Diskrete Mathematik
Diskrete Strukturen & Zahlentheorie

Prof. Christof Schelthoff
FH Aachen - Campus Jülich
Kontakt: schelthoff@fh-aachen.de

6. April 2010

Inhaltsverzeichnis

Kapitel 1

Diskrete Strukturen

Diskrete Mathematik beschäftigt sich mit abzählbaren Strukturen. Grenzwertbetrachtungen, wie Sie in der Analysis vorkommen, spielen hier keine Rolle.

Typische Fragestellungen, die wir beantworten werden, sind von der Gestalt:

1. Kann man ein Schachbrett, bei dem die linke obere und rechte untere Ecke fehlt, lückenlos mit einem 1x2-Dominostein überdecken? (Färbungen)

2. Ist es möglich, dass bei einer Fete, bei der beliebig viele Leute Visitenkarten austauschen (oder auch nicht - jedoch immer paarweise) nachher alle eine verschiedene Anzahl Visitenkarten haben? (Schubfachprinzip)

3. Auf wieviele Arten kann man eine n-Stufige Treppe erklimmen, wenn man stets 1 oder 2 Stufen nimmt? (Fibonacci)

4. Wieviele Zahlen bis 1000 sind durch 3,5 oder 10 teilbar? (Sieb-Prinzip)

5. An welchen Ecken muss man "das Haus vom Nikolaus" beginnen, damit man es in einem Zug durchzeichnen kann? (Graphentheorie)

6. Gibt es in der Folge {1,5,9,13,17,21,...} unendlich viele Primzahlen? Wie sind es in der Folge der anderen ungeraden Zahlen {3,7,11,15,19,23} aus? Gibt es dort unendlich viele Primzahlen? (Zahlentheorie)

Jedes dieser Probleme lässt sich mit "gesundem Menschenverstand" angehen und eine Lösung kann erahnt werden. Beweis und Struktur helfen jedoch, diese Dinge allgemeingültig zu lösen und dann auf weitere Probleme anzuwenden.

1.1 Beweisprinzipien

Um diese Aussagen zu beweisen, sind verschiedene Beweistechniken von Nöten, die hier kurz vorgestellt seien:

1. Der direkte Beweis: Hier wird direkt aus den Vorraussetzungen A die Behauptung B geschlossen.Also:

   $$\boxed{A \Longrightarrow B}$$

   Beispiel: Das Quadrat einer ungeraden Zahl u ist ungerade und lässt der Division durch 4 den Rest 1. Die Vorr. A ist nur das die Zahl ungerade ist, also $u = 2n + 1$. Die Folgerung ist

   $$\begin{aligned} u^2 &= (2n+1)^2 \\ &= 4n^2 + 4n + 1 \\ &= 4(n^2 + n) + 1 \end{aligned}$$

   und damit ist die Behauptung gezeigt.

2. Der indirekte Beweis: Nun wird die Folgerung umgedreht, da dort gilt:

   $$\boxed{(A \Longrightarrow B) \Longleftrightarrow (\neg B \Longrightarrow \neg A)} \tag{1.1}$$

   Die Rolle von Vorr. und Behauptung wird nun vertauscht. Wir nehmen an die Behauptung B sei nicht wahr und zeigen dass auch die Vorr. A nicht erfüllt gewesen sein konnte.

3. Das Prinzip des kleinsten Verbrechers

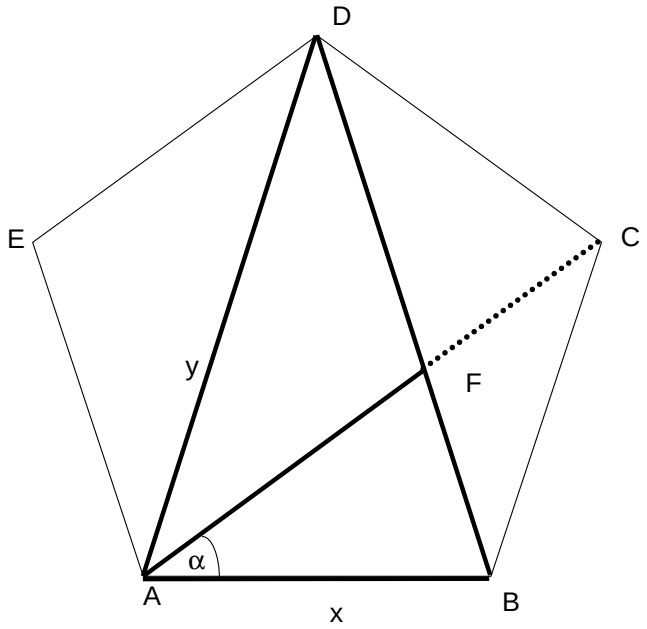
   Grundlage dieses Prinzips ist, das jede nicht leere Teilmenge natürlicher Zahlen ein kleinstes Element besitzt. Dies ist für Teilmengen rationaler oder reeller Zahlen nicht der Fall. Häufig verwendet wird dies, indem wir die Menge derjenigen natürlichen Zahlen betrachten, die eine gewisse Aussage nicht erfüllen. Nehmen wir nun an, diese sei nicht-leer, so gibt es einen kleinsten Übeltäter. Dieser wird betrachtet und ggf gezeigt, dass auch für diesen einen Wert die Ausage wahr ist oder ein anderer Widerspruch gezeigt. Somit ist unsere Prämisse, die Menge sei nicht-leer falsch und es kann diesen kleinsten Überltäter nicht gegeben haben bzw. die betrachete Menge der Zahlen, die eine Aussage nicht erfüllen ist leer. Dies wiederum bedeutet, dass die Aussage für alle natürlichen Zahlen richtig ist.

   Beispiel: Es gibt keine uninteressante natürliche Zahl.

   Beweis: Sei N die Menge aller uninteressanten natürlichen Zahlen $N = \{n_1, n_2, ...\}$. Diese enthält unser uninteressantes n_1 als kleinsten Übeltäter. Damit ist n_1 die kleinste uninteressante natürliche Zahl. Das macht

n_1 aber interessant und n_1 kann nicht zu N gehört haben. Damit ergibt sich N={}.

Machen wir nun noch ein etwas mathematisch anspruchvolleres Modell. Wir betracheten hierzu ein gleichmässiges Fünfeck. An jeder Ecke liegt somit der Winkel $\frac{540^0}{5} = 108^0$.



Verbinden wir nun eine Grundseite mit dem gegenüberliegenden Punkt, z.B. ABD oder ACD so erhalten wir ein gleichschenkliges Dreieck mit zwei Schenkeln der Länge y und der Basisseite x.Es gilt insbesondere $y > x$. Man überlege sich zunächst, (wo taucht der Winkel α überall auf?), dass das Dreieck die Winkel 72^0 an der Basisseite hat sowie 36^0 im spitzen Winkel. Weiterhin sind die Diagonalen wie zB. die Strecke AC Winkelhalbierende. Daher ist auch $\alpha = 36^0$.

Soweit die Geometrie - die Frage ist nun: Gibt es ein solches gleichschenkliges Dreieck mit ganzzahligen Seitenlängen x und y?

Verwenden wir das Prinzip des kleinsten Überltäters und betrachten die kleinste ganzzahlige Basislänge x als diesen Übeltäter. In diesem Fall betrachten wir obige Figur und sehen, dass das Dreieck ABF nun die Schenkellängen x und die Grundseite $y - x$ hat. Da aber x und y ganzzahlig waren mit $y > x$ hat auch das neue Dreieck ganzzahlige positive Seitenlängen. Insbesondere ist nun $y - x < x$.Daher ist $y - x$ nun ein kleinerer Übeltäter und x kann nicht der kleinste gewesen sein. Daher ist die Menge der Übeltäter leer.

Bem.: Wir haben ein ähnliches Dreieck erzeugt und gezeigt, dass es keine

ganzzahligen positiven Lösungen geben kann der Gleichung

$$\frac{y}{x} = \frac{x}{y-x}$$

bzw.

$$\frac{x}{y} = \frac{y-x}{x} = \frac{y}{x} - 1$$

4. Die vollständige Induktion

Da dieses Prinzip in der diskreten Mathematik ein häufig verwendetes ist, widmen wir diesem einen grösseren Abschnitt:

1.1.1 Die vollständige Induktion

Beweisprinzip für unendlich viele, aber abzählbare Objekte

$$\boxed{A(n_0) \Longrightarrow A(n_0+1) \Longrightarrow A(n_0+2)...} \tag{1.2}$$

(Dominoprinzip: Wenn der n-te Stein fällt, fällt auch der n+1-te; Und: Der erste Stein wird umgeschubst !).

Die Aussage hängt von einer natürlichen Zahl n ab, also A(n) und wir wollen die Richtigkeit für alle n zeigen.

1. Zeige A(n_0) ist richtig (Induktionsanfang, meist $n_0 = 0$ oder 1)

2. Für jede natürliche Zahl n folgt aus A(n) (Induktionsvorr.) die Aussage A(n+1) (Induktionsschluss)

2. kann auch verschärft werden, in dem man die Gültigkeit
für ALLE Werte von 1 bis n benutzt, um den Induktionsschluß zu zeigen
Bsp.:

1. A(n)=4n-2 ist gerade für jedes n
Induktionsanfang: n=1: A(1)=2 ist gerade
Induktionsvorr.:n: A(n) ist gerade
Induktionsschluss: A(n+1)=4(n+1)-2= $\underbrace{4n-2}_{gerade \text{ nach Induktionsvorr.}}$ +4 ist gerade

Dabei ist der Induktionsanfang wichtig, sonst hätte die Aussage auch für A(n)=4n-1 gezeigt werden können.

2.

$$A(n) : \sum_{i=0}^{n} i = \frac{n \cdot (n+1)}{2}$$

Induktionsanfang:

$$A(0) : \sum_{i=0}^{0} i = 0 = \frac{0 \cdot (0+1)}{2} \qquad \checkmark$$

Sei nun A(n) wahr für beliebige n, dann ist:

$$A(n+1): \sum_{i=0}^{n+1} i = \frac{(n+1)\cdot((n+1)+1)}{2} = \frac{(n+1)\cdot(n+2)}{2}$$

zu zeigen. Benutzt werden darf (muss) die Aussage A(n). Daher führen wir die Summe auf A(n) zurück und setzen die Induktionsvorr. ein:

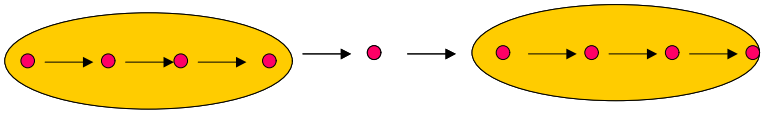
$$\begin{aligned}\sum_{i=0}^{n+1} i &= \sum_{i=0}^{n} i + (n+1) = \frac{n\cdot(n+1)}{2} + (n+1)\\ &= \frac{n\cdot(n+1)}{2} + \frac{2\cdot(n+1)}{2} = \frac{n\cdot(n+1)+2\cdot(n+1)}{2}\\ &= \frac{(n+1)\cdot(n+2)}{2} \quad \text{q.e.d.}\end{aligned}$$

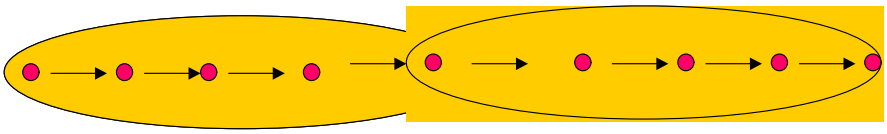
3. Jede(r) Student(in) kann unendlich viel Bier trinken.
Sei n die Anzahl der Biere, also A(n) heisst der Student kann n Bier trinken
Induktionsanfang: 1 Bier kann jeder trinken, daher richtig
Induktionsvorr. n Biere können getrunken werden
Induktionsschluss: Wenn man schon n Biere hat, geht eins mehr - also n+1 - immer noch. Damit ist die Behauptung gezeigt.

Naja
4. Aufgabe: Bei einem Sportturnier spielen n Mannschaften M 1, M2,..., Mn gegeneinander. Jedes Spiel endet mit einem Sieger (notfalls Elfmeterschießen). Dann es gibt immer eine Reihenfolge R1,...,Rn, so dass die Mannschaft an Platz k gegen diedirekt vor ihr stehende Mannschaft verloren hat und gegen die direkt dahinter stehende gewonnen hat.Beachte: Das heisst nicht, gegen ALLE vor ihr stehende Mannschaften gewonnen.

Bsp: 3 Mannschaften
A gewinnt gegen C,
B gewinnt gegen A,
C gewinnt gegen B
Eine Lösung/Reihenfolge wäre: A C B, eine andere C B A.

Ind. Verankerung: n=1, n=2: Ok
Ind. Vorr.: Für alle i<=n gelte die Behauptung
Ind. Schluß: n+1 Mannschaften. Betrachte die letzte (n+1-te) und teile die Mannschaften in 2 Mengen ein: Die gegen Mannschaft n+1 gewonnen haben und die die verloren haben.





Innerhalb der beiden äusseren Mengen, die nun n oder weniger Elemente haben, existiert nach Induktionsvorr. eine solche Reihenfolge. Damit auch insgesamt und die Behauptung ist bewiesen.

5. Aussage: A(n): Bei einer Gruppe von n Studenten können alle gleich schlecht Mathematik !

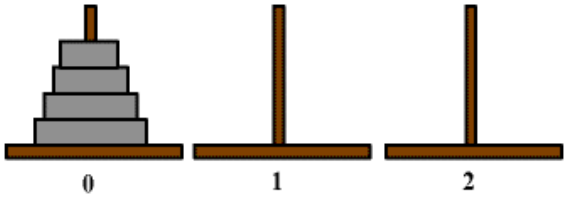
A(1) ist sicherlich wahr

n->n+1: Wir betrachten eine Person k irgendwo in der Mitte der Gruppe.

Die Gruppe bis zu dieser Person hat höchstens n Studenten und ist damit gleich schlecht nach Induktionsvorr. Ab dieser Person bis zum Ende ebenfalls. Damit sind alle gleich schlecht.

Wo ist der Fehler ?

6.



Aufgabe: In jedem Schritt darf nur eine Scheibe bewegt werden. Nie darf eine größere auf eine kleinere gelegt werden

Zeigen Sie: A(n): Bei n Scheiben kann man in $2^n - 1$ Zügen den Stapel von Säule 0 auf Säule 1 bringen!

Beweis: n=1 klar ($2^1 - 1 = 1$ Zug)

n->n+1: Zunächst können nach Induktionsvorr. in $2^n - 1$ Zügen die oberen n Steine auf Säule 2 gebracht werden, dann wird die n+1-te Scheibe auf Säule 1 gelegt (diese kann nun wie ein leeres Feld behandelt werden, da diese die größte Scheibe ist) und dann können wiederum nach Induktionsvorr. in $2^n - 1$ Zügen die Steine von Säule 2 auf Säule 1 gelegt werden.

Insgesamt: $2 \cdot (2^n - 1) + 1 = 2^{n+1} - 2 + 1 = 2^{n+1} - 1$ Züge.

1.2 Modellbildung

" Wenn Sie sich keinen vierdimensionalen Raum vorstellen können, so betrachten Sie einfach einen n-dimensionalen Raum und nehmen den Spezialfall n=4."

Die Prinzipien beruhen stets darauf zwar ein spezielles Problem lösen zu wollen (4 Dimensionen), dieses dann aber zu verallgemeinern (n-dimensional) und dort abstrakt die Problemlösung zu finden.

Versuchen wir dies an einem einfachen Beispiel zu verifizieren: Jeder Student sollte im 1x1 fit sein. Wenn zumindest eine der Zahlen kleiner als 5 ist, geht dies auch gut. Hervorragend wenn beide dies sind. Was aber bei den "schwierigen" Aufgaben $6 \cdot 9, 7 \cdot 7, 7 \cdot 9, ...$ (Sollten Sie vorstehende Behauptung über Studenten als beleidigend empfinden, ersetzen Sie "Student" bitte durch "Grundschüler").

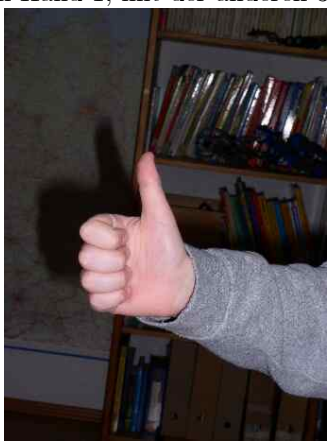
Wir erinnern uns, dass die Addition im Vorschulalter mit Hilfe der Hände durchgeführt wurde. Da man seine Hände meist dabei hat, wären diese als allgegenwärtiger Taschenrechner doch sehr brauchbar. Versuchen wir also diese einzusetzen.

Stellen wir uns zunächst die Frage was wir denn lösen wollen. Das Einmaleins sieht wie folgt aus:

Einfach

	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2	2	4	6	8	10	12	14	16	18	20
3	3	6	9	12	15	18	21	24	27	30
4	4	8	12	16	20	24	28	32	36	40
5	5	10	15	20	25	30	35	40	45	50
6	6	12	18	24	30	36	42	48	54	60
7	7	14	21	28	35	42	49	56	63	70
8	8	16	24	32	40	48	56	64	72	80
9	9	18	27	36	45	54	63	72	81	90

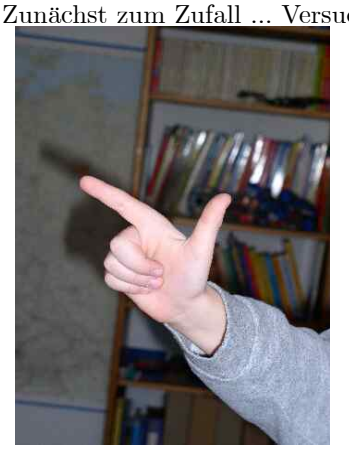
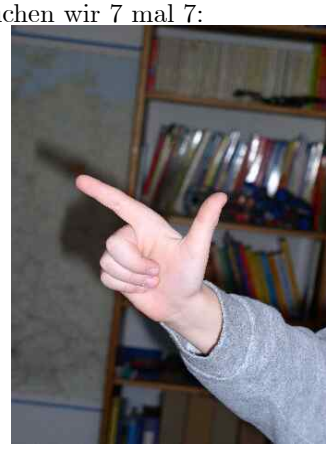
In der Ecke links oben befinden sich die einfachen Aufgaben, rechts unten die schweren. Nehmen wir uns eine schwere - schier unlösbare - heraus: 6 mal 8 (!). Leider reichen unsere Hände nur bis zu 5 Fingern, da aber beide Zahlen größer als 5 sind, zeigen wir nur den über 5 hinausgehenden Anteil an. Mit der einen Hand 1, mit der anderen 3:



Wir wollen nun schauen, ob wir das Ergebnis - 48 - wiederfinden. Die ausgestreckten Finger 3+1 ergeben schon mal die Zehner der Lösung. Wir sehen

abgeklappt einmal 4, einmal 2 Finger. Die Einer (8) sind das Produkt dieser beiden Zahlen. Erstaunlich ! Oder Zufall ?

Zunächst zum Zufall ... Versuchen wir 7 mal 7:

Zehner: 2 plus 2 = 4, Einer: 3 mal 3=9 - zusammen 49 - Stimmt !

Weitere Versuche zeigen, es scheint immer zu gehen. Die Aufgabe reduziert sich also auf eine Addition zweier Zahlen kleiner 5 und einer Multiplikation zweier Zahlen kleiner 5 (die einfache Aufgabe aus der oberen linken Ecke des Einmaleins)

Die Modellbildung:

Bezeichnen wir nun mit x und y bezeichnen die durchzuführende Multiplikation

Zu Bechnen $\mathbf{x \cdot y}$, wobei x und y Zahlen zwischen 5 und 10 bezeichnen.

Anzeige linke Hand: $x - 5$
Anzeige rechte Hand: $y - 5$

nicht eingeklappte links: $5 - (x - 5) = 10 - x$
nicht eingeklappte rechts: $5 - (y - 5) = 10 - y$

Wie berechnen wir nun die Lösung von $x \cdot y$?

Zehner: $10 \cdot (x - 5 + y - 5) = 10x + 10y - 100$
Einer: $(10 - x) \cdot (10 - y) = 100 - 10x - 10y + xy$

Summe: $10x + 10y - 100 + 100 - 10x - 10y + xy = \mathbf{xy}$

Dies entspricht gerade der gesuchten Lösung $x \cdot y$. Beweis geführt !

1.3 Das Schubfachprinzip

Auch hier überführen wir nun ein spezielles Problem auf eine abstrakte Ebene. Einfache Sachverhalte, die mit diesem Verfahren gelöst werden können, sind z.B.

1. Bei 3 Leuten haben mind. zwei das gleiche Geschlecht
2. Bei 13 Leuten haben mind. zwei im gleichen Monat Geburtstag
3. Bei 37 Leuten haben mind. 4 im gleichen Monat Geburtstag

Was sind die Argumente beispielsweise im ersten Beispiel? Jeder kann nur entweder in die Kategorie männlich oder weiblich fallen. Nachdem die eine Kategorie mit der ersten Person belegt ist, bleibt für die zweite nur die andere Kategorie, wenn nicht hier schon beide das gleiche Geschlecht haben sollten. Spätestens beim dritten muss aber eine Kategorie doppelt belegt sein. Im zweiten und dritten Beispiel gibt es 12 Kategorien (die Monate). Verteilt man 13 Elemente muss auch hier wieder eine Kategorie doppelt belegt sein. Bei 36 Personen schafft man es, dass jede Kategorie gerade 3 Elemente enthält, ab der 37. Person muss eine Kategorie 4 Elemente enthalten. Dieses Prinzip wird nun verallgemeinert:

Algorithmus 1 *Verteilt man n+1 oder mehr Elemente auf n Kategorien, so gibt es eine Kategorie mit mindestens zwei Elementen. Verteilt man mehr als k·n - also $k \cdot n + 1$ oder mehr - Elemente. So exisitiert eine Kategorie mit mehr als k Elementen.*

Rein Mathematisch ist das Verfahren wie folgt darstellbar:

Satz 2 *Seien X und Y endliche Mengen. Ist f: $X \to Y$ eine Abbildung und gilt $|X| > |Y|$, so gibt es ein y aus Y mit*

$$|f^{-1}(y)| \geq 2$$

Allgemeiner:Seien X und Y endliche Mengen. Ist f: $X \to Y$ eine Abbildung, so gibt es ein y aus Y mit

$$|f^{-1}(y)| \geq \left\lceil \frac{|X|}{|Y|} \right\rceil$$

Dabei sind die Elemente aus X die betrachteten Objekte, die Elemente aus Y die möglichen Kategorien, die diesen Elementen zugeordnet werden können.

Bem.:

1. Dies ist eine reine Existenzaussage. Wir wissen weder welches die Kategorie ist, noch wieviele Elemente exakt in dieser Kategorie liegen.

2. Die Kategorien werden auch Schubladen genannt, daher das Schubfach- oder Schubladenprinzip. Ebenfalls gibt es den Namen Taubenschlagprinzip - wegen der Aussage: "Wenn man mehr als n Tauben in n Käfige steckt, dann gibt es einen Käfig mit mind. 2 Tauben"

Wenden wir diese Regel nun einmal formal auf obige Beispiele an:

1. Bei 3 Leuten haben mind. zwei das gleiche Geschlecht

Die Schubladen (Kategorien) sind n=2 (männlich oder weiblich). Wenn wir mehr als n=2 Personen - also ab 3 Personen - auf die beiden Schubladen verteilen, erhalten wir eine Schublade mit mindestens 2 Elementen.

2. Bei 13 Leuten haben mind. zwei im gleichen Monat Geburtstag

n=12 Kategorien (die Monate) - ab 13 Personen haben zwei im gleichen Monat Geburtstag

3. Bei 37 Leuten haben mind. 4 im gleichen Monat Geburtstag

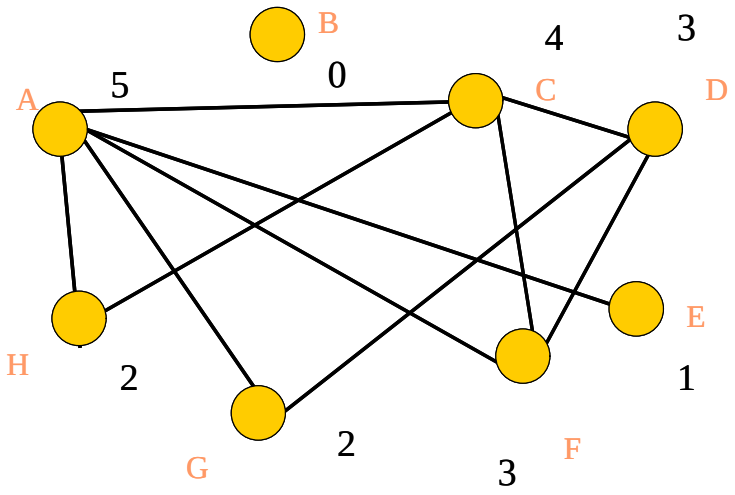
n=12 Kateorien (Monate). Verteilen wir mehr als $n \cdot k = 36$, also k=3, Elemente, so exisitert eine Kategorie mit mehr als $k = 3$, also mindestens 4 Elementen.

Anwendungen:

1. Ein Zerstreuter Dozent hat 10 Paar graue, 10 paar braune und 10 paar blaue Socken im Schrank. Wie viele Socken muss er herausnehmen, um ein passendes Paar zu haben?

Die Kategorien sind die Farben Grau, Braun, Blau. Wir müssen also 4 Elemente (Socken) verteilen, um eine Kategorie mit 2 Elementen zu haben. Wir wissen dann jedoch immer noch, nicht welche Farbe der Dozent tragen wird.

2. Auf einer Feier mit 8 Wissenschaftlern werden paarweise Visitenkarten ausgetauscht (oder auch Hände geschüttelt). Geht es, dass am Ende alle 8 Personen eine verschiedene Anzahl von Visitenkarten haben?



