Diskrete und Strukturelle Mathematik für Informatiker
im SS03

Inhaltsverzeichnis

Kapitel 1

Graphentheorie

1.1 Grundlegende Begriffe

Definition: Graph

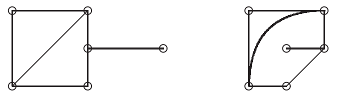
Ein Graph [graph] $G = (V, E)$ besteht aus

- einer Menge V von Knoten [vertices]
- einer Menge E von Kanten [edges]
- $E \subseteq \{\{u, v\} | u, v \in V, u \neq v\}$

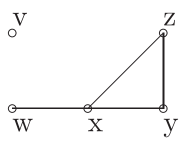
Jede Kante verbindet zwei verschiedene Knoten.
Jedes Paar von Knoten ist durch höchstens eine Kante verbunden.
Die Anzahl der ungeordneten Paare von verschiedenen Elementen einer n- elementigen Menge ist $\binom{n}{2} = \frac{n(n-1)}{2}$. Daher gilt $|E| \leq \frac{1}{2} \cdot |V| \cdot (|V| - 1)$.

Darstellungsarten

Ein gegebener Graph kann auf viele Arten goemetrisch dargestellt werden. Die Form der Kanten ist belanglos und sie Können sich in der Zeichnung in Punkten schneiden, die keine Knoten sind. So stellen die beiden folgenden Zeichnungen den gleichen Graphen dar:

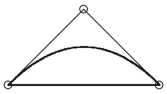


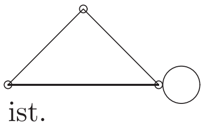
Ein Graph kann natürlich auch aufgeschrieben werden:

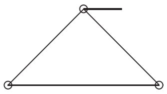


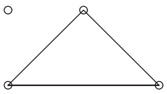
$V = \{u, w, x, y, z\}$
$E = \{\{w, x\}\{x, y\}\{y, z\}\{x, z\}\}$

Welche der Zeichnungen ist ein Graph?

1.  Ist kein Graph, denn zwei Kanten verbinden dieselben Knoten.

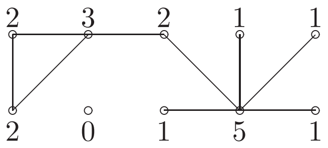
2.  Ist kein Graph, weil ein Knoten gleichzeitig Start- und Endknoten einer Kante ist.

3.  Ist kein Graph, weil eine Kante keinen Endpunkt hat.

4.  Ist ein Graph.

Der Grad eines Knotens

Sei $x \in V$ ein Knoten. Der Grad [degree] $d(x)$ eines Knotens ist definiert als die Anzahl der Kanten, die in x enden. In der folgenden Zeichnung sind die Grade an den entsprechenden Knoten eingetragen.

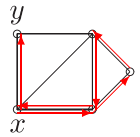


Satz 1.1

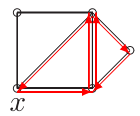
Für jeden Graphen $G = (V, E)$ gilt:
$\sum_{x \in V} d(x) = 2 \cdot |E|$
d.h. die Summe aller Grade ist die doppelte Kantenzahl.
Beweis: Dieser Satz folgt sofort aus der Definition des Grades und der Tatsache, dass jede Kante zwei verschiedene Knoten verbindet.

Kantenfolge

Eine Kantenfolge [edges sequence, chain] von $x_0 \in V$ nach $x_n \in V$ hat die Form $S = \{x_0, x_1\}\{x_1, x_2\} \ldots \{x_{n-1}, x_n\}$, mit der Eigenschaft, dass $x_1, \ldots, x_n \in V, \{x_i, x_{i+1}\} \in E$.
Wenn S eine Kantenfolge von x nach y und T eine Kantenfolge von y nach z ist, so bezeichnet ST die Kantenfolge von x nach z, die aus S durch Anhängen von T entsteht.
Eine Kantenfolge S heißt geschlossen, wenn der Endpunkt gleich dem Startpunkt ist.



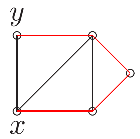
Kantenfolge von x nach y



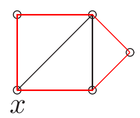
geschlossene Kantenfolge

Weg

Ein Weg [path] von $x \in V$ nach $y \in V$ ist eine Kantenfolge, in der alle Knoten verschieden sind. Dann sind auch alle Kanten verschieden.
Ein Kreis [circle] ist eine Folge von mindestens drei Kanten, die geschlossen ist und in der sonst alle Knoten verschieden sind.



Weg von x nach Y



Kreis

Satz 1.2

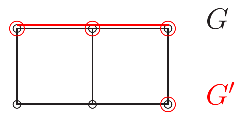
Wenn es in einem Graphen eine Kantenfolge von x nach y gibt, so gibt es auch einen Weg von x nach y.
Beweis: Sei S eine Kantenfolge von x nach y. Wenn alle Knoten von S verschieden sind, so ist S bereits ein Weg. Daher dürfen wir annehmen, dass ein Knoten z zweimal vorkommt. Sei nun A der Teil von S von x bis zum ersten auftreten von z und sei B der Teil von S vom letzten Auftreten von z bis nach y. Dann ist $S_1 = AB$ eine Kantenfolge von x nach y, die weniger Kanten enthält als S. Wenn S_1 immernoch kein Weg ist, so setzen wir diese Konstruktion fort.

Teilgraphen

Sei $G = (V, E)$ ein Graph. Der Graph $G' = (V', E')$ heißt Teilgraph [subgraph] von G, wenn gilt:

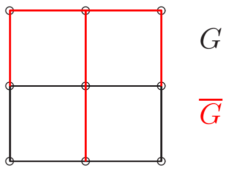
- $V' \subseteq V$
- $E' \subseteq E$

Man beachte, dass G' ein Graph ist.
Wenn also eine Kante in E zu E' gehört, so müssen auch beide Endknoten zu V' gehören.
Der Teilgraph G' heißt (auf-) spannend [spanning], wenn $V' = V$, also alle Knoten von G zu G' gehören.



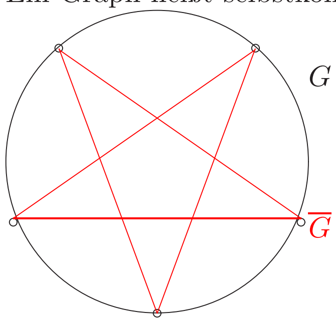
Das Komplement eines Graphen

Das Komplement eines Graphen $G = (V, E)$ ist definiert als der Graph $\overline{G} = (V, \overline{E})$ mit
$\overline{E} = \{\{v, w\}|v, w \in V, v \neq w\} \setminus E$
Also alle Kanten, die nicht in G vorkommen.



Isomorphie eines Graphen

Zwei Graphen $G = (V, E)$ und $G' = (V' = V, E')$ heißen isomorph, falls man G' durch Umbenennung der Knoten von G erhalten kann. Das heißt es gibt eine bijektive Abbildung
$\phi : V \to V'$ mit $\forall v, w \in V$ gilt: $\{\phi(v), \phi(w)\} \in E' \Leftrightarrow \{v, w\} \in E$.
Ein Graph heißt selbstkomplementär, wenn er isomorph zu seinem Komplement ist.



G ist ein selbstkomlementärer Graph.

1.2 Zusammenhängende Graphen

Definition: Zusammenhängender Graph

Der Graph $G = (V, E)$ heißt zusammenhängend [connected], wenn es zu jedem Paar $x, y \in V$ einen Weg von x nach y gibt.

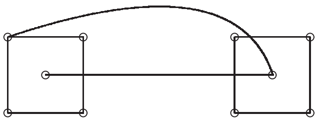
Satz 1.3

Sei $G = (V, E)$ ein Graph, dann gibt es zusammenhängende Graphen $G_k = (V_k, E_k), k = 1, \ldots, n)$, sodass gilt:

1. $V = V_1 \cup \ldots \cup V_n$ mit $V_1, \ldots, V_n$ sind disjunkt und
2. $E = E_1 \cup \ldots \cup E_n$ mit $E_1, \ldots, E_n$ sind disjunkt.

Die Graphen $G_1, \ldots, G_n$ heißen Komponenten von G.
Wenn G zusammenhängend ist, so gilt $n = 1$, sonst $n > 1$.

Graph mit 3 Zusammenhangskomponenten



Graph mit 2 Zusammenhangskomponenten

Widerspruchsbeweis:
Annahme: Es gibt einen Graphen mit einer ungeraden Anzahl von Knoten mit ungeradem Grad.
$\sum\limits_{x\in V} d(x) = \sum\limits_{x\in V, d(x)=2k} d(x) + \sum\limits_{x\in V, d(x)=2K-1} d(x)$
Damit $\sum\limits_{x\in V, d(x)=2K-1} d(x)$ ungerade wird, muss die Anzahl der Knoten ungerade sein. Dann ist aber auch $\sum\limits_{x\in V} d(x)$ ungerade, was aber nach Satz 1.1 nicht sein kann.

Satz 1.4 (geschlossene Eulerkantenfolge

Sei G ein zusammenhängender Graph. Dann sind folgende Aussagen äquivalent:

1. Es gibt eine geschlossene Kantenfolge in der jede Kante von G genau einmal vorkommt.
2. Der Grad d(x) ist gerade für jedes $x \in V$.

Eine Kantenfolge von x nach y muss 2 Knoten mit ungeradem Grad besitzen, die anderen Knoten müssen gerade Grade haben.
Eine geschlossene Kantenfolge darf nur Knoten mit geradem Grad haben.
Beweis:

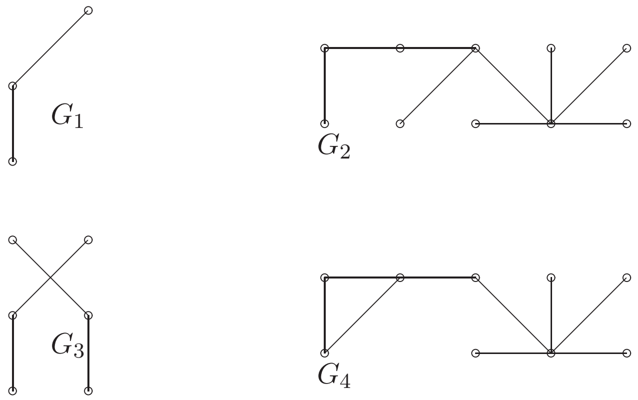
- 1. $\Rightarrow$ 2.: Sei $x \in V$. Jedesmal, wenn die Kantenfolge in x hineingeht, geht sie auf einer anderen Kante wieder heraus. Das gilt auch für Anfangsknoten = Endknoten.
- 2. $\Rightarrow$ 1.: Sei $x \in V$. Wir beginnen in einem belibigen Knoten x_0 und zeichnen eine Kantenfolge S_1 (ohne Mehrfachbenutzung von Kanten) so lange, bis dies nicht mehr möglich ist. Da die Grade $d(x)$ gerade sind, ist S_1 geschlossen.
  - Fall 1: Für jeden Knoten von S_1 gehören alle dort endenden Kanten auch zu S_1: Wir zeigen, dass jede Kante $e \in G$ zu S_1 gehört. Angenommen das wäre falsch. Da G zusammenhängend ist, gibt es einen Weg C von einem Endknoten von e zur Kantenfolge S_1. Im Knoten x, wo C zum ersten Mal S_1 trifft erhalten wir einen Widerspruch zur Fall- Annahme.
  - Fall 2: Es gibt eien Knoten x_1 von S_1 und eine Kante $e_1 \in E \setminus S_1$ mit Endknoten x_1: In jedem Knoten $x \in V$ ist die Anzahl der Kanten immer noch gerade; sie kann 0 sein. Daher können wir eine Kantenfolge $S_1' \subset E \setminus S_1$ finden, die in x_1 beginnt und dort auch wieder endet. Nun fügen wir S_1' in die Folge S_1 an der Stelle x_1 ein. Das gibt wieder eine geschlossene Kantenfolge S_2. Für S_2 verfahren wir genauso.

1.3 Bäume

Definition: Baum

Ein Graph G heißt Baum [tree], wenn gilt:

- G ist zusammenhängend
- G enthält keinen Kreis



G_1 und G_2 sind Bäume. G_3 ist nicht zusammenhängend und G_4 enthält einen Kreis. G_3 und G_4 sind also keine Bäume.

Satz 1.5

Jeder zusammenhängede Graph enthält (mindestens) einen aufspannenden Baum.
Das heißt: Wenn $G = (V, E)$ zusammenhängend ist, so gibt es einen Baum $G' = (V, E')$ mit $E' \subseteq E$. Also hat G' dieselben Knoten, aber eventuell weniger Kanten.
Beweis: Wenn G keinen Kreis enthält, so ist G bereits ein Baum. Nun enthalte G einen Kreis C_1 und sei e_1 eine beliebige Kante von C_1. Wir betrachten den Graphen $G_1 = (V, E \setminus e_1)$, d.h. wir haben die Kante e_1 gelöscht. Da C_1 ein Kreis ist, werden die Endknoten von e_1 durch $C_1 \setminus e_1$ verbunden. Daher ist G immernoch zusammenhängend. So verfahren wir mit allen Kreisen in G. Nach endlich vielen Schritten erhalten wir einen Baum.

Endknoten

Der Knoten x heißt Endknoten [terminal vertex], wenn $d(x) = 1$ ist, d.h. wenn nur eine Kante in x endet.

Satz 1.6

Jeder Baum $G = (V, E)$ mit $|V| \geq 2$ hat mindestens zwei Endknoten.
Beweis (für die Existens eines Endknotens): Sei u ein beliebiger Knoten des Baumes G. Von u aus zeichnen wir einen Weg C solange, bis es nicht mehr weiter geht. Sei x der letzte Knoten von C. Wir behaupten, dass x ein Endknoten ist.
Angenommen das wäre falsch. Dann ist $d(x) \geq 2$, es gibt also eine Kante $e = \{x, y\}$, die nicht zum Weg C gehört. Da C nicht vergrößert werden konnte, darf es nicht möglich sein, e zu C hinzuzunehmen, weil y auf C liegt. Dann wäre aber der Teil von C vom Knoten y bis x zusammen mit e ein Kreis, im Widerspruch dazu, dass G ein Baum ist.

zyklomatische Zahl

Die zyklomatische Zahl [cyclomatic number] des Graphen $G = (V, E)$ ist definiert durch:
$\nu(G) = |E| - |V| + 1$

1. $\nu(G) = 0 \Rightarrow$ G ist ein Baum
2. $\nu(G) > 0 \Rightarrow$ G ist zusammenhängend, aber kein Baum
3. $\nu(G) < 0 \Rightarrow$ G ist nicht zusammen hängend

Satz 1.7

Sei $G = (V, E)$ ein zusammenhängender Graph.

