapsto (a_1, \ldots, a_n, s) \in \mathbb{Z}^{n+1}$, so daß $\mathbf{Ax} = \mathbf{b}$ für $\mathbf{x} = (x_1, ..., x_n)^t \in \{0,1\}^n$ gdw $\sum_{i=1}^{n} a_i x_i = s$.

Addiere die Zeilen von $\mathbf{Ax} = \mathbf{b}$, $\mathbf{A} = [a_{\nu,\mu}] \in \mathbb{Z}^{m \times n}$ stellengerecht.

$$a_\mu := \textstyle\sum_{\nu=1}^{m} a_{\nu,\mu} 2^{\ell_\nu},\ s := \sum_{\nu=1}^{m} b_\nu 2^{\ell_\nu}.$$

Wähle hierzu die Gewichte 2^{ℓ_ν} so groß, daß Überträge nicht stören. Es genügt dass $2^{\ell_\nu} \geq \sum_\mu |a_{\nu,\mu}| \cdot 2^{\ell_{\nu-1}}$..

Gleichheit der Lösungen. Die Lösung $(x_1, ..., x_n)$ von $\sum_{i=1}^{n} a_i x_i = s$ löst auch jede der Gleichungen von $\mathbf{Ax} = \mathbf{b}$, weil die Überträge nicht stören.

Stufe 2: Wir transformieren mit $M := \max_i |a_i|$

$$(a_1, \ldots, a_n, s) \mapsto \left(a_1 + M, \ldots, a_n + M, s + M\tfrac{n}{2}\right).$$

Die Lösungen der Gleichungen bleiben bei der Transformation erhalten. □

Bemerkungen. 1. die Gleichung $\sum_{\mu=1}^{n} a_{m,\mu} x_\mu = b_m$ ist in den führenden Bits der $a_1, ..., a_n, s$ kodiert. Sie wird bei der Suche nach KP-Lösungen $(x_1, ..., x_n)$ durch Gitterreduktion als erstes gelöst. Die Gleichungen von $\mathbf{Ax} = \mathbf{b}$ werden in der Reihenfolge $\nu = m, ..., 1$ gelöst.

2. Knapsack-Probleme beliebig kleiner Dichte d sind $\mathcal{NP}$-vollständig. Die Dichte d kann man beliebig klein machen, durch grosse ℓ_ν.

Anhang A

Gruppen, Normalteiler, Homomorphismen und Ringe

A.1 Gruppen und Normalteiler

Wir beginnen mit der Definition einer Halbgruppe:

Definition A.1 (Halbgruppe)
Eine Halbgruppe $(H, \circ)$ ist eine nicht-leere Menge H zusammen mit einer Abbildung

$$\begin{array}{rccc} \circ & : & H \times H & \to & H \\ & & (x, y) & \mapsto & xy \end{array}$$

die assoziativ ist, d.h. für alle $x, y, z \in H$ es gilt:

$$(xy)z = x(yz).$$

Beispiele für Halbgruppen sind:

- $\mathbb{N} = \{0, 1, \ldots, \}$ die Menge der natürlichen Zahlen mit einer der Operationen $+$, $\cdot$, min, max.
- Die Menge $X^+ := \bigcup_{i=1}^{\infty} X^i$ der Wörter über der Menge X mit der Konkatenation:

$$\circ(x_1 x_2 \cdots x_n, y_1 y_2 \cdots y_m) = x_1 x_2 \cdots x_n y_1 y_2 \cdots y_m$$

- Die Menge $\mathrm{Abb}(X) := \{f \mid f : X \to X\}$ der Abbildungen der Menge X in sich mit der Zusammensetzung als assoziative Verknüpfung:

$$\circ(f, g) = fg \qquad \text{mit } (fg)(x) = f(g(x))$$

Definition A.2 (Neutrales Element)
Ein Element e einer Halbgruppe H heißt neutrales Element, wenn $he = h = ehfür$ alle $h \in H$.

Das neutrale Element einer Halbgruppe ist eindeutig bestimmt, sofern es existiert (siehe Übungsaufgabe B.1).

Definition A.3 (Monoid)
Eine Halbgruppe mit neutralem Element heißt Monoid.

Beispiele für Monide sind neben $(\mathbb{N}, +, 0)$, $(\mathbb{N}, \cdot, 1)$, $(\mathbb{N}, \max, 0)$:

- $(\mathbb{N} \cup \{\infty\}, \min, \infty)$
- $(X^*, \text{Konkatenation}, \Lambda)$, wobei $X^* = X^+ \cup \{\Lambda\}$ und Λ das leere Wort ist
- $(\mathrm{Abb}(X), \circ, id_X)$, wobei $\circ$ die Zusammensetzung ist

Definition A.4 (Gruppe)
Eine Gruppe G ist ein Monoid, so daß jedes $x \in G$ ein inverses Element $x^{-1} \in G$ besitzt mit:

$$x^{-1}x = xx^{-1} = e$$

Das Inverse x^{-1} zu x ist eindeutig bestimmt (siehe Übungsaufgabe B.1). Jedes Rechtsinverse x_r^{-1} zu x stimmt mit jedem Linksinversen x_l^{-1} überein:

$$x_r^{-1} = (x_l^{-1}x)x_r^{-1} = x_l^{-1}(xx_r^{-1}) = x_l^{-1}$$

Definition A.5 (Ordnung)
Die Ordnung einer Gruppe ist die Anzahl der Elemente von G, Bezeichnung: $|G|$ oder $\#G$.

Beispiele für Gruppen sind:

1. $(\mathbb{Z}, +, 0)$ die ganzen Zahlen. Das Inverse zu x ist $-x$.
2. $(\mathbb{Q} - 0, \cdot, 1)$ die rationalen Zahlen. Das Inverse zu x ist $\frac{1}{x}$.

3. $(\mathbb{Z}_n, +, 0)$, wobei $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \{a + n\mathbb{Z} \mid a \in \mathbb{Z}\}$ die Restklasse der ganzen Zahlen modulo n
4. Die Gruppe $\mathrm{Sym}(X) \subseteq \mathrm{Abb}(X)$ der Permutationen der Menge X. Die Gruppe $\gamma_n = \mathrm{Sym}(\{1, 2, \ldots, n\})$ hat die Ordnung $n!$.

Definition A.6 (Abelsche Gruppe)
Eine Gruppe G heißt abelsch, wenn das Kommutativgesetz gilt:

$$xy = yx \qquad \text{für alle } x, y \in G.$$

$\mathbb{Z}, \mathbb{Q}, \mathbb{Z}_n$ sind abelsche Gruppen bezüglich der Addition. Die Gruppe γ_n ist für $n \geq 3$ nicht abelsch.

Definition A.7 (Untergruppe)
Sei G Gruppe. Eine nicht-leere Teilmenge $H \subseteq G$ heißt Untergruppe, wenn:

1. $\forall a, b \in H \ : \ ab \in H$
2. $\forall a \in H \ : \ a^{-1} \in H$

Dann ist H mit der Gruppenoperation von G eine Gruppe.

Falls H endlich ist, gilt in Definition A.7 die Implikation 1. $\Longrightarrow$ 2. Für beliebige Gruppen G gilt:

$$1. + 2. \qquad \Longleftrightarrow \qquad \forall a, b \in H \ : \ ab^{-1} \in H$$

Definition A.8 (Links-Nebenklasse)
Sei G Gruppe, $H \subseteq G$ Untergruppe und $x \in G$. Dann ist

$$xH = \{xh \mid h \in H\}$$

die Links-Nebenklasse von x in H.