Bezeichnen wir mit den Kategorien die Anzahl der Karten, so ist bei 8 Leuten möglich, dass zwischen 0 und 7 Karten getauscht werden. Jede Person gehört nun zu einer Kategorie (macht einen Strich in einer Kategorie), so dass 8 Striche auf 8 Kategorien verteilt werden müssen:

0 Karten	|
1 Karte	|
2 Karten	||
3 Karten	||
4 Karten	|
5 Karten	|
6 Karten	
7 Karten	

Theoretisch wäre es also möglich, dass jede Kategorie genau einen Strich erhält. Dies geht jedoch nicht, da, wenn einer mit allen tauscht (ein Strich bei "7 Karten"), die Rubrik 0 Karten leer sein muss, da jeder mit demjenigen in der Kategorie "7 Karten" getauscht haben. Gibt es umgekehrt einen Strich bei 0 Karten, so kann keiner in der Rubrik "7 Karten" sein. Insgesamt werden also die 8 Elemente auf 7 Kategorien verteilt und gemäß Schubfachprinzip muss damit

eine Kategorie mindestens 2 Striche enthalten. Daher kann es nicht aufgehen, dass alle 8 Personen eine verschiedene Anzahl von Visitenkarten haben.

Natürlich lässt sich die Argumentation bei einer beliebigen Anzahl Personen anwenden. Also auch bei einer Abi-Fete mit 113 Personen werden nachher nicht alle eine unterschiedliche Anzahl von Visitenkarten haben.

3. Wählen Sie aus den Zahlen von 1 bis 2n eine mehr als die Hälfte - also n+1 - Zahlen aus, so dass keine die andere teilt.

Wir betrachten die Zahlen von 1 bis 2n und wählen n+1 Zahlen a(1), a(2), ..., a(n+1) hieraus aus. Jetzt zerlegen wir die Zahlen in ihre geraden und ungeraden Anteile:

$$a(i) = 2^{k_i} \cdot u_i \tag{1.3}$$

mit u(i) ungerade und zwischen 1 und 2n

z.B.: 36=2^2·9, also u(i) = 9

Damit erhalten wir n+1 ungerade Anteile.

Wieviele ungeraden Zahlen gibt es von 1 bis 2n? n Stück. Diese bilden die Kategorien. Verteilen wir nun n+1 Zahlen, so gibt es zwei mit dem gleichen ungeraden Anteil u.

Seien diese Zahlen $a(i)$ und $a(j)$ mit (ohne Einschränkung) $a(i) < a(j)$ und damit $k_i < k_j$ also

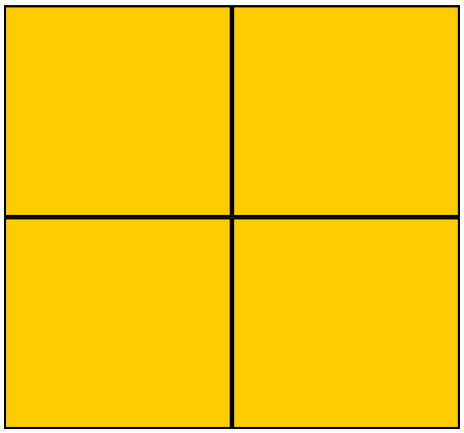
$$2^{k_i} \cdot u \text{ und } 2^{k_j} \cdot u \tag{1.4}$$

dann teilt aber $a(i)$ $a(j)$, da

$$\begin{aligned} a(j) &= 2^{k_j} \cdot u = 2^{k_j - k_i + k_i} \cdot u = 2^{k_j - k_i} \cdot 2^{k_i} \cdot u \\ &= 2^{k_j - k_i} \cdot a(i) \end{aligned}$$

4. In ein Quadrat der Seitenlänge 2 cm sollen Punkte mit einem Abstand $d > \sqrt{2}$ eingezeichnet werden. Wieviel Punkte können maximal eingezeichnet werden?

Unterteilen wir das Quadrat in 4 Quadrate der Seitenlänge 1:

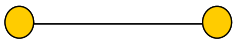


In jedem dieser Teilquadrate ist der Abstand kleiner als $\sqrt{2}$. Bei vier Punkten (z.B. auf den Ecken) ist die Bedingung erfüllt, bei 5 Punkten liegen in mind. einem Teilquadrat mind. 2 Punkte und damit ist deren Abstand $\leq \sqrt{2}$. Es können also maximal 4 Punkte gewählt werden.

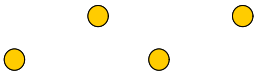
1.3.1 Cliquen

Eine n-Clique ist eine Gruppe von n Personen, bei der alle Mitglieder miteinander verbunden sind.

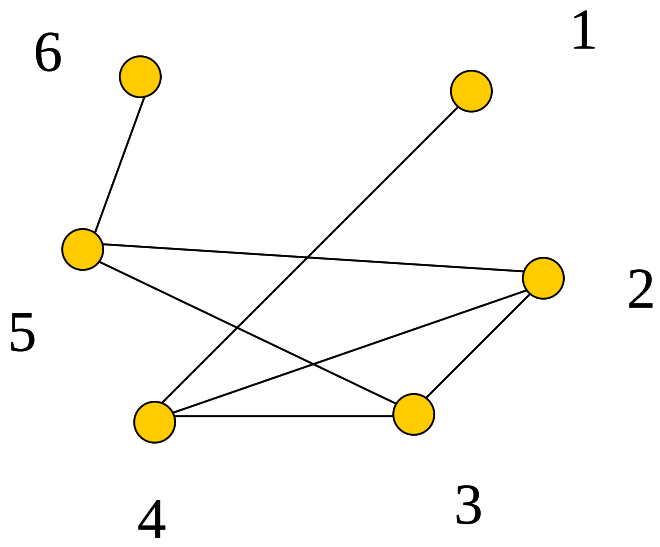
z.B. Beim Visitenkartentausch entstehen 2-er Cliquen



Sind zwei oder mehr Elemente nicht verbunden, so spricht man von Anti-Cliquen, z.B. 4-er Anti-Cliquen.



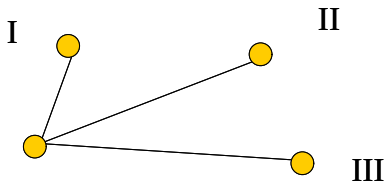
Es interessieren nun Untercliquen, also wir betrachten eine Teilmengen der Punkte mit den Verbindungen zu den verbleibenden anderen Punkten.So enthält folgende Konstellation z.B. eine 3-er Anticlique in (1,2,6) und eine 3-er Clique in (2,3,5).



Existieren bei 6 Elementen denn immer 3-er Cliquen oder Anti-Cliquen? Hierzu bemühen wir wieder das Schubladenprinzip.

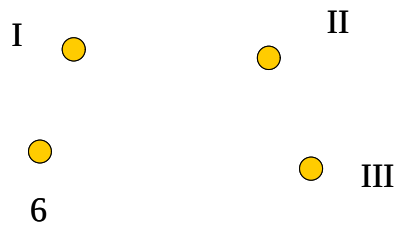
Wir betrachten ein festes Element (z.B. Punkt 6) und dann exisiteren 5 verbleibende Punkte. Diese werden aufgeteilt in die beiden Kategorien "Ist mit Punkt 6 verbunden" und "Ist mit Punkt 6 nicht verbunden". Gemäß Schubladenprinzip existiert dann eine Kategorie mit mindestens 3 Elementen.

Fall 1: Ist mit 6 verbunden enthält mind. 3 Elemente - Nennen wir Sie I,II und III:



Nun gibt es zwei Fälle:
A) Zwei der Punkte I,II,III sind miteinander verbunden; z.B. I und II. Dann bilden (6,I,II) eine 3-er Clique
B) I,II und III sind alle paarweise nicht verbunden. Dann bilden (I,II,III) eine 3-er Anti-Clique

Fall 2: Ist mit 6 nicht verbunden enthält mind. 3 Elemente - Nennen wir Sie ebenfalls I,II und III:



Auch hier gibt es zwei Fälle:

A) Zwei der Punkte I,II,III sind miteinander nicht verbunden; z.B. I und II. Dann bilden (6,I,II) eine 3-er Anti-Clique

B) I,II und III sind alle paarweise verbunden. Dann bilden (I,II,III) eine 3-er Clique

Insgesamt: Es existiert bei 6 Elementen immer eine 3-er Clique oder 3-er Anti-Clique.

1.3.2 Das verallgemeinerte Schubladenprinzip

Verteilen wir "unendlich viele" Elemente auf endlich viele Schubladen, so ergibt sich das eine Schublade mit unendlich vielen Elementen existieren muss.

Z.B. Wir betrachten die Reihen {1,5,9,13,17,21,...} und {3,7,11,15,19,23}. Gibt es dort unendlich viele Primzahlen? Die einen Zahlen sind die ungeraden Zahlen, die bei der Division den Rest 1 lassen, die anderen die den Rest 3 lassen. Damit fällt jede ungerade Zahl in eine der beiden Schubladen. Wir zeigen später noch, daß es unendlich viele (bis auf die 2 natürlich ungerade) Primzahlen gibt. Daher muss eine der Schubladen unendlich viele Elemente enthalten. (Wir werden darüber hinaus zeigen, dass beide unendlich viele Primzahlen enthalten).

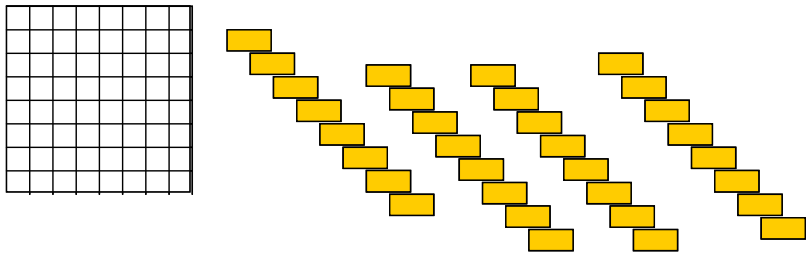
Übung : Ein Vater hat seinen Schwiegersohn zu Besuch. Vor der Heimreise möchte er diesem 3 Flaschen Wein mit nach Hause geben. Er geht in seinen Weinkeller, in dem er 7 Sorten Wein hat, die wild gemischt in Seinen Weinregalen liegen. Als er unten im Weinkeller ist, springt die Sicherung heraus. Er hat einen Korb dabei. Wieviele Flaschen muss er nehmen, damit er oben angekommen mindestens 3 gleiche Flaschen hat?

1.4 Färbungen

Motivation:

Wir betrachten ein 8x8 Schachbrett und Dominosteine,welche je genau 2 Felder des Schachbrettes überdecken.

Frage 1: Kann man das Schachbrett (lückenlos und ohne Überschneidung) mit den Dominos überdecken? Wenn ja mit wievielen ?

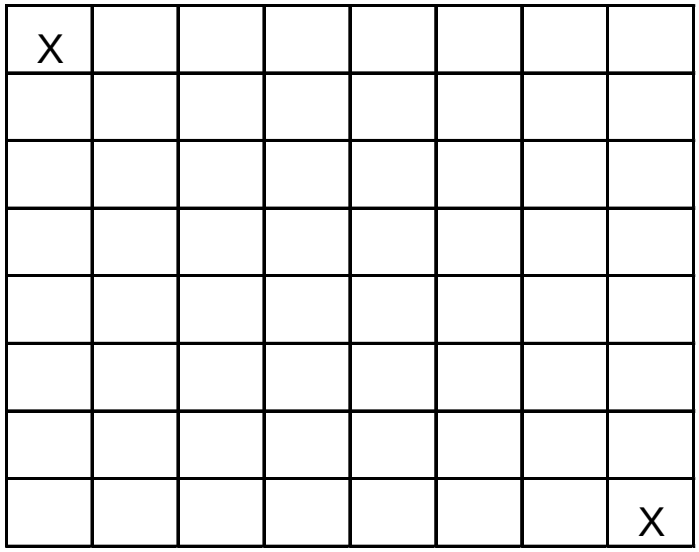


Geht offensichtlich mit 32 Steinen.

Was ist wenn wir die linke obere Ecke abschneiden? Was wenn links oben und links unten?

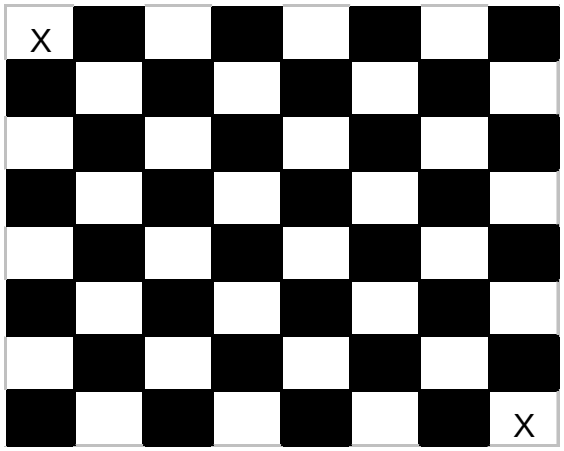
Im ersten Fall verbleiben 63 Felder. 31 Domino-Steine bedecken 62 Felder, 32 64 Felder. Dies kann also nicht gehen.
Im zweiten Fall geht es wiederum.

Wir betrachten nun



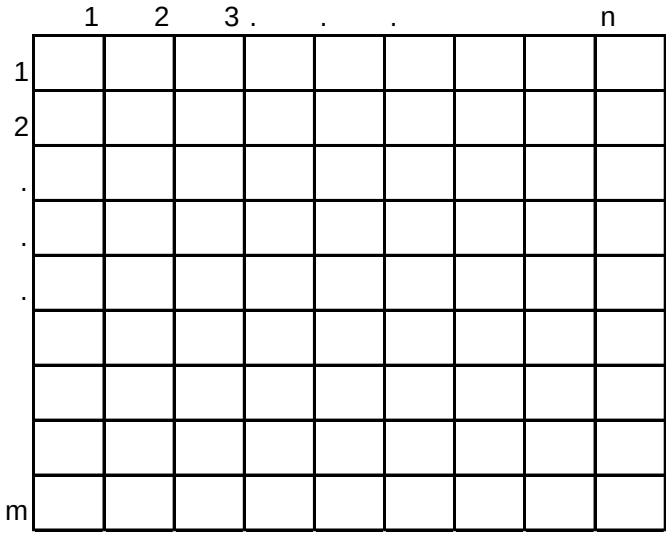
Lässt sich dieses Schachbrett durch die Dominosteine lückenlos überdecken? Die Versuche zeigen: Es scheint nicht zu gehen. Aber warum?

Bisher haben wir das Schachbrett nur als 8x8-Brett betrachtet. Schauen wir uns die Färbung des Brettes an:



und sehen: Wir haben zwei weisse Felder abgeschnitten. Jeder Domino-Stein überdeckt aber ein schwarzes und ein weisses Feld, 31 Steine also 31 schwarze und 31 weisse Felder, das Brett hat jedoch 30 schwarze und 32 weisse Felder. Es kann also nicht aufgehen.

Betrachten wir nun ein $m \times n$ Brett und ein $1 \times a-$Domino.



Einfach zu sehen: Ein $m \times n$-Schachbrett kann mit einem $1 \times$a Domino lückenlos überdeckt werden, wenn a m oder n teilt.

Aber gilt auch die Umkehrung? Betrachte ein $1 \times 4-$Domino auf einem $10 \times 10-$Schachbrett.

Wir färben das Brett mit den Farben (der Einfachheit halber) 1,2,3,4 wie folgt:

1	2	3	4	1	2	3	4	1	2
2	3	4	1	2	3	4	1	2	3
3	4	1	2	3	4	1	2	3	4
4	1	2	3	4	1	2	3	4	1
1	2	3	4	1	2	3	4	1	2
2	3	4	1	2	3	4	1	2	3
3	4	1	2	3	4	1	2	3	4
4	1	2	3	4	1	2	3	4	1
1	2	3	4	1	2	3	4	1	2
2	3	4	1	2	3	4	1	2	3

Wir sehen:
Jeder Dominostein überdeckt die Zahlen (Farben) von 1 bis 4
Also: Wenn es eine lückenlose Überdeckung gibt, so muss jede Zahl gleich oft vorkommen

Beginnen wir das Brett zu überdecken:
Wir sehen: Die Farbe 2 kommt am meisten vor, 4 seltener.

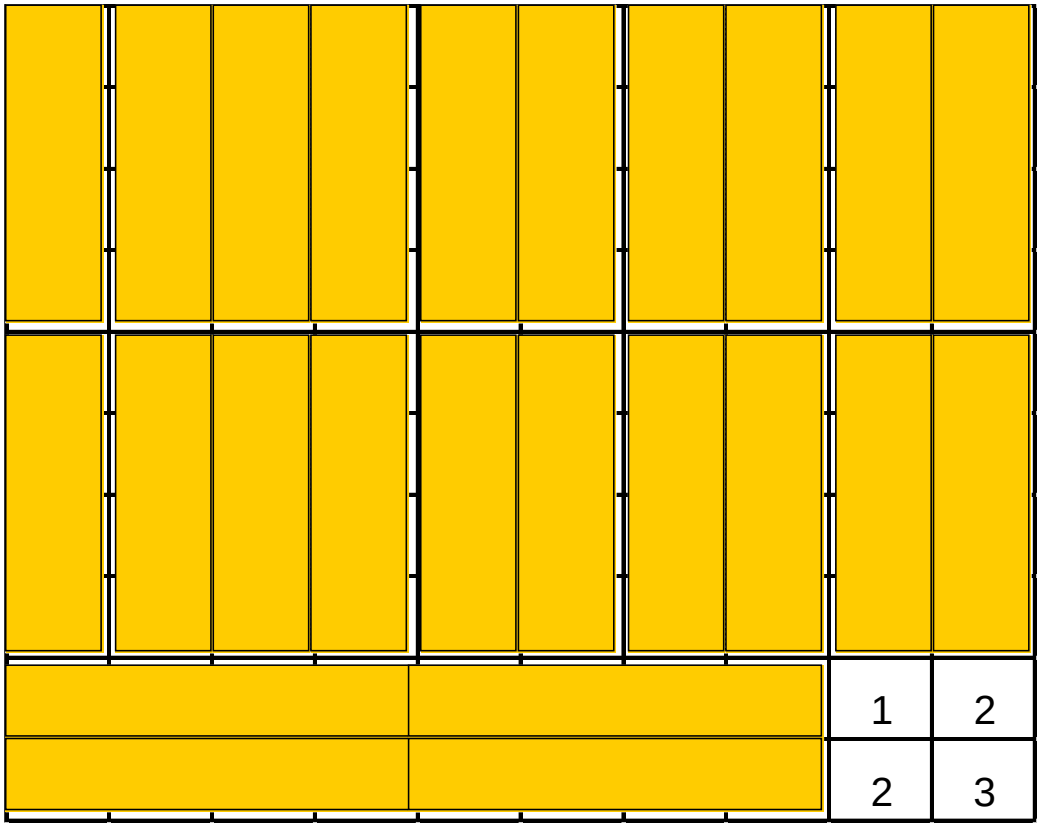
Nun allgemein: Wir zeigen:Wir zeigen: Teilt a weder m noch n, so existiert keine lückenlose Überdeckung.

Also: a teilt weder m noch n, d.h.

$$m = ka + b \text{ mit } b < a \tag{1.5}$$
$$n = la + c \text{ mit } c < a \tag{1.6}$$

Ohne Einschränkung sei $c \geq b$ (sonst drehen wir das Brett).
Wenn eine solche Überdeckung existiert, so kommen alle Farben gleich oft vor.

Wie sieht das Brett aus?


1
2
2
3

1	...	a	1	...	a	1	...	c
...	a	1	...	a	1	...	...	
a	1	...	a	1	...	...	...	
1	...	a	1	...	a	1	...	
...	a	1	...	a	1	...		
a	1	...	a	1	...	a		
1	...	a	1	...	a	1	...	c
...	a	1	...	a	1	...	...	...
b	b+1	...	1	...	...	b	...	...

Bis auf die rechte untere Ecke kommen alle Farben gleich oft vor !Schauen wir uns diese an:

1		...	...	...	c
2		...	...	c	c+1
...			c	c+1	
b		c	c+1		

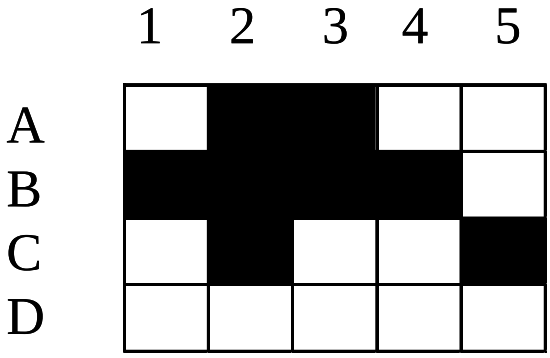
Wir sehen: Die Farbe c+1 ($\leq$a) kommt einmal weniger vor als c. Also kann keine Färbung existieren.

Insgesamt also:Ein m$\times$n-Schachbrett kann von 1$\times$a-Dominos genau dann (und dann auf triviale Art) überdeckt werden, wenn a entweder m oder n teilt.

1.4.1 Monochromatische Rechtecke

Hintergrund ist nun die Färbung der Ebene mit zwei oder mehr Farben. Dies ist - wie Färben generell - nur ein Synonym für zwei oder mehr spezielle Eigenschaften. Die Färbung kann nun als Färbung von Punkten - Alle Punkte erhalten eine Farbe - in der Ebene betrachtet werden.

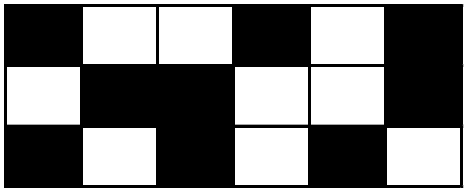
Wir betrachten nun zunächst beliebige Färbungen mit zwei Farben - der Einfachheit halber schwarz und weiß - eines $m \times n$-Schachbrettes. Z.B.



Definition 3 *Ein Rechteck (mind. 2×2), bei dem alle 4 Ecken die gleiche Farbe haben, heißt monochromatisches (einfarbiges) Rechteck*

Ein Rechteck kann dabei dirch die Koordinaten zweier gegenüber liegenden Ecken angegeben werden. Im obigen Beispiel existieren zahlreiche Monochromatische Rechtecke, z.B. A1-C4, A1-D4, A1-D5,A4-D5, C1-D3,C1-D4, C3-D4, A2-B3

Aber: Existieren immer monochromatische Rechtecke? Betrachte folgendes $3 \times 6-$Brett

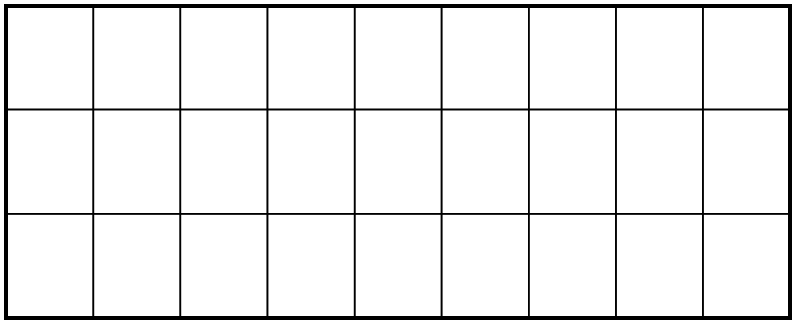


Dort exisitert offensichtlich kein solches Rechteck.Was ist, wenn wir die Dimension auf 3×7 erhöhen? Gibt es eine Färbung ohne monochromatische Rechtecke?

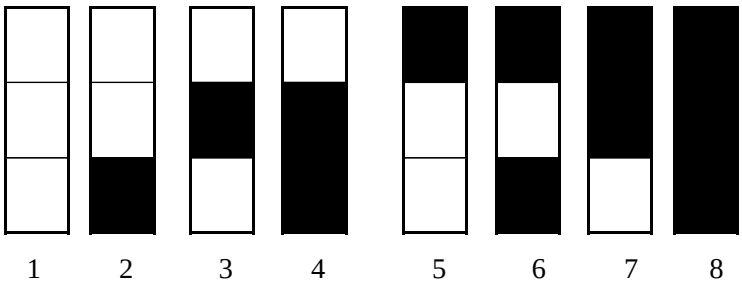
Durch Ausprobieren scheinen wir keine Lösung zu finden. Zum Beweis betrachten wir zunächst ein 3×9-Brett.

Lemma 4 *Es gilt: In einem 3×9-Schachbrett existiert immer ein monochromatisches Rechteck. Damit auch in jedem $m \times n$-Schachbrett mit $m \geq 3$ und $n \geq 9$*

Betrachten wir zunächst das Brett:



Die Spalten dieses Brettes können folgende 8 Färbungen annehmen:



Verteilen wir die 9 Spalten des 3×9-Brettes auf die 8 verschiedenen Spaltenmöglichkeiten, so muß gemäß Schubladenprinzip ein Spaltentyp doppelt vorkommen.Wenn aber einer doppelt vorkommt, so existiert immer ein monochromatisches Rechteck, denn innerhalb eines Spaltentyps kommt immer eine Farbe doppelt vor (ebenfalls gemäß Schubladenprinzip). Diese doppelte Farbe bildet mit der zweiten gleichen Spalte die Ecken des monochromatischen Rechtecks:

Wir betrachten nun wieder unser 3×7−Brett. Würde die rein schwarze Spalte (8) vorkommen, so müssen alle anderen Spalten weniger als 2 schwarze Elemente haben, d.h.vom Typ 1,2,3 oder 5 sein. Dann haben wir aber nur 5 verschiedene Spaltentypen und damit kommt eine doppelt vor (Schubladenprinzip) und es existiert ein monochromat. Rechteck Die gleiche Argumentation gilt, falls die rein weiße Spalte vorkommen würde.