1. Wenn G ein Baum ist, so gilt $|E| = |V| - 1$.
2. Wenn G kein Baum ist, so gilt $|E| \geq |V|$.

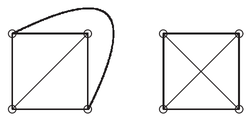
Beweis:

1. Sei G ein Baum. Nach Satz 1.6 hat G einen Endknoten x_1. Sei e_1 die einzige Kante, die in x_1 endet. Dann ist $G_1 = (V \setminus x_1, E \setminus e_1)$ zusammenhängend und natürlich ohne Kreise, also ein Baum. In G_1 gibt es einen Endknoten x_2 mit Kante e_2. Dann ist $G_2 = (V \setminus (x_1 \cup x_2), E \setminus (e_1 \cup e_2))$ wieder ein Baum, usw.
   Schließlich bleibt nur ein Knoten und keine Kante übrig. Bei jedem Schritt wurden ein Knoten und eine Kante entfernt. Es waren $|E|$ Schritte, also ist $|V| = |E| + 1$.
2. Nun sei G kein Baum. Nach Satz 1.5 gibt es einen spannenden Baum $G' = (V, E')$ mit $|E'| < |E|$. Es folgt $\nu(G) = |E| - |V| + 1 > |E'| - |V| + 1 = \nu(G') = 0$

1.4 Ebene Graphen

Definition: Ebener Graph

Der Graph $G = (V, E)$ heißt eben [planar], wenn man ihn so in der Ebene zeichnen kann, dass sich die Kanten nur in ihren Endknoten schneiden.



Beide Zeichnungen stellen den selben ebenen Graphen dar. Nur die erste ist zulässig.

Definition: Gebiet

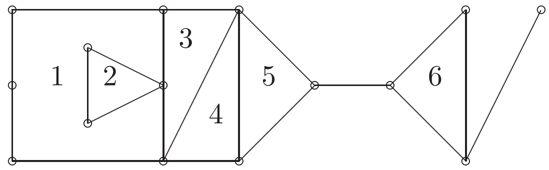
Ein Gebiet [domain] in der Ebene ist eine Punktmenge Ω, für die gilt:

1. kein Randpunkt von Ω gehört zu Ω
2. je zwei Punkte von Ω lassen sich durch eine Kurve innerhalb Ω verbinden.

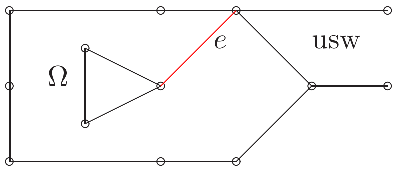
Das Gebiet Ω heißt beschränkt, wenn es nicht bis Unendlich geht.

Satz 1.8

Der zusammenhängende ebene Graph $G = (V, E)$ sei in der Ebene gezeichnet. Dann zerlegt G die Ebene in $\nu(G) = |E| - |V| + 1$ (zyklomatische Zahl) beschränkte und ein unbeschränktes Gebiet.



Beweis (durch Induktion nach $\nu(G)$)
Induktionsanfang: Sei $\nu(G) = 0$. Nach Satz 1.6 ist G dann ein Baum und ein Baum umschließt kein beschränktes Gebiet.
Induktionsschritt: Sei die Behauptung schon für alle zusammenhängenden Graphen G' mit $\nu(G') = n-1$ bewiesen und sei $\nu(G) = n > 0$. Nach Satz 1.7 ist G dann kein Baum. Da G zusammenhängend ist, enthält G einen Kreis. Sei nun e eine Kante auf diesem Kreis. Dann ist $G' = (V, E \setminus e)$ ein zusammenhängender ebener Graph mit $\nu(G') = |E'| - |V| + 1 = |E| - |V| = n - 1$. Nach Induktionsvorraussetzung zerlegt daher G' die Ebene in n beschränkte Gebiete (und ein unbeschränktes). Nun fügen wir die weggelassene Kante e wieder hinzu. Sei Ω' das Gebiet von G', in dem e liegt. Dann besteht $\Omega' \setminus e$ aus zwei verschiedenen Gebieten. Sonst hätte man die Situation der folgenden Zeichnung, die unmöglich ist, da e auf einem Kreis von G liegt.



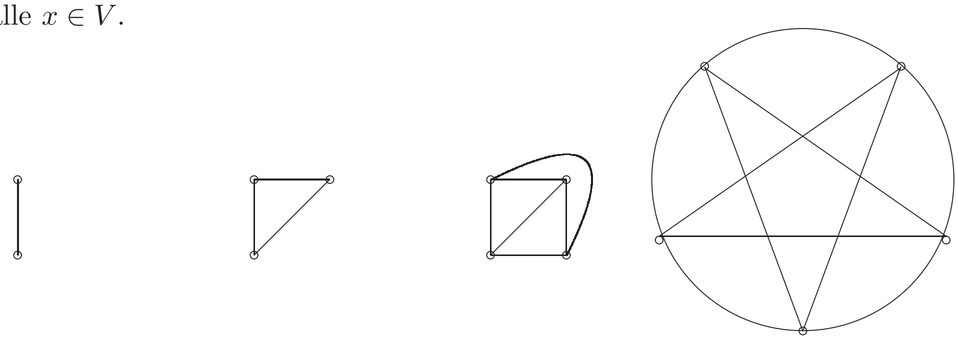
Nun hatte G' genau $(n-1)+1 = n$ Gebiete einschließlich des unbeschränkten. Wir haben gesehen, dass eines davon (es könnte das unbeschränkte sein) durch e in zwei aufgeteilt wird. Also hat G genau $n+1$ Gebiete, also n beschränkte und dass ist die Induktionsbehauptung.

Satz 1.9

Sei $G = (V, E)$ ein zusammenhängender Graph mit $|V| \geq 3$, dann ist $|E| \leq 3|V| - 6$.
Beweis: Nach Satz 1.8 zerlegt G die Ebene in $\nu(G)+1$ Gebiete. Wegen $|V| \geq 3$ wird jedes von ihnen durch mindestens drei Kanten begrenzt. Andererseits ist jede Kante auf dem Rand von höchstens zwei Gebieten. Somit gilt: $2|E| \geq 3(\nu(G)+1) = 3(|E| - |V| + 2) = 3|E| - 3|V| + 6$ und hieraus folgt: $|E| \leq 3|V| - 6$.

Vollständigkeit eines Graphen

Der Graph $G = (V, E)$ heißt vollständig [complete], wenn jedes Paar verschiedener Knoten durch eine Kante verbunden ist, d.h. wenn $|E| = \frac{1}{2}|V|(|V|-1)$ ist. Eine äquivalente Bedingung ist $d(x) = |V| - 1$ für alle $x \in V$.



Diese Graphen sind vollständig.

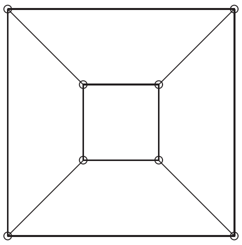
Satz 1.10

Die vollständigen Graphen mit weniger als 5 Knoten sind eben, die mit mehr als 4 Knoten sind nicht eben.
Beweis: Die erste Behauptung ist trivial. siehe oben.

Sei nun G ein vollständiger Graph mit n Knoten, der eben ist. Es gilt also $\frac{1}{2}n(n-1) = |E| \overset{Satz 1.9}{\leq} 3n-6$, also $n^2 - n \leq 6n - 12$. Hieraus folgt $(n - \frac{7}{2})^2 = n^2 - 7n + \frac{49}{4} \leq \frac{1}{4}$, also $|n - \frac{7}{2}| \leq \frac{1}{2}$ und daher $n \leq 4$.

Bipartität

Der Graph $G = (V, E)$ heißt bipartit [bipartite], wenn jeder Kreis eine gerade Zahl von Kanten hat. Zum Beispiel ist jeder Baum bipartit, da es keine Kreise gibt.



Satz 1.11

Sei $G = (V, E)$ ein zusammenhängender Graph mit $|V| \geq 4$. Wenn G bipartit ist, so gilt $|E| \leq 2|V| - 4$.
Beweis: Ein Kreis enthält immer mindestens 3 Kanten. Da G bipartit ist, jeder Kreis also eine gerade Kantenzahl hat, enthält jeder Kreis mindestens 4 Kanten. Jedes der Gebiete von G hat also mindestens vier Randkanten. Wie im Beweis von Satz 1.9 erhalten wir also $2|E| \geq 4(\nu(G) + 1) = 4|E| - 4|V| + 8$ und daher $|E| \leq 2|V| - 4$.

1.5 Färbungen von Graphen

Sei $G = (V, E)$ ein Graph. Wir betrachten Färbungen der Knoten mit k Farben, so dass durch Kanten verbundene Knoten verschiedene Farben haben.

Die chromatische Zahl

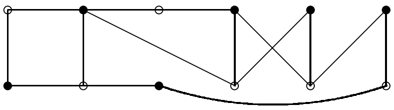
Die chromatische Zahl [chromatic number] $\chi(G)$ von G ist die Minimalzahl von Farben, die man benötigt um einen Graphen zu färben. Natürlich ist $\chi(G) \leq |V|$.
Für vollständige Graphen gilt $\chi(G) = |V|$

Satz 1.12

Es gilt $\chi(G) = 2$ genau dann, wenn der Graph G bipartit ist.
Dieser Satz erklärt den Namen „bipartit“: Es gibt eine Partition

1. $V = V_1 \cup V_2, V_1 \cap V_2 = \varnothing$
   der Knoten in zwei Klassen, die den Farben 1 und 2 entsprechen. Alle Kanten haben die Form

2. $e = \{x_1, x_2\}$ mit $x_1 \in V_1, x_2 \in V_2$.



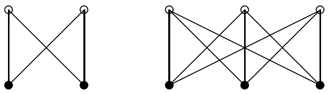
Ein bipartiter Graph

Vollständige Bipartität

Ein Graph G heißt vollständig bipartit mit $2n$ Knoten, wenn gilt:

1. $V = V_1 \cup V_2, V_1 \cap V_2 = \varnothing$ und $|V_1| = |V_2| = n$
2. $e = \{x_1, x_2\}$ mit $x_1 \in V_1, x_2 \in V_2$.

Jedes Paar verschiedenfarbiger Knoten ist also durch eine Kante verbunden.



Die vollständigen bipartiten Graphen mit 4 und 6 knoten. Der erste ist eben, der zweite nicht.

Satz 1.13

Die vollständig bipartiten Graphen mit ≥ 6 Knoten sind nicht eben.
Beweis: Sei $G = (V, E)$ vollständig bipartit und $|V| = 2n$. Dann ist $|E| = n^2$. Wenn G eben ist, so folgt aus Satz 1.11 $n^2 = |E| \leq 2|V| - 4 = 4n - 4$ und daher $(n-2)^2 = n^2 - 4n + 4 \leq 0$, also $n = 2, |V| = 4$.

Satz 1.14 (Kuratowski)

Der Graph G ist nicht eben, genau dann, wenn mindestens eine der folgenden Bedingungen gilt:

1. G enthält eine Unterteilung des vollständigen Graphen mit 5 Knoten
2. G enthält eine Unterteilung des vollständig bipartiten Graphen mit 6 Knoten.

Satz 1.15 (Vierfarbsatz von Appel, Haken und Koch)

Jeder ebene Graph hat eine chromatische Zahl ≤ 4.
Man kann also jeden ebenen Graphen mit vier Farben färben. Dieser Satz löste eine berühmte Vermutung, das „Vierfarbenproblem". Er wurde 1976 mittels Computer bewiesen und es gibt noch keinen Beweis, der ganz ohne Computer auskommt.

Kapitel 2

Zahlen

2.1 Der euklidische Algorithmus

Der euklidische Algorithmus

Sei $\mathbb{N} = \{0, 1, 2, \ldots\}$ und $\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$. Für $m = 1, 2, \ldots$ und $n \in \mathbb{Z}$ hat man

(1). $n = qm + r$ mit $q \in \mathbb{Z}, r \in \mathbb{N}, 0 \leq r < m$.
Zum Beispiel für $m = 10$ und $n = 127$ ist $127 = 12 \cdot 10 + 7$.
Wenn $r = 0$ in (1) ist, so gilt $n = qm$. Dann heißt m ein Teiler [divisor] von n und wir schreiben $m|n$. Sonst schreiben wir $m \not| n$. Also ist

(2). $m|n \Leftrightarrow \frac{n}{m} \in \mathbb{Z}$.
So ist z.B. $3|12, 6|12, 9 \not| 12, 9|0$
Nun beschreiben wir den euklidischen Algorithmus.
Seien $x, y \in \mathbb{N}$ mit $1 \leq x \leq y$. Wir setzen

(3). $x_0 = y, x_1 = x$.
Nach (1) existieren $q_1, x_2 \in \mathbb{N}$, so dass gilt

(4). $x_0 = q_1 x_1 + x_2$ mit $0 \leq x_2 < x_1$.
Der Algorithmus endet, wenn $x_2 = 0$ ist. Wenn $x_2 > 0$ ist, so hat man wieder nach (1)

(5). $x_1 = q_2 x_2 + x_3$ mit $0 \leq x_3 < x_2$.
Wenn $x_3 = 0$ ist, so endet der Algorithmus.
So erhalten wir ganze Zahlen $x_1 > x_2 > \ldots > x_n > \ldots \geq 0$. Der euklidische Algorithmus endet, wenn $x_n = 0$ ist. Wenn $x_n > 0$ ist, so gibt es $q - n, x_{n+1} \in \mathbb{Z}$, so dass

(6). $x_{n-1} = q_n x_n + x_{n+1}$ mit $0 \leq x_{n+1} < x_n$ gilt.
Schließlich erhalten wir k mit

(7). $x_{k-1} = q_k x_k, x_k > 0, x_{k+1} = 0$.
Die Zahl x_k ist das <u>Resultat</u> des euklidischen Algorithmus.
<u>Beispiel:</u> Seien $x = 221$ und $y = 1001$. Es ergibt sich

$$1001 = 4 \cdot 221 + 117, 221 = 1 \cdot 117 + 104, 117 = 1 \cdot 104 + \underline{13}, 104 = 8 \cdot 13 + 0$$

Satz 2.1

Seien $x, y \in \mathbb{N}$ und $0 < x \leq y$.
Das Resultat x_k des euklidischen Algorithmus erfüllt

(8). $x_k|x, x_k|y$

(9). $d|x, d|y \Rightarrow d|x_k$.
Weiter gibt es $\xi, \eta \in \mathbb{Z}$ mit

(10). $x_k = \xi x + \eta y$.
Beweis: Aus (3) und (4) folgt
$x_2 = x_0 - q_1 x_1 = \xi_2 x + \eta_2 y$ mit $\xi_2 = -q_1, \eta_2 = 1$, und aus (5) erhält man dann
$x_3 = x_1 - q_2 x_2 = q_2(\xi_2 x + \eta_2 y) = \xi_3 x + \eta_3 y$ mit $\xi_3 = 1 - q_2\xi_2, \eta_3 = -q_2\eta_2$.
Alle Zahlen ξ_n, η_n sind ganzzahlig. Schließlich ergibt sich $x_k = \xi_k x + \eta_k y$, und das ist die Behauptung (10).
Aus (7) folgt $x_k|x_{k-1}$. Daher ist $x_k|q_{k-1}x_{k-1} + x_k = x_{k-2}$ nach (6) mit $n = k-1$. Schließlich folgt $x_k|x_1 = x$ und $x_k|x_0 = y$. Damit ist (8) bewiesen.
Sei nun $d|x$ und $d|y$. Aus (10) folgt dann $d|\xi x + \eta y = x_k$. Damit ist auch (9) bewiesen.