Lemma A.9
Sei $H \subseteq G$ Untergruppe und $a, b \in G$. Dann sind folgende Aussagen äquivalent:

1. $aH = bH$
2. $aH \cap bH \neq \emptyset$
3. $b \in aH$

4. $a^{-1}b \in H$

Beweis. Ringschluß:

1. $\Rightarrow$ 2. Trivial.

2. $\Rightarrow$ 3. Aus $ah_1 = bh_2$ mit $h_1, h_2 \in H$ folgt $b = ah_1h_2^{-1} \in aH$.

3. $\Rightarrow$ 4. Trivial.

4. $\Rightarrow$ 1. Folgt aus:

$$\begin{array}{lllll} a^{-1}b \in H & \Rightarrow & b \in aH & \Rightarrow & bH \subseteq aH \\ a^{-1}b \in H & \Rightarrow & b^{-1}a \in H & \Rightarrow & a \in bH \quad \Rightarrow \quad aH \subseteq bH \end{array}$$

□

Sei $H \subseteq G$ Untergruppe, dann ist

$$G = \bigcup_{x \in G} xH$$

Zerlegung von G in Nebenklasse gleicher Kardinalität, d.h. $|xH| = |H|$. Beachte: $H \to xH$ mit $h \mapsto xh$ ist bijektiv.

Definition A.10 (Index)
$[G : H]$*, Index von* H *in* G*, ist die Anzahl der Nebenklassen von* H *in* G*.*

Satz A.11 (Lagrange)
Sei G *eine endliche Gruppe mit Untergruppe* $H \subseteq G$*.*
Dann gilt $|G| = [G : H] \cdot |H|$*.*

Somit gilt für jede Untergruppe H einer endlichen Gruppe G: $\#H \mid \#G$.

Definition A.12 (Normalteiler)
Eine Untergruppe $H \subseteq G$ *heißt Normalteiler zu* G*, wenn* $yH = Hy$ *für alle* $y \in G$*.*

Satz A.13
Eine Untergruppe $H \subseteq G$ *ist genau dann ein Normalteiler, wenn* $yHy^{-1} \subseteq H$ *für alle* $y \in G$*.*

Beweis. Wir zeigen beide Richtungen:

„$\Rightarrow$“ Aus $yH = Hy$ folgt $yHy^{-1} = H$.

„⇐“ Aus $yHy^{-1} \subseteq H$ folgt für alle $y \in G$:

$$yH \subseteq Hy \quad \text{und} \quad Hy^{-1} \subseteq y^{-1}H$$

Also gilt $yH = Hy$.

□

Lemma A.14
Sei $H \subseteq G$ Normalteiler, dann wird durch $(xH) \cdot (yH) := xyH$ eine Gruppenoperation auf $\{xH \mid x \in G\}$ erklärt.

Beweis. Das Produkt ist unabhängig von der Wahl der Repräsentanten: Zu zeigen:

$$xH = \overline{x}H \quad \text{und} \quad yH = \overline{y}H \quad \Rightarrow \quad xyH = \overline{x}\,\overline{y}H$$

Es gilt:

$$x(yH) = x(\overline{y}H) = x(H\overline{y}) = (xH)\overline{y} = \overline{x}(H\overline{y}) = \overline{x}\,\overline{y}H$$

□

Bezeichnung A.15 (Faktorgruppe)
$G/H = \{xH \mid x \in G\}$ mit obiger Multiplikation ist die Faktorgruppe von G zum Normalteiler H.

A.2 Homomorphismen

Wir definieren:

Definition A.16 (Gruppen-Homomorphismus)
Seien G und G' Gruppen. Eine Abbildung $\varphi : G \to G'$ heißt (Gruppen-)Homomorphismus, wenn:

$$\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y) \qquad \textit{für alle } x, y \in G.$$

Sei $H \subseteq G$ Normalteiler, dann ist zum Beispiel die Abbildung

$$\begin{array}{rccc} \varphi & : & G & \to & G/H \\ & & x & \mapsto & xH \end{array}$$

ein Homomorphismus.

Bemerkung A.17
Die Normalteiler H von G entsprechen eineindeutig den Isomorphieklassen surjektiven Homomorphismen $\varphi : G \to G'$ modulo der Isomorphie $\varphi(G) \to G/H$.

Bezeichnung A.18 (Surjektiv, injektiv und Isomorphimus)
Sei $\varphi : G \to G'$ ein Homomorphismus.

1. *φ ist surjektiv, wenn $\varphi(G) = G'$.*
2. *φ ist injektiv, wenn φ eineindeutig ist.*
3. *φ ist ein Isomorphismus, wenn φ bijektiv ist ($G \cong G'$).*
4. $\mathrm{Im}(\varphi) := \varphi(G) \subseteq G'$
5. $\ker(\varphi) := \{x \in G \mid \varphi(x) = e_{G'}\} =: \varphi^{-1}(e_{G'})$

Satz A.19 (Homomorphiesatz für Gruppen)
Sei $\varphi : G \to G'$ ein Homomorphismus. Dann gilt

$$\mathrm{Im}(\varphi) \cong G/\ker(\varphi)$$

und die Abbildung $f : G/\ker(\varphi) \to \mathrm{Im}(\varphi)$ mit $a \cdot \ker(\varphi) \mapsto \varphi(a)$ ist ein Isomorphismus.

Beweis. Es gilt:

1. $\mathrm{Im}(\varphi) \subseteq G'$ ist Untergruppe (trivial)
2. $\ker(\varphi) \subseteq G$ ist Normalteiler, denn für alle $y \in \ker(\varphi)$ und für alle $x \in G$ gilt:

   $$\varphi(xyx^{-1}) = \varphi(x)\varphi(x^{-1}) = \varphi(xx^{-1}) = \varphi(e_G) \in \ker(\varphi)$$

   Also: $x\ker(\varphi)x^{-1} \subseteq \ker(\varphi)$.
3. f ist wohldefiniert und bijektiv:

   $$a{\cdot}\ker(\varphi) = b{\cdot}\ker(\varphi) \;\Leftrightarrow\; ab^{-1} \in \ker(\varphi) \;\Leftrightarrow\; \varphi(ab^{-1}) = e_{G'} \;\Leftrightarrow\; \varphi(a) = \varphi(b)$$

4. f ist Homomorphismus:

   $$f\big((a\ker\varphi)(b\ker\varphi)\big) = \underbrace{f(ab\ker\varphi)}_{=\varphi(ab)} = \varphi(a)\varphi(b) = f(a\ker\varphi)f(b\ker\varphi)$$

□

Beispiele für Gruppen-Homomorphismen sind:

- $\mathrm{GL}_n(\mathbb{Q}) := \{A \in M_{n,n}(\mathbb{Q}) \mid \det A \neq 0\}$ ist eine Gruppe bezüglich der Matrizenmultiplikation. Die Abbildung

$$\begin{array}{rccc} \varphi & : & GL_n(\mathbb{Q}) & \to & \mathbb{Q} \\ & & A & \mapsto & \det A \end{array}$$

  ist ein Homomorphismus bezüglich der Multiplikation. $\mathbb{Q}$ ist kommutativ, $\mathrm{GL}_n(\mathbb{Q})$ aber nicht. Jede Untergruppe $H \subseteq \mathbb{Q}$ liefert einen Normalteiler $\varphi^{-1}(H) \subseteq \mathrm{GL}_n(\mathbb{Q})$, z.B. $H = \{\pm 1\} \subseteq \mathbb{Q}$.