Daher:Bei einem 3x7-Brett ohne monochrom. Rechteck könnendie rein schwarze und die rein weiße Spalte nicht vorkommen.Alle Spalten sind somit vom Typ

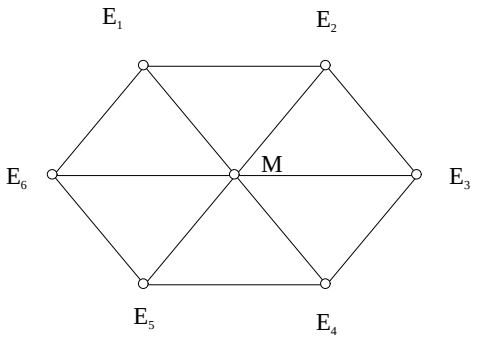
2 bis 7 (6 verschiedene). Da wir jedoch 7 Spalten haben, muß hiervon eine Spalte doppelt vorkommen und es existiert ein monochromat. Rechteck.

Also: Bei einem 3x7-Schachbrett existiert immer ein monochromat. Rechteck

Ähnlich lässt sich zeigen: Färben wir die Ebene mit 3 Farben, so existieren 2 Punkte im Abstand 1 mit gleicher Farbe. Bew.: Wir betrachten einen Punkt und nennen die Farbe Rot. Betrachten wir ein gleichseitiges Dreieck im Abstand 1, so sind wir fertig wenn einer dieser Punkte ebenfalls die Farbe Rot hat. Also bleibt noch die Variante einmal Blau, einmal Gelb. Betrachten wir nun ein gleichseitiges Dreieck dieser beiden Punkte in die entgegengesetze Richtung, so muss dieser Punkt ebenfalls Rot sein. Dieser Punkt hat den Abstand d. Nun rotieren wir dieses Dreieck um den ersten roten Punkt. Insgesamt muss sich ein Kreis mit Radius d ergeben mit nur roten Punkten. Auf einem Kreisrand sind aber sicher auch zwei Punkte im Abstand 1.

Satz 5 *Die Punkte der Ebene seien mit 2 Farben gefärbt. Dann gibt es ein gleichseitiges Dreieck, dessen Ecke alle die gleiche Farbe haben. (Monochromatisches gleichseitiges Dreieck)*

Beweis: Wir betrachten das folgende regelmässige Sechseck mit weissem Mittelpunkt:



und betrachten nun die äusseren Punkte.

Bem.: Haben alle geraden (oder ungeraden) Indizes die gleiche Farbe, so ist ein solches Dreieck gefunden.

Fall 1: Es gibt 4 oder mehr weisse Punkte auf dem Rand: Dann liegen 2 weisse nebeneinander und diese bilden mit dem Mittelpunkt ein monochromatisches gleichseitiges Dreieck.

Fall2: Es gibt 0 oder 1 weissen Punkt, also 5 oder 6 schwarze. Dann liegen entweder auf allen ungeraden Indizes oder auf allen geraden Indizes nur schwarze Punkte. Diese ungeraden/geraden Ecken bilden das monochromatische gleichseitige Dreieck

Fall 3: Es gibt 3 weisse

3.1: zwei davon liegen nebeneinander: Dann bilden diese mit dem Mittelpunkt ein monochromatisches gleichseitiges Dreieck.

3.2: keine zwei liegen nebeneinander: Dann liegen die drei weissen auf geraden, die drei schwarzen auf ungeraden Indizes (oder umgekehrt). Diese bilden dann jeweils ein monochromatisches gleichseitiges Dreieck.

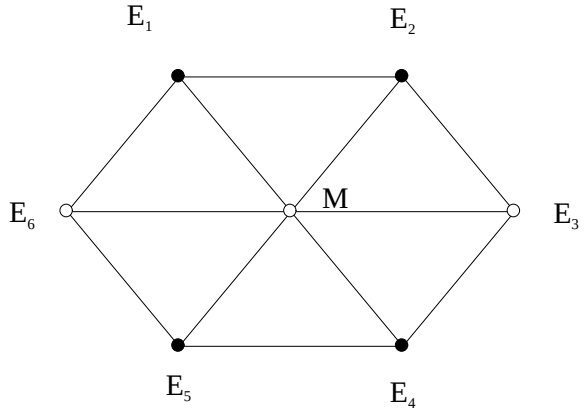
Fall 4: Es gibt 4 schwarze und 2 weisse Ecken:

4.1 Zwei weisse Ecken liegen nebeneinander. Dann bilden diese mit dem Mittelpunkt ein monochromatisches gleichseitiges Dreieck

4.2 Zwei weisse Ecken liegen beide auf geradem oder ungeradem Index. Dann liegen auf geradem oder ungeradem Index ausschliesslich schwarze und diese bilden das monochromatische gleichseitige Dreieck.

(und jetzt der im Buch nicht betrachtete Fall:)

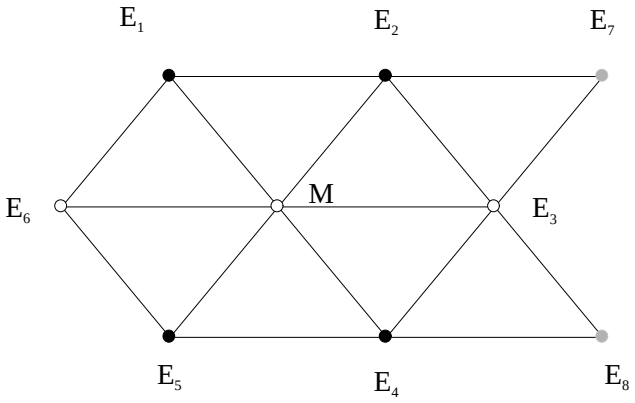
4.3 Zwei weisse liegen nicht nebeneinander jedoch einer auf einem geraden, einer auf einem ungeraden Index. Bis auf Symmetrie ist dies genau bei einem Konstrukt der Fall:



(Allgemein hat weiss die Ecken E_k und E_{k+3})

Dann ist hierin kein monochromatisches gleichseitiges Dreieck enthalten.

Wir erweitern nun das Sechseck nach rechts durch zwei weitere Punkte E_7 und E_8 :



Fall A: Wäre E_7 schwarz so bilden E_1,E_4,E_7 ein monochromatisches gleichseitiges Dreieck.

Fall B: Wäre E_8 schwarz so bilden E_2,E_5,E_8 ein monochromatisches gleichseitiges Dreieck.

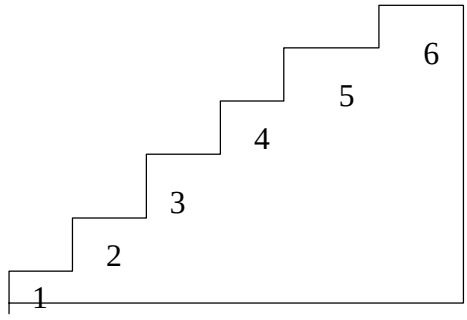
Fall C: Wären beide nicht schwarz - also weiss - so bilden sie - wie im Sechseck, nun um die Mitte E_3 - ein monochromatisches gleichseitiges Dreieck mit M (M,E_7,E_8). Dies ist ja der gleiche Fall wie der Fall nur ungerader oder gerader Ecken im Sechseck.

Beweis fertig.

1.5 Fibonacci-Zahlen

Ein Briefträger muß zu einem Haus 6 Stufen hochgehen. Die erste Stufe nimmt er auf jeden Fall, danach kann er entweder eine oder zwei Stufen auf einmal gehen. Auf wieviele Arten kann er an der Haustür ankommen?

Wieviele Möglichkeiten gibt es bei 3,4,5 und 7 Stufen?

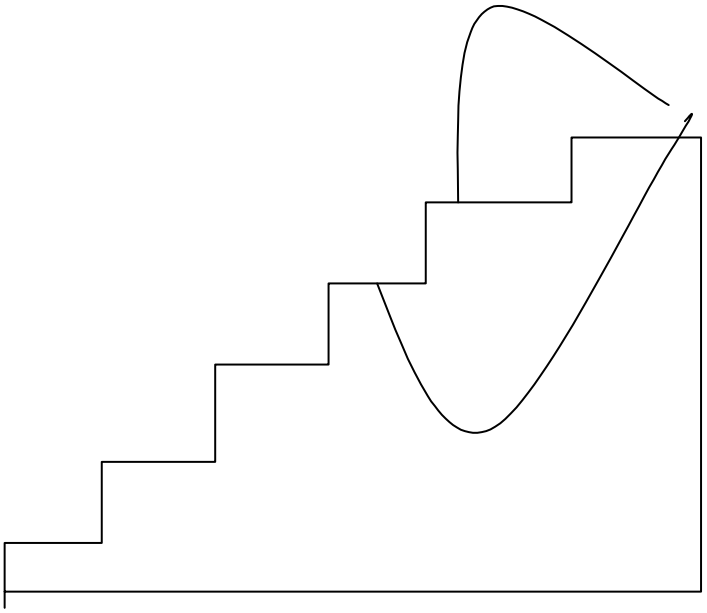


z.B. 1,1,1,1,1,1

Wir zählen die Möglichkeiten:
1,1,1,1,1,1
1,1,1,1,2
1,1,2,1,1
1,1,2,2
1,1,1,2,1
1,2,2,1
1,2,1,2
1,2,1,1,1
(8 Möglichkeiten)

Wie wir das bereits kennen, versuchen wir es nun strukturiert:
f(n) bezeichnet die Anzahl der Möglichkeiten bei n-Stufen
Also hier: f(6)=8
f(1)=1, f(2)=1, f(3)=2, f(4)=3, f(5)=5

Die Lösung besteht darin, sich nur den letzten Schritt anzuschauen. Wie kann der Briefträger zur n-ten Stufe gelangen?



Also entweder er kommt von der n-2-ten Stufe in einem Zweierschritt oder von der n-1-ten Stufe in einem Schritt.

Die eine Möglichkeit besteht darin alle Möglichkeiten bis zur n-2-ten Stufe - f(n-2) Stück - um eine "2" zu ergänzen. Die andere alle Möglichkeiten bis zur n-1-ten Stufe - f(n-1) Stück - um eine "1" zu ergänzen. Die neu erzeugten Möglichkeiten unterscheiden sich auf jeden Fall in der letzten Stelle. Man gewinnt

also verschiedene Möglichkeiten und vergisst auch keine, da es nur die beiden Möglichkeiten gibt, von der letzten oder vorletzten zu kommen.

Insgesamt:

$$f(n) = f(n-1) + f(n-2)$$

mit

$$f(1) = f(2) = 1 \tag{1.7}$$

Damit ist $f(3) = 2, f(4) = 3, f(5) = 5, f(6) = 8$. Also gibt es 8 Möglichkeiten auf die oberste Stufe zu gelangen.

Häufig wird die Reihe bei n=0 begonnen. Dann ist die Folge $f(n)$ gegeben durch

$$\begin{aligned} f(0) &= 1 \\ f(1) &= 1 \\ f(2) &= 2 \\ f(3) &= 3 \\ f(4) &= 5 \\ f(5) &= 8 \\ f(6) &= 13 \end{aligned}$$

Dies führt zur folgenden Definition:

Definition 6 *Die Zahlen, definiert durch* $f(0) = f(1) = 1$ *und*

$$f(n) = f(n-1) + f(n-2) \tag{1.8}$$

heissen Fibonacci-Zahlen.

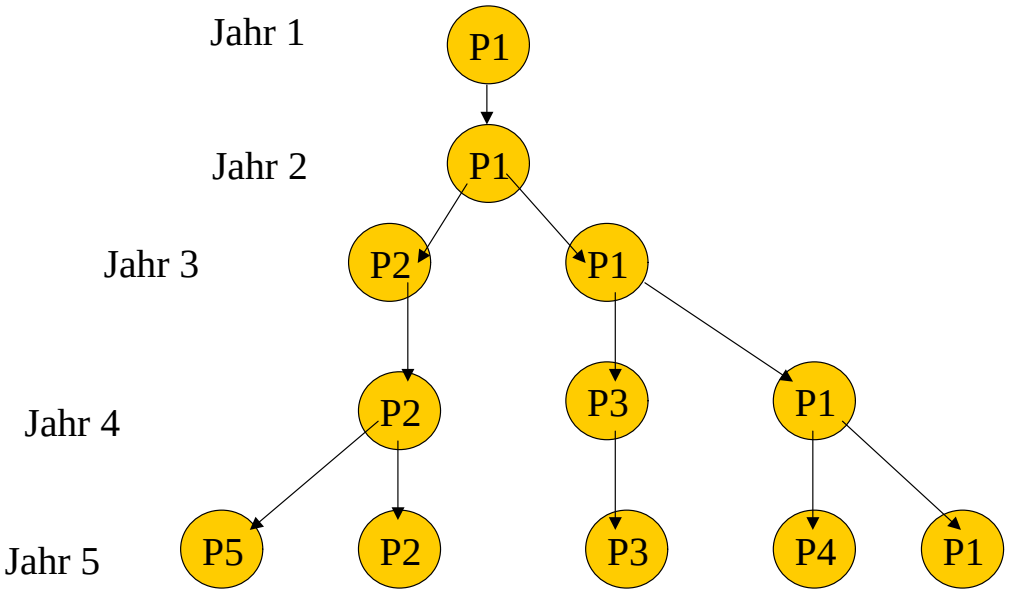
Im Folgenden schreiben wir statt $f(n)$ nun auch kurz $f_{n.}$

Weitere Anwendungen:Wir betrachten die Vermehrung von Kaninchen:

1. Es existiert zu Beginn 1 Kaninchenpaar. Dieses ist im ersten Jahr nicht zeugungsfähig,

2. Im zweiten Jahr wird ein Nachwuchspaar geboren. Allen Nachwuchspaaren gehts genauso. Kein Tier stirbt.

Die Entwicklung ist dann



Im n-ten Jahr gilt, das sich der Bestand im n-ten Jahr f_n zusammensetzt aus den Kaninchenpaaren des Vorjahres (f_{n-1}) plus den Neugeborenen. Diese entsprechen aber gerade genau der Anzahl Paare die zum Zeitpunkt $n-2$ gelebt haben, da jeder von diesen genau 1 Nachwuchspaar beisteuert. Also die Anzahl Neugeborener ist f_{n-2}. Insgesamt erhalten wir

$$f_n = f_{n-1} + f_{n-2}$$

und aus der Startbedingung $f_0 = 1$ ergibt sich auch $f_1 = 1$ und damit wieder die Fibonacci-Folge.

Erweiterungen:

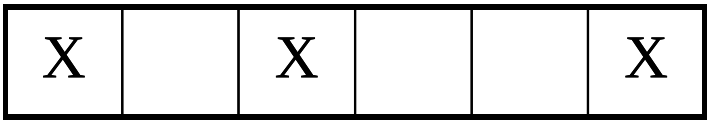
Würde jedes Kaninchenpaar 2 Nachwuchspaare ab dem zweiten Jahr gebären, so wäre die Vorschrift

$$f_n = f_{n-1} + 2 \cdot f_{n-2}$$

Würden 20 % eines Jahrgangs im Folgejahr absterben, so lautet die Gleichung

$$f_n = f_{n-1} + 2 \cdot f_{n-2} - 0,2 \cdot f_{n-1}$$

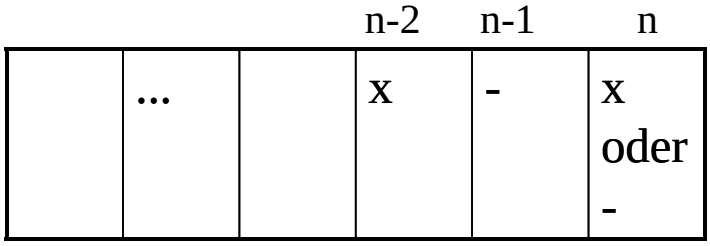
Anwendung: Wir betrachten eine Leiste mit n Stellen, bei der Sie in jede Stelle ein "X" einsetzen können oder diese leer lassen können. Auf wieviele Arten können Sie die "X"-e einsetzen, so dass nicht zwei "X" nebeneinander stehen? Z.B.



Wir bezeichnen die Möglichkeiten bei einer n-elementigen Leiste wiederum mit f_n. Offensichtlich gilt: $f_1 = 2$ (Leer oder "X"), $f_2 = 3$ (Leer,Leer),(Leer,X)(X,Leer)

Wir erahnen ähnlich wie beim Briefträger-Stufen-Problem das wir uns nur "das Ende" anschauen müssen. Schauen wir auf das vorletzte Feld n-1:

Möglichkeit 1: Dieses Feld n -1 ist leer.



Dann gibt es für das lezte Feld noch die zwei Möglichkeiten ein "X" einzusetzen oder dieses leer zu lassen. Aber auf wieviele Arten konnte zuvor der Fall eintreten, dass dort ein leeres Feld steht. Hierzu brauchen wir nur eine gültige Kombination der ersten n-2 Felder um ein Leerfeld zu erweitern. Umgekehrt lässt sich jede gültige Kombination durch Wegnahme des letzten leeren Feldes auf eine gültige Kombination der n-2 Felder eindeutig reduzieren. Daher gibt es

$$2 \cdot f_{n-2}$$

Möglichkeiten mit einer Leerstelle an Position n-1.

Möglichkeit 2: Das Feld n-1 enthält ein "X". Dann muß das Feld n leer sein. Die Anzahl der Möglichkeiten, das dort ein "x" steht erhalten wir aber, in dem wir für die Gesamtzahl gültiger Kombinationen einer n-1 - Leiste (f_{n-1}) diejenigen rausnehmen, die an der Position n-1 leer waren. Diese sind aber genau die f_{n-2} Stück aus Variante 1.

Insgesamt für diesen Fall

$$f_{n-1} - f_{n-2}$$

solcher Möglichkeiten.

Insgesamt ergibt sich durch Addition dieser beiden Fälle

$$\begin{aligned} f_n &= f_{n-1} - f_{n-2} + 2 \cdot f_{n-2} \\ &= f_{n-1} + f_{n-2} \end{aligned}$$

also wiederum eine Fibonacci-Folge.

Aber wie groß ist denn $f(30)$? Zum einen kann mühsam das Bildungsgesetz bis n=30 berechnet werden.

Hilfreicher wäre also die direkte Berechnung von f_n.

Setzen wir versuchsweise $f_n = q^n$ ein so erhalten wir

$$q^n = q^{n-1} + q^{n-2} \tag{1.9}$$

Dividieren wir diese Gleichung durch q^{n-2} so erhalten wir

$$q^2 = q + 1$$

Dieses führt zur quadratischen Gleichung

$$q^2 - q - 1 = 0$$

mit den Lösungen

$$\begin{aligned} q_{1,2} &= \frac{1}{4} \pm \sqrt{\frac{1}{4} + 1} && (1.10) \\ &= \frac{1 \pm \sqrt{5}}{2} \\ (&= \frac{-1 \pm \sqrt{5}}{2} + 1) && (1.11) \end{aligned}$$

Die Zahl $\frac{1+\sqrt{5}}{2}$ heißt der "goldene Schnitt". Wir haben also gezeigt, $u_n = q_1^n$ und $v_n = q_2^n$ erfüllen die Fibonacci Gleichung $u_n = u_{n-1} + u_{n-2}$ bzw. $v_n = v_{n-1} + v_{n-2}$. Welches jedoch die Lösung ist, hängt nun von den Anfangsbedingungen ab. Hierzu betrachten wir eine beliebige Kombination $f_n = a \cdot u_n + b \cdot v_n$. Auch für diese gilt:

$$\begin{aligned} f_n &= a \cdot u_n + b \cdot v_n \\ &= a \cdot (u_{n-1} + u_{n-2}) + b \cdot (v_{n-1} + v_{n-2}) \\ &= a \cdot u_{n-1} + b \cdot v_{n-1} + a \cdot u_{n-2} + b \cdot v_{n-2} \\ &= f_{n-1} + f_{n-2} \end{aligned}$$

Also: auch jede beliebige Kombination $f_n = a \cdot u_n + b \cdot v_n. = a \cdot \left(\frac{1+\sqrt{5}}{2}\right)^n +$

$b \cdot \left(\frac{1-\sqrt{5}}{2}\right)^n$ erfüllt die Fibonacci-Gleichung. Die Zahlen a und b können nun so gewählt werden, dass die Anfangsbedingungen erfüllt sind.

Beispiel: Lösung der Fibonacci-Gleichung mit $f_0 = f_1 = 1$:

$$\begin{aligned} f_0 &= a + b = 1 \\ f_1 &= a \cdot \left(\frac{1+\sqrt{5}}{2}\right) + b \cdot \left(\frac{1-\sqrt{5}}{2}\right) = 1 \end{aligned}$$

Setzen wir aus der ersten Gleichung $b = 1 - a$ in die zweite ein:

$$\begin{aligned} a \cdot \left(\frac{1+\sqrt{5}}{2}\right) + (1-a) \cdot \left(\frac{1-\sqrt{5}}{2}\right) &= 1 \\ a \cdot \left(\frac{1+\sqrt{5}}{2} - \frac{1-\sqrt{5}}{2}\right) + \left(\frac{1-\sqrt{5}}{2}\right) &= 1 \\ a \cdot \sqrt{5} &= 1 - \left(\frac{1-\sqrt{5}}{2}\right) \\ a &= \frac{1+\sqrt{5}}{2\sqrt{5}} \\ b &= 1 - \frac{1+\sqrt{5}}{2\sqrt{5}} \\ &= \frac{2\sqrt{5} - 1 - \sqrt{5}}{2\sqrt{5}} \\ &= \frac{\sqrt{5}-1}{2\sqrt{5}} \end{aligned}$$

Und erhalten die explizite Formel für die Fibonacci-Zahlen

$$\begin{aligned} f_n &= a \cdot u_n + b \cdot v_n \\ &= \frac{1+\sqrt{5}}{2\sqrt{5}} \cdot \left(\frac{1+\sqrt{5}}{2}\right)^n + \frac{\sqrt{5}-1}{2\sqrt{5}} \cdot \left(\frac{1-\sqrt{5}}{2}\right)^n \end{aligned}$$

So ist z.B. $f_{20} = \frac{1+\sqrt{5}}{2\sqrt{5}} \cdot \left(\frac{1+\sqrt{5}}{2}\right)^{20} + \frac{\sqrt{5}-1}{2\sqrt{5}} \cdot \left(\frac{1-\sqrt{5}}{2}\right)^{20} = 10946$

Ausgerechnet ergibt die Formel $\frac{1+\sqrt{5}}{2\sqrt{5}} \cdot \left(\frac{1+\sqrt{5}}{2}\right)^n + \frac{\sqrt{5}-1}{2\sqrt{5}} \cdot \left(\frac{1-\sqrt{5}}{2}\right)^n =$ $0,72361 \cdot 1.618^n + 0,27639 \cdot (-0,61803)^n$. Für große n kann also die Näherung

$$f_n = 0.72361 \cdot 1.618^n \tag{1.12}$$

verwendet werden.

In anderen Fällen müssen entweder die Nullstellen der Gleichung anders berechnet werden oder aus anderen Anfangsbedingungen ergeben sich ebenfalls andere Gleichungen.

Definition 7 *Gleichungen der Form $f_n = c \cdot y_{n-1} + d \cdot y_{n-2}$ heissen* ***Lucas-Gleichungen.*** *Die Lösungen können wie bei den Fibonacci-Folgen durch den Ansatz $f_n = q^n$ berechnet werden.*

Dies führt auf die Gleichung

$$q^2 - c \cdot q - d = 0 \tag{1.13}$$

Beispiel: Ausbreitung von Seuchen

Eine Seuche werde nach einem Jahr Inkubationszeit übertragen. Geht man bei einem HIV-Infizierten von weiteren 6 Ansteckungen pro Jahr aus und betrachtet die Anfangswerte (in Tsd) $f_0 = 10, f_1 = 40$, so ergibt sich zunächst als bestimmende Gleichung

$$f_n = f_{n-1} + 6 \cdot f_{n-2} \tag{1.14}$$

Mit dem Ansatz $y_n = q^n$ ergibt sich das Polynom

$$\begin{aligned} q^2 &= q + 6 \\ q^2 - q - 6 &= 0 \\ q_{1,2} &= \frac{1}{2} \pm \sqrt{\frac{1}{4} + 6} \\ q_1 &= -2, q_2 = 3 \end{aligned}$$

und damit

$$f_n = a \cdot (-2)^n + b \cdot 3^n \tag{1.15}$$

Die Anfangsbedingungen liefern

$$\begin{aligned} 10 &= a + b \\ 40 &= -2a + 3b \end{aligned}$$

Mit der Lösung :$a = -2, b = 12$ (nachrechnen) und damit

$$f_n = -2 \cdot (-2)^n + 12 \cdot 3^n \tag{1.16}$$

So ergibt sich nach 4 Jahren eine Infektionsrate von $f_4 = -2 \cdot (-2)^4 + 12 \cdot 3^4 = 940$.

Nach 10 Jahren ergibt sich $f_{10} = -2 \cdot (-2)^{10} + 12 \cdot 3^{10} = 7065\,40$ Tsd, also etwa 700 Millionen Infizierte.

Näherungsweise kann der Verlauf beschrieben werden durch $f_n = 12 \cdot 3^n$

1.5.1 Der goldene Schnitt

Da bei der Berechnung der Fibonacci Zahlen auf den goldenen Schnitt verwiesen wurde, hier auch ein kleiner Abschnitt zu dieser faszinierenden Zahl:

Der goldene Schnitt beschreibt zunächst - wie oft in der Mathemtik - in einem völlig anderen Zusammenhang ein eher künstlerisches Problem:

Z.B. empfindet man in der Kunst ein Bild harmonisch, wenn es wohlproportioniert ist.