Größter gemeinsamer Teiler

Man nennt x_k den größten gemeinsamen Teiler [greatest common divisor] von x und y, geschrieben

(11). $x_k = ggT(x, y)$.
Nach Satz 2.1 ist also

(12). $ggT(x, y)|x, ggT(x, y)|y$,

(13). $d|x, d|y \Rightarrow d|ggT(x, y)$,

(14). $ggT(x, y) = \xi x + \eta y$ mit $\xi, \eta \in \mathbb{Z}$.
Beispiel: Wir haben festgestellt, dass $ggT(221, 1001) = 13$. Man hat $13 = 117 - 104 = 117 - (221 - 117) = 2 \cdot 117 - 221 = 2 \cdot (1001 - 4 \cdot 221) - 221 = 2 \cdot 1001 - 9 \cdot 221$ und somit $13 = ggT(221, 1001) = (-9) \cdot 221 + 2 \cdot 1001$.

relativ prim

Die Zahlen $x, y \in \mathbb{N} \setminus \{0\}$ heißen relativ prim [relavively prime], wenn $ggT(x, y) = 1$ ist. Aus (14) folgt

(15). x, y relativ prim $\Leftrightarrow$ es gibt $\xi, \eta \in \mathbb{Z}$ mit $\xi x + \eta y = 1$.

Satz 2.2

Seien $a, b, c \in \mathbb{N}, a > 0$. Dann gilt

(16). $a|bc$ und a, b relativ prim $\Rightarrow a|c$.
Beweis: Nach (15) gibt es $\xi, \eta \in \mathbb{Z}$ mit $1 = \xi a + \eta b$. Also ist $c = (\xi a + \eta b)c = (\xi c + \eta \frac{bc}{a})a$.
Wegen $a|bc$ ist der Faktor von a ganzzahlig. Also ist $a|c$.

positive rationale Zahlen

Nun beschreiben wir kurz die positiven rationalen Zahlen.

(17). $z = \frac{x}{y}$ mit $x, y \in \mathbb{N} \setminus \{0\}$
Sei $c = ggT(x, y)$ und $x' = \frac{x}{c}, y' = \frac{y}{c}$. Aus (14) folgt $c = \xi x + \eta y$, also $1 = \xi x' + \eta y'$ mit $\xi, \eta \in \mathbb{Z}$.
Nach (15) und (17) ist daher

(18). $z = \frac{x'}{y'}$ mit x', y' relativ prim.

2.2 Primzahlen

Definition: Primzahl

Die Zahl $p \in \mathbb{N}$ heißt Primzahl [prime], wenn $p > 1$ ist und wenn p keine Divisoren $d \in \mathbb{N}$ mit $1 < d < p$ hat.

Satz 2.3

Jede natürliche Zahl $n > 1$ hat genau eine Primfaktorzerlegung.

(1). $n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_m^{k_m}$ mit Primzahlen $p_1 < \ldots < p_m$, wobei $m \geq 1$ und $k_1 \geq 1, \ldots, k_m \geq 1$ ist. Zum Beispiel ist $3240 = 2^3 \cdot 3^4 \cdot 5$, also $m = 3, p_1 = 2, p_2 = 3, p_3 = 5, k_1 = 3, k_2 = 4, k_3 = 1$
Beweis:
a) Zum Nachweis der Existenz einer Primfaktorzerlegung benutzen wir eine Variante der Induktion. Sei die Existenz schon für alle Zahlen $< n$ bewiesen.
Nun sei $n > 1$ gegeben. Wenn n eine Primzahl ist, so ist (1) trivial (mit $m = 1, p_1 = n, k_1 = 1$). Wenn n keine Primzahl ist, so ist $n = a \cdot b$ mit $1 < a < n, 1 < b < n$. Nach Induktionsvoraussetzung haben a und b Primfaktorzerlegungen. Diese multiplizieren wir und ordnen dann um. So erhalten wir (1).
b) Nun beweisen wir die Eindeutigkeit. Sei

(2). $n = q_1^{l_1} \cdot \ldots \cdot q_s^{l_s}$ mit Primzahlen $q_1 < \ldots < q_s$ eine weitere Primfaktorzerlegung derselben Zahl n. Wir müssen zeigen, dass sie identisch mit (1) ist.
Aus (1) folgt, dass p_m ein Teiler von n ist. Da verschiedene Primzahlen relativ prim sind , folgt aus (2) nach Satz 2.2 $p_m = q_j$ mit einem $j \leq s$. Nach (2) ist q_s ein Teiler von n. Nach (1) und Satz 2.2 ist also $q_s = p_i$ mit einem $i \leq m$.
Wäre $i < m$, so hätten wir nach (1) $q_s = p_i < p_m = q_j \leq q_s$, was ein Widerspruch ist. Also gilt $i = m$, d.h. $q_s = p_m$. Nun dividieren wir (1) und (2) durch $p_m = q_s$ und fahren fort.

Wir zeigen noch, dass es unendlich viele Primzahlen gibt:
Angenommen p ist die größte Primzahl, dann ist $\mathbb{P}$, die Menge aller Primzahlen endlich.
$\dfrac{1 + \sum\limits_{\mathbb{P}} p}{p'} = \underbrace{\dfrac{1}{p'}}_{\notin \mathbb{N}} + \underbrace{\dfrac{\sum\limits_{\mathbb{P}} p}{p'}}_{\in \mathbb{N}} \Rightarrow 1 + \sum\limits_{\mathbb{P}} p$ ist relativ prim zu jedem $p \in \mathbb{P} \Rightarrow$ Es gibt immer eine noch größere Primzahl.

Satz 2.4 (Primzahlsatz von DelaVallée-Poisson)

Die Anzahl der Primzahlen $p \leq x$ erfüllt

$$\pi(x)/\frac{x}{\ln x} \to 1 \text{ für } x \to \infty$$

Also gilt

$$\pi(x) \approx \frac{x}{\ln x} \text{ für große } x.$$

Zum Beispiel ist $\pi(1000000) \approx \frac{1000000}{13{,}8} \approx 72382$. Das heißt etwa 7% der ersten Million Zahlen sind Primzahlen.
Der Beweis des Primzahlsatzes benutzt Methoden der komplexen Analysis, insbesondere die Riemannsche Zetafunktion

$$\zeta(z) = \sum_{n=1}^{\infty} \frac{1}{n^2}, z = x + iy \in \mathbb{C}, x < 0.$$

Die Primzahlen p kommen so herein:

$$\zeta(z) = \prod_p \frac{1}{1-\frac{1}{n^2}} = \frac{1}{1-\frac{1}{2^2}} \cdot \frac{1}{1-\frac{1}{3^2}} \cdot \frac{1}{1-\frac{1}{5^2}} \cdot \frac{1}{1-\frac{1}{7^2}} \cdot \ldots$$

Diese Formel folgt leicht aus der eindeutigen Primfaktorzerlegung.

Vermutungen

Es gibt eine Anzahl berühmter mathematischer Vermutungen, die bisher trotz großer Anstrengungen noch nicht bewiesen, oder widerlegt werden konnten. Hier sind ein paar Beispiele:

(1). Riemannsche Vermutung: $\zeta(x+iy) \neq 0$ für $x > \frac{1}{2}$.

(2). Goldbachsche Vermutung: Jede gerade Zahl $n > 2$ kann als Summe $n = p + q$ zweier Primzahlen geschrieben werden.

(3). Primzahlzwillinge: Es gibt unendlich viele Primzahlen p, so dass auch $p+2$ eine Primzahl ist.

2.3 Kongruenzen

Definition: Kongruent modulo

Sei $m = 1, 2, \ldots$ gegeben. Die Zahlen $x, y \in \mathbb{Z}$ heißen kongruent modulo m [congruent modulo], geschrieben

(1). $x \equiv y \mod m$, wenn $m | x - y$ ist, d.h. wenn gilt

(2). $x = y + qm$ mit $q \in \mathbb{Z}$
Wenn $m \not| x - y$ ist, so heißen x und y inkongruent modulo m, geschrieben $x \not\equiv y \mod m$.
Beispiele:
$23 \equiv 3 \equiv -7 \equiv -17 \mod 10, 2 \not\equiv 11 \mod 10$
$255 \equiv -1 \equiv -257 \mod 256, 128 \not\equiv 0 \mod 256$

Satz 2.5

Modulo m gilt

(3). $x \equiv y, x' \equiv y' \Rightarrow x + x' \equiv y + y'$
$x \equiv y, x' \equiv y' \Rightarrow xx' \equiv yy'$

(4). $xz \equiv yz, ggT(z, m) = 1 \Rightarrow x \equiv y,$

(5). es gibt $\xi \in \mathbb{Z}$ mit $x\xi \equiv 1 \Leftrightarrow ggT(x, m) = 1$.
Beweis:

(a) Sei $x \equiv y$ und $x' \equiv y' \mod m$, also $x = y + qm, x' = y' + q'm$ mit $q, q' \in \mathbb{Z}$.
Dann ist zum Beispiel $xx' = (y + qm)(y' + q'm) = yy' + (yq' + y'q + qq'm)m \equiv yy' \mod m$.

(b) Aus $xz \equiv yz \mod m$ folgt $m | xz - yz = (x - y)z$.
Wenn m und z relativ prim sind, so folgt hieraus $m | x - y$ nach Satz 2.2. Also gilt $x \equiv y \mod m$.

(c) Die Kongruenz $x\xi \equiv 1 \mod m$ bedeutet

(6). $\xi x + qm = 1$ für ein $q \in \mathbb{Z}$
Hieraus folgt, dass x und m keinen gemeinsamen Teiler > 1 haben können. Umgekehrt hat (6) nach Satz 2.2 eine Lösung $\xi \in \mathbb{Z}$, wenn $ggT(x, m) = 1$ ist.
Beispiele:
$7\xi \equiv 1 \mod 10$ hat eine Lösung wegen $ggT(7, 10) = 1$
$5\xi \equiv 1 \mod 10$ hat keine Lösung wegen $ggT(5, 10) = 5 > 1$

Satz 2.6 (Chinesischer Restsatz)

Seien $m_1, \ldots, m_k$ relativ prim und seien $r_1, \ldots, r_k$ „Reste“ mit

(7). $0 \leq r_j < m_j$ für $j = 1, \ldots, k$.
Dann existiert genau ein $x \in \mathbb{N}$ mit $0 \leq x < m_1 \cdot \ldots \cdot m_k$, so dass gilt

(8). $x \equiv r_j \mod m_j$ für $j = 1, \ldots, k$.
Die Voraussewtzung, dass die Zahlen $m_1, \ldots, m_k$ relativ prim sind, ist wichtig. Dies heißt, dass in den Primfaktorzerlegungen dieser Zahlen keine Primzahl mehrfach vorkommt. So sind z.B. $24 = 2^3 \cdot 3, 25 = 5^2, 1001 = 7 \cdot 11 \cdot 13$ relativ prim. Das Bemerkenswerte ist, dass dieselbe Zahl x alle k Kongruenzen (8) erfüllt.
Beispiel: Sei $k = 2$ und $m_1 = 10, m_2 = 21$, weiter $r_1 = 1, r_2 = 15$. Die Lösung von $x \equiv 1 \mod 10, x \equiv 15 \mod 21$ mit $0 \leq x < 210$ ist $x = 141$.
Beweis:
(a) Wir benutzen eine nicht triviale Idee. Sei

(9). $n = m_1 \cdot \ldots \cdot m_k$.
Wir beobachten die Mengen

(10). $A = \{x \in \mathbb{N} : 0 \leq x < n\}$,

(11). $B = \{(r_1, \ldots, r_k) : 0 \leq r_j < m_j \text{ für } j = 1, \ldots, k\}$.
In unserem Beispiel $m_1 = 10, m_2 = 21$ ist
$A = \{0, 1, \ldots, 209\}$,
$B = \{(0, 0), \ldots, (0, 20), (1, 0), \ldots, (1, 20), \ldots, (9, 20)\}$.
Nach (9) gilt:

(12). $|A| = n = |B|$, das heißt A und B haben gleichviele Elemente.
(b) Nun definieren wir eine Abbildung $f : A \to B$ wie folgt: Sei $x \in A$ gegeben. Wir schreiben

(13). $x = q_j m_j + r_j$ mit $0 \leq r_j < m_j$ $(j = 1, \ldots, k)$
Dies definiert Zahlen $r_j \equiv x \mod m_j$. Nun setzen wir

(14). $f(x) = (r_1, \ldots, r_k)$.
In unserem Beispiel hat man $f(0) = (0, 0)$ und $f(24) = (4, 3)$.
(c) Als nächstes zeigen wir, dass f injektiv ist, d.h. $f(x) = f(y) \Rightarrow x = y$.
Sei also $f(x) = f(y)$. Nach (14) ist dann $f(x) = (r_1, \ldots, r_k)$ und auch $f(y) = (r_1, \ldots, r_k)$. Nach (13) ist daher

(15). $x \equiv r_j \equiv y \mod m_j$ für $j = 1, \ldots, k$.
Hieraus folgt $m_1 | x - y$, also $\frac{x-y}{m_1} \in \mathbb{Z}$. Aus (15) folgt weiter $m_2 | x - y = m_1 \frac{x-y}{m_1}$.
Da m_1 und m_2 relativ prim sind, erhält man aus Satz 2.2 $m_2 | \frac{x-y}{m_1}$, das heißt $\frac{x-y}{m_1 m_2} \in \mathbb{Z}$.
Nach (15) ist $m_3 | x - y = m_1 m_2 \frac{x-y}{m_1 m_2}$.
Da $m_1 m_2$ und m_3 relativ prim sind, folgert man $m_3 | \frac{x-y}{m_1 m_2}$.
Schließlich erhält man $m_k | \frac{x-y}{m_1 \cdot \ldots \cdot m_{k-1}}$, es ist also $n = m_1 \cdot \ldots \cdot m_k | x - y$. Aus $0 \leq x < n$ und

$0 \le y < n$ folgt $-n < x - y < n$.
Da n ein Teiler von $x - y$ ist , gilt $x - y = 0$, also $x = y$.
(d) Somit wissen wir:
(i) f ist eine injektive Abbildung von A nach B,
(ii) $|A| = |B|$.
Hieraus folgt, dass f eine bijektive Abbildung von A auf B ist. Zusätzlich gilt also $f(A) = B$. Damit haben wir: Zu jedem $(r_1, \dots, r_k) \in B$ gibt es genau ein $x \in A$ mit $f(x) = (r_1, \dots, r_k)$; dazu (14). Nach (13) gibt es also genau ein x mit $0 \le x < n$, das (8) erfüllt. Damit ist der Chinesische Restsatz bewiesen.