- Die symmetrische Gruppe $\gamma_n = \mathrm{Sym}(\{1, 2, \ldots, n\})$

$$\gamma_n \cong \left\{ (p_{i,j}) \in \mathrm{GL}_n(\{0,1\}) \;\middle|\; \sum_i p_{i,j} = \sum_j p_{i,j} = 1 \right\} \subseteq \mathrm{GL}_n(\mathbb{Q})$$

  ist eine Untergruppe von $\mathrm{GL}_n(\mathbb{Q})$. Das Signum einer Permutation $\mathrm{sign} : \gamma_n \to \{\pm 1\}$ ist ein Gruppenhomorphismus (siehe Übungsaufgabe B.5):

$$\pi \leftrightarrow (p_{i,j}), \qquad \mathrm{sign}(\pi) := \det(p_{i,j}) \in \{\pm 1\}$$

  $A_n := \{\pi \in \gamma_n \mid \mathrm{sign}(\pi) = 1\} \subseteq \gamma_n$ ist ein Normalteiler vom Index 2.

$$\gamma_n / A_n \cong \{\pm 1\}$$

Definition A.20 (Ordnung)
Sei G eine Gruppe. Das Gruppenelemente $x \in G$ hat die Ordnung

$$\mathrm{ord}(x) = \min \left\{ k \in \mathbb{N} \,:\, x^k = e \right\}$$

sofern $\mathrm{ord}(x) < \infty$*, d.h. falls x von endlicher Ordnung ist.*

Satz A.21
Sei G Gruppe, $x \in G$ von endlicher Ordnung. Dann gilt:

1. $\forall d \in \mathbb{N} : \left[x^d = e \iff \mathrm{ord}(x) \mid d \right]$
2. $\{e, x, x^2, \ldots, x^{\mathrm{ord}(x)-1}\} \subseteq G$ *ist Untergruppe der Ordnung* $\mathrm{ord}(x)$
3. $\mathrm{ord}(x) \mid \#G$

Beweis. Es gilt:

1. Division mit Rest liefert:

$$d = a \cdot \operatorname{ord}(x) + b \qquad \text{mit } 0 \leq b < \operatorname{ord}(x)$$

Somit:

$$x^d = x^{a \cdot \operatorname{ord}(x) + b} = \left(x^{\operatorname{ord}(x)}\right)^a \cdot x^b = x^b$$

Also:

$$x^d = e \quad \Longleftrightarrow \quad b = 0 \quad \Longleftrightarrow \quad \operatorname{ord}(x) \mid d$$

2. $\{e, x, x^2, \ldots, x^{\operatorname{ord}(x)-1}\}$ ist abgeschlossen bezüglich Multiplikation. Weil die Menge endlich ist, folgt Abgeschlossenheit bezüglich Inversen. x^i für $i = 0, 1, \ldots, \operatorname{ord}(x) - 1$ sind paarweise verschieden, sonst liefert $x^i = x^j$, daß $x^{|i-j|} = e$ mit $|i - j| < \operatorname{ord}(x)$, Widerspruch.

3. Wegen 2. und nach Satz A.11 (Satz von Lagrange).

□

A.3 Ringe

Wir betrachten Ringe:

Definition A.22 (Ring)
Ein Ring $(R, +, \cdot)$ ist eine Menge R mit zwei Abbildungen $+, \cdot : R \times R \to R$, so daß

1. *$(R, +, 0)$ ist abelsche Gruppe mit neutralem Element 0*
2. *$(R, \cdot)$ ist Halbgruppe*
3. *$+$ und $\cdot$ sind distributiv:* $a(b + c) = ab + ac, \quad (b + c)a = ba + ca$

Beispiele für Ringe sind:

- $(\mathbb{Z}, +, \cdot)$
- $(\mathbb{Q}, +, \cdot)$
- $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \{a + n\mathbb{Z} \mid a = 0, 1, \ldots, n-1\}$. Als Repräsentanten für $\mathbb{Z}_n$ wählen wir $\{0, 1, \ldots, n-1\}$, d.h. die kleinsten nicht-negativen Residuen mod$n$. Die Multiplikation in $\mathbb{Z}_n$ wird über Repräsentanten erklärt:

$$(a + n\mathbb{Z}) \cdot (b + n\mathbb{Z}) := (a \cdot b + n\mathbb{Z})$$

Zu zeigen: wohldefiniert (unabhängig von Repräsentanten). Es folgt: Multiplikation ist assoziativ, kommutativ und distributiv.

- Nicht-kommutativer Ring: $M_{n,n}(\mathbb{Z})$.

Definition A.23 (Ring, Schiefkörper und Körper)
Wir definieren:

1. *Ein Ring $(R,+,\cdot)$ heißt kommutativ, wenn $\cdot$ kommutativ ist.*
2. *Ein Ring $(R,+,\cdot)$ heißt Ring mit 1, wenn $(R,\cdot,1)$ ein Monoid ist.*
3. *Ein Ring R mit 1 heißt Schiefkörper, wenn $(R-0,\cdot,1)$ Gruppe ist.*
4. *Ein Ring R mit 1 heißt Körper, wenn $(R-0,\cdot,1)$ abelsche Gruppe ist.*

Im Ring R mit 1 ist $R^* := \left\{a \in R \;\middle|\; \exists a^{-1} \in R\right\}$ die Gruppe der invertierbaren Elemente (Einheiten).

Bemerkung A.24
Es gilt:

1. *Ein Ring R mit 1 ist genau dann Schiefkörper, wenn $R^* = R - \{0\}$ ist.*
2. *Ein Ring R mit 1 ist genau dann Körper, wenn $R^* = R - \{0\}$ abelsch ist.*

Die Einheiten von $\mathbb{Z}_6$ sind $\mathbb{Z}_6^* = \{1 \bmod 6,\ 5 \bmod 6\}$. Schreibweise: $a \pmod n$ für $a + n\mathbb{Z}$. Wegen $5 \cdot 5 = 25 = 1 \bmod 6$ ist $5^{-1} = 5 \bmod 6$.

Satz A.25
Es gilt:

1. $\mathrm{ggT}(a,n)\,\mathbb{Z} = a\mathbb{Z} + n\mathbb{Z}$ *(Satz von Bézout)*
2. $a \bmod n \in \mathbb{Z}_n^* \iff \mathrm{ggT}(a,n) = 1$

Beweis. Wir beweisen beide Aussagen:

1. Sei c die kleinste positive Zahl in $a\mathbb{Z} + n\mathbb{Z}$. Division durch c liefert:

$$\begin{array}{rcll} a &=& s \cdot c + r & 0 \le r < c \\ n &=& s' \cdot c + r' & 0 \le r' < c \end{array} \tag{A.1}$$

   Weil c minimal ist, folgt $r = r' = 0$ und somit: $c \mid a$, $c \mid n$, also $c \mid \mathrm{ggT}(a,n)$. Ferner gilt wegen $c \in a\mathbb{Z} + n\mathbb{Z}$, daß $\mathrm{ggT}(a,n) \mid c$. Wir erhalten $c = \mathrm{ggT}(a,n)$. Mit $c = \mathrm{ggT}(a,n)$ folgt $c\mathbb{Z} \supseteq a\mathbb{Z} + n\mathbb{Z}$ und wegen $c \in a\mathbb{Z} + n\mathbb{Z}$ gilt $c\mathbb{Z} \subseteq a\mathbb{Z} + n\mathbb{Z}$.