Wir suchen - um uns dem Problem einfach zu nähern - bei einem Stab der Länge 1 die Stelle x, so dass sich beim Teilen des Stabes an dieser Stelle ergibt, dass das Verhältnis Längere zur kürzeren Strecke sich verhält, wie die Gesamtlänge zum längeren Stück, also:

$$\frac{x}{1-x} = \frac{1}{x} \tag{1.17}$$

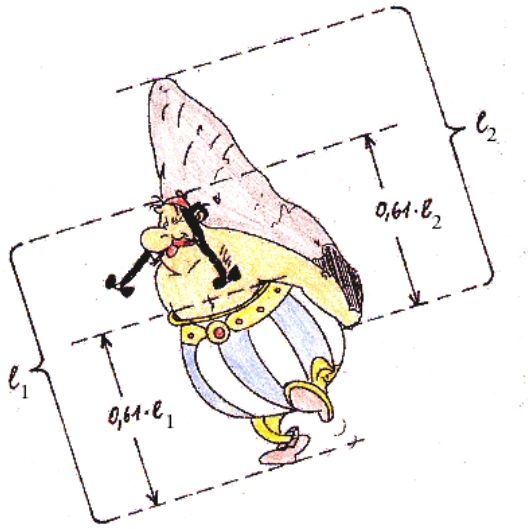
Dies führt auf die quadratische Gleichung

$$\begin{aligned} x^2 &= 1-x \\ x^2+x-1 &= 0 \end{aligned}$$

mit der Lösung

$$x_{1,2} = -\frac{1}{2} \pm \frac{1}{2}\sqrt{5} \tag{1.18}$$

Dabei heisst die oben einzig relevante positive Lösung $-\frac{1}{2} + \frac{1}{2}\sqrt{5} = 0,618$ bzw. der auftretende Term $\frac{1}{2} + \frac{1}{2}\sqrt{5} = 1,618...$ der goldene Schnitt. Und dieser wird in der klassischen Kunst (und nicht nur dort) zur Konstruktion verwendet ...



Anwendung: Zeigen Sie per Induktion:

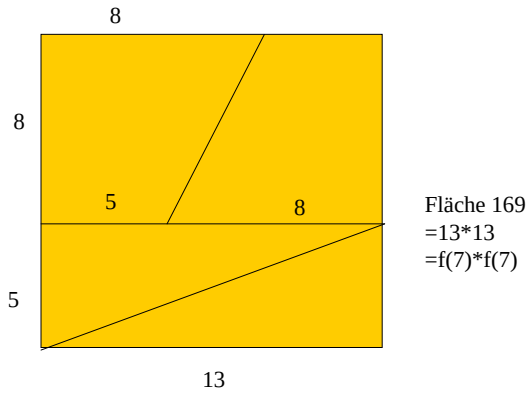
1. $f_{n+1} \cdot f_{n-1} - f_n^2 = (-1)^{n-1}$

Ind. Anfang: n=1: $f_2 \cdot f_0 - f_1^2 = 2 - 1 = 1 = (-1)^{1-1}$
Ind.vorr: $f_{n+1} \cdot f_{n-1} - f_n^2 = (-1)^{n-1}$
Ind. schluß: z.Z. $f_{n+2} \cdot f_n - f_{n+1}^2 = (-1)^n$
Wg $f_{n+2} = f_{n+1} + f_n$ ist auch $f_{n+2} - f_{n+1} = f_n$

$$\begin{aligned} f_{n+2} \cdot f_n - f_{n+1}^2 &= f_{n+2} \cdot f_n - f_{n+1} \cdot (f_n + f_{n-1}) \\ &= f_n \cdot (f_{n+2} - f_{n+1}) - f_{n+1} \cdot f_{n-1} \\ &= f_n^2 - f_{n+1} \cdot f_{n-1} \\ &= -(-1)^{n-1} = (-1)^n \end{aligned}$$

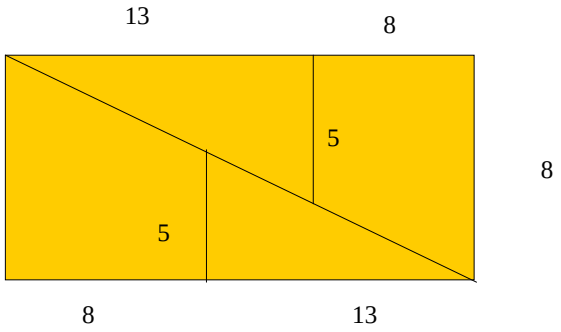
2. $f_{2n+1} = 1 + f_2 + ... + f_{2n}$
3. $f_{n+2} = 1 + f_0 + f_1 + f_2 + ... + f_n$

Aus der ersten Aufgabe folgert folgendes Phänomen: Bilden Sie zunächst ein Quadrat mit der Seitenlänge f_n (n>2 sollten Sie wählen), z.B. für n=7 mit $f_n = 13$:



Sie erhalten eine Fläche von 169 FE.

Zerlegen Sie das Rechteck in die Seitenlängen f_{n-2} und f_{n-1}, dann das obere Rechteck in zwei deckungsgleiche Trapeze, das untere in zwei deckungsgleiche Dreiecke. Zerschneiden Sie das Quadrat und setzen es erneut wie folgt zusammen:



Wir sehen: Die neue Fläche ist $21 \cdot 8 = 168$ FE, also um 1 FE kleiner.

Zunächst: Die 1 FE Differenz entsteht gerade aus der Formel $f_{n+1} \cdot f_{n-1} - f_n^2 = (-1)^n$. Rechteck und Quadrat haben nicht die gleiche Fläche. Die verlorene Flächeneinheit steckt in den nicht ganz passenden Steigungen zwischen Dreieck und Trapez. Beim Dreieck ist die Steigung $\frac{5}{13} = 0.\,384\,62$, beim Trapez $\frac{3}{8} = 0.375$. Diese Differenz ist beim "Basteln" für das bloße Auge unsichtbar.

1.6 Zählprobleme

Ein zentrales Problem der diskreten Mathematik ist die Kombinatorik und damit die Frage nach der Mächtigkeit von Mengen. Hierbei sind sinnvollerweise Fragestellungen nach endlichen Mengen zu beantworten (Wieviele natürliche Zahlen gibt es ? Unendlich ... ist also kein hier behandeltes Problem).

Definition 8 *Die Anzahl der Elemente der Menge M wird mit ihrer Mächtigkeit* $n = |M|$ *bezeichnet.*

Bem.: Eine Menge M hat genau n Elemente, wenn es eine bijektive (ein-eindeutige) Abbildung

$$f : M \to \{1, 2, ..., n\}$$

gibt.

Wird eine Menge dabei durch Aufzählen ihrer Elemente definiert, so ist die Mächtigkeit durch Abzählen ihrer Elemente bestimmt:

$$\begin{aligned} M &= \{1, a, x, y\} \\ |M| &= 4 \end{aligned}$$

Bei der Beschreibung einer Menge durch Eigenschaften wird dieses schon schwieriger

$$\begin{aligned} M &= \{a | a \text{ ist einstellige Primzahl}\} \\ |M| &= 4 \end{aligned}$$

Schliesslich interessieren noch Konstruktionen aus einfachen Mengen wie z.B. Wieviele Teilmengen hat die Menge $M = \{1, a, x, y\}$?

1.6.1 Einfache Zählformeln

Im folgenden bezeichne $\mathbb{N} = \{1, 2, 3, ...\}$ die Menge der (positiven) natürlichen Zahlen und falls nötig $\mathbb{N}_0 = \{0, 1, 2, 3, ...\}$ die Menge der nicht-negativen natürlichen Zahlen.

Kardinalitäten (Mächtigkeiten)

Wir definieren die Kardinalität einer Menge wie folgt: Eine Menge S hat genau dann die Kardinalität n, falls es eine bijektive Funktion gibt der Gestalt

$$f : S \to \{1, ..., n\}$$

Wir schreiben

$$|S| = n$$

Lemma 9 *Zwei endliche Mengen S und T haben genau dann die gleiche Anzahl Elemente, falls eine bijektive Abbildung von S nach T gibt.*

Bew.: Haben die beiden Mengen die gleiche Kardinalität n, so gibt es bijektive Abbildungen

$$\begin{aligned} f &: S \to \{1, ..., n\} \\ g &: T \to \{1, ..., n\} \end{aligned}$$

Damit ist $g^{-1}f$ eine bijektive Abbildung von S nach T.

Gibt es andererseits eine Bijektion h von S nach T und S hat n Elemente, so gibt es zunächst eine Bijektion

$$f : S \to \{1, ..., n\}$$

und weiterhin ist

$$fh^{-1}$$

eine Bijektion von T auf $\{1, ..., n\}$. Somit hat auch T n Elemente.

Summen von Mengen

Vereinigung und Durchschnitt

Definition 10 *Unter der Vereinigung $A \cup B$ versteht man alle Elemente, die entweder in A* ***oder*** *in B enthalten sind.*

Definition 11 *Unter dem Durchschnitt $A \cap B$ versteht man alle Elemente, die in A* ***und*** *in B enthalten sind.*

Definition 12 *Haben zwei Mengen keine gemeinsamen Elemente ($A \cap B = \{\}$), so heißen die Mengen diskjunkt.*

Beispiel: Ist A die Menge der Studierenden im Fach Bioingenieurwesen und B die Menge der Studierenden im Fach Chemieingenieurwesen, so ist $A \cup B$ die Menge derjenigen die das eine oder das andere (oder beides) studieren, $A \cap B$ ist die Menge, die beides studieren.

Satz 13 *"Summen" Es gilt für Mengen:*

1. Sind S und T disjunkte Mengen, so ist $|S \cup T| = |S| + |T|$

2. Sind S_i und S_j paarweise disjunkte Mengen (jeweils zwei haben leeren Durchschnitt), so gilt: $|S_1 \cup S_2 \cup ... \cup S_n| = |S_1| + |S_2| + ... + |S_n|$

3. Für beliebige Mengen gilt: $|S \cup T| = |S| + |T| - |S \cap T|$

Bew. 1.,2. klar durch abzählen,

3. Betrachte die 3 Mengen $S_1 = S - T, S_2 = S \cap T, S_3 = T - S$.

Dann ist $|S \cup T| = |S_1 \cup S_2 \cup S_3| = |S_1| + |S_2| + |S_3| = (|S| - |S \cap T|) + |S \cap T| + (|S| - |S \cap T|) = |S| + |T| - |S \cap T|$

Produkte von Mengen

Definition 14 *Für 2 Mengen A und B definieren wir das kartesische Produkt* $A \times B$ *als*

$$A \times B := \{(a, b) | a \in A \text{ und } b \in B\} \tag{1.19}$$

Also: alle Paare, wobei der erste Teil aus der Menge A und der zweite Teil aus der Menge B entnommen wird.

Beispiel: Wir betrachten das kartesische Produkt der Mengen $A = \{1, 2\}$ und $B = \{x, y\}$. Dann ist $A \times B = \{(1, x), (1, y), (2, x), (2, y)\}$

Es gilt:

Satz 15 *Für zwei nicht-leere Mengen A und B ist*

$$|A \times B| = |A| \cdot |B| \tag{1.20}$$

Beweis: Die Menge A habe die Elemente $a_1, a_2, ..., a_n$ und B die Elemente $b_1, b_2, ..., b_m$. Diese Elemente schreiben wir nun in eine Binärmatrix

$$\begin{array}{c|cccc} & a_1 & a_2 & ... & a_n \\ b_1 & x & x & x & x \\ b_2 & x & x & x & x \\ ... & & & & \\ b_m & x & x & x & x \end{array} \tag{1.21}$$

Abzählen der möglichen Kombinationen ergibt $n \cdot m$ mögliche Kombinationen.

Definition 16 *Für nicht-leere Mengen* $A_1, ..., A_n$ *ist*

$$A_1 \times A_2 \times ... \times A_n = \{(a_1, a_2, ..., a_n) | a_i \in A_i\} \tag{1.22}$$

Satz 17 *Für nicht-leere Mengen* $A_1, ..., A_n$ *ist*

$$|A_1 \times A_2 \times ... \times A_n| = |A_1| \cdot |A_2| \cdot ... \cdot |A_n| \tag{1.23}$$

Beispiel: Die 4-stellige PIN einer EC-Karte besteht aus 4 Zahlen, wobei die erste eine Zahl zwischen 1 und 9, die anderen zwischen 0 und 9 sind. Wieviele Kombinationen gibt es?

PIN ist (a_1, a_2, a_3, a_4) mit $a_1 \in A_1 = \{1, ..., 9\}, a_2 \in A_2 = \{0, ..., 9\}, a_3 \in A_3 = \{0, ..., 9\}, a_4 \in A_4 = \{0, ..., 9\}$ und damit

$$\begin{aligned} n &= |A_1| \cdot |A_2| \cdot |A_3| \cdot |A_4| \\ &= 9 \cdot 10 \cdot 10 \cdot 10 \\ &= 9000 \end{aligned}$$

Aufgabe: Eine Geldscheinnummer (z.B. W20001234321) besteht aus einem Buchstaben und 11 weiteren Ziffern, wobei die erste von 0 verschieden ist. Wieviele Möglichkeiten gibt es, Geldscheinnummern zu vergeben?

Bem. Werden kartesische Produkte mit Elementen aus gleicher Grundmenge gewählt, so definieren wir $A \times A = A^2$ bzw $\underbrace{A \times A \times ... \times A}_{n-mal} = A^n$ und für die Mächtigkeit gilt $|A \times A \times ... \times A| = |A^n| = |A|^n$

Binärmatrizen

Definition 18 *Eine $n \times m-$Matrix M, dessen Einträge m_{ij} nur 0 oder 1 sind, heißt Binärmatrix.*

Häufig werden Binärmatrizen verwendet, um eine Beziehung in einem kartesichen Produkt auszudrücken:

$$\begin{array}{cccccc} & b_1 & b_2 & ... & b_n \\ a_1 & 1 & 0 & & 1 \\ a_2 & 0 & 0 & & 1 \\ ... & & & & \\ a_n & 1 & 1 & & 0 \end{array} \tag{1.24}$$

Summieren wir zunächst die Spalten und addieren wir die Ergebnisse, so kommt hierbei das gleiche Ergebnis heraus als wenn wir dies über die Zeilen durchführen würden.

Beispiel:

A) An einer Hochschule besucht jeder Student genau 5 Vorlesungen. Jede Vorlesung wird dabei von genau 11 Studenten besucht. Welche der folgenden Aussagen können nicht stimmen:

1. Die Hochschule hat 100 Studenten
2. Es werden 5 Vorlesungen angeboten

B) In einer Mathe-Vorlesung sind 32 weibliche Teilnehmerinnen. Jede von Ihnen kennt 5 männliche. Die Männer kennen jeweils 8 weibliche. Wieviele männliche Teilnehmer sind in der Vorlesung?

Binärfolgen

Definition 19 *Sei B={0,1}. Dann heißt* $(b_1, b_2, ..., b_n)$ *mit* $b_i \in B$ *Binärfolge der Länge n.*

Beispiel: Welche Binärfolgen der Länge 3 gibt es?
$(0,0,0), (0,0,1), (0,1,0), (0,1,1),$
$(1,0,0), (1,0,1), (1,1,0), (1,1,1)$
- also 8 Stück.

Satz 20 *Die Anzahl der Binärfolgen der Länge n ist gleich* 2^n.

Beweis:$|B \times B \times ... \times B| = |B^n| = |B|^n = 2^n$

Definition 21 *Eine Menge B heißt Teilmenge von A, wenn jedes Element von B auch Element von A ist. Schreibweise:* $B \subset A$.

Definition 22 *Die Menge aller Teilmengen vom M heißt Potenzmenge P(M).*

Beispiel: Potenzmenge von $M = \{a, b, c\}$ ist $\{\}, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}$

Wie groß ist denn allgemein die Potenzmenge einer n-elementigen Menge?

Beweis 1. Sei $M = \{m_1, ..., m_n\}$ eine n-elementige Menge. Betrachte für jede Teilmenge T die Menge $B(T) = (b_1, b_2, ..., b_n)$ mit $b_i \in \{0, 1\}$. Dabei bedeutet $b_i = 1$ dass $m_i \in T$, und 0 sonst. Damit ist $B(T)$ eine bijektive Abbildung zwischen allen Binärfolgen der Länge n und allen möglichen Teilmengen. Da es 2^n mögliche Binärfolgen gibt, ist dies auch die Anzahl der Teilmengen.
Beweis 2.Die Anzahl der Teilmengen ist 2^n mit vollständiger Induktion:

Ind. Anfang: n=1, damit M=$\{m_1\}$: Die Teilmengen sind {},$\{m_1\}$. Anzahl: $2=2^1$.

Ind.vorr.: Jede n-elementige Menge hat 2^n Teilmengen

Ind. Schluß: Betrachte $M = \{m_1, ..., m_{n+1}\}$. Betrachte das Element m_1.
Es gibt zwei Sorten von Teilmengen: Die, die m_1 enthalten und die, dies nicht tun.

Die Teilmengen, die m_1 nicht enthalten, sind diejenigen Teilmengen von $\{m_2, ..., m_{n+1}\}-$ Nach Induktionsvorr. gerade 2^n Stück.

Die Teilmengen, die m_1 enthalten, sind diejenigen Teilmengen von $\{m_2, ..., m_{n+1}\}$, denen dann jeweils noch das Element m_1 hinzugefügt wird − Nach Induktionsvorr. ebenfalls gerade 2^n Stück.

Insgesamt ist die Anzahl der Teilmengen : $2^n + 2^n = 2 \cdot 2^n = 2^{n+1}$

Wie können wir nun Teilmengen in eine Reihenfolge bringen, so dass sich von einer Teilmenge zur nächsten nur ein Element ändert (hinzukommt oder wegfällt - nicht ersetzt wird)?

Oben: $\{\}, \{c\}, \{b, c\}, \{b\}, \{a, b\}, \{a, b, c\}, \{a, c\}, \{c\}$

Dieses entspricht der Binärreihenfolge

000
001
011
010
110
111
101
100

Also: Äquivalentes Problem besteht darin eine Binärsequenz zu finden, bei der sich jeweils nur eine Ziffer ändert.

Satz 23 *Für $n \in \mathbb{N}$ ist es stets möglich, eine Binärsequenz der Länge n zu finden, bei der sich jeweils nur eine Ziffer ändert.*

Beweis: Induktion. n=1,2 klar.

Ind. vorr.: Wir haben eine solche Sequenz für n gefunden: $a_1, ..., a_{2^n}$

Ind. schluß: Betrachte:

0,a_1
0,a_2
...
0,a_{2^n}
1,a_{2^n}
...
1,a_2
1,a_1

In den ersten und letzten 2^n Stellen ist dies der Fall gemäß Ind. vorr., in der "Mitte" ändert sich nur die führende Ziffer.

Eine so erzeugte Folge heißt Gray Code.

1.6.2 Binomialzahlen

In diesem Abschnitt betrachten wir wiederum Teilmengen, jedoch nicht alle sondern diejenigen, die eine feste Mächtigkeit haben.

Betrachte $A = \{a, b, c, d\}$. Wieviele 2-elementige Teilmengen dieser 4-elementigen Menge gibt es?
$\{a, b\}, \{a, c\}, \{a, d\}, \{b, c\}, \{b, d\}, \{c, d\}$ - also 6 Stück.

Definition 24 *Die Anzahl der k-elementigen Teilmengen einer n-elementigen Menge bezeichnen wir mit* $\binom{n}{k}$. *Diese Zahlen heißen Binomialkoeffizienten oder Binomialzahlen.*

Es ist $\binom{n}{0} = 1$ (leere Menge)
$\binom{n}{n} = 1$ (gesamte Menge)
$\binom{n}{1} = n$ (jedes Element einzeln)

Besipiel: Beim Lotto wird aus der Menge {1,...,49} eine 6-elementige Teilmenge gewählt. Die Anzahl ist somit $\binom{49}{6}$, welche wir im folgenden ausrechnen werden.

Wie bei den Fibonacci-Zahlen werden wir eine rekursive und eine explizite Formel zur Berechnung herleiten.

Satz 25 *Rekursionsformel für Binomialkoeffizienten. Für* $k, n \in \mathbb{N}$ *mit* $k \leq n$ *gilt:*

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1} \tag{1.25}$$

Damit:

$$\begin{aligned}\binom{5}{3} &= \binom{4}{3} + \binom{4}{2} = \binom{3}{3} + \binom{3}{2} + \binom{3}{2} + \binom{3}{1} \\ &= 1 + 2 \cdot \left(\binom{2}{2} + \binom{2}{1} \right) + 3 \\ &= 1 + 2 \cdot 3 + 3 = 10\end{aligned}$$

Beweis: Wir betrachten eine n-elementige Menge M und ein Element m dieser Menge. Dann kann man die k-elementigen Teilmengen in 2 Rubriken einteilen:

1. k-elementige Teilmengen, die das Element m nicht enthalten
2. k-elementige Teilmengen, die das Element m enthalten

Zu 1.: Diese Mengen sind alle k-elementigen Teilmengen der (n-1)-elementigen Menge M-{m}. Deren Anzahl ist

$$\left(\begin{array}{c} n-1 \\ k \end{array} \right) \tag{1.26}$$

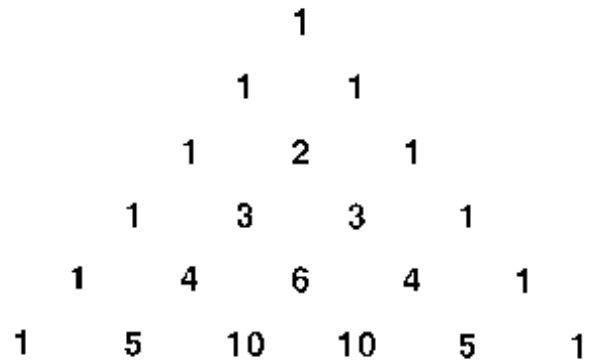
zu 2.: Betrachtet man die Mengen, welche entstehen, wenn wir das Element m aus jedem dieser Teilmengen entfernen, so verbleiben (k-1)-elementige Teilmengen der (n-1)-elementigen Menge M-{m}.
Hiervon existieren

$$\left(\begin{array}{c} n-1 \\ k-1 \end{array} \right) \tag{1.27}$$

Mengen. Umgekehrt kann auch jede Teilmenge in 2. durch eine solche Teilmenge und Hinzufügen des Elementes m erzeugt werden.

Insgesamt ergibt sich $\left(\begin{array}{c} n \\ k \end{array} \right) = \left(\begin{array}{c} n-1 \\ k \end{array} \right) + \left(\begin{array}{c} n-1 \\ k-1 \end{array} \right)$.

Das obige Bildungsgesetz wird im Pascal'schen Dreieck festgehalten:



Die oberste Zeile ist für n=0, die nächste n=1, usw. Dabei steht innerhalb einer Zeile der Wert $\left(\begin{array}{c} n \\ 0 \end{array} \right)$ an erster Stelle, dann $\left(\begin{array}{c} n \\ 1 \end{array} \right)$ usw.

Hieraus lässt sich per Induktion über n folgende explizite Formel herleiten

$$\left(\begin{array}{c} n \\ k \end{array} \right) = \frac{n!}{k! \cdot (n-k)!} \tag{1.28}$$

wobei $n! = 1 \cdot 2 \cdot ... \cdot n$ ist.

Insbesondere ist der Bruch auf der rechten Seite kein echter Bruch, sondern ergibt stets eine ganzzahlige Lösung.

Beim Lotto ergibt sich hiermit

$$\left(\begin{array}{c} 49 \\ 6 \end{array} \right) = \frac{49!}{6! \cdot 43!} = 13.983.816$$

Eine weitere wichtige Anwendung dieser Zahlen ist der Binomialsatz

Satz 26

$$(x+y)^n = \sum_{i=0}^{n} \left(\begin{array}{c} n \\ i \end{array} \right) \cdot x^i \cdot y^{n-i} \tag{1.29}$$

Bew.: Zunächst: Wenn wir die linke Seite ausmultiplizieren, erhalten wir n Klammern und beim Ausklammern Terme der Gestalt $x^i \cdot y^{n-i}$. Dieser Term kommt immer dann vor, wenn wir in i Klammern x auswählen und aus den verbleibenden $n-i$ das y. Die Anzahl Möglichkeiten dies zu tun ist aber gerade $\left(\begin{array}{c} n \\ i \end{array} \right)$

Zum Beispiel ist $(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$

Anwendungen:

1. x=y=1:

$$2^n = \sum_{i=0}^{n} \left(\begin{array}{c} n \\ i \end{array} \right) \tag{1.30}$$

Also: Die Summe aller möglichen Teilmengen (s.o.) ist 2^n

2. x=-1, y=1

$$0 = \sum_{i=0}^{n} \left(\begin{array}{c} n \\ i \end{array} \right) (-1)^i \tag{1.31}$$

oder

$$\sum_{\substack{i=0 \\ i \text{ gerade}}}^{n} \left(\begin{array}{c} n \\ i \end{array} \right) = \sum_{\substack{i=0 \\ i \text{ ungerade}}}^{n} \left(\begin{array}{c} n \\ i \end{array} \right) \tag{1.32}$$

Also: Es gibt genau so viele gerade wie ungerade Teilmengen.

3. Berechnen Sie 101^3

Es gilt weiterhin:

Satz 27 *Vandermond Identität*

$$\binom{m+w}{k} = \sum_{l=0}^{k} \binom{m}{l} \cdot \binom{w}{k-l}$$

Bew.: Betrachte eine Menge G mit m+w Elementen und splitte diese in zwei Mengen M mit m Elementen und W mit w Elementen auf. Eine k-elementige Teilmenge der Gesamtmenge kann nun auf zwei Arten gebildet werden:

1. Als k-elementige Teilmenge der Gesamtmenge

$$\binom{m+w}{k}$$

2. Wir schauen uns nun noch genauer an, aus welchen Elementen diese k-Elementige Menge gebildet werden kann. Werden l Elemente aus der Menge M genommen, verbleiben k-l Elemente aus W. Die Anzahl der Möglichkeiten ist dann

$$\binom{m}{l} \cdot \binom{w}{k-l}$$

Alle Möglichkeiten erhalten wir, in dem wir nun alle möglichen Werte von l zwischen 0 und k betrachten, also

$$\binom{m+w}{k} = \sum_{l=0}^{k} \binom{m}{l} \cdot \binom{w}{k-l}$$

1.6.3 Partitionen

Definition 28 *Eine Partition (Zerlegung) einer Menge S ist eine Menge von Teilmengen* $\{T_1, T_2, ..., T_k\}$ *mit*

$T_i \neq \emptyset$

$T_1 \cup T_2 \cup ... \cup T_k = S$

$T_i \cap T_k = \emptyset$

Die Menge T_k heißen Komponenten der Partition

Definition 29 *Die Anzahl der Partitionen einer n-elementigen Menge wird mit* B_n *(**Bell-Zahlen**) notiert. Die Anzahl der Partitionen mit genau k Komponenten heissen **Stirling-Zahlen*** $S(n,k)$.