Beispiel: Es sei $x \equiv 2 \mod 5, x \equiv 4 \mod 7, x \equiv 3 \mod 9$. Wir stellen nun eine einfache Methode zur Berechnung von x vor:

Index	Reste a_i	$\mod n_i$	Produkte der anderen n_i N_i	Reste $N_i \mod n_i$	Multiplikatives Inverses von$N_i \mod n_i$ $Y_i : (Y_i \cdot N_i \equiv 1 \mod n_i)$
1	2	5	63	3	2
2	4	7	45	3	5
3	3	9	35	8	8

$x \equiv \sum_{i=1}^{k} a_i N_i Y_i \mod \prod_{i=1}^{k} n_i$
$x \equiv 2 \cdot 63 \cdot 2 + 4 \cdot 45 \cdot 5 + 3 \cdot 35 \cdot 8 = 1992 \equiv 102 \mod 315$

Eulersche Funktion

Die Eulersche Funktion $\varphi(n)$ ist für $n = 1, 2, \dots$ definiert durch

(16). $\varphi(n) = |\{x \in \mathbb{N} : 0 < x < n, ggT(x, n) = 1\}|$.
Das heißt $\varphi(n)$ ist die Anzahl der $x < n$, die zu n relativ prim sind. So gilt zum Beispiel $\varphi(6) = 2$ und $\varphi(8) = 4$. Allgemein ist

(17). $\varphi(p) = p - 1$ für p ist Primzahl

(18). $\varphi(p^v) = p^{v-1}(p - 1)$ für p ist Primzahl und $v = 1, 2, \dots$.

Aus dem folgenden Satz folgt z.B.: $\varphi(720) = \varphi(2^4 \cdot 3^2 \cdot 5) = 720(1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{5}) = 192$.

Satz 2.7

Wenn $m_1, \dots, m_k$ relativ prim sind, so gilt

(19). $\varphi(m_1 \cdot \dots \cdot m_k) = \varphi(m_1) \cdot \dots \cdot \varphi(m_k)$.
Mit der Primfaktorzerlegung $n = p_1^{v_1} \cdot \dots \cdot p_k^{v_k}, p_1, \dots, p_k$ Primzahlen, $v_1, \dots, v_k = 1, 2, \dots$ gilt

(20). $\varphi(n) = n(1 - \frac{1}{p_1}) \cdot \dots \cdot (1 - \frac{1}{p_k}) = \prod_{j=1}^{k} (p_j - 1) p_j^{v_j^{-1}}$.
Beweis: Sei $n = m_1 \cdot \dots \cdot m_k$. Dann gilt

(21). $ggT(x, n) = 1 \Leftrightarrow ggT(x, m_j) = 1$ für $j = 1, \dots, k$.
Die durch (14) definierte Funktion f bildet daher $A^* = \{x \in \mathbb{N} : 0 < x < n, ggT(x, n) = 1\}$ auf $B^* = \{(r_1, \dots, r_k) : 0 < r_j < m_j, ggT(r_j, m_j) = 1, j = 1, \dots, k\}$ ab. Da f injektiv ist folgt aus (16) $\varphi(n) = |A^*| = |f(A^*)| = |B^*| = \varphi(m_1) \cdot \dots \cdot \varphi(m_k)$.
Also gilt (19). Schließlich setzen wir $m_j = p_j^{v_j}$ und erhalten (20) aus (18).

2.4 Potenzreste

Sei $\varphi(m)$ wieder die Anzahl der $x < m$, die zu m relativ prim sind.

Satz 2.8 (kleiner Fermat)

Für $ggT(x, m) = 1$ gilt

(1). $x^{\varphi(m)} \equiv 1 \mod m$.
Beweis: Sei $n = \varphi(m)$ und seien $y_1, \dots, y_n$ die Zahlen $< m$, die zu m relativ prim sind. Es ist

(2). $xy_k = q_k m + r_k$ mit $q_k \in \mathbb{N}, 0 \leq r_k < m$ für $k = 1, \dots, m$. Die Reste r_k sind zu m teilerfremd, da x zu m und y_k zu m teilerfremd sind. Weiter gilt

(3). $r_j \neq r_k$ für $j \neq k$.
Denn angenommen $r_j = r_k$. Aus (2) folgt $xy_j - q_j m = r_j = r_k = xy_k - q_k m$, also $xy_j \equiv xy_k \mod m$. Wegen $ggT(x, m) = 1$ ist daher $y_j \equiv y_k$ nach Satz 2.5, woraus $j = k$ folgt. Somit gilt (3). Die n-Tupel $y_1, \dots, y_n$ bzw. $r_1, \dots, r_n$ stellen alle Zahlen $< m$ dar, die zu m relativ prim sind, sind also bis auf die Reihenfolge gleich. Daher ist $y_1 \cdot \ldots \cdot y_n = r_1 \cdot \ldots \cdot r_n$ und somit $x^n(y_1 \cdot \ldots \cdot y_n) = (xy_1) \cdot \ldots \cdot (xy_n) \equiv r_1 \cdot \ldots \cdot r_n = y_1 \cdot \ldots \cdot y_n \mod m$.
Da das Produkt $y_1 \cdot \ldots \cdot y_n$ ebenfalls zu m relativ prim ist, folgt aus Satz 2.2 $x^n \equiv 1 \mod m$.

Der wichtigste Spezialfall des „kleinen Fermat“ ist, dass m eine Primzahl p ist. Dann gilt $\varphi(p) = p-1$ und $ggT(x, p) = 1$ für $1 < x < p$.
Aus Satz 2.8 erhält man daher den ersten Teil des folgenden Satzes. Den zweiten Teil beweisen wir nicht.

Satz 2.9

Sei p eine Primzahl und $0 < x < p$. Dann ist

(4). $x^{p-1} \equiv 1 \mod p$
Weiter existiert a mit $0 < a < p$ und

(5). $a^k \not\equiv 1 \mod p$ für $0 < k < p - 1$.

Beispiel: Sei $p = 7$. Dann gilt $\mod 7$
$3^1 = 3, 3^2 = 9 \equiv 2, 3^3 \equiv 6, 3^4 \equiv 4, 3^5 \equiv 5, 3^6 \equiv 1$, aber
$2^1 = 2, 2^2 = 4, 2^3 \equiv 1, 2^4 \equiv 2, 2^5 \equiv 4, 2^6 \equiv 1$.
Daher wird (5) für $a = 3$ erfüllt, nicht aber für $a = 2$.

Satz 2.10

Sei p eine Primzahl und a erfülle (5). Zu $x \in \mathbb{N}$ mit $0 < x < p$ gibt es dann genau ein i mit $1 \leq i \leq p-1$, so dass gilt

(6). $x \equiv a \mod p$.
Beweis: Zuerst zeigen wir

(7). $a^i \not\equiv a^j \mod p$ für $1 < i < j \leq p - 1$
Aus $a^i \equiv a^j$ folgt nämlich $a^{j-i} \equiv 1$. Da $0 < j - i < p - 1$ ist, erhalten wir einen Widerspruch zu (5).
Daher sind die $p - 1$ Zahlen $a^i, 1 \leq i \leq p - 1$ untereinander inkongruent ($\mod p$). Die $p - 1$ Zahlen x mit $1 \leq x < p - 1$ sind auch untereinander inkongruent $\mod p$. Also gibt es zu jedem $1 \leq x \leq p - 1$ ein i mit $a^i \equiv x \mod p$.

Probabilistischer Primzahlsatz von Rabin

Der probabilistische Primzahlsatz von Rabien dient zum Auffinden großer Primzahlen. Sei $m = 3, 5, 7, ...$ Damm ist

(8). $m - 1 = 2^n q, n \geq 1, q$ ungerade
Beispiel: für $m = 49$ ist $m - 1 = 48 = 2^4 \cdot 3$, also $n = 4, q = 3$.
Seien

(9). $A(m) = \{x \in \mathbb{N} : 0 < x < m, ggT(x, m) = 1\}$,

(10). $B(m) = \{x \in A(m) : \begin{cases} x^q \equiv 1 \mod m \text{ oder} \\ x^{2^k q} \equiv -1 \mod m \text{ mit } k < n \end{cases} \}$

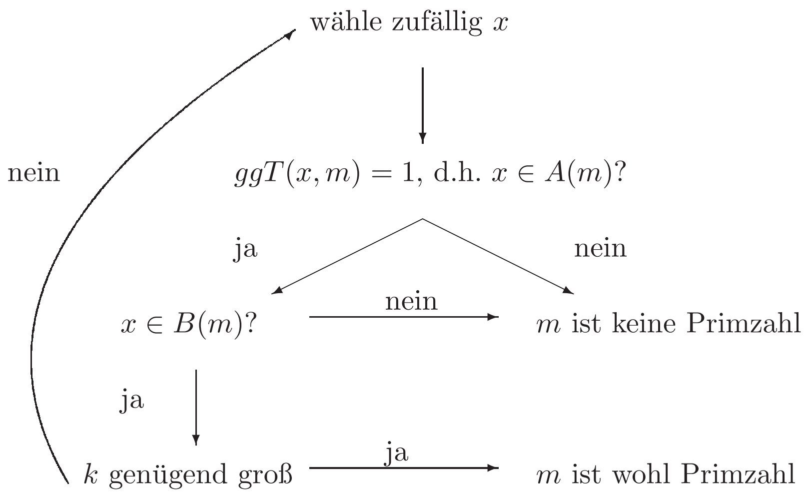
Satz 2.11

Sei $m > 1$ und $2 \not| m, 2 \not| m$. Dann gilt

(11). m Primzahl $\Rightarrow B(m) = A(m)$,

(12). m keine Primzahl $\Rightarrow |B(m)| \leq \frac{1}{4}|A(m)|$.

Beweis: von (11) für den Fall $n = 3$ in (8). Es ist also $m = 1+8q, q$ ungerade. Sei nun m eine Primzahl. Aus (10) folgt sofort $B(m) \subset A(m)$. Wir müssen daher $A(m) \subset B(m)$ zeigen. Dazu sei $x \in A(m)$. Wir setzen $z = x^9$. Dann ist $z^8 = x^{8q} = x^{m-1} \equiv 1 \mod m$ nach dem kleinen Fermat. Aus der binomischen Formel folgt $(z-1)(z+1)(z^2+1)(z^4+1) = z^8 - 1 \equiv 0 \mod m$. Da m eine Primzahl ist, erhalten wir aus Satz 2.5, dass einer der Faktoren $\equiv 0$ ist, das heißt, dass gilt $2^9 \equiv 1$ oder $x^9 \equiv -1$ oder $x^{2q} \equiv -1$ oder $x^{4q} \equiv -1 \mod m$. Somit ist $x \in B(m)$ nach Definition (10) mit $n = 3$.
Die Methode von Rabin ist die folgende: Sei $m > 1$, und nicht durch 2 oder 3 teilbar. Dieses m ist ein „Kandidat" für eine Primzahl. Nun wählen wir zufällig $x \in \mathbb{N}$ mit $1 < x < m$. Wenn $ggT(x, m) > 1$ ist, so ist m keine Primzahl. Sonst ist $x \in A(m)$. Nun berechnen wir $z = x^1, z^2, z^4, \ldots, z^{2^n} \mod m$. Falls $z \not\equiv \pm 1, z^2 \not\equiv -1, \ldots, z^{2^n} \not\equiv -1$ ist, so ist $x \notin B(m)$, nach (11) kann also m keine Primzahl sein. Im anderen Fall ist $x \in B(m)$. Dann bleibt m ein Kandidat für eine Primzahl. Aus (12) folgt für den Fall, dass m eine Primzahl ist: $P(x \in B(m)) = \frac{|B(m)|}{|A(m)|} \leq \frac{1}{4}$, wobei $P(\ldots) =$ Wahrscheinlichkeit von ... bedeuten soll.
Nun wählen wir k Zahlen $x_1, \ldots, x_k$ unabhängig voneinander aus. Wir erhalten, falls m keine Primzahl ist:
$P(\text{Algorithmus hat } m \text{ nach } k \text{ Versuchen noch nicht verworfen}) = P(x_1 \in B(m), \ldots, x_k \in B(m)) \leq \frac{1}{4^k}$
Für große k ist es daher außerordentlich wahrscheinlich, dass ein Kandidat m in einem der k Tests durchfällt, falls er keine Primzahl ist.



2.5 Kryptografie

Einführende Worte

Es geht darum, die Zahlentheorie auf die Kryptografie anzuwenden und etwas zu Methoden der Geheimhaltung von Daten durch Verschlüsselung zu sagen.
Als einführendes Beispiel betrachten wir den Text „Cafe de Guatemala“. Dieser Text soll im 8-Bit ASCII Forat vorliegen. Wir benutzen Blöcke von 32 bits, also jeweils 4Charaktere. Der letzte Block wird mit Null als „padding“ aufgefüllt.

$$|\underbrace{01000011}_{C}\underbrace{01100001}_{a}\underbrace{01100110}_{f}\underbrace{01100101}_{e}|\underbrace{00100000}_{Leer}\ldots\underbrace{01101100}_{l}|\underbrace{01100001}_{a}\underbrace{00000000}_{f\ddot{u}llen}\underbrace{00000000}_{f\ddot{u}llen}\underbrace{00000000}_{f\ddot{u}llen}|$$

exclusive-or

Wir betrachten zunächst ein sehr einfaches Verfahren zur Kodierung und Dekodierung. Die Operation „exclusive-or“ ist bitweise definiert durch: $0 \oplus 0 = 0, 0 \oplus 1 = 1, 1 \oplus 0 = 1, 1 \oplus 1 = 0$.
Für jeden Block wird ein geheimer Schlüssel verwandt.

Originalblock		01000011	01100001	01100110	01100101
geheimer Schlüssel	$\oplus$	10010101	11111000	01100000	10110100
kodierter Block		11010110	10011001	00000110	11010001
geheimer Schlüssel	$\oplus$	10010101	11111000	01100000	10110100
dekodierter Block		01000011	01100001	01100110	01100101

Diese Methode eignet sich nur für kurze Nachrichten. Außerdem muss der Codierer den Schlüssel kennen.

RSA-Algorithmus

Nun beschreiben wir den RSA-Algorithmus (genannt nach Rivest-Shamir-Adleman), der wesentlich aufwendiger ist. Er ist aber deutlich sicherer und hat andere zusätzliche Vorteile.
Seien p und q zwei sehr große Primzahlen. Wir setzen

(1). $m = pq$.
Wir wählen $e \in \mathbb{N}$ mit

(2). e relativ prim zu $\varphi(m) = (p-1)(q-1)$;
dazu Satz 2.7. Nach Satz 2.5 existiert d mit

(3). $ed \equiv 1 \mod (p-1)(q-1)$.
Die Bitblöcke interpretieren wir als Zahlen. Der Block "Cafe" ist also $2^{30} + 2^{25} + 2^{24} + 2^{22} + \ldots + 2^2 + 1$.
Sei x der Originalblock mit $0 \leq x < m$ und $x \neq p, q$. Der kodierte Block wird durch

(4). $y \equiv x^e \mod m, 0 \leq y < m$ definiert.
Wir beweisen anschließend

(5). $x \equiv y^d \mod m, 0 \leq x < m$,
d.h. man erhält den Originalblock zurück.
Zum Nachweis von (5) setzen wir $z \equiv y^d \mod m$ mit $0 \leq z < m$. Zu zeigen ist also $z = x$. Nach (3) ist $ed = 1 + n(p-1)(q-1)$. Wenn $x \neq 0, p, q$ ist, so sind x und $m = pq$ teilfremd, aus dem kleinen Fermat folgt also $x^{p-1)(q-1)} = x^{\varphi(m)} \equiv 1 \mod m$.
Nach (3) ist $ed = 1 + n(p-1)(q-1)$ mit $n \in \mathbb{N}$. Also ist nach (4)

(6). $z \equiv y^d \equiv x^{ed} = x(x^{(p-1)(q-1)})^n \equiv x \mod m$.
Da es nur ein z mit $x \equiv z \mod m$ und $0 \leq x < m, 0 \leq z < m$ gibt, folgt $z = x$.