2. Wir zeigen beide Richtungen:

   „⇒“ Sei $a \cdot b = 1 \bmod n$, also $a \cdot b = 1 + \nu \cdot n$. Somit $1 \in a\mathbb{Z} + n\mathbb{Z} \overset{1.}{\Rightarrow} \mathrm{ggT}(a, n) = 1$

   „⇐“ Sei $1 = \mathrm{ggT}(a, n)$. Nach 1. gilt: $1 \in a\mathbb{Z} + n\mathbb{Z}$, also

   $$1 = a\nu + n\mu \quad \text{mit } \nu, \mu \in \mathbb{Z}.$$

   Somit $\nu = a^{-1} \bmod n$.

□

Definition A.26 (Euler'sche φ-Funktion)
Die Euler'sche φ-Funktion:

$$\varphi(n) := \begin{cases} 1 & \textit{falls } n = 1 \\ |\mathbb{Z}_n^*| & \textit{falls } n > 1 \end{cases}$$

Nach Satz A.25 gilt: $\varphi(n) = |\{a \in \mathbb{Z} \,:\, 0 < a < n \text{ mit } \mathrm{ggT}(a, n) = 1\}|$.

Korollar A.27 (Fermat, Legendre)
Es gilt:

1. *Sei* $\mathrm{ggT}(a, n) = 1$*, dann gilt* $a^{\varphi(n)} = 1 \bmod n$.
2. *Sei p Primzahl mit $p \nmid a$, dann gilt* $a^{p-1} = 1 \bmod p$.

Beweis. Nach Satz A.21 gilt $\mathrm{ord}(a) \mid \varphi(n)$. Ferner ist $\varphi(p) = p - 1$. □

Anhang B

Übungsaufgaben

B.1 Gruppen, Normalteiler, Homomorphismen und Ringe

Aufgabe B.1 (5 Punkte)
Zeige:

1. Sei $(H, \cdot)$ eine Halbgruppe: In H gibt es höchstens ein neutrales Element e, also $\forall h \in H : e \cdot h = h \cdot e = h$.

2. Sei $(M, \cdot)$ ein Monoid mit neutralem Element e. Zu jedem $a \in M$ gibt es höchstens ein inverses Element $a^{-1} \in M$, also $a \cdot a^{-1} = e = a^{-1} \cdot a$.

Aufgabe B.2 (5 Punkte)
Sei $\varphi : G \to G'$ Gruppenhomomorphismus. Zeige:

1. Ist $H \subseteq G$ Untergruppe (Normalteiler), so auch $\varphi(H) \subseteq \varphi(G)$.

2. Ist $H \subseteq \varphi(G)$ Untergruppe (Normalteiler), so auch $\varphi^{-1}(H) \subseteq \varphi(G)$.

Aufgabe B.3 (5 Punkte)
Gib alle Untergruppen und Normalteiler der Gruppen $(\mathbb{Z}_6, +)$ und $\gamma_3 = \mathrm{Sym}\{1, 2, 3\}$ an. Begründe die Lösung.

Aufgabe B.4 (5 Punkte)
Zeige:

1. $10^i = 1 \pmod 9$ und $10^i = (-1)^i \pmod{11}$

2. Sei $n = \sum_{i=0}^{t} a_i 10^i$ mit $0 \leq a_i \leq 9$ eine natürliche Zahl in Dezimaldarstellung mit Quersumme $Q(n) := \sum_{i=0}^{t} a_i$.
   (a) Begründe die Neunerprobe: $Q(n) = n \pmod 9$, $\quad 9 \mid n \Leftrightarrow 9 \mid Q(n)$.
   (b) Entwickle die Elferprobe.

Aufgabe B.5 (5 Punkte)
Wir identifizieren Permutationen $\sigma \in \gamma_n$ mit Permutationsmatrizen in $\mathrm{GL}_n(\{0,1\})$:

$$\varphi : \ \sigma \mapsto (p_{ij})_{1 \leq i,j \leq n} \qquad \text{mit} \quad p_{ij} = \delta_{i,\sigma(j)}$$

Zeige: $\mathrm{sig}(\sigma) := \det \varphi(\sigma)$ ist ein Homomorphismus $\gamma_n \to \{\pm 1\}$ mit:

$$\mathrm{sign}\,(\sigma) = 1 \quad \Longleftrightarrow \quad \begin{array}{l} \sigma \text{ ist Produkt einer geraden Anzahl} \\ \text{von Vertauschungen (Transpositionen)} \end{array}$$

Aufgabe B.6 (10 Punkte)
Sei G eine endliche, zyklische Gruppe der Ordnung M und $G^k := \left\{ x^k \mid x \in G \right\}$ die Menge der k-ten Potenzen. Zeige:

1. $G^k \subseteq G$ ist eine Untergruppe der Ordnung $m / \,\mathrm{ggT}\,(m,k)$.
2. $\mathrm{ord}\left(x^k\right) = \dfrac{\mathrm{ord}\,(x)}{\mathrm{ggT}\,(\mathrm{ord}\,(x)\,,k)}$.
3. Zu jedem $y \in G$ hat die Gleichung $x^k = y$ entweder genau $\mathrm{ggT}\,(m,k)$ viele oder keine Lösung $x \in G$.

Aufgabe B.7 (5 Punkte)
Sei G eine endliche Gruppe. Zeige, daß jede Untergruppe H vom Index 2 Normalteiler ist.

Aufgabe B.8 (5 Punkte)
Gilt im Ring R, daß $a \cdot b = 0$ mit $a \neq 0$ und $b \neq 0$, so sind a und b *Nullteiler*. Zeige, daß für jeden endlichen Ring gilt: R ist nullteilerfrei genau dann, wenn R ein Schiefkörper ist.

Aufgabe B.9 (5 Punkte)
Die *inneren Automorphismen* einner Gruppe G sind die Abbildungen ($a \in G$):

$$G \to G \qquad x \mapsto a \cdot x \cdot a^{-1}$$

Die Elemente x und $x \cdot a^{-1}$ heißen *konjugiert*. Zeige, daß die Konjugiertrelation symmetrisch, reflexiv und transitiv ist.

B.2 Euklidischer Algorithmus

Aufgabe B.10 (10 Punkte)
Die Fibonacci-Folge (F_n), $n = 0, 1, 2, \ldots,$, ist definiert durch:

$$F_n := \begin{cases} 0 & \text{falls } n = 0 \\ 1 & \text{falls } n = 1 \\ F_{n-1} + F_{n-2} & \text{falls } n \geq 2 \end{cases}$$

1. Zeige:

   (a) $F_n = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right]$

   (b) $\lim_{n\to\infty} \frac{F_{n+1}}{F_n} = \frac{1+\sqrt{5}}{2}$

2. Sei $N(n, m)$ die Anzahl der Iterationen des Euklidischen Algorithmus' bei der Berechnung von $\mathrm{ggT}(m, n)$ zu $m > n > 0$. Zeige:

   (a) Für $i \geq 1$ gilt $N(F_{i+2}, F_{i+1}) = i$.

   (b) Für $n < F_{i+1}$ gilt $N(m, n) \leq N(F_{i+1}, F_i)$.

Aufgabe B.11 (5 Punkte)
Nutze den erweiterten Euklidischen Algorithmus:

1. Bestimme, sofern möglich, die inversen Elemente von 3 in $\mathbb{Z}_{25}^*$ und 7 in $\mathbb{Z}_{77}^*$.

2. Finde alle Lösungen der drei Kongruenzen:

$$\begin{aligned} 2142x &= 422 \pmod{238} \\ 12y &= 7 \pmod{73} \\ 14z &= 21 \pmod{77} \end{aligned}$$

Aufgabe B.12 (5 Punkte)
Löse:

- $1 = 7247u + 3721v$ mit dem erweiterten, binären Euklidischen Algorithmus.
- $31408u + 2718v = \mathrm{ggT}(31408, 2718)$ mit dem erweiterten, Euklidischen Algorithmus.