Beispiel: Wir betrachten $S = \{a, b, c\}$. Folgende Zerlegungen existieren:

1 Komponente a, b, c d.h. $S(3,1) = 1$

2 Komponenten $\{a|b,c\}$ oder $\{b|a,c\}$ oder $\{c|a,b\}$ d.h. $S(3,2)=3$
3 Komponenten $\{a|b|c\}$ d.h. $S(3,3)=1$

Insgesamt gibt es $B_3 = 5$ Partitionen

Es gilt:

$$B_n = \sum_{k=1}^{n} S(n,k)$$

Für Stirling Zahlen gilt stets

$$S(n,1) = S(n,n) = 1$$

und weiterhin

$$S(n,k) = S(n-1,k-1) + k \cdot S(n-1,k) \quad 1 < k < n \tag{1.33}$$

Beweis:

Wir betrachten zu einer beliebigen Partition P einer Menge S ein beliebiges Element {s} dieser Menge. Jede gültige Partition ist dann von einer der folgenden Typen:

1. {s} ist eine Komponente (1-elementig)
2. s liegt in einer Menge mit mehr als einem Element.

Typ 1: Wir nehmen das Element und die Komponente heraus und erhalten eine k-1 elementige Partition von der n-1 elementigen Menge S-{s}. Hiervon gibt es gerade $S(n-1,k-1)$ Stück, welche eindeutig zur Partition von S mit k Komponenten vervollständigt werden kann.

Typ 2: Nach Wegnahme des Elementes s verbleiben k Komponenten der n-1 elementigen Menge. Hiervon gibt es $S(n-1,k)$ Stück. Das Element s kann jetzt zur jeder der k Komponenten hinzugefügt werden, also auf k Arten zu einer Partitiion von S vervollständigt werden. Insgesamt also $k \cdot S(n-1,k)$
qed

Für die Bell-Zahlen gilt:

$$B_{n+1} = \sum_{k=0}^{n} \left(\begin{array}{c} n \\ k \end{array} \right) B_k \tag{1.34}$$

(definiert wird $B_0 = B_1 = 1$)
Beweis: Wir betrachten eine $n+1-$elementige Menge S und ein festes Element s dieser Menge. In einer beliebigen Partition sei T die Komponente mit

l +1−Elementen, die dieses Element s enthalte. In den anderen Komponenten sind $n-l$ Elemente. Diese können auf B_{n-l} Arten mit T zu einer Partition von S vervollständigt werden. Da T l Elemente (ausser s) hat, kann man T auf $\left(\begin{array}{c} n \\ l \end{array} \right)$ Arten aus der Menge S bilden. Wir betrachten nun alle möglichen Zerlegungen, also l kann alle Werte zwischen 0 und n annehmen. Damit

$$\begin{aligned} B_{n+1} &= \sum_{l=0}^{n} \left(\begin{array}{c} n \\ l \end{array} \right) B_{n-l} = \sum_{k=0}^{n} \left(\begin{array}{c} n \\ n-k \end{array} \right) B_k \qquad (1.35) \\ &= \sum_{k=0}^{n} \left(\begin{array}{c} n \\ k \end{array} \right) B_k \end{aligned}$$

1.6.4 Kombinationen mit Wiederholung

Die bisher betrachteten Teilmengen waren Auswahlen aus der Menge ohne Wiederholung (Lotto: Jede Zahl nur höchstens einmal) und ohne Anordnung (egal an welcher Stelle die Zahl gezogen wurde).

Nun betrachten wir Auswahlen mit Wiederholung.

Bsp: A={a,b,c}. Betrachte die k=4-elementigen Auswahlen der n=3-elementigen Menge

aaaa, aaab, aaac, aabb, aabc, aacc, abbb, abbc, abcc, accc, bbbb, bbbc, bbcc, bccc, cccc

15 Stück - Wie können wir diese Anzahl berechnen?

Wir betrachten folgende Darstellung:

1. Zunächst betrachten wir das erste Element a und zählen wie oft dieses vorkommt, in dem wir eine Sequenz von 1-en aufschreiben. (Beispiel aaac: "111")
2. Wir schreiben zur Kennzeichnung das nun das nächste Element betrachtet wird nun eine "0" hieran anschließend (Bsp. 1110)
3. Nun das 2-te Element (Bsp: kommt nicht vor)
4. Wiederum eine "0" (Bsp.: 11100)
5 und nun das dritte genau so (Bsp: 111001)

Umgekehrt können wir aus einer solchen Sequenz direkt die zugehörige Auswahl ablesen: 110101 entspricht aabc

Damit haben wir eine bijektive Abbildung geschaffen. Die Frage verbleibt auf wieviele Arten die 4 (allgemein k) Einsen auf die 6 Stellen (4 Einsen und k-1 = 2 Trennstellen ; allgemein: n+k-1) verteilt werden können:

$$\left(\begin{array}{c} n+k-1 \\ k \end{array} \right) \tag{1.36}$$

Anwendung:

1. Auf einem Schachbrett der Gestalt 6x8 können Sie links unten beginnend nach rechts oben gelangend auf verschiedenen Wegen gelangen. Wieviele solcher Wege gibt es?

2. Wieviele 4-stellige Zahlen gibt es, deren Quersumme 9 ist?

3. Bei der Vorstandswahl des SV Mathe 04 stehen 3 Kandiaten zur Verfügung. Wieviele Wahlausgänge gibt es bei 20 stimmberechtigten Wählern?

1.7 Das Sieb-Prinzip

Auch: Einschluß-Ausschluß-Verfahren oder Inclusion/Exclusion

Es ist

$$\begin{aligned} |A \cup B| &= |A| + |B| - |A \cap B| \\ |A \cup B \cup C| &= |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C| \end{aligned}$$

Allgemein:

$$|A_1 \cup A_2 \cup ... \cup A_n| = \alpha_1 - \alpha_2 + ... + (-1)^{n+1} \cdot \alpha_n \tag{1.37}$$

mit

α_i : (1.38)

1. Bestimme den Durchschnitt von je i Mengen aus A_1 bis A_n
2. Summiere alle Mächtigkeiten dieser Mengen- Ergebnis ist α_i

z.B.

$$\begin{aligned} \alpha_1 &= |A_1| + |A_2| + ... + |A_n| \\ \alpha_n &= |A_1 \cap A_2 \cap ... \cap A_n| \end{aligned}$$

Beweis: Wir betrachten ein Element $m \in A_1 \cup .. \cup A_n$ und zeigen, dass wir dies über obige Formel genau ein mal zählen. m sei (ohne Einschränkung) in

den Mengen $A_1, ..., A_r$ enthalten. Dann wird

$$\begin{aligned} m \text{ in } \alpha_1 \text{ genau r-mal } (&= \left(\begin{array}{c} r \\ 1 \end{array} \right) - mal) \text{ gezählt} \\ m \text{ in } \alpha_2 \text{ genau } &= \left(\begin{array}{c} r \\ 2 \end{array} \right) - mal) \text{ gezählt} \\ &\vdots \\ m \text{ in } \alpha_r \text{ genau 1-mal } (&= \left(\begin{array}{c} r \\ r \end{array} \right) - mal) \text{ gezählt} \\ m \text{ in } \alpha_n \text{ mit r } &> \text{ n genau 0-mal gezählt} \end{aligned}$$

Insgesamt:

$$\begin{aligned} & \left(\begin{array}{c} r \\ 1 \end{array} \right) - \left(\begin{array}{c} r \\ 2 \end{array} \right) + ... + (-1)^{r+1} \left(\begin{array}{c} r \\ r \end{array} \right) \\ = & \sum_{i=1}^{r} \left(\begin{array}{c} r \\ i \end{array} \right) (-1)^{i+1} = - \sum_{i=1}^{r} \left(\begin{array}{c} r \\ i \end{array} \right) (-1)^{i} \\ = & - \left(\sum_{i=0}^{r} \left(\begin{array}{c} r \\ i \end{array} \right) (-1)^{i} - \left(\begin{array}{c} r \\ 0 \end{array} \right) \right) \\ = & \left(\begin{array}{c} r \\ 0 \end{array} \right) = 1 \end{aligned}$$

Beispiel:
Wieviele Zahlen kleiner gleich 100 sind entweder durch 2, 5 oder 9 teilbar? (2,4,5,6,8,9,10,12,14,15,...)

$A_1 = \{$Zahlen kleiner gleich 100, die durch 2 teilbar sind$\}$
$A_2 = \{$Zahlen kleiner gleich 100, die durch 5 teilbar sind$\}$
$A_3 = \{$Zahlen kleiner gleich 100, die durch 9 teilbar sind$\}$

Gesucht: $|A_1 \cup A_2 \cup A_3| = \alpha_1 - \alpha_2 + \alpha_3$

$\alpha_1 = |A_1| + |A_2| + |A_3| = 50 + 20 + 11 = 81$

$\alpha_2 = |A_1 \cap A_2| + |A_2 \cap A_3| + |A_1 \cap A_3| = 10 + 2 + 5 = 17$

$\alpha_3 = |A_1 \cap A_2 \cap A_3| = 1$

und damit $|A_1 \cup A_2 \cup A_3| = \alpha_1 - \alpha_2 + \alpha_3 = 81 - 17 + 1 = 65$

Satz 30 *(Folgerung) : Sei* $|A| = k$

$$|A \setminus (A_1 \cup A_2 \cup ... \cup A_n)| = k - (\alpha_1 - \alpha_2 + ... + (-1)^{n+1} \cdot \alpha_n) \qquad (1.39)$$

1.7.1 Permutationen

Definition 31 *Eine Permutation π ist eine bijektive Abbildung einer endlichen Menge auf sich selbst, z.B.*

$$\pi : \{1, 2, 3, 4\} \to \{4, 1, 2, 3\} \tag{1.40}$$

Notation:

$$\pi = \begin{pmatrix} 1\ 2\ 3\ 4 \\ 4\ 1\ 3\ 2 \end{pmatrix} \tag{1.41}$$

Häufig wird auch nur die Sequenz notiert $\pi = (1\ 4\ 2)(3)$.

also: $\pi(1) = 4, \pi(4) = 2, \pi(2) = 1, \pi(3) = 3$

Frage: Wieviele Permutationen einer n-elementigen Menge gibt es?

Das erste Element kann auf alle n verschiedenen Elemente abgebildet werden, also n Möglichkeiten. Das zweite auf alle außer auf das, auf welches das erste Element abgebildet wurde, also n-1 Möglichkeiten usw. für das letzte Element verbleibt nur eine Möglichkeit (das letzte noch nicht verwendete Element). Insgesamt

$$n \cdot (n-1) \cdot ... \cdot 1 = n! \text{ Möglichkeiten} \tag{1.42}$$

Beispiel: 50 Studenten können sich auf 50 freie Plätze auf 50! - Möglichkeiten ($\approx 3 \cdot 10^{64}$).

Wird ein Element auf sich selbst abgebildet, so heißt dieses Fixpunkt der Permutation:

Definition 32 *Ein Element i mit $\pi(i) = i$ heißt Fixpunkt der Permutation π.*

Oben ist wegen $\pi(3) = 3$ das Element 3 ein Fixpunkt.

Wieviele Permutationen einer 4-elementigen Menge ohne Fixpunkt gibt es?
z.B Auf wieviele Arten kann es passieren, dass bei 4 Personen, welche nachher jeweils zufällig eine Jacke wählen, alle die falsche Jacke erwischen?

Abzählen: (2 3 4 1), (2 4 1 3),(2 1 4 3), (3 1 4 2), (3 4 1 2), (3 4 2 1),(4 1 2 3), (4 3 2 1), (4 3 1 2) = 9 Möglichkeiten.

Nun strukturiert:

Satz 33 *Die Anzahl Permutationen einer n-elementigen Menge ohne Fixpunkt ist*

$$a(n) = \sum_{i=0}^{n} \frac{n!}{k!}(-1)^k = n! - \frac{n!}{1!} + \frac{n!}{2!} - ... + (-1)^n \frac{n!}{n!} \tag{1.43}$$

Oben: 4! - 4!+12-4+1=9

Beweis: Siebformel

$$\begin{aligned} A &= \{\text{alle Permutationen}\} \\ A_1 &= \{\text{Permutationen mit } \pi(1) = 1\} \\ A_2 &= \{\text{Permutationen mit } \pi(2) = 2\} \\ A_i &= \{\text{Permutationen mit } \pi(i) = i\} \\ &\vdots \\ A_n &= \{\text{Permutationen mit } \pi(n) = n\} \end{aligned} \tag{1.44}$$

Dabei kann eine Permutation in mehreren Mengen liegen, z.B. $\begin{pmatrix} 1\,2\,3\,4 \\ 1\,4\,3\,2 \end{pmatrix}$ liegt in A_1 und A_3. Damit sind alle Permutationen mit Fixpunkten beschrieben durch $A_1 \cup A_2 \cup ... \cup A_n$.
Gesucht ist $|A \setminus (A_1 \cup A_2 \cup ... \cup A_n)| = n! - \alpha_1 + \alpha_2 - ... + (-1)^n \cdot \alpha_n$

α_2 bedeutet dabei, den Durchschnitt von A_i und A_j für alle möglichen i und j zu bilden und diese Möglichkeiten aufzusummieren. Wieviele Mengen $A_i \cap A_j$ gibt es? $\begin{pmatrix} n \\ 2 \end{pmatrix}$
Entsprechend bei α_k : $\begin{pmatrix} n \\ k \end{pmatrix}$

Die Mächtigkeit eines jeden solchen Durchschnittes ist dabei gleich groß: Bei α_2 sind 2 Stellen fix, der Rest kann auf (n-2)! Weisen variiert werden. Entsprechend wiederum bei α_k (n-k)!

Damit ist

$$\begin{aligned} \alpha_k &= \begin{pmatrix} n \\ k \end{pmatrix} \cdot (n-k)! \\ &= \frac{n!}{(n-k)!k!} \cdot (n-k)! \\ &= \frac{n!}{k!} \end{aligned}$$

und damit

$$\begin{aligned} a(n) &= \alpha_1 - \alpha_2 + ... + (-1)^{n+1} \cdot \alpha_n \\ &= n! - \frac{n!}{1!} + ... + (-1)^n \cdot \frac{n!}{n!} \end{aligned}$$

Auf wieviele Möglichkeiten können sich an einen Tisch mit 5 Tischkärtchen alle Personen an einen falschen Platz setzen?

$$\begin{aligned} a(5) &= 5! - \frac{5!}{1!} + \frac{5!}{2!} - \frac{5!}{3!} + \frac{5!}{4!} - \frac{5!}{5!} \\ &= 120 - 120 + 60 - 20 + 5 - 1 \\ &= 44 \end{aligned}$$

Umgekeht: Auf wieviele Möglichkeiten sitzt mindestens einer auf dem richtigen Platz? 5! - a(5)=120-44=76.

Damit ist beispielsweise die Wahrscheinlichkeit, dass alle an einem falschen Platz sitzen

$$p_5 = \frac{44}{120} = 0,367 = 36,7\% \tag{1.45}$$

Nun betrachten wir den Fall n=6: Es gibt 6!=720 Möglichkeiten. a(6)=720-720+360-120+30-6+1=265 Möglichkeiten ohne Fixpunkt. Damit ist $p_6 = \frac{265}{720} = 36,8\%$

Allgemein:

$$\begin{aligned} p_n &= \frac{a(n)}{n!} = \frac{n! - \frac{n!}{1!} + ... + (-1)^n \cdot \frac{n!}{n!}}{n!} = 1 - \frac{1}{1!} + ... + (-1)^n \cdot \frac{1}{n!} \\ &= \sum_{i=0}^{n} (-1)^i \frac{1}{i!} \end{aligned}$$

Wegen $\lim_{n\to\infty} \sum_{i=0}^{n} \frac{x^i}{i!} = e^x$ ist damit der Grenzwert

$$\lim_{n\to\infty} p_n = e^{-1} = \frac{1}{e} = 36,7\% \tag{1.46}$$

Kapitel 2

Zahlentheorie

Notation: Gegenstand der Zahlentheorie sind die ganzen Zahlen. Alle Buchstaben bezeichnen daher - sofern nicht anders beschrieben - ganze Zahlen. Kleine lateinische Buchstaben (a-z) bezeichnen diese Zahlen, m und n sind speziell natürliche Zahlen.

Werden reelle Zahlen benötigt, werden kleine griechische Buchstaben verwendet.

2.1 Teilbarkeit

Die Beziehung, welche zwei Zahlen in der Zahlentheorie auszeichnet, ist die Teilbarkeit. Insbesondere werden hierbei die Primzahlen analysiert werden können.

2.1.1 Einleitung

Definition 34 *Eine Zahl d "teilt" eine Zahl a, wenn es eine Zahl q gibt mit*

$$a = q \cdot d$$

Wir schreiben: $d|a$. a heisst Vielfaches von d. Die Negation (ein solches q existiert nicht) wird beschrieben durch: $d \nmid a$.

Also: $-3|6$ (da $6 = (-2) \cdot (-3)$) , $d|0$, $d|d$ .Es gilt das jedes a die Teiler 1,-1,a

und -a hat (z.B. $-1|a$, da $a = (-a) \cdot (-1)$

Satz 35 *Es gilt*

1. $d|0$ *für alle* d
2. $0|a \Longleftrightarrow a = 0$
3. $d|a$ *und* $a|b \Longrightarrow d|b$
4. $d|a \Longrightarrow db|ab$

5. $d|a$ *und* $e|b \Longrightarrow de|ab$
6.(!) $d|a$ *und* $d|b \Longrightarrow d|ax + by$ *für alle* x *und* y
7. $d|a \Longrightarrow d|ab$ *für alle* b
8. $d|a \Longrightarrow d|-a$
9. $d|a \Longrightarrow -d|a$
10. $a|b$ *und* $b|a \Longleftrightarrow a = \pm b$

Beweise:
z.B.

zu 3. $a = q_1 \cdot d, b = q_2 \cdot a \Longrightarrow b = q_2 \cdot a = (q_2 \cdot q_1) \cdot d$
zu 6: $a = q_1 \cdot d, b = q_2 \cdot d \Longrightarrow ax + by = (q_1 \cdot d)x + (q_2 \cdot d)y = d \cdot (q_1 x + q_2 y)$

zu 7: $a = q \cdot d \Rightarrow a \cdot b = (q \cdot d) \cdot b = (q \cdot b) \cdot d = q' \cdot d$

Insbesondere ergibt sich aus Teil 6 mit $x = 1$ und $y = \pm 1$
Bem. Da jeder Teiler von a auch Teiler von -a ist (Punkt 8.) werden wir

uns häufig bei der Berechnung von Teilern (und später grössten Teilern) nur auf positive Zahlen beschränken.

Lemma 36 *Seien* d, a, b *ganze Zahlen mit* $d|a$ *und* $d|b$*. Dann ist auch* $d|a + b$ *bzw.* $d|a - b$

Bsp.: Sei d eine Zahl, welche 143 und 169 teilt. Da d dann auch die Differenz teilt, muss d ein Teiler von 26 sein, also 1,2 oder 13 sein. Durch Probe erhält man d=±1 oder d=±13.

Lemma 37 *Gelte für positive Zahlen* a *und* d *das* d a *teilt* $(d|a)$*. Dann ist:* $d = a$ *oder* $d \leq \frac{a}{2}$

Beweis: Es ist $a = qd$.Ist q=1, so ist $d = a$.Sonst ist q≥ 2 und damit

$$a = qd \geq 2d$$

und damit $d \leq \frac{a}{2}$.

Für beliebige - auch negative - Zahlen ergibt sich entsprechend:

Lemma 38 *Gelte* $d|a, a \neq 0$*.Dann ist:* $|d| = |a|$ *oder* $|d| \leq \left|\frac{a}{2}\right|$.

Insgesamt gilt (wie in Satz 35 Nr. 10) abgeschwächt für Zahlen, $d \neq 0$, die a teilen

$$|d| \leq |a|$$

Folgerung: Eine Zahl a, die von einem positivem d geteilt wird, liege zwischen $-(d-1)$ und $(d-1)$, so ist $a = 0$.

Ann.: Sei $a \neq 0$: Dann ist $|a| \leq d - 1 < |d|$. Im Widerspruch zu $|d| \leq |a|$. Damit gilt $a = 0$.

2.1.2 Der größte gemeinsame Teiler (a,b)

Definition 39 *$T_a = \{d|a\}$ heisst die Teilermenge von a.*

Also: $T_1 = \{-1, 1\}, \qquad T_0 = \mathbb{Z}, \qquad T_a = T_{-a}, \qquad |T_a| < \infty$

Definition 40 *Elemente aus $T_a \cap T_b$ heissen gemensame Teiler (g.T.) von a und b. Für positive a und b heisst*

$$\max(T_a \cap T_b) \tag{2.1}$$

grösster gemeinsamer Teiler (ggt) von a und b. Schreibweise (a, b).

Es gilt:

$$\begin{aligned} (a,b) &= (b,a) && (2.2)\\ (a,0) &= a && (2.3)\\ 1 &\leq (a,b) \leq \min(a,b) && (2.4) \end{aligned}$$

Bem.: Es wird zusätzlich definiert:

$$(0,0) := 0 \tag{2.5}$$

Bem.: $(a, b) = 1$ bedeutet ± 1 sind die einzigen gemeinsamen Teiler von a und b. Solche Zahlen heissen "teilerfremd".

Da $(a, b) = (-a, b) = (a, -b) = (-a, -b)$ betrachten wir wie bereits oben erwähnt den ggt zweier postiver Zahlen.

Lemma 41 *Sei $a, b > 0, (a, b) = b \Leftrightarrow b|a$*

Bew.:
$\Rightarrow$Trivial: b ist gemeinsamer Teiler von a und b und daher auch von a.
$\Leftarrow$ Sei b ein Teiler von a. Da b grösster Teiler von sich selbst ist, ist er auch größtmöglicher gemeinsamer Teiler von a und b.Da b Teiler ist, gilt $(a, b) = b$

Lemma 42 $(a,b) = d \Longrightarrow (\frac{a}{d}, \frac{b}{d}) = 1$

Bew.: Klar, dass $\frac{a}{d}$ bzw. $\frac{b}{d}$ ganzzahlig und positiv. Sei

$$c = (\frac{a}{d}, \frac{b}{d}) \tag{2.6}$$

dann ist

$$\begin{array}{rclcl} \frac{a}{d} & = & q_1 c, & \qquad & \frac{b}{d} = q_2 c \\ a & = & q_1 cd, & & b = q_2 cd \end{array}$$

also $cd \in T_a \cap T_b$. Damit $cd \leq (a,b) = d$ und somit $c \leq 1$. Da $c = (\frac{a}{d}, \frac{b}{d}) \geq 1$ ergibt sich $c = 1$. q.e.d.

Satz 43 *(Division mit Rest) Seien a und b ganze Zahlen mit $a, b > 0$. Dann gibt es eindeutig bestimmte Zahlen q und r mit*

$$b = qa + r \text{ und } 0 \leq r < a$$

Bem.: Der Satz sichert Existenz und Eindeutigkeit von q und r.

1. Existenz: Sei $M = \{t | b - ta \geq 0\}$. M ist nicht leer (wähle t "klein genug") und nach oben beschränkt. Setze $q = \max M$ und $r = b - qa$.Damit $r \geq 0$ ist klar.Wäre $r \geq a$,so wäre auch

$$b - (q+1)a = b - qa - a = r - a \geq 0 \tag{2.7}$$

und damit $q + 1 \in M$ im Widerspruch zu $q = \max M$

2. Eindeutigkeit: Seien

$$\begin{array}{rcl} qa + r & = & q'a + r' \text{ mit } 0 \leq r, r' < |a| \\ (q - q')a & = & r' - r \end{array}$$

Also: a teilt $r' - r$. $r' - r$ liegt aber zwischen $-(a-1)$ und $(a-1)$. Damit ist $r' - r = 0$ und damit wiederum $r' = r$. Wegen $a \neq 0$ aber auch $q - q' = 0$, also $q = q'$.

Bem. q ist durch

$$\frac{b}{a} - 1 < q \leq \frac{b}{a} \tag{2.8}$$

eindeutig festgelegt.

Wichtige Erkenntnis zur Berechnung der Teiler ist:das jeder Teiler von a und b auch Teiler von r und a (trivial) ist.

Beweis: Sei t Teiler von a und b, also $a = mt$ und $b = nt$, dann ist $r = b - qa = nt - qmt = (n - qm)t$, also ist t Teiler von r.

Umgekehrt sei t Teiler von $a(= mt)$ und $r(= nt)$, dann ist $b = qa + r = qmt + nt = (qm + n)t$, also ist t Teiler von b. q.e.d.

Dies bedeutet

$$T_a \cap T_b = T_b \cap T_r \tag{2.9}$$

Gemäß der Division mit Rest sind also alle Teiler von a und b auch Teiler von r und a. Damit bleibt auch der ggt erhalten und es gilt

$$(b, a) = (a, r) \tag{2.10}$$

Wiederholte Anwendung führt wiederum zum Euklid'schen Algorithmus

Algorithmus 44 *Seien a und b Zahlen mit $a > 0$*
1. Berechne die Division mit Rest $b = qa + r$ mit $0 \leq r < a$
2.a) Ist $r = 0$, so ist (a,b)=a
b) Ist $r \neq 0$, so ist (b,a)=(a,r), Setze b:=a und a:=r und gehe zu 1.

Beispiel: Berechne den ggt von 20 und 56 ((56,20))

1.	$56 = 2 \cdot 20 + 16$	damit: (56,20)=(20,16)
2.	$20 = 1 \cdot 16 + 4$	(20,16)=(16,4)
3.	$16 = 4 \cdot 4 + 0$	(16,4)=4

Der ggt ist also der letzte positive Rest (in der vorletzten Zeile) des Euklid'schen Algorithmus.

(s.o.) Haben zwei Zahlen a und b den ggt (a,b)=1, so heißen diese Zahlen teilerfremd.