Nun beschreiben wir das RSA-Kryptiersystem aus Sicht der Benutzer.
Die beiden Primzahlen p und q sind stremg geheim, aber $m = pq$ ist öffentlich bekannt. Ein eingetragener Benutzer A erhält zwei Zahlen

- den öffentlichen Schlüssel e, dazu (2),
- den geheimen Schlüssel d, dazu (3).

Nehmen wir nun an, das ein anderer Benutzer B eine Nachricht an A senden will. er benutzt den öffentlichen Schlüssel e von A zur Kodierung gemäß (4). Nach Eintreffen der Nachricht bei A benutzt dieser seinen geheimen Schlüssel d zur Dekodierung gemäß (5).
Es ist außerordentlich wichtig, dass die Primzahlen p und q geheim bleiben. Wenn man p und q kennt, so kennt man auch $(p-1)(q-1) = m - p - q + 1$, kann also d aus (3) berechnen. Alles beruht darauf, dass es (noch) keinen effizienten Algorithmus zur Faktorisierung großer Zahlen gibt. Man beachte, dass ja m öffentlich ist.
Als Beispiel betrachten wir Blöcke von 100 Charakteren zu 8 Bit, also Blöcke von 800 Bits. Diese Blöcke entsprechen Zahlen x mit $0 \leq x < 2^{800}$.
Daher muss $m \geq 2^{800} = (2^{10})^{80} \approx (10^3)^{80} = 10^{240}$ sein. Zuerst suchen wir zwei Primzahlen p und q mit $2^{400} < p < 2^{400,5}, 2^{400} < q < 2^{400,5}$. Dann ist $2^{800} < m = pq < 2^{801}$.
Die kodierte Nachricht benutzt also Blöcke von 801 Bits, um alle Zahlen $< m$ verpacken zu können.
In umgekehrter Reihenfolge geht z.B. die „elektronische Unterschrift". Der Benutzer A kodiert seinen Namen nach (5) mit dem geheimen Schlüssel d. Nun dekodiert der Empfänger B dies nach (4) mit dem öffentlichen Schlüssel e. Wenn der Name von A erscheint, so stammt die Nachricht wirklich von A, denn nur A kannte ja die Zahl d.
Welch Optimismus!

Kapitel 3

Algebra

3.1 Ringe und Körper

Ring

Ein Ring ist eine Menge $\mathcal{R}$ mit einer Addition und Multiplikation. Die Addidtion ist eine Abbildung

(1). $x, y \in \mathcal{R} \mapsto x + y \in \mathcal{R}$,
und die Multiplikation eine Abbildung

(2). $x, y \in \mathcal{R} \mapsto xy \in \mathcal{R}$.
Bezüglich der Addition verlangen wir

(3). $(x + y) + z = x + (y + z)$ für $x, y, z \in \mathcal{R}$

(4). $x + y = y + x$ für $x, y \in \mathcal{R}$

(5). es gibt $0 \in \mathcal{R}$, so dass $x + 0 = x$ für alle $x \in \mathcal{R}$ gilt,

(6). zu jedem $x \in \mathcal{R}$ gibt es $-x \in \mathcal{R}$ mit $x + (-x) = 0$.
Bezüglich der Multiplikation verlangen wir nur

(7). $x(yz) = (xy)z$ für $x, y, z \in \mathcal{R}$
Schließlich soll noch

(8). $(x + y)z = xz + yz$
$z(x + y) = zx + zy$ für $x, y, z \in \mathcal{R}$ gelten.
Der Ring $\mathcal{R}$ heißt kommutativ [commutative] , wenn

(9). $xy = yx$ für $x, y \in \mathcal{R}$ gilt.
Wir sagen, dass $\mathcal{R}$ eine Eins [unity] hat, wenn gilt

(10). es gibt $1 \in \mathcal{R}$ mit $x1 = 1x = x$ für $x \in \mathcal{R}$.

Körper

Der Ring $\mathcal{K}$ heißt Körper [field], wenn $\mathcal{K}$ kommutativ ist, eine Eins mit $0 \neq 1$ hat und gilt

(11). (a) zu $x \in \mathcal{K}, x \neq 0$ existiert $x^{-1} \in \mathcal{K}$ mit $xx^{-1} = 1$.
(b) zu $x, y \in \mathcal{K} \setminus \{0\}$ gilt $xy \in \mathcal{K} \setminus \{0\}$

In einem Ring $\mathcal{R}$ definiert man die Subtraktion durch

(12). $x - y = x + (-y)$ für $x, y \in \mathcal{R}$.
In einem Körper $\mathcal{K}$ definiert man die Subtraktion durch

(13). $\frac{x}{y} = xy^{-1}$ für $x, y \in \mathcal{K}, y \neq 0$.

Beispiel 1

Die Menge $\mathbb{Z}$ aller ganzen Zahlen mit der üblichen Addition und Multiplikation bildet einen kommutativen Ring mit Eins. Dagegen ist $\mathbb{N}$ kein Ring, da (6) nicht gilt.

Beispiel 2

Die folgenden Mengen (mit der üblichen Addition und Multiplikation) sind Körper:

- $\mathcal{R} = \{\frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0\}$ (rationale Zahlen)
- $\mathbb{R}$ (reelle Zahlen)
- $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}, i^2 = 1$ (komplexe Zahlen).

Beispiel 3

Sei $n > 1$. Die quadratischen Matrizen mit n Reihen und z.B. reellen Elementen bilden einen nichtkommutativen Ring mit Eins, nämlich der Einheitsmatrix.
Die meisten algebraischen Eigenschaften von Zahlen gelten auch in allgemeinen Körpern oder auch schon in Ringen. Als Beispiel dazu soll nur eine Eigenschaft bewiesen werden.

Satz 3.1

Sei $\mathcal{R}$ ein Ring. Dann ist $x0 = 0x = 0$ für $x \in \mathcal{R}$.
Beweis: Sei $x \in \mathcal{R}$. Wir setzen $z = x0$ und müssen zeigen, dass $z = 0$ ist. Es gilt $0 = 0 + 0$ nach (5), $z = x0 = x(0 + 0) = x0 + x0 = z + z$ nach (8), $z + (-z) = (z + z) + (-z) = z + (z + (-z))$ nach (6), $= z + 0 = z$ nach (6) und (5).
Also ist $z = z + (-z) = 0$ nach (6). Ähnlich zeigt man $0x = 0$.

Beispiel 4

Jeder Körper hat mindestens zwei Elemente, nämlich 0 und 1. Aber mehr Elemente braucht es nicht zu geben.
Sei $\mathcal{K} = \{0, 1\}$. Damit $\mathcal{K}$ ein Körper ist, muss nach (5) gelten: $0 + 0 = 0, 1 + 0 = 1, 0 + 1 = 1$
Es fehlt noch $1 + 1$. Wir definieren $1 + 1 = 0$, d.h. $-1 = 1$.
Aus (10) und Satz 3.1 folgt $0 \cdot 0 = 0, 0 \cdot 1 = 0, 1 \cdot 0 = 0, 1 \cdot 1 {=} 1$.
Man könnte nun verifizieren, dass dies wirklich einen Körper gibt. Dieser kleinste alle Körper wird im folgenden sehr oft vorkommen. Wenn man 0 und 1 als Bits interpretiert, so ist Addition=“exclusive or“, Multiplikation=“and“. Dieser Körper hat viele merkwürdige Eigenschaften, z.B. $-x = x$ für alle x.

Unterring

Sei $\mathcal{R}$ ein Ring. Ein Unterring [subring] von $\mathcal{R}$ ist eine Menge $\varnothing \neq \mathcal{R}' \subseteq \mathcal{R}$ mit

(14). $x, y \in \mathcal{R}' \Rightarrow x \pm y \in \mathcal{R}', xy \in \mathcal{R}'$.

Es ist wichtig, dass $x \pm y$ und xy zu $\mathcal{R}'$ gehören und nicht nur zu $\mathcal{R}$, was ja trivial wäre. Man kann nachweisen, dass $\mathcal{R}'$ die Ringeigenschaften (3) bis (8) erfüllt.

Unterkörper

Nun sei $\mathcal{K}$ ein Körper. Ein Unterkörper [subfield] von $\mathcal{K}$ ist eine Menge $\mathcal{K}' \subset \mathcal{K}$ mit

(15). $x, y \in \mathcal{K}' \Rightarrow x \pm y \in \mathcal{K}', xy \in \mathcal{K}'$,

(16). $x \in \mathcal{K}', x \neq 0 \Rightarrow x^{-1} \in \mathcal{K}'$.

Man kann zeigen, dass $\mathcal{K}'$ die Körpereigenschaften (3) bis (11) erfüllt.

Beispiel 5

Wir definieren $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ und zeigen, dass dies ein Unterkörper von $\mathbb{R}$ ist. Seien $x_1, x_2 \in \mathbb{Q}$, also $x_j = a_j + b_j\sqrt{2}$ mit $a_j, b_j \in \mathbb{Q}, j = 1, 2$
Es folgt $x_1 \pm x_2 = (a_1 \pm a_2) + (b_1 \pm b_2)\sqrt{2} \in \mathbb{Q}(sqrt2)$,
$x_1x_2 = (a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) = (a_1a_2 + 2b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{2} \in \mathbb{Q}(\sqrt{2})$.
Also git (15). Nun sei $x = a + b\sqrt{2} \neq 0$. Dann ist $\frac{1}{x} = \frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{(a+b\sqrt{2})(a-b\sqrt{2})} = \frac{a-b\sqrt{2}}{a^2-2b^2}$; man beachte, dass $a^2 - 2b^2 \neq 0$ ist, da $\sqrt{2}$ nicht rational ist.
Somit ist $x^{-1} = a^* + b^*\sqrt{2}$ mit $a^* = \frac{a}{a^2-2b^2} \in \mathbb{Q}, b^* = \frac{-b}{a^2-2b^2} \in \mathbb{Q}$. Also ist $x^{-1} \in \mathbb{Q}(\sqrt{2})$, so dass auch (16) gilt.

3.2 Restklassenringe

Sei $m = 2, 3, \ldots$ fest gewählt. Alle Kongruenzen sollen modulo m sein. Ein Rest modulo m ist eine ganze Zahl r mit

(1). $0 \leq r < m$

Die Restklassen modulo m sind $\bar{r} = \{x \in \mathbb{Z} : x \equiv r \mod m\} = \{qm + r : q \in \mathbb{Z}$. Es gibt also genau m Restklassen modulo m.

Für $m = 10$ ist z.B. $\bar{0} = \{0, \pm 10, \pm 20, \ldots\}, \bar{3} = \{3, 13, 23, \ldots, -7, -17, \ldots\}$.
Wir werden aber direkt mit den Resten rechnen, da dies vielleicht einfacher verständlich ist.
Seien r und s Reste, also auch $0 \leq s < m$. Dann ist

(2). $r + s \equiv x \mod m$ mit $0 \leq x < m$,

(3). $rs \equiv y \mod m$ mit $0 \leq y < m$.

Wir definieren x und y als die Summe bzw. das Produkt modulo m.

Beispiel 1:

Sei $m = 10$. Dann ist
$7 + 5 = 12 \equiv 2$, also Summe=2
$7 \cdot 5 = 35 \equiv 5$, also Produkt=5

Satz 3.2

Mit der Addition und Multiplikation modulo m ist

(4). $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$ ein kommutativer Ring mit Eins.

Beweis: Nach (2) und (3) ist es klar, dass Summe und Produkt wieder in $\mathbb{Z}_m$ liegen.
Wir wollen nur eine der Ringeigenschaften nachweisen. Zum Nachweis von (6) sei ein Rest r gegeben. Wenn $r = 0$ ist, setzen wir $-r \equiv 0$; wenn $0 < r < m$ ist, so ist $0 < m - r < m$. Deshalb setzen wir $-r \equiv m - r \mod m$.
Es gilt $r + (-r) \equiv r + (m - r) = m \equiv 0$, also $r + (m - r) = 0$ in $\mathbb{Z}_m$. Die Kommutativität ist klar, da $rs = sr$ ist. Die Eins von $\mathbb{Z}_m$ ist 1, da ja $r1 = r$ ist.

Satz 3.3

Der Ring $\mathbb{Z}_m$ ist genau dann ein Körper, wenn m eine Primzahl ist.
Beweis:

(1). Sei m eine Primzahl und sei $r \neq 0$, also $0 < r < m$. Dann ist r zu m teilerfremd. Nach Satz 2.5 gibt es also s mit $rs \equiv 1 \mod m$. Es sei $s \equiv t \mod m$ mit $0 < t < m$. Also ist $t \in \mathbb{Z}_m$ und es gilt $rt \equiv 1$.

(2). Nun nehmen wir an, dass m keine Primzahl ist. Dann ist $m = rq$ mit $1 < r < m, 1 < q < m$. Also ist $ggT(r, m) = r > 1$. Nach Satz 2.5 gibt es also kein t mit $rt \equiv 1 \mod m$.

Beispiel 2

Den Körper $\mathbb{Z}_2 = \{0, 1\}$ kennen wir bereits. Die merkwürdige Definition $1 + 1 = 0$ wird jetzt klar, da ja $1 + 1 = 2 \equiv 0 \mod 2$ ist.

Beispiel 3

Im Körper $\mathbb{Z}_3 = \{0, 1, 2\}$ gilt:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Beispiel 4

Im Ring $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ hat man

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Man sieht, dass 2 kein Reziprokes hat; $\mathbb{Z}_4$ ist ja auch kein Körper.

Beispiel 5

Sei $m = 2^{16} = 65536$ wie in einem 16-Bit-Computer. Es ist $\mathbb{Z}_m = \{0, 1, \ldots, 2^{16} - 1\} = \{0, 1, \ldots, 65535\}$.
So hat man z.B. $-2 \equiv 2^{16} - 2 = 65534$,
$2000 \cdot 33 \equiv 464$, d.h. $2000 \cdot 33 = 464$ in $\mathbb{Z}_m$.
$40000 + 30000 \equiv 4464$, d.h. $40000 + 30000 = 4464$ in $\mathbb{Z}_m$.
Schließlich formulieren wir Satz 2.10 für $\mathbb{Z}_p$.

Satz 3.4

Sei p eine Primzahl. Für $r \in \mathbb{Z}_p, r \neq 0$ gilt $r^{p-1} = 1$ in $\mathbb{Z}_p$ und es gibt $a \in \mathbb{Z}_p$ mit $\mathbb{Z}_p = \{0\} \cup \{a : 1 \leq i \leq p-1\}$.