B.3 Kettenbrüche und Kontinuanten

Aufgabe B.13 (5 Punkte)
Zeige, daß gilt: $\frac{\sqrt{5}-1}{5} = < 1, 1, 1, \ldots >$.

B.4 Chinesischer Restsatz, Ideale und Faktorringe

Aufgabe B.14 (5 Punkte)
Bestimme zu den Moduln $m_i = 2, 3, 5, 7$ die Zahlen σ_i mit $\sigma_i = \delta_{i,j} \pmod{m_j}$ für $i = 1, 2, 3, 4$.

Aufgabe B.15 (5 Punkte)
Berechne ganzzahliges $u \in [0, 23 \cdot 41 \cdot 18 - 1]$ mit:

$$u = 7 \pmod{23}, \qquad u = 19 \pmod{41}, \qquad u = 12 \pmod{18}$$

Aufgabe B.16 (5 Punkte)
Diskutiere die Abbildung $f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ mit

$$f(x \bmod mn) = (x \bmod m, x \bmod n)$$

für den Fall, daß m und n nicht teilerfremd sind. Ist f ein Ringhomomorphismus? Bestimme $|f(\mathbb{Z}_{nm})|$ und $|\ker(f)|$.

Aufgabe B.17 (5 Punkte)
Sei p eine Primzahl. Zeige, daß die Anzahl der Elemente $a \in \mathbb{Z}_p^*$ mit $\mathrm{ord}\,(a) = p - 1$ gleich $\varphi(p-1)$ ist.

Aufgabe B.18 (5 Punkte)
Zu $y \in \mathbb{Z}$ seien die Residuen $\overline{y} = y \bmod m$ und $y' = y \bmod m$ gegeben, wobei $\mathrm{ggT}\,(m, n) = 1$. Gib für $y^* = y \bmod (mn)$ eine Formel der Form an:

$$y^* = f(\overline{y}, y')[m^{-1} \bmod n]m + \left[g(\overline{y}, y') \bmod m\right]$$

Weise die Korrektheit nach.

Aufgabe B.19 (5 Punkte)
Zeige, daß für ungerade Primzahlen p gilt:

$$a^{(p-1)/2} = \pm 1 \pmod{p} \qquad \forall a \in \mathbb{Z}_p^*$$

Aufgabe B.20 (5 Punkte)
Sei $N = \prod_{i=1}^{r} p_i^{e_i}$ ungerade Primfaktorzerlegung von $N \in \mathbb{N}$. Zeige:

1. Jedes $a \in \mathrm{QR}_N := \{b^2 \mid b \in \mathbb{Z}_n^*\}$ genau 2^r Quadratwurzeln hat.

2. Für zufällige $x, y \in \mathbb{Z}_n^*$ mit $x^2 = y^2 \pmod N$ gilt:

$$\mathrm{Ws}[\,\mathrm{ggT}(x \pm y, N) \neq 1] = 1 - 2^{-r+1}$$

Aufgabe B.21 (5 Punkte)
Sei $R = \mathbb{Z}_2[x]$, $I \subset R$ mit $I \neq \{0\}$, $I \neq R$ und $I = g \cdot R$. Das Ideal $I \neq R$ ist genau dann maximal, wenn $I + aR = R$ für alle $a \in R \setminus I$. Zeige daß I genau dann maximal ist, wenn g irreduzibel und der höchste Koeffizient 1 ist.

Aufgabe B.22 (5 Punkte)
Die folgenden drei Polynome

$$p_1 = x + 1, \qquad p_2 = x^2 + x + 1, \qquad p_3 = x^3 + x + 1$$

aus $\mathbb{Z}_2[x]$ sind paarweise teilerfremd. Bestimme Polynome $q_1, q_2, q_3 \in \mathbb{Z}_2[x]$, so daß $q_i = \delta_{i,j} \pmod{p_j}$ für $1 \leq i, j \leq 3$.

Aufgabe B.23 (5 Punkte)
Sei p prim und $a \in \mathbb{Z}_p$. Untersuche den Restklassenring $\mathbb{Z}_p[x]/(x^2 - a)$. Gib die Restklassen in R^* an. Welches sind die Nullteiler in R? Unterscheide die Fälle, das a Quadrat bzw. Nichtquadrat modulo p ist.

Aufgabe B.24 (5 Punkte)
Löse modulo 99 und modulo 101, setze die Lösung zusammen:

$$\begin{bmatrix} 101 & -131 \\ 70 & -92 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 30 \\ -100 \end{bmatrix}$$

Aufgabe B.25 (10 Punkte)
Bestimme die kleinste Zahl $a \in \mathbb{N}$ mit $\mathrm{ord}(a) = 112$ in $\mathbb{Z}_{113}$. Führe die Rechnung geschickt durch. Löse dann für die Zahl a:

$$a^x = 5 \pmod{113}$$

Bestimme $x_1 = x \pmod 7$ und $x_2 = x \pmod{16}$ durch Lösen von:

$$a^{16x_1} = 5^{16} \pmod{113} \qquad a^{7x_1} = 5^7 \pmod{113}$$

und setze x mit dem Chinesischen Restsatz zusammen.

B.5 RSA-Chiffrierschema und die Struktur von $\mathbb{Z}_N^*$

Aufgabe B.26 (5 Punkte)
Seien N_1, N_2, N_3 paarweise verschiedene RSA-Moduln mit $3 \nmid \varphi(N_i)$ für $i = 1, 2, 3$. Sei x eine Nachricht mit $0 < x < N_i$ für $i = 1, 2, 3$. Zeige, daß man aus den Ziffertexten

$$x^3 \pmod{N_i} \qquad i = 1, 2, 3$$

die Nachricht ermitteln kann. Hinweis: Verwende den Chinesischen Restsatz, falls man keinen der RSA-Moduln sofort faktorisieren kann.

Definition B.27 (Legendre-Jacobi-Symbol)
Sei $N = p_1 p_2 \cdots p_r > 2$ das Produkt ungerader Primzahlen $p_1, p_2 \ldots, p_r$. Das Legendre-Jacobi-Symbol $\left(\frac{x}{N}\right) \in \{0, \pm 1\}$ ist erklärt durch:

$$\left(\frac{x}{p}\right) := 0 \qquad \text{für } p > 2 \text{ prim mit } \mathrm{ggT}(x, p) \neq 1$$

$$\left(\frac{x}{p}\right) := x^{(p-1)/2} \pmod{p} \qquad \text{für } p > 2 \text{ prim und } \mathrm{ggT}(x, p) = 1$$

$$\left(\frac{x}{N}\right) := \left(\frac{x}{p_1}\right) \cdot \left(\frac{x}{p_2}\right) \cdots \left(\frac{x}{p_r}\right)$$

Aufgabe B.28 (5 Punkte)
Zeige, daß für das Legendre-Jacobi-Symbol gilt:

1. $x = y \pmod{N} \quad \Longrightarrow \quad \left(\frac{x}{N}\right) = \left(\frac{y}{N}\right)$
2. $\left(\frac{x}{N}\right) \cdot \left(\frac{y}{N}\right) = \left(\frac{xy}{N}\right)$
3. $\left(\frac{-1}{N}\right) = (-1)^{(N-1)/2}$

Aufgabe B.29 (5 Punkte)
Zeige, daß für die RSA-Kodierung $E : \mathbb{Z}_N \to \mathbb{Z}_N$, $E(x) = x^e \pmod{N}$ gilt:

$$\left(\frac{E(x)}{N}\right) = \left(\frac{x}{N}\right)$$

Beachte, daß N das Produkt zweier Primzahlen P und Q mit $2 \nmid P$ und $2 \nmid Q$ ist.