Übung: Zeigen Sie zwei aufeinanderfolgende Fibonacci-Zahlen sind teilerfremd. (Wie sieht der euklid'sche Algorithmus in diesem Fall aus?)

Satz 45 *Ist (a,b)=d, so existieren ganze Zahlen a' und b' mit $d = a \cdot a' + b \cdot b'$. Insbesondere gilt für teilerfremde Zahlen $1 = a \cdot a' + b \cdot b'$.*

Als Beweis kann der euklidische Algotithmus betrachtet werden. Ausgehend von der vorletzten Zeile kann der (a,b) rückwärts berechnet werden.

Am Beispiel:

$$\begin{aligned} 4 &= 20 - 1 \cdot 16 \text{ und } 16 = 56 - 2 \cdot 20 \text{ ist} \\ 4 &= 20 - 1 \cdot (56 - 2 \cdot 20) \\ 4 &= 3 \cdot 20 - 1 \cdot 56 \end{aligned}$$

Übung: Berechnen Sie d=(101,35) und bestimmen Sie die Zahlen a' und b' mit

$d = 101 \cdot a' + 35 \cdot b'$

Der Beweis wird wie gesagt aus dem euklidschen Algorithmus hergeleitet:

$$\begin{aligned} b &= q_1 a + r_2 \qquad \text{mit } 0 < r_2 < a \\ a &= q_2 r_2 + r_3 \qquad \text{mit } 0 < r_3 < r_2 \\ r_2 &= q_3 r_3 + r_4 \qquad \text{mit } 0 < r_4 < r_3 \\ &\vdots \\ r_{n-2} &= q_{n-1} r_{n-1} + r_n \qquad \text{mit } 0 < r_n < r_{n-1} \\ r_{n-1} &= q_n r_n \end{aligned}$$

Der Abbruch des Algorithmus muss wegen $a > r_2 > ... > r_n > 0$ zwingend erfolgen und es gilt

$$(b, a) = (a, r_2) = ...(r_{n-1}, r_n) = r_n \tag{2.11}$$

oder allgemeiner

$$T_a \cap T_b = T_b \cap T_r = ... = T_{r_n} = T_{(a,b)} \tag{2.12}$$

Dies bedeutet auch, das jeder gemeinsame Teiler auch ein Teiler des ggt ist.

Beispiel: Welches sind die gemeinsamen Teiler von 56 und 20 ? $T_{56} \cap T_{20} = T_4 = \{\pm 1, \pm 2, \pm 4\}$

Es stellt sich die Frage, ob man mit einer endlichen Anzahl von Schritten im euklidschen Algorithmus stets auskommt. Die Antwort liefert die Fibonacci-Folge, bei der die Anzahl der Schritte beliebig gross werden kann. Mit

$$f_{n+1} = f_n + f_{n-1} \qquad f_0 = f_1 = 1 \tag{2.13}$$

liefert der euklidsche Algorithmus zur Berechnung von (f_{n+1}, f_n)

$$\begin{aligned} f_{n+1} &= 1 \cdot f_n + f_{n-1} \\ f_n &= 1 \cdot f_{n-1} + f_{n-2} \\ &\vdots \\ f_2 &= 2 \cdot f_1 \end{aligned}$$

Es sind also stets n Schritte nötig. Die Fibonacci-Zahlen sind aber offensichtlich der "Worst-Case" für diesen Algorithmus.

Das der Aufwand bei kleinen Zahlen jedoch nicht beliebig gross ist, liefert quasi als Gegenstück das

Lemma 46 *Lame: Ist 0<a<b, so ist die Zahl der Schritte beim euklidschen Algorithmus nicht grösser als das fünffache der Ziffernzahl von a.*

Bew (zu zeigen für den WorstCase, also die Fibonacci-Zahlen, für f_0, f_1 trivial).: Induktion für $n \geq 1$ liefert zunächst, dass nach 5 Schritten in der Fibonacci Folge eine weitere Stelle hinzukommt. Also

$$f_{n+5} > 10 f_n.$$

n=1: $f_6 = 13 > 10 \cdot f_1 = 10$
$n \to n+1 : f_{n+6} = f_{n+5} + f_{n+4} > 10 f_n + f_{n+4} > 10 f_n + 10 f_{n-1} = 10 f_{n+1}$

Diese Induktion liefert fortgeführt dass nach $5l$ Schritten l Stellen erreicht sind.

$$f_{n+5l} > 10^l f_n \tag{2.14}$$

Ausgehend von $f_1 = 1$ ist damit nach mehr als $5l$ bzw $n \geq 5l + 1$ Schritten

$$10^l = 10^l \cdot f_1 < f_{5l+1} < f_{n+1} \tag{2.15}$$

d.h. f_{n+1} besitzt $l+1$ Ziffern. Besitzt f_{n+1} umgekehrt nur l Ziffern, so muss damit $n \leq 5l$ sein.

Bem.:Für $b = 144$ und $a = 89$ ist $n = 10$:

$$\begin{aligned} 144 &= 89 + 55 \\ 89 &= 55 + 34 \\ 55 &= 34 + 21 \\ 34 &= 21 + 13 \\ 21 &= 13 + 8 \\ 13 &= 8 + 5 \\ 8 &= 5 + 3 \\ 5 &= 3 + 2 \\ 3 &= 2 + 1 \\ 2 &= 2 \cdot 1 \end{aligned}$$

Der Faktor (a ist zweistellig$\Longrightarrow$maximal 10 Schritte) "5" kann also nicht weiter reduziert werden.

Satz 47 *1.* $(ac, bc) = (a, b)|c|$

2. Ist d gemeinsamer Teiler von a und b, dann ist $(\frac{a}{d}, \frac{b}{d}) = \frac{(a,b)}{|d|}$

Bew.: 1. Multiplikation im euklidschen Algorithmus jeder Zeile mit $|c|$
2. Nach 1. ist

$$(a, b) = (\frac{a}{d}d, \frac{b}{d}d) = (\frac{a}{d}, \frac{b}{d})|d| \quad \text{q.e.d.} \tag{2.16}$$

Bem. Damit ist insbesondere

$$(\frac{a}{(a,b)}, \frac{b}{(a,b)}) = 1 \tag{2.17}$$

Satz 48 *Ist* $(c, b) = 1$, *dann ist*

$$(ac, b) = (a, b)$$

Beweis: Sei $d_1 = (ac, b)$ und $d_2 = (a, b)$. (Gleichheit ist zu Zeigen), dann gilt

$$d_1|ac \text{ und } d_1|ab \implies d_1|(ac, ab) = (c, b)|a| = |a| \tag{2.18}$$
$$\implies d_1|a \tag{2.19}$$
$$\text{ebenso } d_1|b \text{ und damit } d_1|(a, b) = d_2 \tag{2.20}$$

Umgekehrt:

$$d_2|ac \text{ und } d_2|b \implies d_2|(ac, b) = d_1 \tag{2.21}$$

und damit $d_1 = d_2$

Beispiel: $(6 \cdot 5, 8) = (6, 8) = (2 \cdot 3, 8) = (2, 8) = 2$

Satz 49 *Ist* $(a, b) = 1 \implies (a^m, b^n) = 1$

Bew.: Durch Induktion über m folgt zunächst mit dem vorigen Satz $(a^m, b) = 1$. Dann liefert Induktion über n $(a^m, b^n) = 1$.

Satz 50 *Gilt d|ab und (a,d)=1* $\Rightarrow d|b$

Bew.: Es ist mit Satz 48 $(ab, d) = (b, d)$. Wegen $d|ab$ ist $d = (ab, d) = (b, d)$ und damit $d|b$.

Satz 51 *$\sqrt[n]{a}$ ist ganz oder irrational.*

Bew.: Sei $\sqrt[n]{a} = \frac{p}{q}$ mit $(p,q) = 1$. Dann ist

$$\begin{aligned} a &= \left(\frac{p}{q}\right)^n \\ a \cdot q^n &= p^n \\ \text{Insbesondere} &: \ p^n | a \cdot q^n \\ \text{Nach vorigem Satz ist aber } (p^n, q^n) &= 1 \\ \text{also} &: \ p^n | a \text{ bzw. } a = l \cdot p^n \\ \text{Damit} &: \ l \cdot q^n = 1 \\ \text{Deshalb} &: \ q = 1 \\ \text{Also} &: \ \sqrt[n]{a} = p \in \mathbb{Z} \end{aligned}$$

2.1.3 Das kleinste gemeinsame Vielfache (kgV)

Nun bezeichne V_a die Vielfachen einer Zahl a. Es gilt damit

1. $0 \in V_a$
2. $V_0 = \{0\}$
3. $V_a = V_{-a} = V_{|a|}$

Genau wie zuvor die gemeinsamen Teiler zweier Zahlen a und b betrachtet wurden, untersuchen wir nun gemeinsame Vielfache (Abk. g.V.), also Elemente $V_a \cap V_b$.

Definition 52 *Für $a \neq 0$ und $b \neq 0$ ist $\min(V_a \cap V_b \cap \mathbb{N})$ das kleinste gemeinsame Vielfache von a und b. Notation: $[a,b]$*

Vereinbarung: $[0,b] = [a,0] = 0$

Es ist damit

1.$[a,b] = [b,a] = [|a|,|b|]$
2.$[a,b] = |b| \Longleftrightarrow a|b$

3.Für $a \neq 0$ und $b \neq 0$ ist $1 \leq [a,b] \leq |a| \cdot |b|$

Sei nun $a \neq 0$ und $b \neq 0$. Mit

$$\begin{aligned} a_1 &= \frac{a}{(a,b)} \\ b_1 &= \frac{b}{(a,b)} \end{aligned}$$

ist $(a_1, b_1) = 1$. Jedes gemeinsame Vielfache v von a und b ist darstellbar als

$$\begin{aligned} v &= qa = rb \\ &\quad \text{Dies ergibt nach Division durch } (a,b) \\ qa_1 &= rb_1 \end{aligned}$$

Damit gilt

$$b_1 | qa_1 \tag{2.22}$$

Da $(a_1, b_1) = 1$ gilt

$$\begin{aligned} & b_1 | q \\ b_1 l &= \frac{b}{(a,b)} l = q \end{aligned}$$

Daher

$$v = qa = \frac{ab}{(a,b)} l \tag{2.23}$$

Jedes Vielfache ist also von der Gestalt $\frac{ab}{(a,b)} l$, $l \in \mathbb{Z}$. Das kleinste gemeinsame Vielfache ergibt sich (je nach Vorzeichen von a und b) durch $l = \pm 1$. Dies ist ein Vielfaches beider Zahlen, da

$$\frac{ab}{(a,b)} = a\frac{b}{(a,b)} = b\frac{a}{(a,b)}$$

Also

$$[a,b] = \frac{|ab|}{(a,b)}$$

Dies liefert:

Satz 53 $(a,b)\,[a,b] = |ab|$

Dies wiederum eingesetzt bedeutet, dass jedes gemeinsame Vielfache von a und b die Darstellung

$$v = \frac{ab}{(a,b)} l = [a,b] \cdot l \tag{2.24}$$

hat. Damit ist ein gemeinsames Vielfaches auch Vielfaches des kleinsten gemeinsamen Vielfachen, also $V_a \cap V_b = V_{[a,b]}$

Beispiel: $[4,6] = \frac{4 \cdot 6}{(4,6)} = \frac{24}{2} = 12$, $V_4 \cap V_6 = V_{[4,6]} = \{\pm 0, \pm 12, \pm 24, \pm 36, ...\}$

2.1.4 Primzahlen und Primfaktoren

Definition 54 *Eine Zahl p>1 heisst Primzahl, wenn p nur die trivialen Teiler* ± 1 *und* $\pm p$ *besitzt.*

Analog können Primzahlen definiert werden durch:

"Für eine Zerlegung einer Primzahl $p = ab$ gilt stets $a = \pm 1$ oder $b = \pm 1$" oder "Für eine Zerlegung einer Primzahl $p = ab$ gilt stets $a = \pm p$ oder $b = \pm p$"

Die Primzahlfolge beginnt mit 2,3,5,7,11,13,17,19,23,29,31,...

Bem.: Obige Folge zeigt, Primzahlen werden immer seltener (dünner) desto grösser der Zahlenbereich wird. Aber: Es gibt unendlich viele Primzahlen (Beweis später) und es ist ein mathematischer "Sport" die nächst grössere zu finden. Weiterhin lässt sich zeigen, dass die Primzahldichte so gross ist, dass

$$\sum \frac{1}{p} \text{ divergiert} \tag{2.25}$$

Definition 55 *Ist n keine Primzahl, so heisst die Zahl zusammengesetzt.*

Satz 56 *Jedes n>1 besitzt einen Teiler der Primzahl ist. (sog. Primteiler)*

Bew,: Betrachte die Menge $M = \{d > 1 \text{ und } d|n\}$. Die Menge ist nichtleer (n selber gehört hierzu) und nach unten beschränkt (da alle Elemente >1). Wir betrachten das kleinste Element p dieser Menge. Wäre dieser Teiler kein Primteiler, so existiert ein q mit $q|p$ und $1 < q < p$. Dieses q würde aber auch n teilen im Widerspruch zur Minimalität von p.

Satz 57 *(Euklid) Es gibt unendlich viele Primzahlen*

Wir nehmen an, es gäbe nur endlich viele Primzahlen und $p_{\max}$ sei die grösste. Nach vorigem Satz hat dann aber auch

$$p_{\max}! + 1 \tag{2.26}$$

einen Primteiler p. $p_{\max}!$ wird aber von allen Zahlen von 2 bis $p_{\max}$ geteilt.Diese Zahlen teilen somit nicht $p_{\max}! + 1$. Die Primzahl p als Teiler dieser Zahl ist somit größer als $p_{\max}$ im Widerspruch zur Maximalität von $p_{\max}$.

Satz 58 *Für $a \neq 0$ gilt*

$$(p,a) = \begin{array}{ll} 1 & \textit{falls } p \textit{ kein Teiler von } a \\ p & \textit{falls } p \textit{ Teiler von } a \end{array} \tag{2.27}$$

Bew.: p hat nur die Teiler ± 1 und $\pm p$.Ist p kein Teiler von a,so ist $(p,a) = 1$.Ist p Teiler von a, so ist damit $(p,a) = p$.

Also: $(p,a) = 1 \Leftrightarrow p \nmid a$

Damit gilt insbesondere: Zwei Primzahlen sind genau dann verschieden, wenn $(p_1, p_2) = 1$

Satz 59 $p|ab \Longrightarrow p|a$ *oder* $p|b$

Bew.: Ann.: p teile weder a noch $b \Longrightarrow (p,b) = 1 \Longrightarrow (p,ab) = 1 \Longrightarrow p \nmid ab$

Fortgeführt ergibt dies:

Satz 60 $p|p_1p_2....p_n \Longrightarrow$ *ex. ein* m *mit* $p = p_m$

Nach Satz 56 exisitert damit zu jeder Zahl eine Zerlegung

$$n = p_1p_2....p_r \tag{2.28}$$

Satz 61 *(Hauptsatz der Zahlentheorie):Bis auf die Reihenfolge der Faktoren ist die Primfaktorzerlegung eindeutig.*

Bew. Seien $n = p_1p_2....p_r = q_1....q_s$ zwei verschiedene Zerlegungen, wobei ohne Einschränkung $r \leq s$ und die Primfaktoren der grösse nach sortiert seien. Es gilt

$$p_1|q_1....q_s \tag{2.29}$$

Somit muss p_1 mit einem Prifaktor q_j übereinstimmen, also nach ggf Ummumerierung $p_1 = q_1$. Damit verbleibt

$$p_2....p_r = q_2...q_s \tag{2.30}$$

Dieses wird fortgeführt bis

$$1 = q_{r+1}....q_s \tag{2.31}$$

Dies ist wegen $q_j > 1$ nicht möglich, also $r = s$.

Durch Zusammenfassung gleicher Primfaktoren erhält man zu jeder Zahl eine eindeutige Zerlegung

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot ... \cdot p_r^{e_r} \tag{2.32}$$

("Kanonische Primzerlegung")

Übung: Bei einem Ozeandampfer weiß man, das das Produkt vom Alter des Kapitäns in Jahren (welche der Schiffslänge in Metern entspricht), der Anzahl seiner Kinder und der Länge des Schiffes in Metern gerade 6627 ist. Wie alt ist der Kapitän ?

2.1.5 Bekannte Primzahlen

Zu den bekanntesten Primzahlen zählen die Primzahlen der Form

$$2^n + 1 \tag{2.33}$$

und

$$2^n - 1 \tag{2.34}$$

Im folgenden sei nur gezeigt, welche Gestalt der Exponent haben muss, damit überhaupt eine Lösung existieren kann.

2.1.6 Mersennesche Primzahlen

Definition 62 *Zahlen der Gestalt*

$$M_n = 2^n - 1 \tag{2.35}$$

heissen Mersennesche Zahlen. Sind Sie prim, spricht man von Mersenneschen Primzahlen.

Notwendige Vorraussetzung ist das der Exponent eine Primzahl n=p ist. Wäre der Exponent eine zusammengesetzte Zahl n=pq, so wäre M_n durch $2^q - 1$ teilbar,da

$$\frac{2^{pq} - 1}{2^q - 1} = \frac{(2^q)^p - 1}{2^q - 1} = 1 + 2^q + 2^{2q} + ... + 2^{(p-1)q} \tag{2.36}$$

damit die Lösung der Division gemäss der geometrischen Reihe liefert.

Die ersten Mersenneschen Primzahlen sind

p	M_p	Prim ?
2	3	Ja
3	7	Ja
5	31	Ja
7	127	Ja
11	2047	$Nein$ - $23 \cdot 89$

Bis heute sind 31 Mersenneschen Primzahlen bekannt.

2.1.7 Fermatsche Primzahlen

Definition 63 *Zahlen der Gestalt*

$$F_n = 2^n + 1 \tag{2.37}$$

heissen Fermatsche Zahlen. Sind Sie prim, spricht man von Fermatschen Primzahlen.

Notwendige Vorraussetzung ist das der Exponent eine Zweierpotenz n=2^k ist. Enthielte der Exponent einen ungeraden Anteil n=g·u, so wäre F_n durch $1+2^g$ teilbar,da

$$\frac{1+2^{g\cdot u}}{1+2^g} = \frac{1-(-2^g)^u}{1-(-2^g)} = 1 + (-2^g) + (-2^g)^2 + ... + (-2^g)^{(u-1)} \tag{2.38}$$

damit die Lösung der Division gemäss der geometrischen Reihe liefert.

Die ersten Fermatschen Primzahlen sind

k	F_p	Prim ?
1	5	Ja
2	17	Ja
3	257	Ja
4	65537	Ja
5	4294 967 297	$Nein$ - $641 \cdot 6700\,417$ s.o.

Bis heute sind keine weiteren Fermatschen Primzahlen bekannt noch ist deren Existenz bewiesen.

Satz 64 *Sei $n = p_1^{e_1} \cdot p_2^{e_2} \cdot ... \cdot p_r^{e_r}$ die kanonische Primzerlegung von n, so sind die Teiler von n*

$$T_n = \{\pm p_1^{l_1} \cdot p_2^{l_2} \cdot ... \cdot p_r^{l_r} | 0 \leq l_1 \leq e_1, 0 \leq l_2 \leq e_2, ..., 0 \leq l_r \leq e_r\} \tag{2.39}$$

Bew.: Aus der Eindeutigkeit der kanonischen Zerlegung klar.

Bsp.:12=$2^2 \cdot 3$. Damit ergeben sich alle Teiler: $2^0 \cdot 3^0 = 1, 2^1 \cdot 3^0 = 2, 2^2 \cdot 3^0 = 4, 2^0 \cdot 3^1 = 3, 2^1 \cdot 3^1 = 6, 2^2 \cdot 3^1 = 12$.

Wir sehen: Für die erste Stelle können wir 3 verschiedene Potenzen verwenden (0,1,2), für die zweite 2 und damit exisiteren 6 verschiedene Teiler. Allgemein werde die Anzahl der Teiler ≥ 1 mit $\tau(n)$ "Teilerfunktion" bezeichnet und es gilt somit

$$\tau(n) = \#T_n \cap \mathbb{N} \tag{2.40}$$

Es gilt wie oben bereits gesehen:

$$\tau(n) = (e_1 + 1) \cdot (e_2 + 1) \cdot ... \cdot (e_r + 1) \tag{2.41}$$

Nun zum Satz von Euler:

Satz 65 $\sum_{p\ prim} \frac{1}{p}$ *divergiert*

Bew.:

Der Beweis wird dabei in folgende Schritte zerlegt:
1. $\sum_{p\leq s} \frac{1}{p} \geq \frac{1}{2} \sum_{p\leq s} -\log(1 - \frac{1}{p})$ bzw. $\sum_{p\leq s} -\log(1 - \frac{1}{p}) \leq \sum_{p\leq s} 2 \cdot \frac{1}{p}$

2. Dann wird die Divergenz von

$$\begin{aligned} \lim_{s\to\infty} \sum_{p\leq s} -\log(1 - \frac{1}{p}) &= \lim_{s\to\infty} \sum_{p\leq s} \log \left(\frac{1}{1 - \frac{1}{p}} \right) \\ &= \lim_{s\to\infty} \log \left(\prod_{p\leq s} \frac{1}{1 - \frac{1}{p}} \right) \end{aligned}$$

gezeigt, in dem für jede feste Primzahl der Term $\frac{1}{1 - \frac{1}{p}}$ durch seine geometrische Reihe ersetzt wird. Führen wir den Beweis in umgekehrter Reihenfolge durch:

Zunächst gilt für jede (feste) Primzahl p, da p$\geq$ 2 :

$$1 + \frac{1}{p} + \frac{1}{p^2} + ... = \frac{1}{1 - \frac{1}{p}} \tag{2.42}$$

Deshalb

$$\prod_{p\leq s} \frac{1}{1 - \frac{1}{p}} = \prod_{p\leq s} (1 + \frac{1}{p} + \frac{1}{p^2} + ...) \tag{2.43}$$

Seien die Primzahlen bis s die Zahlen $p_1, ..., p_r$

$$\prod_{p \leq s} \frac{1}{1 - \frac{1}{p}} = \prod_{i=1}^{r} (1 + \frac{1}{p_i} + \frac{1}{p_i^2} + ...)$$

Ausmultiplizieren ergibt

$$\prod_{p \leq s} \frac{1}{1 - \frac{1}{p}} = \prod_{i=1}^{r} (1 + \frac{1}{p_i} + \frac{1}{p_i^2} + ...) = \sum_{e_1, e_2, ..., e_r = 0}^{\infty} \frac{1}{p_1^{e_1} \cdot p_2^{e_2} \cdot ... \cdot p_r^{e_r}} \geq \sum_{n \leq s} \frac{1}{n}$$

Da aber $\sum \frac{1}{n}$ divergiert (harmonische Reihe), muss auch $\prod_{i=1}^{r} (1 + \frac{1}{p_i} + \frac{1}{p_i^2} + ...)$ divergieren. Bilden wir den Logarithmus der linken Seite, so muss auch dieser divergieren, wenn wir $s \to \infty$ betrachten:

$$\begin{aligned} \lim_{s \to \infty} \log(\prod_{p \leq s} \frac{1}{1 - \frac{1}{p}}) &= \lim_{s \to \infty} \sum_{p \leq s} \log(\frac{1}{1 - \frac{1}{p}}) && (2.44) \\ &= \lim_{s \to \infty} \sum_{p \leq s} -\log(1 - \frac{1}{p}) \longrightarrow \infty && (2.45) \end{aligned}$$

Nun zum ersten Teil des Beweises: Es ist gemäss Taylor ($x = \frac{1}{p}$ ist eine Zahl zwischen 0 und $\frac{1}{2}$)

$$\begin{aligned} \log(z) &= \sum_{n=1}^{\infty} (-1)^{n+1} \frac{1}{n} (z-1)^n \\ \log(1-z) &= \sum_{n=1}^{\infty} (-1)^{n+1} \frac{1}{n} (-z)^n \\ &= -\sum_{n=1}^{\infty} \frac{z^n}{n} \end{aligned}$$

$$\begin{aligned} -\log(1-x) &= x + \frac{x^2}{2} + \frac{x^3}{3} + ... \\ &\leq x + x^2 + x^3 + ... \\ &= 1 + x + x^2 + x^3 + ... - 1 \\ &= \frac{1}{1-x} - 1 = \frac{x}{1-x} \leq \frac{x}{\frac{1}{2}} = 2x \qquad \text{für } 0 \leq x \leq \frac{1}{2} \end{aligned}$$

Und damit:

$$\sum_{p \leq s} -\log(1 - \frac{1}{p}) \leq \sum_{p \leq s} 2 \cdot \frac{1}{p} \qquad (2.46)$$

Somit divergiert auch $\sum 2 \cdot \frac{1}{p}$ und damit schliesslich $\sum \frac{1}{p}$ (q.e.d.)

Zur Konvergenzgeschwindigkeit sei noch bemerkt, dass wegen

$$\sum_{k=1}^{n} \frac{1}{k} \approx \log n$$

gilt (wir haben diese Divergenz mit Hilfe des Logarithmus der obigen Funktion gezeigt):

$$\sum_{p \leq s} \frac{1}{p} \geq \log \log s \tag{2.47}$$

2.1.8 Lineare diophantische Gleichungen

Definition 66 *Eine Gleichung in $f(x_1,...,x_r) = 0$, welche nur ganzzahlige Lösungen für x_i zulässt, heißt diophantische Gleichung.*

Definition 67 *Speziell:*

$$a_1x_1 + a_2x_2 + ... + a_rx_r = k$$

heisst lineare diophantische Gleichung.