3.3 Polynome

Definitionen

Sei $\mathcal{K}$ ein Körper und sei x ein zusätzliches Symbol. Dieses x ist weder ein Körperelement, noch eine Variable. Wir definieren $x^0 = 1 \in \mathcal{K}, x^1 = x, \ldots x^n = x \cdots x$.
Ein Polynom mit Koeffizienten in $\mathcal{K}$ (oder über $\mathcal{K}$) ist ein formaler Ausdruck der Form

(1). $f(x) = a_0 + a_1 x + \ldots + a_m x^m, m = 0, 1, 2, \ldots$.
Die Koeffizienten $a_0, a_1, \ldots, a_m$ sind Elemente des Körpers $\mathcal{K}$. Man hat zwei Fälle:

(a) Alle Koeffizienten sind $= 0$: Dann ist f das Nullpolynom, geschrieben 0. Wir Wir definieren den Grad $grad\ 0 = -\infty$.

(b) Es gibt mindestens einen Koeffizienten $\neq 0$: Dann können wir

(2). $f(x) = a_0 + a_1 x + \ldots + a_m x^m$ mit $a_m \neq 0$ schreiben. Der Grad [degree] von f ist definiert durch $grad\ f = m$.
Sei nun $g(x) = b_0 + b_1 x + \ldots + b_n x^n$ ein weiteres Polynom. Wir definieren

(3). $f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \ldots$

(4). $f(x)g(x) = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + (a_0 b_2 + a_1 b_1 + a_2 b_0)x^2 + \ldots + a_m b_n x^{m+n}$.
Also ist

(5). $grad(f+g) \leq max(grad\ f, grad\ g)$,

(6). $grad(fg) = grad\ f + grad\ g$;
Dies gilt auch für Nullpolynome.

Beispiel 1

Sei $\mathcal{K} = \mathbb{R}$. Wir betrachten die Polynome
$f(x) = 1 + 2x - 8x^2 + x^3$ mit $grad\ f = 3$,
$g(x) = 3 + 5x^2$ mit $grad\ g = 2$.
Wir könneten auch $g(x) = 3 + 0x + 5x^2 + 0x^3$ schreiben. Also ist $f(x) + g(x) = 4 + 2x - 3x^2 + x^3$ und $f(x)g(x) = (1 + 2x - 8x^2 + x^3)(3 + 5x^2) = 3 + 6x + 19x^2 + 13x^3 - 40x^4 + 5x^5$.

Beispiel 2

Sei $\mathcal{K} = \mathbb{Z}_2 = \{0, 1\}$. Wir betrachten
$f(x) = 1 + x + x^3 + x^5$ mit $grad\ f = 5$,
$g(x) = x + x^2 + x^4$ mit $grad\ g = 4$.
Wir erhalten $f(x) + g(x) = 1 + (1+1)x + x^2 + x^3 + x^4 + x^5 = 1 + x^2 + x^3 + x^4 + x^5$, da ja $1 + 1 = 0$ in $\mathbb{Z}_2$ ist. Weiter ist
$f(x)g(x) = (1 + x + x^3 + x^5)(x + x^2 + x^4) = x + x^3 + x^6 + x^9$.

Satz 3.5

Die Polynome mit Koeffizienten in $\mathcal{K}$ bilden einen kommutativen Ring mit Eins, den Polynomring $\mathcal{K}[x]$ über $\mathcal{K}$.
Zum Beispiel ist $x^3 + \frac{7}{8}x - \frac{1}{6} \in \mathbb{Q}[x]$
$x^2 + 6x + \sqrt{3} \in \mathbb{R}[x]$, aber $\notin \mathbb{Q}[x]$.
Dieser Satz ist leicht zu beweisen. Die Eins ist das Polynom 1 des Grades 0.

Satz 3.6

Seien $f, g \in \mathcal{K}[x]$ und $f \neq 0$, d.h. f ist nicht das Nullpolynom. Dann gilt:

(7). $g = qf + r$ mit $q, r \in \mathcal{K}[x], grad\ r < grad\ f$.
Der Beweis beruht auf bekanntem Divisionsalgorithmus für Polynome, den wir nur für Beispiele vorführen.

Beispiel 3

Sei $\mathcal{K} = \mathbb{Q}$ und $f(x) = x^2 - 2$. Sei $g_1(x) = 4x$. Dann ist bereits $grad\ g_1 < grad\ f$, also $q_1 = 0, r_1 = g_1$ in (7). Nun sei $g_2(x) = 3x^4 + 7x^3 + 1$. Es ist

$$\begin{array}{ccccccl}
 & 3x^4 & +7x^3 & & & +1 & 3x^2+7x+6\text{(Quotient)} \\
- & 3x^4 & & -6x^2 & & & \\
\hline
 & & 7x^3 & +6x^2 & & +1 & \\
- & & 7x^3 & & -14x & & \\
\hline
 & & & 6x^2 & +14x & +1 & \\
- & & & 6x^2 & & -12 & \\
\hline
 & & & & 14x & +13\text{(Rest)} &
\end{array}$$

Also ist $\underbrace{3x^4 + 7x^3 + 1}_{g_2} = \underbrace{(3x^2 + 7x + 6)}_{q_2}\underbrace{(x^2 - 2)}_{f}\underbrace{(14x + 13)}_{r_2}$

Beispiel 4

Sei $\mathcal{K} = \mathbb{Z}_2 = \{0, 1\}$ und $f(x) = x^3 + x^2 + 1, g(x) = x^4 + x^2 + x$. Man hat

$$\begin{array}{ccccccl}
 & x^4 & & +x^2 & +x & & x+1\text{(Quotient)} \\
- & x^4 & +x^3 & & +x & & \\
\hline
 & & x^3 & +x^2 & & & \\
- & & x^3 & +x^2 & & +1 & \\
\hline
 & & & & & 1\text{(Rest)} &
\end{array}$$

Also ist $x^4 + x^2 + x = (x + 1)(x^3 + x^2 + 1) + 1$

Euklidischer Algorithmus

Nun beschreiben wir den euklidischen Algorithmus für Polynome. Seien $f, g \in \mathcal{K}[x], f \neq 0, grad\ g \geq grad\ f$. Wir setzen

(8). $f_0 = g, f_1 = f$. Mit dem Divisionsalgorithmus aus Satz 3.6 erhalten wir

(9). $f_0 = q_1 f_1 + f_2$ mit $grad\ f_2 < grad\ f_1$,
$f_1 = q_2 f_2 + f_3$ mit $grad\ f_3 < grad\ f_2$,
...
Der euklidische Algorithmus bricht ab, wenn $f_{k+1} = 0$ ist, d.h. zum Schluss erhlt man als Ergebnis f_k mit

(10). $f_{k-1} = q_k f_k, f_k \neq 0$.

Beispiel 5

Sei $\mathcal{K} = \mathbb{Z}_2$ und
$f_0(x) = g(x) = x^4 + x^2 + x + 1$,
$f_1(x) = f(x) = x^3 + x^2 + x$.
Dann ist

$$\begin{array}{lll} f_0(x) & = (x+1)f_1(x) + (x^2+1) & , f_2(x) = x^2+1 \\ f_1(x) & = (x+1)f_2(x) + 1 & , f_3(x) = 1 \\ f_2(x) & = (x^2+1)f_3(x) & , f_4(x) = 0 \end{array}$$

Also ist $k = 3, f_k(x) = 1$.
Wir sagen, dass f ein Teiler [divisor] von g ist, wenn $r = 0$ in Satz 3.6 gilt, d.h. wenn gilt $g = qf$ mit $q \in \mathcal{K}[x]$.

Beispiel 6

Sei $\mathcal{K} = \mathbb{Q}$. Wegen $x^4 + 3x^3 - 2x^2 - 6x = (x^2 + 3x)(x^2 - 2)$ ist $x^2 - 2$ ein Teiler von $x^4 + 3x^3 - 2x^2 - 6x$. Wegen $7x^3 + x^2 - 14x = (7x + 1)(x^2 - 2) + 2$ ist aber $x^2 - 2$ kein Teiler von $7x^3 + x^2 - 14x$.

Satz 3.7 (entspricht Satz 2.1)

Seien $f, g \in \mathcal{K}[x], f \neq 0, grad\ g \geq grad\ f$. Sei f_k das Ergebnis des euklidischen Algorithmus; dazu (10). Dann gilt:

(i). f_k ist Teiler von f und von g;

(ii). wenn das Polynom h ein Teiler von f und g ist, so ist h ein Teiler von f_k;

(iii). es gibt Polynome φ und ψ mit $f_k = \varphi f + \psi g$.

Nach (i) und (ii) ist also f_k der größte gemeinsame Teiler von f und g.
Im Beispiel 5 ist $f_k = 1$, d.h. f und g haben „keinen“ gemeinsamen Teiler.

3.4 Irreduzible Polynome

Die Irreduziblen Polynome entsprechen den Primzahlen. Zuerst definieren wir das Gegenteil, nämlich reduzibel.

Definitionen

Sei $\mathcal{K}$ ein Körper. Das Polynom $f \in \mathcal{K}[x]$ mit $grad(f) \geq 1$ heißt reduzibel, wenn es eine Zerlegung

(1). $f = gh$ mit $g, h \in \mathcal{K}[x], 0 < grad(g) < grad(f)$ gibt. Für die Frage der Reduzibilität kann man annehmen, dass f der höchste Koeffizient $= 1$ ist. Ein Polynom der Form $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$ mit $a_0, \ldots, a_{n-1} \in \mathcal{K}$ ist also genau dann reduzibel, wenn man

(2). $f(x) = (x^j + b_{j-1}x^{j-1} + \ldots + b_0)(x^k + c_{k-1}x^{k-1} + \ldots + c_0)$ mit $0 < j < n, 0 < k < n$ und $b_0, \ldots, b_{j-1}, c_0, \ldots, c_{k-1} \in \mathcal{K}$ schreiben kann; es ist sehr wichtig, dass die Koeffizienten in $\mathcal{K}$ liegen.
Das Polynom f heißt irreduzibel, wenn es nicht reduzibel ist, wenn es also keine Zerlegung (1) gibt.

Beispiel 1

Sei $\mathcal{K} = \mathbb{Q}$.

(1). Das Polynom $x^2 - 4$ ist reduzibel wegen $x^2 - 4 = (x-2)(x+2)$ und $\pm 2 \in \mathbb{Q}$.

(2). Das Polynom $x^2 - 2$ ist irreduzibel. Nehmen wir an, dass $x^2 - 2$ reduzibel ist. Nach (2) ist dann $x^2 - 2 = (x + b_0)(x - c_0) = x^2 + (b_0 + c_0)x + b_0 c_0$ mit $b_0, c_0 \in \mathbb{Q}$. Also gilt $b_0 + c_0 = 0$ und $b_0 c_0 = -2$. Es folgt $b_0^2 = 2, b_0 = \pm\sqrt{2} \notin \mathbb{Q}$, und das ist ein Widerspruch.

Beispiel 2

Sei $\mathcal{K} = \mathbb{Z}_2$.

(1). Das Polynom $x^2 + 1$ ist reduzibel wegen $x^2 + 1 = (x+1)(x-1)$.

(2). Das Polynom $f(x) = x^3 + x + 1$ ist irreduzibel. Angenommen dass f reduzibel ist. In (2) gilt $j + k = 3, 0 < j < 3$, also $j = 1$ und $k = 2$ (oder umgekehrt). Daher hat man $x^3 + x + 1 = (x + b_0)(x^2 + c_1 x + c_0) = x^3 + (b_0 + c_1)x^2 + (b_0 c_1 + c_0)x + b_0 c_0$.
Also gilt $b_0 + c_1 = 1, b_0 c_1 + c_0 = 0$ und $b_0 c_0 = 1$. Wegen $b_0, c_0 \in \mathbb{Z}_2$ folgt aus $b_0 c_0 = 1$, dass $b_0 = c_0 = 1$ ist. Aus $b_0 + c_1 = 1$ ergibt sich daher $c_1 = 0$, während aus $b_0 c_1 + c_0 = 0$ folgt, dass $c_1 = 1$ ist. Widerspruch!

Kongruent modulo

Sei $\mathcal{K}$ ein Körper und sei $0 \neq f \in \mathcal{K}[x]$, also ein

(3). $f(x) = a_0 + a_1 x + \ldots + a_m x^m, a_m \neq 0$ mit Koeffizienten in $\mathcal{K}$, gegeben. Es gilt $grad(f) = m$. Die Polynome g und h in $\mathcal{K}$ heißen kongruent modulo f, wenn f ein Teiler von $g - h$ ist, d.h. wenn gilt

(4). $g = h + qf$ mit $q \in \mathcal{K}[f]$.
Wir schreiben

(5). $g(x) \equiv h(x) \mod f(x)$,
oder kürzer $g \equiv h \mod f$. Man zeigt leicht

(6). $g_1 \equiv h_1, g_2 \equiv h_2 \Rightarrow \begin{cases} g_1 \pm g_2 \equiv h_1 \pm h_2 \mod f \\ g_1 g_2 \equiv h_1 h_2 \mod f \end{cases}$
Wenn $h \in \mathcal{K}[x]$ ist, so gilt nach Satz 3.6

(7). $h = qf + g$ mit $g \in \mathcal{K}[x], grad(g) < m$
und daher natürlich $g \equiv h \mod f$. Also ist jedes Polynom h kongruent zu einem Polynom der Form

(8). $g(x) = b_0 + b_1 x + \ldots + b_{m-1} x^{m-1}$ mit Koeffizienten $b_0, \ldots, b_{m-1} \in \mathcal{K}$, und zwar zu genau einem Polynom dieser Form.

Produkt modulo

Seien $g, h \in \mathcal{K}[x]$. Dann ist $gh \in \mathcal{K}[x]$. Nach (4) können wir also schreiben

(9). $gh = qf + p$ mit $grad(p) < m$.
Wir nennen p das Produkt modulo f. Das Produkt $\mod f$ ist also das Polynom p, dass

(a) zu gh kongruent $\mod f$ ist,

(b) $grad(p) < m = grad(f)$ erfüllt.

Satz 3.8

Sei $f \in \mathcal{K}[x]$ irreduzibel. Dann ist $\mathcal{K}(f) = \{g \in \mathcal{K}[x] : grad(g) < m\}, m = grad(f)$, ein Körper, wobei die Multiplikation modulo f durchgeführt wird.
Beweis: Die meißten Körpereigenschaften lassen sich leicht nachweisen. Das Produkt liegt wieder in $\mathcal{K}(f)$ wegen (ii).
Am schwierigsten ist es, die Existenz des Reziproken zu beweisen. Das wollen wir nun tun. Sei $g \in \mathcal{K}(f)$ nicht das Nullpolynom. Wir müssen zeigen, dass es ein $h \in \mathcal{K}(f)$ gibt mit $gh \equiv 1 \mod f$.
Nach Satz 3.7(iii) gibt es Polynome $d, \varphi, \psi \in \mathcal{K}[x]$ mit

(10). $d = \varphi f + \psi g,$

und nach Satz 3.7(i) ist d ein Teiler von f und von g. Da d ein Teiler von f und da f irreduzibel ist, gilt $grad(d) = 0$, oder $grad(d) = m$. Da d ein Teiler von g ist gilt $grad(d) \leq grad(g) < m$.
Also bleibt nur der Fall $grad(d) = 0$ übrig, d.h. d ist eine Konstante, also $d \in \mathcal{K}$. Aus (10) folgt $\psi(x)g(x) = d - \varphi(x)f(x) \equiv d \mod f(x)$ und $h(x) = d^{-1}\psi(x)$ erfüllt daher $grad(h) < m$, also $h \in \mathcal{K}(f)$ und weiter $g(x)h(x) \equiv 1 \mod f$.