Aufgabe B.30 (15 Punkte)
Wir zeigen, daß RSA-Moduln $N = PQ$ nicht sicher sind, wenn $P-1$ oder $Q-1$ nur kleine Primfaktoren besitzt:

1. Sei $M = \prod_{i=1}^{r} p_i^{e_i}$ Primfaktorzerlegung von $M \in \mathbb{N}$. Zeige, daß die für Abbildung $E : \mathbb{Z}_M^* \to \mathbb{Z}_M^*$ mit $x \mapsto x^e \pmod M$ gilt:

$$|\ker(E)| = \prod_{i=1}^{n} |\mathrm{ggT}(e, \varphi(p_i^{e_i}))|$$

2. Sei $N = PQ$ das Produkt zweier Primzahlen P und Q.

   (a) Zeige, daß $P \mid \mathrm{ggT}\left(a^{p-1} - 1, N\right)$ für alle $a \in \mathbb{Z}$ mit $a \not| P$.

   (b) Begründe, daß RSA-Moduln $N = PQ$ nicht sicher sind, wenn $P-1$ oder $Q-1$ nur kleine Primfaktoren besitzt. Nimm an, $P-1$ haben nur Primfaktoren kleiner als 100, $Q-1$ habe Primfaktoren größer als 100. Bestimme zu $a \in_R \mathbb{Z}_N^*$ eine untere Schranke für:

$$\mathrm{Ws}\left[\, Q \not| \mathrm{ggT}\left(a^{p-1} - 1, N\right)\right]$$

   Wie kann man N faktorisieren? Hinweis: Bestimme ein e mit $e \mid (P-1)$ und betrachte den Kern der Abbildung $E : \mathbb{Z}_N^* \to \mathbb{Z}_N^*$ mit $x \mapsto x^e \pmod N$.

Aufgabe B.31 (5 Punkte)
Sei $N > 1$ keine Primzahl. Zeige:

$$U := \left\{ a \in \mathbb{Z}_N^* \;\middle|\; a^{(N-1)/2} = \left(\frac{a}{N}\right) \pmod N \right\}$$

ist eine echte Untergruppe von $\mathbb{Z}_N^*$.

Aufgabe B.32 (5 Punkte)
Sei p prim, $e \in \mathbb{N}$, $p^e > 2$ und $y \in \mathbb{Z}$. Zeige: $y = 1 \pmod{p^e}$ und $y \neq 1 \pmod{p^{e+1}}$ impliziert $y = 1 \pmod{p^{e+1}}$ und $y \neq 1 \pmod{p^{e+2}}$.

B.6 Gitterreduktion und ganzzahlige, lineare Ungleichungssysteme in zwei Variablen

Aufgabe B.33 (5 Punkte)
Sei b_1, b_2 reduzierte Basis bezüglich $\|\cdot\|$. Zeige, daß die folgenden Aussagen äquivalent sind:

1. b_1, b_2 und $-b_1, -b_2$ sind die einzigen, reduzierten Basen des Gitters.

2. $\|b_1\| < \|b_2\| < \|b_1 - b_2\| < \|b_1 + b_2\|$

Aufgabe B.34 (10 Punkte)
Zeige:

1. Sei b_1, b_2 wohlgeordnete Basis. Die minimale k-te Vorgängerbasis b_1^k, b_2^k ist gegeben durch:

$$\begin{bmatrix} b_1^{(k)} & b_2^{(k)} \end{bmatrix} = \begin{bmatrix} b_1 & b_2 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 1 & 2 \end{bmatrix}^k$$

   Für $k = 1$ Zeige ferner, daß folgende Basis b_1, b_2^{alt} Vorgängerbasis zu $b_2^{\text{alt}} = b_1 + \mu b_2$ mit $\mu \geq 2$, $b_2^{\text{alt}} = -b_1 + \mu b_2$ mit $\mu \geq 3$.

2. Es gilt

$$\begin{bmatrix} 0 & 1 \\ 1 & 2 \end{bmatrix}^k = \begin{bmatrix} a_{k-2} & a_{k-1} \\ a_{k_1} & a_k \end{bmatrix}^k$$

   mit $a_0 = 1$, $a_1 = 2$, $a_2 = 5$, $a_k = 5a_{k-2} + 2a_{k-3}$ für $k > 3$ und:

$$\left(1 + \sqrt{2}\right)^{k-1} < a_k < \left(1 + \sqrt{2}\right)^k \qquad \text{für } k > 0$$

Aufgabe B.35 (5 Punkte)
Entscheide mittels Gitterbasenreduktion, ob es zur Zahl π eine rationale Approximation $\frac{p}{q}$ gibt mit:

$$\left|\pi - \frac{p}{q}\right| \leq \frac{1}{20q} \qquad \text{für } |q| \leq 10$$

Aufgabe B.36 (5 Punkte)
Löse das Ungleichungssystem in $x, y \in \mathbb{Z}$:

$$\begin{aligned} |52x + 22y| &\leq 1 \\ |-12x - 7y| &\leq 1 \\ x &\geq 1 \end{aligned}$$

durch Reduktion der Basis $(52, -12)$, $(22, -7)$.

Aufgabe B.37 (5 Punkte)
Seien $u_i, v_i, w_i \in \mathbb{Z}$ für $i = 1, 2, \ldots, n$. Zeige, daß mit $x, y \in \mathbb{Z}$

$$|u_i x + v_i y| \leq w_i \qquad i = 1, 2, \ldots, n$$

genau dann lösbar ist, wenn $\lambda_{1,\|\cdot\|_\infty}(L) \leq 1$ für das gitter $L = L(b_1, b_2)$ mit:

$$\begin{aligned} b_1 &:= \begin{bmatrix} \frac{u_1}{w_1} & \frac{u_2}{w_2} & \cdots & \frac{u_n}{w_n} \end{bmatrix} \\ b_2 &:= \begin{bmatrix} \frac{v_1}{w_1} & \frac{v_2}{w_2} & \cdots & \frac{v_n}{w_n} \end{bmatrix} \end{aligned}$$

Aufgabe B.38 (5 Punkte)
Weise die Korrektheit des Reduktionsverfahren 11 für eine beliebige Norm nach.

Algorithmus 11 Reduktionsverfahren für beliebige Norm

EINGABE: $b_1, b_2 \in \mathbb{R}^n$

1. $b_2 := b_2 - \mu b_1$, wobei $\mu \in \mathbb{Z}$ so gewählt wird, daß $\|b_2^{\text{neu}}\|$ minimal ist.

2. IF $\|b_1 - b_2\| > \|b_1 + b_2\|$ THEN $b_2 := -b_2$

3. IF $\|b_1\| > \|b_2\|$ THEN

3.1. vertausche b_1 und b_2

3.2. GOTO 1

END if

AUSGABE: reduzierte Basis b_1, b_2

B.7 Fehlererkennende und fehlerkorrigierende Codes

Aufgabe B.39 (5 Punkte)
Sei $\mathbb{F}$ ein endlicher Körper mit $q = p^n$ Elementen, wobei p prim.