Im Falle $r = 2$:

$$ax + by = k \tag{2.48}$$

Für die Lösbarkeit erkennt man das auf der linken Seite ein Vielfaches von (a, b) steht, also gelten muss

$$(a, b)|k \tag{2.49}$$

$$k = q \cdot (a, b) \tag{2.50}$$

Andererseits lässt sich der ggt gemäss euklidschem Algorithmus stets darstellen als

$$ax' + by' = (a, b) \tag{2.51}$$

und damit

$$a \cdot qx' + b \cdot qy' = k \tag{2.52}$$

und wir haben eine Lösung der diophant. Gleichung gefunden mit

$$x_0 = qx',\ y_0 = qy' \tag{2.53}$$

Aus $ax + by = k$ und $ax_0 + by_0 = k$ ergibt sich weiterhin

$$a(x - x_0) + b(y - y_0) = 0$$

und mit $a = (a, b)a_1$ bzw. $b = (a, b)b_1$

$$a_1(x - x_0) + b_1(y - y_0) = 0 \tag{2.54}$$

Da $(a_1, b_1) = 1$ muss b_1 den Faktor $(x - x_0)$ teilen, also

$$x - x_0 = b_1 \cdot t \tag{2.55}$$

$$x = x_0 + b_1 \cdot t$$

$$x = x_0 + \frac{b}{(a, b)} \cdot t \tag{2.56}$$

Damit ergibt sich

$$\begin{aligned} a(x_0 + \frac{b}{(a, b)} \cdot t - x_0) + b(y - y_0) &= 0 \\ a\frac{b}{(a, b)} \cdot t + b(y - y_0) &= 0 \\ y - y_0 &= -\frac{a}{(a, b)} \cdot t \end{aligned}$$

$$y = y_0 - \frac{a}{(a, b)} \cdot t \tag{2.57}$$

Umgekehrt (Probe!) ist ein so gewähltes Paar x und y für jedes t eine Lösung. Deshalb:

Satz 68 *1. Die lineare diophantische Gleichung $ax + by = k$ ist genau dann lösbar, wenn $(a, b)|k$*

2. Eine Lösung (x_0, y_0) erhält man durch den euklidschen Algorithmus, alle weiteren Lösungen sind von der Gestalt

$$x = x_0 + \frac{b}{(a, b)} \cdot t \tag{2.58}$$

$$y = y_0 - \frac{a}{(a, b)} \cdot t \tag{2.59}$$

für beliebiges ganzzahliges t.

Beispiel:

Welche Lösungen besitzt die diophantische Gleichung

$$20x + 56y = 32 \tag{2.60}$$

und welche ist die Lösung mit kleinstem positivem y?

Es ist zunächst der ggt zu berechnen und zu überprüfen, ob dieser die rechte Seite teilt:

$$(20, 56) = 4 \tag{2.61}$$

und damit ist die Existenz der Lösung sichergestellt. Weiterhin ergibt sich aus dem euklidschen Algorithmus $4 = 3 \cdot 20 - 1 \cdot 56$ (s.o). Damit ist $x' = 3$ und $y' = -1$. Der Wert von q ergibt sich aus $q = \frac{32}{4} = 8$ und damit ergibt sich eine Lösung

$$x_0 = 8 \cdot 3 = 24 \tag{2.62}$$

$$y_0 = 8 \cdot (-1) = -8 \tag{2.63}$$

Probe: $20 \cdot 24 - 56 \cdot 8 = 32$

Die allgemeine Lösung ist

$$x = 24 + \frac{56}{4}t = 24 + 14t \tag{2.64}$$

$$y = -8 - \frac{20}{4}t = -8 - 5t \tag{2.65}$$

Positiv wird y für $t \leq -2$ also für $t = -2$ mit der Lösung $x = -4, y = 2$. Probe: $20 \cdot (-4) + 56 \cdot 2 = -80 + 112 = 32$

Anwendung: Wir wollen einen Brief mit 1 Euro frankieren und haben hierzu 5 Cent und 12 Cent-Briefmarken. Wieviele (und welche Möglichkeiten) gibt es dies zu tun?

Wir suchen also positive Lösungen x und y der diophantischen Gleichung

$$5x + 12y = 100$$

Lösungen existieren, da

$$(5, 12) = 1 | 100 \tag{2.66}$$

Zunächst ist gemäß euklidischem Algorithmus

$$1 = 5 \cdot 5 + (-2) \cdot 12$$

$$100 = 500 \cdot 5 + (-200) \cdot 12$$

Damit ist $x_0 = 500, y_0 = -200$ eine Lösung der Gleichung.
Die Allgemeine Lösung ist

$$\begin{aligned} x &= 500 + \frac{12}{1}t \\ y &= -200 - \frac{5}{1}t \end{aligned}$$

Wir suchen positive Lösungen:

$$500 + 12t \geq 0 \Longleftrightarrow t \geq -\frac{500}{12} = -41,67$$

$$-200 - \frac{5}{1}t \geq 0 \Longleftrightarrow t \leq -\frac{200}{5} = -40$$

Also existieren zwei Lösungen für t=-40 und t=-41:

$$\begin{aligned} t &= -40 : x = 500 - 480 = 20, y = -200 + 200 = 0 \text{ (20 5-er)} \\ t &= -41 : x = 500 - 492 = 8, y = -200 + 205 = 5 \text{ (8 5-er,5 12-er)} \end{aligned}$$

Interessiert uns nur die Anzahl der Möglichkeiten, so lässst sich auch hier mit einer diskreten Struktur dieses lösen. Hierzu werden 2 Möglichkeiten vorgestellt:

1. Polynomstrukturen: Die Lösung von

$$kx + ly = c \tag{2.67}$$

zu gegebenem k, l und c wird zunächst in eine Polynomgleichung überführt. Wir suchen Lösungen für

$$\begin{aligned} z^{kx+ly} &= z^c \\ z^{kx} \cdot z^{ly} &= z^c \end{aligned}$$

Dabei dürfen für x und y beliebige positive Zahlen verwendet werden. Dabei machen nur Zahlen für x zwischen 0 und $\frac{c}{k}$, für y zwischen 0 und $\frac{c}{l}$ Sinn.
Wir setzen alle Werte ein und summieren alle Resultate.

$$\begin{aligned} \sum_{x=0}^{\lfloor \frac{c}{k} \rfloor} \sum_{y=0}^{\lfloor \frac{c}{l} \rfloor} z^{kx} \cdot z^{ly} &= \sum_{x=0}^{\lfloor \frac{c}{k} \rfloor} z^{kx} \sum_{y=0}^{\lfloor \frac{c}{l} \rfloor} z^{ly} \\ &= (1 + z^k + ... + z^{\lfloor \frac{c}{k} \rfloor \cdot k}) \cdot (1 + z^l + ... + z^{\lfloor \frac{c}{l} \rfloor \cdot l}) \end{aligned}$$

und schauen welchen Vorfaktor der Faktor von z^c hat. Dieser Faktor ergibt sich aus den jeweiligen Möglichkeiten.

Bsp von oben $k = 5, l = 12, c = 100$:

$$(1 + z^5 + z^{10} + ... + z^{100}) \cdot (1 + z^{12} + ... + z^{96}) \tag{2.68}$$

Nach Ausmulitplikation ergibt sich der Term

$$2 \cdot z^{100} \tag{2.69}$$

Im Übrigen aus den beiden Mulitplikationen

$$z^{100} \cdot 1 \text{ und } z^{40} \cdot z^{60} \tag{2.70}$$

Der erste steht eben für die Möglichkeit 20 5-er zu verwenden, der zweite für 8 5-er und 5 12-er, wie oben.

2. Matrixstrukturen

Wir bilden nun eine Matrix bei der wir in der ersten Spalte 0,k,2k,....,$\left\lfloor \frac{c}{k} \right\rfloor \cdot k$, in der zweiten Spalte 0,l,....,$\left\lfloor \frac{c}{l} \right\rfloor \cdot l$ bilden und im Koeffizienten die Summe von Spalte und Zeile

Im Besipiel:

	0	12	24	36	48	60	72	84	96
0	0	...							
5	5								
10	10								
15	15								
20	20								
25	25								
30	30								
35	35								
40	40	52	64	76	88	**100**	112	...	
45	45								
50	50								
55	55								
60	60								
65	65								
70	70								
75	75								
80	80								
85	85								
90	90								
95	95								
100	**100**								

und schauen an welchen Stellen $c = 100$ angenommen wird. Auch hier finden wir die gleichen beiden Lösungen.

2.2 Kongruenzen

Teilbarkeit und Vielfache beruhten darauf, das zwei Zahlen in relation miteinander gebracht wurden. Insbesondere bei Teilbarkeit waren Zahlen gesucht die einander teilen, also bei der Division der grösseren durch die kleinere den Rest Null liessen. Aber wie kann man mit Zahlen rechnen, die bezüglich einer dritten Zahl (dem Modul) den gleichen Rest - nicht zwingenderweise Null - lassen?

Diese Themenstellung wird von den Kongruenzen beantwortet.

Definition 69 *Zwei Zahlen a und b heissen kongruent modulo m ($m \neq 0$), wenn $b-a$ ein Vielfaches von m ist, also $m|b-a$. Schreibweise:* $a \equiv b \bmod m$

Bem.: 1. Diese Zahlen lassen also bei der Division durch m den gleichen Rest.
2. Lassen die beiden Zahlen nicht den gleichen Rest, heissen sie inkongruent modulo m

Bsp: $25 \equiv -3 \bmod 4$

Bem.: Es gilt:
1. $a \equiv 0 \bmod m \Longleftrightarrow m|a$
2. $a = b \Longleftrightarrow a \equiv b \bmod m$ für alle m
3. $a \equiv b \bmod 1$ für alle a und b
4. $a \equiv b \bmod mn \Longrightarrow a \equiv b \bmod m$

Bew.: z.B. 4.

$$\begin{aligned} & & mn|b-a \\ qmn & = & b-a \\ (qm)n & = & b-a \\ & & n|b-a \end{aligned}$$

Satz 70 *Seien a und n teilerfremde Zahlen dann gibt es eine Zahl* $a' \in \{1, 2, ..., n-1\}$ *mit* $a \cdot a' \equiv 1 \bmod n$

Beweis: Es ist

$$1 = a \cdot a' + n \cdot b' \tag{2.71}$$

also

$$1 \equiv a \cdot a' \bmod n$$

Dabei ist $a' \neq 0$ und $a' \neq n$. Ist $a' > n$ oder $a' \leq 0$, so ist $a' = a'' + k \cdot n$ mit $a'' \in \{1, 2, ..., n-1\}$ und damit

$$1 = a \cdot (a'' + k \cdot n) + n \cdot b \equiv a \cdot a'' \bmod n \tag{2.72}$$

Definition 71 *Die Zahl a'' heißt Inverse von a modulo n und kann ohne Einschränkung zwischen 1 und $n-1$ gewählt werden.*

Satz 72 *Rechenregeln für Kongruenzen: Ist $a \equiv b \bmod m$ und $c \equiv d \bmod m$, so ist*

$$\begin{aligned} a \pm c &\equiv b \pm d \bmod m \\ ac &\equiv bd \bmod m \end{aligned}$$

Speziell für $d = c$:

$$\begin{aligned} a \pm c &\equiv b \pm c \bmod m \\ ac &\equiv bc \bmod m \end{aligned}$$

und für $a = c, b = d$ durch mehrmaliges anwenden

$$a^n \equiv b^n \bmod m$$

Da die unteren Fälle Spezialfälle sind, müssen nur die ersten beiden Gleichungen bewiesen werden.

Sei $a \equiv b \bmod m$ und $c \equiv d \bmod m$, so ist

$$\begin{aligned} & & m|b-a \\ q_1 m &= b-a \\ b &= q_1 m + a \end{aligned}$$

entsprechend

$$d = q_2 m + c$$

Dann ist aber

$$\begin{aligned} b \pm d &= q_1 m + a \pm (q_2 m + c) \\ &= a \pm c + (q_1 \pm q_2) m \end{aligned}$$

also

$$a \pm c \equiv b \pm d \bmod m$$

Multiplikation liefert

$$\begin{aligned} b \cdot d &= (q_1 m + a) \cdot (q_2 m + c) \\ &= m \cdot (q_1 c + q_2 a + q_1 q_2 m) + ac \end{aligned}$$

und damit

$$ac \equiv bd \bmod m$$

Anwendung: $2^{32}+1$ ist keine Primzahl. Beweis: Es ist $641 = 5 \cdot 2^7 + 1$ also

$$\begin{aligned} 5 \cdot 2^7 &\equiv -1 \bmod 641 \\ 5^4 \cdot 2^{28} &\equiv 1 \bmod 641 \end{aligned}$$

Andererseits ist $641 = 5^4 + 2^4$ und damit $5^4 \equiv -2^4 \bmod 641$

$$\begin{aligned} -2^4 \cdot 2^{28} &\equiv 1 \bmod 641 \\ -2^{32} &\equiv 1 \bmod 641 \\ 2^{32} &\equiv -1 \bmod 641 \end{aligned}$$

und damit

$$641 | 2^{32} + 1$$

Weiteres Beispiel: Zahlen der Gestalt 8l+7 (kongruent 7 modulo 8) lassen sich nicht durch die Summe dreier Quadratzahlen ausdrücken, also:
Es gibt keine Lösung zu

$$x^2 + y^2 + z^2 = 8l + 7$$

Wir rechnen modulo 8 und erhalten für x die möglichen Reste 0,1,...,7. Quadrieren ergibt

$$\begin{aligned} 0 &\to 0 \\ 1 &\to 1 \\ 2 &\to 4 \\ 3 &\to 1 \\ 4 &\to 0 \\ 5 &\to 1 \\ 6 &\to 4 \\ 7 &\to 1 \end{aligned}$$

Also drei verschiedene mögliche Reste (0,1, und 4). Gleiches gilt für y und z. Addition dieser drei Reste ergibt die möglichen Reste modulo 8: 0,1,2,3,4,5,6. q.e.d.

Bem.: Kongruenz mod m ist eine Äquivalenzrelation, d.h.
1. $a \equiv a \bmod m$
2. $a \equiv b \bmod m \Longrightarrow b \equiv a \bmod m$
3. $a \equiv b \bmod m, b \equiv c \bmod m \Longrightarrow a \equiv c \bmod m$

Deshalb zerfällt der Ring der ganzen Zahlen in Äquivalenzklassen (Restklassen modulo m) und jede Zahl fällt genau in eine Restklasse. Da hiermit die Restklasse eindeutig bestimmt wird, reicht die Angabe eines Repräsentanten a.

$$[a]_m = \{x | x \equiv a \bmod m\} \tag{2.73}$$

Zwei Zahlen gehören also dann in die gleiche Restklasse, wenn sie modulo m den gleichen Rest lassen. Daher gibt es m verschiedene Restklassen (Zahlen, die die Reste 0,1,...,m-1 haben). Eine Menge von Zahlen, die aus jeder Restklasse genau eine Zahl enthält heisst "vollständiges Restsystem" modulo m.

Zum Beweis das eine Menge vollständiges Restsystem ist, muss gezeigt werden:

Satz 73 *$\{r_1, r_2, ..., r_m\}$ vollständiges Restsystem $\Longleftrightarrow$ Aus $r_i \equiv r_k \bmod m$ folgt stets $i = k$ bzw. Aus $r_i \neq r_k \bmod m$ folgt stets $i \neq k$*

Beispiele:
1. {0,1,2,...,m-1} ist vollständiges Restsystem, ebenso {a,a+1,....,a+m-1}

2. Ist $\{r_1, r_2, ..., r_m\}$ vollständiges Restsystem, dann auch $\{a+r_1, a+r_2, ..., a+r_m\}$
3. Ist $\{r_1, r_2, ..., r_m\}$ vollständiges Restsystem und $(a, m) = 1$, dann auch $\{ar_1, ar_2, ..., ar_m\}$ volles Restsystem
4. Zu jedem beliebigem x existiert im vollständigem Restsystem $\{r_1, r_2, ..., r_m\}$

genau ein r_i mit $x \equiv r_i \bmod m$

Satz 74 *Sind $\{r_1, r_2, ..., r_m\}$ und $\{s_1, s_2, ..., s_n\}$ vollständige Restsystem modulo m bzw. n mit $(m, n) = 1$, dann ist $\{ms_i + nr_j | 1 \leq i \leq n, 1 \leq j \leq m\}$ vollständiges Restsystem modulo mn.*

Bew.: Sei $ms_{i_1} + nr_{j_1} \equiv ms_{i_2} + nr_{j_2} \bmod mn \Longrightarrow nr_{j_1} \equiv nr_{j_2} \bmod m \Longrightarrow r_{j_1} \equiv r_{j_2} \bmod m \Longrightarrow j_1 = j_2$ (entspr. $i_1 = i_2$)

Weitere Anwendung: Die Äquivalenzklasse

$$x \equiv 3 \bmod 4$$

enthält unendlich viele Primzahlen.Betrachte hierzu die Zahl $c = n! - 1$ für $n \geq 4$.c habe die Primfaktorzerlegung

$$c = p_1 \cdot ... \cdot p_r$$

Es gilt (da n!$\equiv 0 \bmod 4$) c$\equiv 3 \bmod 4$. Jeder dieser Primfaktoren ist grösser als n (Alle Zahlen von 1 bis n teilen n!) und insbesondere ungerade. Jeder

Primfaktor ist damit kongruent 1 oder 3 modulo 4. Wären alle $p_1, ..., p_r \equiv 1$, so auch

$$c = p_1 \cdot ... \cdot p_r \equiv 1 \bmod 4$$

im Widerspruch zur Annahme c$\equiv 3 \bmod 4$..

Satz 75 *Für jedes Polynom P(x) gilt:*
Ist $a \equiv b \bmod m$, *so auch* $P(a) \equiv P(b) \bmod m$

Definition 76 *Die Lösungszahl von P(x)*$\equiv k \bmod m$ *ist die Anzahl der Restklassen modulo m, in die die Lösungsmenge zerfällt.*

Bsp: $x^2 \equiv 1 \bmod 8$:

$$\begin{aligned} 1 &\rightarrow 1 \\ 2 &\rightarrow 4 \\ 3 &\rightarrow 1 \\ 4 &\rightarrow 0 \\ 5 &\rightarrow 1 \\ 6 &\rightarrow 4 \\ 7 &\rightarrow 1 \\ 8 &\rightarrow 0 \end{aligned}$$

hat also 4 Lösungen, nämlich [1],[3],[5] und [7].

Was ist aber mit der Division, wenn wir modulo m rechnen? Es ist offensichtlich

$$16 \equiv 2 \bmod 14 \tag{2.74}$$

Dividieren wir durch 2 erhalten wir das offensichtlich falsche Ergebnis

$$8 \equiv 1 \bmod 14 \tag{2.75}$$

Also ist die Division so nicht erlaubt.
Es gilt jedoch, wenn der Faktor c, durch den wir dividieren ein Faktor des Moduls ist, das

$$ac \equiv bc \bmod m|c| \Longrightarrow a \equiv b \bmod m$$

Bew.: klar (folgt aus den Teilbarkeitsregeln) -

$$\begin{aligned} (ac - bc) &= km|c| \\ a - b &= \pm km \\ a &\equiv b \bmod m \end{aligned}$$

Was ist jedoch wenn der Faktor nicht im Modul vorkommt? Z.B.

$$20 \equiv 50 \bmod 15 \tag{2.76}$$

Eine Division durch 10 geht an dieser Stelle nicht im Modul. Hier gilt:

$$ac \equiv bc \bmod m \Longrightarrow a \equiv b \bmod \frac{m}{(m,c)} \tag{2.77}$$

Zunächst der Beweis: Mit $m = (c,m) \cdot m'$ und $c = (c,m) \cdot c'$ ist wegen $c \cdot (a-b) = qm$ auch $c' \cdot (a-b) = qm'$ und damit teilt wg $(c', m') = 1$ der Wert $a - b$ den Wert $m' = \frac{m}{(m,c)}$ also die Beh.

Also oben:

$$\begin{aligned} 2 &\equiv 5 \bmod \frac{15}{5} \\ 2 &\equiv 5 \bmod 3 \end{aligned}$$

Insbesondere darf der Modul unverändert gelassen werden, wenn der Divisor teilerfremd zum Modul ist:

$$-3 \equiv 18 \bmod 7$$

Daher gilt:

$$-1 \equiv 6 \bmod 7 \tag{2.78}$$

2.2.1 Prime Restklassen

Satz 77 *Ist* $a \equiv b \bmod m \Longrightarrow (a,m) = (b,m)$

Bew.: wg a=qm+b aus der ggt-Theorie Also ist mit einem Repräsentanten

der ggt für alle Zahlen dieser Restklasse definiert.

Definition 78 *Eine Restklasse* $[a]_m$ *heisst zu* m *prime Restklasse, wenn* $([a]_m, m) = 1$

Dies bedeutet, das ein (beliebiger) - und damit alle - Repräsentant teilerfremd zum Modul ist.

Definition 79 *Eulersche* $\varphi-$*Funktion. Sei* $\varphi(m) = \#\{a | 1 \leq a \leq m$ *und* $(a,m) = 1\}$

Bem.: $\varphi(m)$ entspricht also den teilerfremden Zahlen zu m oder analog der Anzahl der primen Restklassen.

Bsp: 1. $m = 6 \Longrightarrow \{1, 5\}$ ist primes Restsystem und $\varphi(6) = 2$

2. p Primzahl $\Longrightarrow \varphi(p) = p - 1$ (Die Zahlen von 1 bis p-1)

3. $\phi(p^e)$: Die teilerfremden Zalen zu p^e sind alle Zahlen ausser den Vielfachen von p

$$p, 2p, ..., p^{e-1} \cdot p \tag{2.79}$$

also p^{e-1} Stück, damit

$$\begin{aligned} \phi(p^e) &= p^e - p^{e-1} \\ &= p^e \cdot (1 - \frac{1}{p}) \end{aligned}$$

Satz 80 *Sind $\{r_1, r_2, ..., r_{\phi(m)}\}$ und $\{s_1, s_2, ..., s_{\phi(n)}\}$ prime Restsysteme modulo m bzw. n mit $(m, n) = 1$, dann ist $\{ms_i + nr_j | 1 \leq i \leq n, 1 \leq j \leq m\}$ primes Restsystem modulo mn.*

Bew.: Seien $\{r_1, r_2, ..., r_{\phi(m)}, ..., r_m\}$ und $\{s_1, s_2, ..., s_{\phi(n)}, ..., n\}$ die vollständigen Restsysteme modulo m bzw. n, d.h. für $j > \phi(m)$ bzw $i > \phi(n)$ gilt $(r_j, m) > 1$ bzw. $(s_i, n) > 1$. Dann ist nach Satz 74 $\{ms_i + nr_j | 1 \leq i \leq n, 1 \leq j \leq m\}$ vollständiges Restsystem modulo mn. Zu zeigen bleibt, dass $(ms_i + nr_j, mn) > 1$ genau dann gilt, wenn $j > \phi(m)$ oder $i > \phi(n)$. Dies bedeutet, dass dann die durch $1 \leq i \leq n, 1 \leq j \leq m$ erzeugten Elemente gerade das prime Restsystem bilden und die anderen nicht zu $\phi(mn)$ gehören.

Teil 1:"$\Longrightarrow$ " : Sei $(ms_i + nr_j, mn) > 1$. Dann existiert ein Primteiler p ((p,n)=(p,m)=1) mit $p | ms_i + nr_j$ und $p | mn$. Ohne Einschränkung wg (m,n)=1 gelte $p | m$. Dann gilt auch $p | ms_i + nr_j - ms_i = nr_j$. und da (p,n)=1 gilt $p | r_j$ und damit $(r_j, m) \geq p > 1$,da p ja auch m teilt. Damit gilt $j > \phi(m)$ q.e.d.

Teil 2:"$\Longleftarrow$ " : Sei $j > \phi(m)$ bzw. $(r_j, m) > 1$. Wegen $(r_j, m) | ms_i + nr_j$ und $(r_j, m) | mn$ gilt $(ms_i + nr_j, mn) \geq (r_j, m) > 1$ q.e.d

Damit ergibt sich insbesondere für die Anzahl der teilerfremden Elemente und damit für die Anzahl primer Repräsentanten:

$$\varphi(mn) = \phi(m) \cdot \phi(n) \text{ für } (m, n) = 1 \tag{2.80}$$

Übung: Bilden Sie aus den primen Restsystemen modulo 3 und 4 nach vorigem Satz das prime Restsystem modulo 12.