Beispiel 3

Sei $\mathcal{K} = \mathbb{Q}$ und $f(x) = x^2 - 2, m = 2$. Nach Beispiel 1(1) ist f über $\mathbb{Q}$ irreduzibel. Nach Satz 3.8 ist daher $\mathbb{Q}(f) = \{b_0 + b_1 x : b_0, b_1 \in \mathbb{Q}\}$ ein Körper. Wir wollen Summe und Produkt $\mod f$ von $g(x) = 2 + 3x$ und $h(x) = 5 + 6x$ ausrechnen. Die Summe ist wie üblich $g(x) + h(x) = 7 + 9x$. Das übliche Produkt ist $g(x)h(x) = (2 + 3x)(5 + 6x) = 10 + 27x + 18x^2$, hat aber den Grad 2, welcher zu groß ist. Aber es ist $x^2 - 2 \equiv 0$, also $x^2 \equiv 2 \mod f$ und daher $g(x)h(x) \equiv 10 + 27x + 18 \cdot 2 = 46 + 27x$. Dieses Produkt hat den Grad 1, ist also Produkt $\mod f$.

Beispiel 4

Sei $\mathcal{K} = \mathbb{Z}_2$ und $f(x) = 1 + x + x^3, m = 3$. Nach Beispiel 2(2) ist f über $\mathbb{Z}_2$ irreduzibel. Nach Satz 3.8 ist daher $\mathbb{Z}_2(f) = \{b_0 + b_1 x + b_2 x^2 : b_0, b_1, b_2 \in \mathbb{Z}_2\}$ ein Körper mit 8 Elementen. Wir wollen Summe und Produkt $\mod f$ von $g(x) = 1 + x + x^2$ und $h(x) = 1 + x^2$ ausrechnen. Es ist $g(x) + h(x) = x$, weiter $g(x)h(x) = 1+x+x^2+x^2+x^3+x^4 = 1+x+x^3+x^4$ wegen $1+1 = 0$ in $\mathbb{Z}_2$. Nun ist $1+x+x^3 = f(x) \equiv 0$, also $x^3 \equiv 1+x$ und daher $x^4 \equiv x+x^2$. Wir erhalten somit $g(x)h(x) \equiv 1+x+(1+x)+(x+x^2) = x+x^2$, und dieses Polynom hat den Grad 2, ist also das Produkt $\mod f$.

3.5 endliche Körper

Satz 3.9

Sei $\mathcal{L}$ ein endlicher Körper. Dann gibt es eine Primzahl p mit

(1). $\underbrace{1 + \ldots + 1}_{<p \text{ mal}} \neq 0, \underbrace{1 + \ldots + 1}_{p \text{ mal}} = 0$ und

(2). $|\mathcal{L}| = p^n$ mit $n = 1, 1, \ldots$.

Ungekehrt gibt es zu jeder Primzahl p und jedem $n \in \mathbb{N}$ einen Körper $\mathcal{L}$, sodass (1) und (2) erfüllt sind.

Beispiel 1

Wenn p eine Primzahl ist, so ist $\mathbb{Z}_p$ ein Körper nach Satz 3.3 und es gilt $|\mathbb{Z}_p| = p$, also (2) mit $n = 1$.

Beispiel 2

Man sieht leicht, dass $f(x) = x^2 + x + 1$ über $\mathbb{Z}_2$ irreduzibel ist. Also ist $\mathbb{Z}_2(f) = \{0, 1, x, x + 1\}$ ein Körper. Hier ist $p = 2$ und $n = 2$ in Satz 3.9. In Beispiel 4 hatten wir einen Körper mit 8 Elementen, also $p = 2$ und $n = 3$.
Nach Satz 3.9 gibt es also Körper mit $2, 3, 4, 5, 7, 8, 9, 11, 13, 16, 17, 19, \ldots$ Elementen, aber keinen Körper mit $1, 6, 12, 14, 15, 18, 20, 21, \ldots$ Elementen.
Man kann zeigen, dass es bis auf die Bezeichnung jeweils nur einen Körper mit mit p^n Elementen gibt, vornehmer ausgedrückt: Alle Körper mit p^n Elementen sind zueinander isomorph.

Beispiel 3

Wir wollen alle Körper $\mathcal{K}$ mit 4 Elementen bestimmen. Es ist also $\mathcal{K} = \{0, 1, a, b\}$. Die Additions- und Multiplikationstabellen sind:

$+$	0	1	a	b
0	0	1	a	b
1	1	1	b	a
a	a	b	0	1
b	b	a	1	0

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

Bei der Addition haben wir benutzt, dass $1 + 1 = 0$ ist nach Satz 3.9 mit $p = 2$. Da in jeder Zeile alle vier Elemente vorkommen und z.B. $a + 1 \neq 0$ und $\neq 1$ ist. Bei der Multiplikation tritt das Problem auf: Was ist a^2? Es ist $a^2 \neq 0$, wegen $a \neq 0, 1$. Angenommen es wäre $a^2 = 1$. Dann bliebe für ab nur noch $ab = a$, was auf $b = 1$ führen würde. Also ist $a^2 = b$ und daher $ab = 1$. Natürlich ist dies dasselbe wie Beispiel 2 mit $a = x$ und $b = x + 1$.
Den Satz 3.4 kann man auf beliebige endliche Körper verallgemeinern.

Satz 3.10

Sei $\mathcal{K}$ ein endlicher Körper mit m Elementen. Dann gilt $r^{m-1} = 1$ für alle $r \in \mathcal{K}, r \neq 0$ und es gibt $a \in \mathcal{K}$ mit $\mathcal{K} = \{0\} \cup \{a^i : 1 \leq i \leq m - 1\}$.

Kapitel 4

Kodierung

4.1 Fehlerkorrektur

Im Abschnitt 2.5 haben wir über die Geheimhaltung von Daten gesprochen. In diesem Kapitel geht es dagegen um die Sicherung von Daten bei übertragung und Speicherung. Wir betrachten immer digitale Daten, die in Form von Bit-Blöcken vorliegen. Das allgemeine Schema ist

Originaldaten	$\xrightarrow{Kodierung}$	abgesandte Daten
		$\downarrow$ Übertragung mit seltenen Fehlern
Originaldaten(meistens)	$\xleftarrow[Dekodierung]{}$ mit Fehlerkorrektur	empfangene Daten

Das einfachste Beispiel ist die Kodierung

$$0 \to 010 \to \begin{cases} 000 \\ 011 \\ 010 \\ 110 \end{cases} \to 0, \quad 1 \to 101 \to \begin{cases} 001 \\ 100 \\ 101 \\ 100 \end{cases} \to 1.$$

Hier wurde vorausgesetzt, dass höchstens ein übertragungsfehler auftritt. Dieser kann dann korregiert werden. Natürlich ist dieses Kodierung sehr aufwendig, da sich das Datenvolumen verdreifacht. Zwei Fehler geben eine falsche Dekodierung.

Nun beschreiben wir die allgemeine Situation. Seien

B^n = Menge aller Blöcke von n Bits

C = Menge aller Blöcke, die als Codewörter auftreten.

Im obigen Beispiel ist $n = 3$ und $C = \{010, 101\}$. So ist z.B. $011 \in B^3 \setminus C$, d.h. 011 kann nur durch einen übertragungsfehler entstehen. Bei einem (n, k)- Code hat man Blöcke von k Bits für die Originaldaten und von n Bits für die kodierten Daten. Also gilt für die Anzahl der Elemente $|B^k| = |C| = 2^k, |B^n| = 2^n$. Das Schema ist

$B^k \underset{Kodierung}{\longleftrightarrow} C \underset{\ddot{U}bertragung}{\longmapsto} B^n \underset{Fehlerkorrektur}{\longrightarrow} C \longleftrightarrow B^k.$

Bei $\longrightarrow$ hat man eine umkehrbar eindeutige Entsprechung, bei $\longmapsto$ können Fehler auftreten, man kann also Blöcke in $B^n \setminus C$ empfangen.

Das Ziel ist es, Codes C zu finden, bei denen die Wahrscheinlichkeit einer falschen Dekodierung (Schritt $B^n \to C$) sehr klein ist. Ein überraschendes Ergebnis von Shannon besagt, dass es sehr gute Codes gibt, ohne allerdings zu sagen, wie man diese Codes finden kann. Man geht von einem Übertragungskanal mit (Fehlerwahrscheinlichkeit pro Bit)= $p < \frac{1}{2}$ aus. Sei ld der Duallogarithmus. Der Satz von Shannon sagt aus, dass es zu jedem $\epsilon > 0$ Zahlen k und n mit $1 < \frac{n}{k} \leq \frac{1}{(1-pld\frac{1}{p}-(1-p)ld\frac{1}{1-p})+\epsilon}$ und einen (n, k)-Code C gibt, so dass die Wahrscheinlichkeit einer falschen Dekodierung $< \epsilon$ ist.

Wenn z.B. $p = 0,02$ ist, d.h. 2% Fehler/Bit auftreten können, so gibt es einen (n, k)-Code C mit $\frac{n}{k} < 1,17$, d.h. man braucht nur 17% mehr Bits. Trotzdem kann man den Restfehler beliebig klein wählen, muss dafür aber sehr grosse Blocklängen n in Kauf nehmen.

Hamming-Code

Wir wollen nun effiziente konkrete Codes finden. Ein Beispiel ist der sogenannte $(7,4)$-Hamming-Code:

0000 →	0000 000	0100 →	0100 101	1000 →	1000 011	1100 →	1100 110
0001 →	0001 111	0101 →	0101 010	1001 →	1001 100	1101 →	1101 001
0010 →	0010 110	0110 →	0110 011	1010 →	1010 101	1110 →	1110 000
0011 →	0011 001	0111 →	0111 100	1011 →	1011 010	1111 →	1111 111

Wenn $b_1b_2b_3b_4$ der Originaltext ist, so ist der kodierte Block $b_1b_2b_3b_4b_5b_6b_7$ mit
$b_5 = b_2 + b_3 + b_4, \quad b_6 = b_1 + b_3 + b_4, \quad b_7 = b_1 + b_2 + b_4,$
wobei die Addition in $\mathbb{Z}_2$ stattfindet, also die „exclusive-or“ Operation ist.
Seien $a, b \in B^n$, d.h. a und b sind Blöcke von je n Bits. Der Abstand [distance] von a und b ist definiert als $dist(a, b) =$(Anzahl der unterschiedlichen Bits).
Also ist $dist(a, b) =$(Anzahl der 1 in a xor b).
So ist z.B. $dist(01101, 01011) = 2$.
Der Hamming- Abstand des Codes $C \subset B^n$ ist definiert als

(1). $min\{dist(c, d) : c, d \in C, c \neq d\}$.

Man prüft nach, dass der $(7,4)$-Hamming-Code den Hamming- Abstand 3 hat.

Satz 4.1

Sei C ein (n, k)- Code mit einem Hamming- Abstand $\geq 2m + 1$. Dann kann man bis zu m Übertragungsfehler korrigieren.
Beweis: Sei $c \in C$ der ausgesandte Block und $b \in B^n$ der empfangene Block, der also 0 bis m Fehler enthält, d.h. es ist $dist(b, c) \leq m$. Wir zeigen nun, dass es kein $d \in C$ mit $d \neq c$ und $dist(b, d) \leq m$ gibt. Sonst wäre $dist(c, d) \leq dist(c, b) + dist(b, d) \leq m + m = 2m$, welches unserer Voraussetzung (dazu(1)) $dist(c, d) \geq 2m + 1$ für $c, d \in C, c \neq d$ widerspricht. Also kann c eindeutig als der ausgesandte Code-Block identifiziert werden. Damit ist der Satz bewiesen.
Nach Voraussetzung gibt es $c, d \in C$ mit $dist(c, d) = 2m + 1$. Man kann $b \in B^n \setminus C$ finden mit

(2). $dist(b, c) = m + 1, dist(b, d) = m$.

Nun nehmen wir an, dass c ausgesandt und b empfangen wird. Es treten also $m+1$ Fehler auf. Wegen (2) gibt also der oben beschriebene Korrektur- Algorithmus fälschlicherweise d als den ausgesandten Block. Also kann man nicht $> m$ Fehler sicher korrigieren.

4.2 Lineare Codes

Die bitweise [bit wise] Addition von Blöcken ist die „exclusive-or“ Operation. Z.B. ist
$10011 + 11001 = 01010, \quad 11010 + 11010 = 00000$; geschrieben 0.
Also gilt $a + a = 0$, d.h. $-a = a$ und somit $a - b = a + b$.
Im nächsten Abschnitt werden wir Bitblöcke mit Polynomen über $\mathbb{Z}_2$ identifizieren, z.B. $10011 \to x^4 + x + x$. Dann ist unsere bitweise Addition gerade die übliche Addition von Polynomen.
Der (n, k)-Code C heißt linear [linear], wenn

(1). $c, d \in C \Rightarrow c + d \in C$.
Insbesondere gilt $0 \in C$ wegen $c + c = 0$. Der $(7,4)$-Hamming-Code ist linear.
Das Gewicht [weight] von $b \in B^n$ ist definiert durch

(2). $x(b) =$(Anzahl der Bits 1 in b).
So ist z.B. $w(10011) = 3, w(0) = w(00000) = 0$. Man hat

(3). $dist(a, b) = w(a + b)$ für $a, b \in B^n$.

Satz 4.2

Der Hamming- Abstand des linearen Codes C ist

(4). $min\{w(c) : c \in C, c \neq 0\}$

Beweis: Nach Definition ist der Hamming- Abstand= $min\{dist(a, b) : a, b \in C, a \neq b\}$ und nach (3) ist dies $= min\{w(a + b) : a, b \in C, a \neq b\}$.
Da C linear ist, gilt $c = a + b \in C$ für $a, b \in C$. Weiter gilt $c = a + b = 0$ genau dann, wenn $a = b$ ist. Also ist der Hamming- Abstand=$min\{w(c) : c \in C, c \neq 0\}$.

Matrizen und Vektoren

Nun brauchen wir Matrizen und Vektoren mit Elementen in $\mathbb{Z}_2$, d.h. die Elemente sind Bits. Wir interpretieren Blöcke von n Bits als Zeilenvektor mit n Komponenten. Z.B. ist

$$(11001)\begin{pmatrix}110\\011\\001\\000\\100\end{pmatrix} = (001).$$

Satz 4.3

Sei C ein linearer (n, k)- Code. Dann gibt es eine Matrix H mit n Zeilen und $n - k$ Spalten, so dass gilt $c \in C \Leftrightarrow cH = 0$.
Da c ein Zeilenvektor mit n Komponenten und H eine Matrix mit n Zeilen und $n - k$ Spalten ist, ist cH ein Zeilenvector mit $n - k$ Komponenten. Die Bedingung $cH = 0$ besagt also, dass die $n - k$ Bits von cH alle =0 sein sollen.
Für unseren $(7, 4)$-Hamming- Code hat man z.B.

$$H = \begin{pmatrix}011\\101\\110\\111\\100\\010\\001\end{pmatrix} \qquad \underbrace{(1000011)}_{\in C}H = (000) = 0, \quad \underbrace{(1100011)}_{\notin C}H = (101) \neq 0$$

Satz 4.4

Sei C ein linearer Code mit einem Hamming- Abstand $\geq 2m + 1$. Zu jedem $s \in B^{n-k}$ bestimmt man $f = f(s) \in B^n$ mit

(5). $w(f) = min\{w(x) : x \in B^n, xH = s\}, fH = s$.
Wenn $c \in C$ und $b \in B^n$ mit $dist(b, c) \leq m$ ist, so gilt

(6). $c = b + f(s), s = bH$.