1. Definiere einen $\left[\frac{q^r-1}{q-1}, \frac{q^r-1}{q-1} - r\right]$-Hamming-Code $C \subseteq \mathbb{F}^n$ mit $n = \frac{q^r-1}{q-1}$ durch seine PCH-Matrix.
2. Zeige, daß $d(C) = 3$ und der Code C 1-perfekt ist.
3. Gib die PCH-Matrix für den Fall $\mathbb{F} = \mathbb{Z}_3$ und $r = 3$ an.
4. Zeige, daß es für $q > 2$ keinen $[q^r - 1, q^r - 1 - r]$-Hamming-Code mit $d(C) = 3$ gibt.

Aufgabe B.40 (5 Punkte)
Sei $C \subseteq \mathbb{Z}_2^n$ ein $[n, k]$-Code, in dem es Codewörter mit ungeradem Gewicht gibt. Der erweiterte Code $\hat{C}$ zu C ist der $[n+1, k]$-Code:

$$\hat{C} := \left\{ (c_1, c_2, \ldots, c_n, c_{n+1}) \in \mathbb{Z}_2^{n+1} \;\middle|\; (c_1, c_2, \ldots, c_n) \in C,\ c_{n+1} = \sum_{i=1}^{n} c_i \right\}$$

Zeige: Falls $d(C)$ ungerade ist, gilt $d(\hat{C}) = d(C) + 1$.

Aufgabe B.41 (5 Punkte)
Zeige, daß der erweiterte Code zum $[2^r - 1, 2^r - 1 - r]$-Hamming-Code ein $[2^r - 1, 2^r - 1 - r]$-Code $\hat{C}$ mit $d(\hat{C}) = 4$ ist. Gib für $r = 4$ eine Basis zu $\hat{C}$ an.

B.8 Endliche Körper

Aufgabe B.42 (5 Punkte)
Sei p prim und $R := \mathbb{Z}_p[x]$. Zeige, daß $R/(f)$ ist genau dann ein Körper, wenn f irreduzibel ist.

Aufgabe B.43 (5 Punkte)
Sei p prim und $R := \mathbb{Z}_p[x]$. Zeige:

1. Jedes $f \in R \setminus R^*$ ungleich 0_R hat eine Zerlegung $f = f_1 f_2 \cdots f_n$ in irreduzible Faktoren $f_1, f_2, \ldots, f_n$.
2. Diese Zerlegung ist bis auf Einheiten eindeutig, d.h. sind

   $$f = f_1 f_2 \cdots f_n = f'_1 f'_2 \cdots f'_m$$

   Zerlegungen, so ist $n = m$ und gibt eine Permutation $\sigma \in \gamma_n$ mit $f_i / f'_{\sigma(i)} \in R^*$ für $i = 1, 2, \ldots, n$.

Aufgabe B.44 (10 Punkte)
Die Anzahl der irreduziblen, normierten Polynome vom Grad d in $\mathbb{Z}_q[x]$ bezeichnen wir mit $N_q(d)$.

1. Berechne $N_2(4)$ und bestimme alle irreduzible, normierte Polynome $f_i \in \mathbb{Z}_2[x]$ vom Grade 4 ($i = 1, 2, \ldots, N_2(4)$).
2. Gib für $i = 1, 2, \ldots, N_2(4) - 1$ die folgenden Isomorphismen an:

   $$\mathbb{Z}_2[x]/(f_i) \cong \mathbb{Z}_2[x]/(f_{i+1})$$

3. Gib für die Körper $\mathbb{Z}_2[x]/(f_i)$, $i = 1, 2, \ldots, N_2(4)$, Normalenbasen über $\mathbb{Z}_2$ an.

Aufgabe B.45 (5 Punkte)
Konstruiere einen endlichen Körper $\mathbb{F}$ mit 8 Elementen (gib die Elemente an). Ist $\mathbb{F}$ isomorph zu $\mathbb{Z}_8$? Ist $\mathbb{F}^*$ isomorph zu $\mathbb{Z}_8^*$? Begründe die Antwort.

Aufgabe B.46 (5 Punkte)
Sei p prim und $q := p^n$. Zeige, daß zu jedem endlichen Körper $\mathbb{F}_q$ die Einheitengruppe $\mathbb{F}_q^*$ zyklisch ist.

Aufgabe B.47 (5 Punkte)
Zeige, für p prim gilt $(p-1)! = -1 \pmod p$. Lösungsvorschlag: Betrachte die Nullstellen des Polynoms $x^{p-1} - 1 \in \mathbb{Z}_p[x]$ und werte das Polynom an der Stelle $x = 0$ aus. Alternative Beweise?

B.9 Irreduzible Polynome

Aufgabe B.48 (5 Punkte)
Sei p prim. Die Anzahl der irreduziblen, normierten Polynome vom Grad d in $\mathbb{Z}_p[x]$ bezeichnen wir mit $N_p(d)$. Zeige:

1. $N_p(2) = \frac{1}{2}\left(p^2 - p\right)$
2. $N_p(3) = \frac{1}{3}\left(p^3 - p\right)$

Aufgabe B.49 (5 Punkte)
Die Anzahl der irreduziblen, normierten Polynome vom Grad d in $\mathbb{Z}_p[x]$ bezeichnen wir mit $N_p(d)$. Zeige ohne Satz 7.31 zu verwenden:

$$N_p(n) \geq \frac{1}{n}\left(p^n - \sigma(n)p^{n/2}\right) \quad \text{mit } \sigma(n) := \left(\sum\nolimits_{d|n} 1\right) - 1$$

B.10 Algebraische Codes

Aufgabe B.50 (5 Punkte)
Sei $q = p^d$ mit p prim und $\mathbb{F}_q = \{0, 1, a_1, a_2, \ldots, a_{q-2}\}$. Die PCH-Matrix zum Reed-Salomon-Code C über $\mathbb{F}_q$ sei:

$$\begin{bmatrix} 0 & 1 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 0 & 1 & a_1 & a_2 & \cdots & a_{q-2} \\ 0 & 0 & 1 & a_1^2 & a_2^2 & \cdots & a_{q-2}^2 \\ \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 1 & a_1^{d-3} & a_2^{d-3} & \cdots & a_{q-2}^{d-3} \\ 1 & 0 & 0 & a_1^{d-2} & a_2^{d-2} & \cdots & a_{q-2}^{d-2} \end{bmatrix} \in M_{d-1,q+1}(\mathbb{F}_q)$$

Zeige, daß je $d-1$ Spalten von H linear unabhängig sind. Zeige, daß H einen $[q+1, q+2-d]$-Code $C \subseteq \mathbb{F}_q^{q+1}$ mit Distanz $d(C) \geq d$ definiert.

B.11 Erzeugende Funktionen

Aufgabe B.51 (5 Punkte)
Gegeben seien $n+1$ Variablen $x_0, x_1, \ldots, x_n$, deren Produkt mit n Multiplikationen berechnet werden soll. Wieviel mögliche Klammerungen C_n des Produkts $x_0 x_1 \ldots x_n$ gibt es, so daß die Reihenfolge der Multiplikationen durch die jeweilige Klammerung vollständig spezifiziert ist? Es gilt $C_0 = C_1 = 1$. Für $n = 2$ gibt es genau zwei Möglichkeiten:

$$x_0(x_1 x_2) \quad \text{und} \quad (x_0 x_1)x_2$$

Für $n = 3$ gibt es genau fünf Möglichkeiten:

$$x_0(x_1(x_2 x_3)), \quad x_0((x_1 x_2)x_3), \quad (x_0 x_1)(x_2 x_3), \quad (x_0(x_1 x_2))x_3, \quad ((x_0 x_1)x_2)x_3$$

Finde einen geschlossenen Ausdruck für C_n (Tip: Catalan-Zahlen).

Aufgabe B.52 (5 Punkte)
Finde mit Hilfe einer erzeugenden Funktionen einen geschlossenen Ausdruck für folgende Rekursion:

$$a_n = \begin{cases} a_{n-1} + n & \text{falls } n > 0 \\ 0 & \text{sonst} \end{cases}$$

B.12 Boole'sche Algebren und Funktionen, $\mathcal{NP}$-Vollständigkeit

Aufgabe B.53 (15 Punkte)
Betrachte den Restklassenring

$$B_n := \mathbb{Z}_2[x_1, x_2, \ldots, x_n]/I_n$$

mit dem Ideal $I_n \subseteq \mathbb{Z}_2[x_1, x_2, \ldots, x_n]$, das von den Polynomen $x_1 + x_1^2, x_2 + x_2^2, \ldots, x_n + x_n^2$ erzeugt wird. Zeige:

1. Die Polynome einer Restklasse $f + I_n$ induzieren eine eindeutig bestimmte Boole'sche Funktion $\overline{f} : \{0,1\}^n \to \{0,1\}$, d.h. $\overline{f}$ hängt nicht von der Wahl des Repräsentanten f ab.
2. Es gilt: $\overline{g \cdot f} = \overline{g} \wedge \overline{f}, \quad \overline{1 + f} = \neg\, \overline{f}$
3. Jede Boole'sche Funktion $\{0,1\}^n \to \{0,1\}$ wird genau von einer Restklasse induziert.

Wir nennen B_n den Ring der Boole'schen Polynome in n Variablen. Wir identifizieren $\overline{f}$ mit $f + I_N$ und schreiben f für $f + I_n$. Es sei:

$$B_{n,k} := \left\{ \sum_{1 \le i_1 \le i_2 \le \ldots \le i_k \le n} a_{i_1,i_2,\ldots,i_k} x_{i_1} x_{i_2} \cdots x_{i_k} \;\middle|\; a_{i_1,i_2,\ldots,i_k} \in \mathbb{Z}_2 \right\} \subseteq B_n$$

Zeige: Zu $f \in B_n$ gibt es eindeutig bestimmte $f_i \in B_{n,i}$ für $i = 1, 2, \ldots, n$ mit $f = \sum_{i=0}^{n} f_i$.

Aufgabe B.54 (5 Punkte)
Zeige, daß für alle $f \in \mathbb{Z}_2[x_1, x_2, \ldots, x_n]$ gilt $(1 \le i \le n)$:

$$\overline{f} = \overline{x_i \cdot f_{x_i=1} + (1 + x_i) \cdot f_{x_i=0}}$$

Entscheidungsproblem SAT
Gegeben KNF $\gamma = \bigwedge_{1 \le \nu \le m} \bigvee_{1 \le \mu \le k_\mu} x_{i_{\nu,\mu}}^{j_{\nu,\mu}}$ in den Booleschen Variablen mit Indizes $i_{\mu,\nu} \in \{1, \ldots, n\}$.
Entscheide, ob es eine Belegung $b : x_i \mapsto \{0, 1\}$ gibt mit $\bigwedge_{1 \le \nu \le m} \bigvee_{1 \le \mu \le k_\nu} b(x_{i_{\nu,\mu}})^{j_{\nu,\mu}} = 1$.

Betrachte folgende Sprachen in NP:

$$\text{SAT} = \{\gamma \mid \gamma \text{ erfüllbare KNF}\}.$$

$$\text{Clique} = \left\{ (V, E, k) \middle| \begin{array}{l} G = (V, E) \text{ ist ungerichteter Graph} \\ \exists S \subset V : S \times S \subset E, \#S = k \end{array} \right\}.$$

Aufgabe B.55
Zeige SAT $\le_{\text{pol}} 3 - SAT$,
somit 3-SAT ist NP-vollständig.

Aufgabe B.56
Zeige SAT $\le_{\text{pol}}$ Clique.
Hinweis: ordne der obigen KNF den Graphen (V, E) zu mit
$V = \{(\nu, \mu) \mid 1 \le \nu \le m, 1 \le \mu \le k_\nu\}$,
$E = \{((\nu, \mu), (\nu', \mu')) \mid \nu \ne \nu', (i_{\nu,\mu}, j_{\nu,\mu}) \ne (i_{\nu',\mu'}, \rceil j_{\nu',\mu'})\}$.

Algorithmenverzeichnis

Index

Literaturverzeichnis

[A94] M. Aigner: **Diskrete Mathematik**, Vieweg Braunschweig/Wiesbaden, 1994.

[CP01] R. Crandall and C. Pomerance: **Prime Numbers, A Computational Perspektive.** Springer New York, 2001.

[FS78] G. Fischer und R. Sacher: **Einführung in die Algebra**, B.G. Teubner Stuttgart, 1978.

[GS78] Von zur Gathen und M. Sieveking: *A Bound on Solution of linear integer Equations and Inequations*, Proceedings of the American Mathematical Society, Band 72, Seiten 155–158, 1978.

[GKP89] R.L. Graham, D.E. Knuth und O. Patashnik: **Concrete Mathematics — A Foundation for Computer Science**, Addison-Wesley Reading, 1989.

[I94] T. Ihringer: **Diskrete Mathematik**, B.G. Teubner Stuttgart, 1994.

[I96] M.C. Irwin: **Geometry of Continued Fractions**, Americ. Math. Monthly, 1996.

[KS94] M. Kaib und C.P. Schnorr: *The generalized Gauss Reduktion Algorithm*, Journal Algorithms, 1994.

[K63] A.Y. Khintchine: **Continued Fractions**, P. Nordhoff, Groningen, 1963.

[K73a] D.E. Knuth: **The Art of Computer Programming**, Band I, Fundamental Algorithms, Addison-Wesley Reading, 1973.

[K81] D.E. Knuth: **The Art of Computer Programming**, Band II, Seminumerical Algorithms, Addison-Wesley, Reading, 1981.

[LLL82] A.K. Lenstra, H.W. Lenstra Jr. and L. Lovàsz *Factoring polynomials with rational coefficients*, Mathematical Annalen, 1982.

[L83] H.W. Lenstra Jr., *Integer programming in a fixed number of variables*, Mathematics of Operation Research 8, 1983.

[LN86] R. Lidl und H. Niederreiter: **Introduction to Finite Fields and their Applications**, Cambridge University Press, 1986.

[Po81] C. Pomerance: **On the distribution of pseudoprimes**, Math. Comp. 37:587–593, 1981.

[Pe54] O. Perron: **Die Lehre von den Kettenbrüchen**, B.G. Teubner Stuttgart, 1954.

[R89] M.O. Rabin: *Efficient Dispersal of Information for Security, Load Balancing and Fault Tolerance*, Journal of the ACM, Band 36, Nr. 2, Seiten 335–348, 1989.

[RSA78] R. Rivest, A. Shamir und L. Adleman: *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, Communications of the ACM, Band 21, Nr. 2, Seiten 120–126, 1978.

[S91] R.H. Schulz: **Codierungstheorie — eine Einführung**, Vieweg Braunschweig/Wiesbaden, 1991.

[W90] M. Wiener: *Cryptanalysis of Short RSA Secret Exponents*, IEEE Transaction on Information, Band 36, Nr. 3, Seiten 553–558, 1990.

Zur linearen Programmierung:

C.H. Papadimitriou and K. Steiglitz: Combinatorial Optimization
Dover Publ. Inc. 1998.

A. Schrijver: Theory of Linear and Integer Programming
John Wiley & Sons, 1987.

M. Aigner: Diskrete Mathematik
Vieweg, 1996.