Beweis: Wir setzen $a = b + f$ und müssen $a = c$ zeigen.
Sei $s = bH$ und $f = f(s)$. Es gilt $aH = (b+f)H = bH + fH = s + s = 0$ nach (6). Aus Satz 4.3 folgt daher $a \in C$.
Weiter gilt $f = b + a$ und $(b+c)H = bH + cH = s + 0 = s$ nach (6) und Satz 4.3. Aus (5) folgt daher $w(b+a) = w(f) \leq w(b+c)$ und nach (3) und der Voraussetzung ist daher $dist(b,a) \leq dist(b,c) \leq m$.
Wäre nun $a \neq c$, so würde (wie im Beweis von Satz 4.1) $2m+1 \leq dist(a,c) \leq dist(a,b) + dist(b,c) \leq m + m = 2m$ folgen, was ein Widerspruch ist. Also gilt $a = c$, also $c = b + f$.

Zusammenfassung des Algorithmus

$d \in B^k$	Original Datenblock
$\downarrow$	Kodierung
$c \in C \subset B^n$	Kodierter Block
$\downarrow$	Übertragung
$b \in B^n$	Empfangener Block
$\downarrow$	$x = bH$ berechnen
$b \in B^n, s \in B^{n-k}$	
$\downarrow$	$f = f(s)$ aus Tabelle mit 2^{n-k} Wertepaare holen; $f = 0$ falls $b \in C$
$b \in B^n, f \in B^n$	
$\downarrow$	$c^* = b + f$ berechnen
$c^* \in C \subset B^n$	$c^* = c$ falls maximal m Übertragungsfehler
$\downarrow$	dekodieren
$d^* \in B^k$	Original Datenblock falls maximal m Fehler

4.3 Zyklische Codes

Die Bitblöcke $b \in B^n$ haben die Form

(1). $b = b_{n-1}b_{n-2}\cdots b_1 b_0$ mit $b_k \in \mathbb{Z}_2$.
Der (n,k)- Code C heißt zyklisch, wenn

(a) $b, c \in C \Rightarrow b + c \in C$, d.h. C ist linear,

(b) $b_{n-1}b_{n-2}\ldots b_1 b_0 \in C \Rightarrow b_{n-2}\cdots b_1 b_0 b_{n-1} \in C$.

Anders ausgedrückt: Die CPU- Operationen „xor“ und „rot“ führen nicht aus C heraus.

$\boxed{7\,|\,6\,|\,5\,|\,4\,|\,3\,|\,2\,|\,1\,|\,0} \xrightarrow{rot} \boxed{6\,|\,5\,|\,4\,|\,3\,|\,2\,|\,1\,|\,0\,|\,7}$

Der $(7,4)$- Hamming- Code ist nicht zyklisch, kann aber in einen zyklischen Code verwandelt werden.
Bei linearen Codes hatten wir die Addition benutzt. Bei zyklischen Codes benutzen wir zusätzlich noch die Multiplikation und zwar von Polynomen.
Jedem Block der Form (1) ordnen wir ein Polynom mit Koeffizienten in $\mathbb{Z}_2 = \{0,1\}$ zu: $b_{n-1}b_{n-2}\cdots b_1 b_0 \in B^n \leftrightarrow x^{n-1} + \ldots + b_1 x + b_0 \in \mathbb{Z}_2[x]$.
Für $n = 8$ haben wir z.B. $01101001 \leftrightarrow x^6 + x^5 + x^3 + 1$.
Nun betrachten wir Kongruenzen modulo $x^n + 1$, d.h. $g(x) \equiv h(x) \Leftrightarrow g(x) = q(x)(x^n+1) + h(x)$ mit $q \in \mathbb{Z}_2[x]$.
Es gilt $x^n + 1 \equiv 0$ und daher

(2). $x^n \equiv 1 \mod x^n + 1$.
Wir betrachten den Polynomring R_n, der aus allen Polynomen

(3). $g(x) = b_{n-1}x^{n-1} + \ldots + b_1 x + b_0 \in \mathbb{Z}_2[x]$ besteht,
d.h. R_n entspricht B^n. In R_n ist die Multiplikation $\mod x^n + 1$.

Beispiel

Der Ring R_5 besteht aus den 2^5 Polynomen $g(x) = b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0$ mit $b_0, \dots, b_4 \in \mathbb{Z}_2$.
Es ist $x^5 \equiv 1$, also $x^6 \equiv x$ und daher z.B.
$(x^4+x^3+x^2+1)(x^2+1) = x^6+x^5+x^4+x^2+x^4+x^3+x^2+1 = x^6+x^5+x^3+1 \equiv x+1+x^3+1 = x^3+x$.
Das Produkt $\mod x^5+1$ ist also $= x^3+x$.
Nun kehren wir zu zyklischen Codes zurück. Das dem Block $b_{n-1}b_{n-2}\cdots b_0$ entsprechende Polynom ist $g(x) = b_{n-1}x^{n-1}+\ldots+b_1x+b_0$, und dem linksrotierenden Block $b_{n-2}\cdots b_0b_{n-1}$ entspricht $b_{n-2}x^{n-1}+\ldots+b_0x+b_{n-1} = (b_{n-1}x^{n-1}+\ldots+b_0)x+b_{n-1}(x^n+1) \equiv xg(x) \mod x^n+1$.
Daher kann man die Bedingung (b) für zyklische Codes als

(4). $g(x) \in C(x) \Rightarrow xg(x) \in C(x) \mod x^n+1$ schreiben.
Hierbei bezeichnet $C(x)$ die Menge der Polynome, die den Codes $C \subset B^n$ entsprechen.

Satz 4.5

Sei C einn zyklischer (n,k)- Code. Dann gibt es ein Polynom $f \in C(x)$ mit $grad(f) = n-k$, so dass jedes $g \in C(x)$ genau eine Darstellung

(5). $g(x) = h(x)f(x)$ mit $h \in \mathbb{Z}_2[x], grad(h) < k$ hat, und jedes solche g gehört umgekehrt zu $C(x)$.
Weiter ist

(6). $f(x)$ ist ein Teiler von x^n+1.
Nach (4) gilt also für alle $g \in C$

(7). $g(x) = (c_{k-1}x^{k-1}+\ldots+c_1x+c_0)f(x)$ mit $c_j \in \mathbb{Z}_2$.
Beweis: (a) Zuerst konstruieren wir das Polynom f. Sei f ein Polynom $\neq 0$ in $C(x)$, das minimalen Grad hat. Wir setzen

(8). $m = grad(f)$.
Also ist $0 \le m \le n$. Später zeigen wir $m = n-k$.
(b) Nun zeigen wir, dass jedes $g \in C(x)$ genau eine Darstellung

(9). $g(x) = h(x)f(x)$ mit $h \in \mathbb{Z}_2[x], grad(h) \le n-m$ hat.
Sei $g \in C(x)$ gegeben. Nach Satz 3.6 ist

(10). $g(x) = h(x)f(x) + r(x)$ mit $grad(r) < n-m$.
Wegen $g \in C8x)$ folgt aus (4)
$xf(x) \in C(x), x^2f(x) \in C(x), x^3f(x) \in C(x)$, usw., wobei die Multiplikation modulo x^n+1 zu verstehen ist. Da C linear ist, erhalten wir somit

(11). $h(x)f(x) = c_{k-1}x^{k-1}f(x)+\ldots+c_1xf(x)+c_0f(x) \in C(x)$.
Da auch $g \in C(x)$ ist, folgt aus (10) und der Linearität $r(x) = g(x) - h(x)f(x) \in C(x)$.
Aber es ist $grad(r) < m = grad(f)$. Aus Teil (a) ergibt sich somit $r(x) = 0$. Nach (10) gibt es also eine Darstellung (9); es ist $grad(h) = grad(g) - grad(f) < n-m$.
Angenommen es gäbe eine weitere Darstellung der Form (9), also $g(x) = h^*(x)f(x)$. Aus (9) folgt dann $(h^*-h)f = g-g = 0$, und wegen $f \neq 0$ folgert man $h^*-h = 0$, d.h. $h^* = h$. Also ist die Darstellung (9) eindeutig.
(c) Nun zeigen wir $m = n-k$. Nach (11) gehört jedes Polynom der Form (9) zu $C(x)$. Nach Teil (b) stellt also (9) alle Polynome in $C(x)$ genau einmal dar und keine anderen. Da es genau 2^{n-m} Polynome $h \in \mathbb{Z}_2[x]$ mit $grad(h) < n-m$ gibt, gilt $2^{n-m} = |C(x)| = 2^k$, da C ein (n,k)-Code ist. Also ist $m = n-k$. Die Darstellung (9) ist also mit der Darstellung (5) identisch.
(d) Schließlich beweisen wir (b). Es gilt $x^n+1 = p(x)f(x)+s(x)$ mit $grad(s) < m = n-k$. Also ist $s(x)$ das Produkt $\mod x^n+1$ von $p(x)$ und $f(x)$. Wie in (11) folgert man, dass $s \in C(x)$

ist. Wegen $grad(s) < m$ ergibt sich also aus Teil (a), dass $s = 0$ ist. Somit ist $x^n + 1 = p(x)f(x)$, d.h. $f(x)$ ist ein Teiler von $x^n + 1$.
Nach (6) ist

(12). $x^n + 1 = p(x)f(x)$ mit $p \in \mathbb{Z}_2[x]$, also $grad(p) = n - grad(f) = k$. Man definiert:
f erzeugende Polynome von C mit $grad(f) = n - k$,
p Prüfpolynom von C mit $grad(p) = k$.
Der Name „Prüfpolynom“ wird durch den folgenden Satz gerechtfertigt.

Satz 4.6

Sei C ein zyclischer Code und $p(x)$ das Prüfpolynom von C. Sei $g \in \mathbb{Z}_2[x]$ mit $grad(g) < n$. Dann gilt $g \in C(x) \Leftrightarrow p(x)g(x) \equiv 0 \mod x^n + 1$.
Beweis: Zuerst sei $g \in C(x)$. Nach (5) ist $g = hf$, nach (12) also $g(x)p(x) = h(x)f(x)p(x) = h(x)(x^n + 1) \equiv 0 \mod x^n + 1$.
Umgekehrt sei $gp \equiv 0$. Dann ist nach (12) $g(x)p(x) = h(x)(x^n + 1) = h(x)p(x)f(x)$, und wegen $p \neq 0$ folgt daraus $g = hf$. Es ist $grad(h) = grad(g) - grad(f) < n - (n - k) = k$. Also ist $g \in C(x)$ nach Satz 4.5.
Wenn wir das Prüfpolynom als $p(x) = x^k + p_{k-1}x^{k-1} + \ldots + p_1x + p_0$ schreiben, so ist die Matrix aus Satz 4.3

$$H = \begin{pmatrix} p_0 & 0 & 0 & \ldots & 0 \\ p_1 & p_0 & 0 & \ldots & 0 \\ p_2 & p_1 & p_0 & \ldots & 0 \\ & & & \ddots & \\ & \ldots & & & \\ 1 & p_{k-1} & p_{k-2} & \ldots & p_0 \\ 0 & 1 & p_{k-1} & \ldots & p_1 \\ & & & \ddots & \\ 0 & 0 & 0 & \ldots & 1 \end{pmatrix} n \text{ Zeilen, } n-k \text{ Spalten}$$

Diese sehr regelmäßige Form erleichtert die Berechnung von $s = bH$; dazu Satz 4.4.

4.4 Die Konstruktion zyklischer Codes

Wir wollen nur ein paar Beispiel geben. Die allgemeine Methode benutzt endliche Körper.

Beispiel 1

Sei $n = 7$. Man hat die Faktorisierung $x^7 + 1 = (x^3 + x + 1)(x^3 + x^2 + 1)(x + 1)$ in irredizible Faktoren. Wir wählen $k = 4$ und das erzeugende Polynom $f(x) = x^3 + x + 1$. Das Prüfpolynom ist $p(x) = (x^3 + x^2 + 1)(x + 1) = x^4 + x^4 + x + 1$.
Nach Satz 4.5 ist der Code durch $C(x) = \{(b_3x^3 + b_2x^2 + b_1x + b_0)(x^3 + x + 1) : b_0, b_1, b_2, b_3 \in \mathbb{Z}_2\}$ gegeben. Einige Polynome in $C(x)$ und die dazugehörigen Blöcke in C sind
$(x^3 + 1)(x^3 + x + 1) = x^6 + x^4 + x + 1 \rightarrow 1010011$,
$(x^2 + x + 1)(x^3 + x + 1) = x^5 + x^4 + 1 \rightarrow 0110001$.
Dies ist im Wesentlichen der $(7, 4)$- Hamming- Code mit dem Hamming- Abstand 3.

Beispiel 2

Sei $n = 15$ und $k = 11$. Es ist $x^{15} + 1 = \underbrace{(x^4 + x + 1)}_{=f(x)}\underbrace{(x^{11} + x^8 + x^7 + x^5 + x^3 + x^2 + x + 1)}_{=p(x)}$
Der Code ist $C(x) = \{(b_{10}x^{10} + \ldots + b_0)(x^4 + x + 1) : b_0, \ldots, b_{10} \in \mathbb{Z}_2\}$.

Dies ist der $(15, 11)$- Hamming- Code. Der Hamming- Anbstand ist wieder 3, man kann also einen Fehler in jedem 15- Bit- Block korregieren. Dieser Code ist etwas effizienter als der $(7, 4)$- Hamming-Code, bei dem jedoch ein Fehler pro 7- Bit- Block erlaubt war.

Beispiel 3

Sei wieder $n = 15$, jetzt aber $k = 7$. Der zweite Faktor in Beispiel 2 kann noch weiter aufgespalten werden. Man erhält jetzt $x^{15} + 1 = \underbrace{(x^4 + x + 1)(x^4 + x^3 + 1)}_{=f(x)}\underbrace{(x^7 + x^6 + x^5 + x^2 + x + 1)}_{=p(x)}$

Der Code wird jetzt durch $C(x) = \{(B_6 x^6 + \ldots + b_0) f(x) : b_0, \ldots, b_6 \in \mathbb{Z}_2\}$ gegeben. Der Hamming-Abstand ist 5. Nach Satz 4.1 kann man also 2 Fehler in jedem 15- Bit- Block korrigieren.

Zusammenfassung

Datenbits $= k$	Korrekturbits $= n - k$	Bits pro Block $= n$	korrigierbare Fehler
4	3	7	1
11	4	15	1
7	8	15	2
5	10	15	3