Per Induktion ergibt sich:

Für $n = p_1^{e_1} \cdot p_2^{e_2} \cdot ... \cdot p_r^{e_r}$ ist

$$\begin{aligned}\phi(n) &= \phi(p_1^{e_1} \cdot p_2^{e_2} \cdot ... \cdot p_r^{e_r}) \\ &= \phi(p_1^{e_1}) \cdot ... \cdot \phi(p_r^{e_r}) \\ &= p_1^e \cdot (1 - \frac{1}{p_1}) \cdot p_2^e \cdot (1 - \frac{1}{p_2}) \cdot ... \cdot p_r^e \cdot (1 - \frac{1}{p_r}) \\ &= n \cdot \prod_{i=1}^{r} (1 - \frac{1}{p_i}) = n \cdot \prod_{p_i | n} (1 - \frac{1}{p_i})\end{aligned}$$

Beispiel: $\phi(720)$ Zunächst die Primfaktorzerlegung

$$720 = 2^4 \cdot 3^2 \cdot 5$$

Damit

$$\begin{aligned}\phi(720) &= 720 \cdot \frac{2-1}{2} \cdot \frac{3-1}{3} \cdot \frac{5-1}{5} \\ &= 24 \cdot 2 \cdot 4 = 192\end{aligned}$$

Schliesslich sei noch erwähnt,. dass die Summe der eulerschen $\phi-$Funktionen aller positiven Teiler einer Zahl m wiederum diese Zahl ergibt, also

$$\sum_{d|n, d>0} \phi(d) = n$$

Bew.: Es ist zu

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot ... \cdot p_r^{e_r}$$

wie oben erläutert

$$T_n = \{\pm p_1^{l_1} \cdot p_2^{l_2} \cdot ... \cdot p_r^{l_r} | 0 \leq l_1 \leq e_1, 0 \leq l_2 \leq e_2, ..., 0 \leq l_r \leq e_r\}$$

und damit

$$\begin{aligned}\sum_{d|n, d>0} \phi(d) &= \sum_{0 \leq l_1 \leq e_1, 0 \leq l_2 \leq e_2, ..., 0 \leq l_r \leq e_r} \phi(p_1^{l_1} \cdot p_2^{l_2} \cdot ... \cdot p_r^{l_r}) \\ &= \sum_{0 \leq l_1 \leq e_1, 0 \leq l_2 \leq e_2, ..., 0 \leq l_r \leq e_r} \phi(p_1^{l_1}) \cdot \phi(p_2^{l_2}) \cdot ... \cdot \phi(p_r^{l_r}) \\ &= \sum_{0 \leq l_1 \leq e_1, 0 \leq l_2 \leq e_2, ..., 0 \leq l_r \leq e_r} \prod_{i=1}^{r} \phi(p_i^{l_i}) \\ &= \prod_{i=1}^{r} \sum_{0 \leq l_1 \leq e_1, 0 \leq l_2 \leq e_2, ..., 0 \leq l_r \leq e_r} \phi(p_i^{l_i}) \\ &= \prod_{i=1}^{r} \phi(p_i^0) + \phi(p_i^1) + ... + \phi(p_i^{e_i}) \\ &= \prod_{i=1}^{r} 1 + (p_i - 1) + (p_i^2 - p_i) + ... + (p_i^{e_i} - p_i^{e_i - 1}) = \prod_{i=1}^{r} p_i^{e_i} = n\end{aligned}$$

2.2.2 Die Sätze von Euler und Fermat

Die Elemente aus $\{a|1 \leq a \leq m \text{ und } (a,m) = 1\}$ bilden eine multiplikative Gruppe Z_m^*, denn ist (a,m)=1 so ex. a' und m' mit

$$aa' + mm' = 1 \tag{2.81}$$
$$aa' \equiv 1 \bmod m \tag{2.82}$$

Also ist a' die multiplikative Inverse zu a und umgekehrt. Andererseits kann auch a' gemäß $1 \leq a' \leq m$ gewählt werden und ist damit Element in Z_m^*. Damit wären Existenz und Abgeschlossenheit gezeigt. Das neutrale Element ist die 1 (f ür die ebenfalls gilt (1,m)=1). Verbleibt die Assoziativität (Vertauschbarkeit), wobei auch hier gilt

$$ab = ba \tag{2.83}$$

und damit insbesondere auch Gleichheit (sogar =1) modulo m.

Satz 81 *(Euler) Ist (a,m)=1, dann gilt*

$$a^{\varphi(m)} \equiv 1 \bmod m \tag{2.84}$$

Da die Gruppenordnung von Z_m^* gerade $\varphi(m)$ ist, muss fü r jedes Element der Gruppe gelten, dass Element hoch Gruppenordnung wiederum das neutrale Element ergibt.

Satz 82 *(Kleiner Satz von Fermat): Ist p Primzahl und a positiv und kein Vielfaches von p, so ist*

$$a^{p-1} \equiv 1 \bmod p \text{ bzw.} \tag{2.85}$$
$$a^p \equiv a \bmod p \tag{2.86}$$

Letztere Aussage gilt trivialerweise auch für a, die Vielfache von p sind.

Beweis: Variante A: Setze im Satze von Euler für m=p, so folgt die erste Zeile. Multiplikation mit a liefert dann Zeile 2.

Variante B: 1. Die Binomialkoeffizienten $\left(\begin{array}{c} p \\ k \end{array} \right), k = 1, ..., p-1$ erfüllen

$$\left(\begin{array}{c} p \\ k \end{array} \right) \equiv 0 \bmod p \tag{2.87}$$

da $\frac{p!}{(p-k)!k!}$ einen nicht kürzbaren Faktor p im Zähler hat. 2. Induktion über a I.Verankerung

$$1^p \equiv 1 \bmod p$$

I.Vorr.

$$a^p \equiv a \bmod p$$

I.Schluss

$$(a+1)^p = a^p + \left(\begin{array}{c} p \\ 1 \end{array} \right) a^{p-1} + ... + \left(\begin{array}{c} p \\ p-1 \end{array} \right) a + 1 \equiv a^p + 1 \equiv a + 1 \bmod p$$

Beispiel

$$3^{16} \equiv 1 \bmod 17$$

Probe:

$$\begin{aligned} 3^4 &= 13 \equiv -4 \bmod 17 && (2.88) \\ (-4)^2 &\equiv -1 \bmod 17 && (2.89) \\ 3^{16} &\equiv ((-4)^2)^2 \equiv 1 \bmod 17 && (2.90) \end{aligned}$$

2.2.3 Lineare Kongruenzen

Wir betrachten nun die Kongruenz in der Unbekannten x

$$ax \equiv k \bmod m \tag{2.91}$$

Satz 83 *Die Lösung von $ax \equiv k \bmod m$ ist entweder die leere Menge (für (a,m)$\nmid$ k) oder eine Restklasse mod $\frac{m}{(a,m)}$ (sonst)*

Bew

$$\begin{aligned} ax &\equiv k \bmod m \\ ax - k &= my \\ ax - my &= k \end{aligned}$$

Ist der ggt (a,m) kein Teiler der rechten Seite, so ist das System unlösbar, ansonsten gemäss Satz 68 Restklasse mod $\frac{m}{(a,m)}$.

Beispiele:

$$\begin{aligned} 3x &\equiv 2 \bmod 9 \text{ nicht lösbar, da } (3,9)=3 \nmid 2 \\ 16x &\equiv 14 \bmod 6 \text{ lösbar} \end{aligned}$$

Lösung:

$$\begin{aligned} 8x &\equiv 7 \bmod 3 \\ -x &\equiv 7 \bmod 3 \\ x &\equiv -7 \bmod 3 \\ x &\equiv 2 \bmod 3 \end{aligned}$$

Wie findet man nun strukturiert eine Lösung von

$$ax \equiv k \bmod m$$

Zunächst kann die Gleichung - falls eine Lösung existiert - durch (a,m) dividiert werden.

$$\frac{a}{(a,m)}x \equiv \frac{k}{(a,m)} \bmod \frac{m}{(a,m)} \tag{2.92}$$

oder neu benannt

$$a_1 x = k_1 \bmod m_1$$

Dann ist $(a_1, m_1) = 1$ und damit

$$a_1^{\phi(m_1)} \equiv 1 \bmod m_1$$

Damit finden wir eine Lösung. Denn für

$$x = k_1 \cdot a_1^{\phi(m_1)-1} \tag{2.93}$$

ist

$$a_1 x = k_1 \cdot a_1^{\phi(m_1)} \equiv k_1 \bmod m_1 \tag{2.94}$$

Bsp:

$$\begin{aligned} 16x &\equiv 14 \bmod 6 \text{ lösbar} \\ 8x &\equiv 7 \bmod 3 \end{aligned}$$

also $a_1 = 8, k_1 = 7, m_1 = 3$.
Damit

$$x = 7 \cdot 8^{2-1} = 56$$

Wie findet man nun die gesamte Lösungsmenge?

$$x = 56 \equiv 2 \bmod 3 \tag{2.95}$$

Wie findet man nun aus der Lösung

$$x \equiv 2 \bmod 3$$

alle Lösungen $x \equiv a \bmod 6$?

Satz 84 *Die Lösungszahl von* $ax \equiv k \bmod m$ *ist für* $(a,m)|k$ *gleich* (a,m)

Bew.:Zu einer Lösung x finden wir alle Lösungen (siehe ggt-Theorie)

$$x + \frac{m}{(a,m)}t \tag{2.96}$$

Zwei Lösungen sind gleich mod m?

$$\begin{aligned} x + \frac{m}{(a,m)}t_1 &\equiv x + \frac{m}{(a,m)}t_2 \bmod m \\ t_1 &\equiv t_2 \bmod \frac{m}{\frac{(a,m)}{m}} \\ t_1 &\equiv t_2 \bmod (a,m) \end{aligned}$$

Also: Durch Addition von (a,m) zu einer Lösung mod m erhalten wir alle Lösungen.

Im Beispiel: Lösung von

$$16x \equiv 14 \bmod 6$$

ist

$$x \equiv 2 \bmod 3$$

und damit modulo 6

$$\begin{aligned} x &\equiv 2 \bmod 6 \\ x &\equiv 5 \bmod 6 \end{aligned}$$

2.2.4 Der chinesische Restsatz

Wir betrachten das System in der Unbekannten x

$$\begin{aligned} x &\equiv a \bmod m \\ x &\equiv b \bmod n \end{aligned}$$

mit $(m,n) = 1$. Alle Zahlen seien nicht-negativ. Dann existiert eine (sogar eindeutige) Lösung in {0,1,...,mn-1}

Bew.: Zeige $x = a \cdot n^{\varphi(m)} + b \cdot m^{\varphi(n)}$ erfüllt beide Gleichungen. (trivial)

Noch allgemeiner lässt sich ein solches System mit

$$\begin{aligned} x &\equiv a \bmod m \\ x &\equiv b \bmod n \end{aligned}$$

mit $(m,n) = d$ (beliebig) lösen.

Das System bedeutet

$$x = k \cdot m + a \tag{2.97}$$
$$x = l \cdot n + b \tag{2.98}$$

und damit

$$k \cdot m - l \cdot n = b - a \tag{2.99}$$

Notwendig muss nun $(m,n)|(b-a)$ sein. Umgekehrt folgt hieraus $b - a = u \cdot (m,n)$ und damit bereits die Lösung des ursprünglichen Systems:

$$k_1 \cdot m - l_1 \cdot n = (m,n) \tag{2.100}$$
$$u \cdot k_1 \cdot m - u \cdot l_1 \cdot n = (m,n) \cdot u = b - a \tag{2.101}$$

Damit ist mit $k = u \cdot k_1$ und $l = u \cdot l_1$ eine Lösung gefunden. Einsetzen von $x = k \cdot m + a$ bzw. $x = l \cdot n + b$ leifert die Lösung.

Übung: Berechnen Sie eine Lösung von

$$x \equiv 7 \bmod 20$$
$$x \equiv .11 \bmod 56$$

Zunächst brauchen wir den euklidschen Algorithmus und erhalten (20,56)=4 mit

$$4 = 3 \cdot 20 - 1 \cdot 56 \tag{2.102}$$

Das System ist lösbar da $4|(11-7)$. Damit $k_1 = 3, l_1 = 1, u = 1$ und dies liefert $k = 3, l = 1$. Damit ist

$$x = 3 \cdot 20 + 7 = 67 \tag{2.103}$$

bzw.

$$x = 1 \cdot 56 + 11 = 67 \tag{2.104}$$

Also: $x = 67$ löst das System.

2.3 Quadratische Reste

Wir betrachten nun Funktionen höherer Ordnung - insbesondere quadratische. Hier gilt zunächst über die Lösbarkeit

Satz 85 *$P(x) \equiv 0 \bmod m_1 m_2 \cdot .... \cdot m_r$ ist lösbar für paarweise teilerfremde $m_i \Longleftrightarrow$ Das System*

$$\begin{aligned} P(x) &\equiv 0 \bmod m_1 \\ P(x) &\equiv 0 \bmod m_2 \\ &\vdots \\ P(x) &\equiv 0 \bmod m_r \end{aligned}$$

ist lösbar.
Die Lösungszahl ist gleich dem Produkt der Lösungszahlen von $P(x) \equiv 0 \bmod m_i$

Beispiel: $x^2 \equiv 1 \bmod 3$ besitzt 2 Lösungen {1,2} und $x^2 \equiv 1 \bmod 8$ besitzt 4 Lösungen {1,3,5,7}. Daher besitzt die Gleichung $x^2 \equiv 1 \bmod 24$ 8 Lösungen.

Definition 86 *Sei nun n eine natürliche Zahl. Ein Element a heisst quadratischer Rest, wenn es hierzu eine passende Zahl x gibt mit*

$$x^2 \equiv a \bmod n \tag{2.105}$$

andernfalls quadratischer Nichtrest.

Aus vorigem Satz ergibt sich für die Lösbarkeit:

Satz 87 *$x^2 \equiv a \bmod n$ mit $n = p_1^{e_1} \cdot .... \cdot p_r^{e_r}$ ist lösbar $\Longleftrightarrow$ Das System*

$$\begin{aligned} x^2 &\equiv a \bmod p_1^{e_1} \\ x^2 &\equiv a \bmod p_2^{e_2} \\ &\vdots \\ x^2 &\equiv a \bmod p_r^{e_r} \end{aligned}$$

ist lösbar.

Bem.
1. Für $n = pq$ ist eine Zahl a quadratischer Rest, wenn a quadratischer Rest modulo p und modulo q ist.
2. $0, 1^2, 2^2, ...$ sind quadratische Reste zu jedem Modul n
3. Jede Zahl ist quadratischer Rest modulo 1

4. Ist 3 quadratischer Rest modulo 4? Gesucht: $x^2 \equiv 3 \bmod 4$ ... Es ist für
   $x = 0 : x^2 = 0$
   $x = 1 : x^2 = 1$
   $x = 2 : x^2 = 4 \equiv 0 \bmod 4$
   $x = 3 : x^2 = 9 \equiv 1 \bmod 4$

Also: 3 ist quadratischer Nichtrest (2 auch, 1 und 0 sind quadratische Reste)

Oben hatten wir gesehen, dass für n=8, die quadratischen Reste a in der Menge $\{0, 1, 4\}$ sein müssen. Das heisst wiederum 0,1 und 4 sind quadratische Reste modulo 8. Die Zahlen 2,3,5,6,7 sind sog. quadratische Nicht-Reste. Zum quadratischen Rest existieren dann die Urbilder (Quadratwurzeln). So sind die Quadratwurzeln der 4 modulo 8 die Zahlen 2 und 6. Bem. Haben wir eine

Quadratwurzel x gefunden, also eine Zahl x mit

$$x^2 \equiv a \bmod n \tag{2.106}$$

so ist auch

$$(n-x)^2 = n^2 - 2nx + x^2 \equiv x^2 \equiv a \bmod n \tag{2.107}$$

Betrachten wir den Fall n=6: Bsp: $x^2 \equiv a \bmod 6$:

$$\begin{array}{lcl} 1 & \rightarrow & 1 \\ 2 & \rightarrow & 4 \\ 3 & \rightarrow & 3 \\ 4 & \rightarrow & 4 \\ 5 & \rightarrow & 1 \\ 6 & \rightarrow & 0 \end{array}$$

hat also 4 Lösungen. $x^2 \equiv a \bmod 7$:

$$\begin{array}{lcl} 1 & \rightarrow & 1 \\ 2 & \rightarrow & 4 \\ 3 & \rightarrow & 2 \\ 4 & \rightarrow & 2 \\ 5 & \rightarrow & 4 \\ 6 & \rightarrow & 1 \\ 7 & \rightarrow & 0 \end{array}$$

hat 4 Lösungen.

Wir betrachten nun speziell Primzahlen als Modul m und führen folgende Notation ein:

Definition 88 *Legendre Symbol für p>2 und p$\nmid$ k, so heisst*

$$\left(\frac{k}{p}\right) = \{ \begin{array}{c} 1 \quad \textit{falls k quadratischer Rest modulo p} \\ -1 \textit{ falls k quadratischer Nichtrest modulo p} \end{array} \tag{2.108}$$

Es gilt:

1. $\left(\frac{1}{p}\right) = 1$
2. $\left(\frac{l^2}{p}\right) = 1$
3. $\left(\frac{3}{7}\right) = -1$ (s.o. 3 taucht als quadratischer Rest nicht auf)

Satz 89 *Für p>2, p$\nmid k_1$ und $k_1 \equiv k_2 \bmod p$ ist*

$$\left(\frac{k_1}{p}\right) = \left(\frac{k_2}{p}\right) \tag{2.109}$$

Trivial. Wg $x^2 \equiv k_1 \bmod p$ und $k_1 \equiv k_2 \bmod p$ ist auch $x^2 \equiv k_2 \bmod p$ und umgekehrt (p$\nmid k_2$ ergibt sich aus p$\nmid k_1$ und $k_1 \equiv k_2 \bmod p$.

Satz 90 *Jedes prime Restsystem besteht aus* $\frac{p-1}{2}$ *quadratischen Resten und* $\frac{p-1}{2}$ *quadratischen Nichtresten.*

Bew.: Modulo p können nur die Zahlen $1^2, 2^2, ..., (p-1)^2$ quadratische Reste sein. Wegen

$$(p-x)^2 = p^2 - 2px + x^2 \equiv x^2 \bmod p \tag{2.110}$$

ist mit jedem quadratischem Rest x auch $p-x$ quadratischer Rest. Wir betrachten daher nur $1^2, 2^2, ..., \left(\frac{p-1}{2}\right)^2$. Diese Zahlen sind modulo p inkongruent, denn wären zwei Zahlen kongruent, also

$$x^2 = y^2 \bmod p \tag{2.111}$$

so wäre (ohne Einschränkung sei $x \geq y$):

$$x^2 - y^2 = (x-y) \cdot (x+y) = kp \tag{2.112}$$

und wegen $1 \leq x, y \leq \frac{p-1}{2}$ wäre $x + y < p$ und $0 \leq x - y < p$.Damit muss $x = y$ gelten. q.e.d.

Bsp: p=11: Im primen Restsystem {1,2,3,4,5,6,7,8,9,10} sind die Zahlen 1,3,4,5,9 quadratische Reste, 2,6,7,8,10 sind die quadratischen Nichtreste.

Hieraus folgt nun

Satz 91 $\sum_{k=1}^{p-1} \left(\frac{k}{p}\right) = 0$

Zur praktischen Berechnung hilft nun folgender Satz

Satz 92 $\left(\frac{k}{p}\right) = k^{\frac{p-1}{2}} \bmod p$

Zunächst erscheint es erstaunlich, dass die rechte Seite stets einen Wert ± 1 modulo p annehmen soll. Gemäß Fermat ist jedoch

$$k^{p-1} \equiv 1 \bmod p \tag{2.113}$$

also

$$p | k^{p-1} - 1 = (k^{\frac{p-1}{2}} - 1) \cdot (k^{\frac{p-1}{2}} + 1) \tag{2.114}$$

Sei nun $\left(\frac{k}{p}\right) = 1$. Dann exisitert ein x mit

$$x^2 \equiv k \bmod p \tag{2.115}$$

und damit

$$k^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \bmod p \tag{2.116}$$

(da $p \nmid k$ gilt auch $p \nmid x$).

Da nun aber mit dieser Lösung bereits $\frac{p-1}{2}$ Lösungen gefunden werden, verbleiben für den Rest nur die Werte (etwas verkürzt ...)

$$k^{\frac{p-1}{2}} \equiv -1 \bmod p \tag{2.117}$$

Satz 93 *Es gilt*

$$\left(\frac{k_1 k_2}{p}\right) = \left(\frac{k_1}{p}\right) \cdot \left(\frac{k_2}{p}\right) \tag{2.118}$$

Also: Das Produkt ist genau dann ein quadratischer Rest, wenn beide Faktoren quadratischer Rest oder quadratischer Nichtrest waren.

Beweis:

$$\left(\frac{k_1 k_2}{p}\right) \equiv (k_1 \cdot k_2)^{\frac{p-1}{2}} \bmod p \tag{2.119}$$

$$\equiv k_1^{\frac{p-1}{2}} \cdot k^{\frac{p-1}{2}} \bmod p \tag{2.120}$$

$$\equiv \left(\frac{k_1}{p}\right) \cdot \left(\frac{k_2}{p}\right) \bmod p \tag{2.121}$$

Die rechte Seite ist -1 oder 1, die linke auch. Daher unterscheiden sich beide Seiten um -2,0 oder 2. Da aber p>2 und die Werte modulo p kongruent sind (p die Differenz teilen muss), bleibt nur 0 und damit $\left(\frac{k_1 k_2}{p}\right) = \left(\frac{k_1}{p}\right) \cdot \left(\frac{k_2}{p}\right)$

Durch Induktion ergibt sich dann:

Satz 94 *Es gilt*

$$\left(\frac{k_1 \cdot k_2 \cdot ... \cdot k_r}{p}\right) = \left(\frac{k_1}{p}\right) \cdot \left(\frac{k_2}{p}\right) \cdot .... \cdot \left(\frac{k_r}{p}\right) \tag{2.122}$$

Insbesondere

$$\left(\frac{k_1 \cdot k_2^2}{p}\right) = \left(\frac{k_1}{p}\right) \cdot \left(\frac{k_2}{p}\right)^2 = \left(\frac{k_1}{p}\right) \tag{2.123}$$

Dies bedeutet, dass man die Bestimmung des Legendre-Symbols zurückführen kann, indem man zunächst alle quadratfreien Anteile herausnimmt und schliesslich nur noch die Legendre-Symbole für

$$\left(\frac{\pm 1}{p}\right), \left(\frac{2}{p}\right) \text{ und } \left(\frac{q}{p}\right) \text{ für Primzahlen } q \text{ benötigt.} \tag{2.124}$$

Bsp:

$$\left(\frac{360}{127}\right) = \left(\frac{4 \cdot 9 \cdot 2 \cdot 5}{127}\right) = \left(\frac{2 \cdot 5}{127}\right) = \left(\frac{2}{127}\right) \cdot \left(\frac{5}{127}\right) \tag{2.125}$$

Wie diese nun berechnet werden können wird weiter unten gelöst.

Es gilt:

Satz 95 *1.*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \tag{2.126}$$

$$\textit{Analog} \quad : \quad \textit{1 falls } p \equiv 1 \bmod 4 \textit{ oder p=2} \tag{2.127}$$

2.

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} \tag{2.128}$$

$$\textit{Analog} \quad : \quad \textit{1 falls } p \equiv \pm 1 \bmod 8 \textit{ oder p=2} \tag{2.129}$$

3.

$$\left(\frac{3}{p}\right) = (-1)^{\left\lfloor \frac{p+1}{6} \right\rfloor} \tag{2.130}$$

$$\textit{Analog} \quad : \quad \textit{1 falls } p \equiv \pm 1 \bmod 12 \tag{2.131}$$

4.

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) \cdot a \textit{ (Quadratisches Reziprozitätsgesetz)} \tag{2.132}$$

$$\textit{mit } a = \textit{1 falls } p \equiv q \equiv 3 \bmod 4 \textit{ und a=-1 sonst} \tag{2.133}$$

Damit zum obigen Beispiel:

$$\left(\frac{2}{127}\right) = 1 \tag{2.134}$$

$$\left(\frac{5}{127}\right) = -\left(\frac{127}{5}\right) = -\left(\frac{2}{5}\right) = -(-1) = 1 \tag{2.135}$$

Weitere Anwendung:

Satz 96 *Es gibt unendlich viele Primzahlen p*$\equiv 1 \bmod 4$

Es ist

$$\left(\frac{-1}{p}\right) = 1 \text{ falls } p \equiv 1 \bmod 4 \tag{2.136}$$

damit ist für n>1

$$x^2 \equiv -1 \bmod p \tag{2.137}$$

lösbar, falls $p \equiv 1 \bmod 4$. Nun ist aber jeder (Prim-)Teiler von $(n!)^2 + 1$ grösser als n und eben $p \equiv 1 \bmod 4$. Wäre er $p \equiv 3 \bmod 4$ wäre eine Lösung zu

$$x^2 \equiv -1 \bmod p$$

gefunden (mit x=n!.), welche es aber wegen $\left(\frac{-1}{p}\right)$ =-1 nicht geben kann.

2.3.1 Teilbarkeitsregeln

Auch bekannte Sätze der Teilbarkeit lassen sich mit Hilfe der Zahlentheorie bewältigen. Es stellt sich die Frage wann eine Zahl durch 3,9 oder 11 teilbar ist.

Betrachten wir hierzu zunächst die Zerlegung der Zahl in das Zehnersystem. Jede $(k+1)$-stellige Zahl hat eine eindeutige Darstellung

$$n = \sum_{i=0}^{k} a_i \cdot 10^i$$

und gesucht ist zunächst für die Teilbarkeit durch 3

$$n \equiv 0 \bmod 3 \tag{2.138}$$

Da aber

$$\begin{aligned} 1 &\equiv 1 \bmod 3 \\ 10 &\equiv 1 \bmod 3 \end{aligned}$$

ist auch

$$10^i \equiv 1 \bmod 3$$

und

$$\begin{aligned} a_i \cdot 10^i &\equiv a_i \bmod 3 \\ n &= \sum_{i=0}^{k} a_i \cdot 10^i \equiv \sum_{i=0}^{k} a_i \bmod 3 \end{aligned}$$

Damit gilt

$$n \equiv 0 \bmod 3 \Longleftrightarrow \sum_{i=0}^{k} a_i \equiv 0 \bmod 3 \tag{2.139}$$

Dies bedeutet: Eine Zahl ist genau dann durch 3 teilbar, wenn die Summe ihrer Ziffern (also die Quersumme) durch 3 teilbar ist.

Der Beweis geht für die Teilbarkeit durch 9 völlig analog !

Nun zur 11:

$$n \equiv 0 \bmod 11 \tag{2.140}$$

Da aber

$$\begin{aligned} 1 &\equiv 1 \bmod 11 \\ 10 &\equiv -1 \bmod 11 \\ 10^2 &= 100 \equiv 1 \bmod 11 \end{aligned}$$

ist auch

$$10^i \equiv (-1)^i \bmod 11$$

und

$$\begin{aligned} a_i \cdot 10^i &\equiv a_i \cdot (-1)^i \bmod 11 \\ n &= \sum_{i=0}^{k} a_i \cdot 10^i \equiv \sum_{i=0}^{k} a_i \cdot (-1)^i \bmod 11 \end{aligned}$$

Damit gilt

$$n \equiv 0 \bmod 11 \Longleftrightarrow \sum_{i=0}^{k} a_i \cdot (-1)^i \equiv 0 \bmod 11 \tag{2.141}$$

Dies bedeutet: Eine Zahl ist genau dann durch 11 teilbar, wenn die alternierende Summe ihrer Ziffern (also die alternierende Quersumme) durch 11 teilbar ist.

Beispiel: Ist 93765432607 durch 11 teilbar? Die alternierende Quersumme ist $9-3+7-6+5-4+3-2+6-0+7 = 22$. Diese Zahl ist durch 11 teilbar - damit auch die ursprüngliche Zahl.

2.4 Zahlenteorie in der Kryptographie

Kryptographisch notwendig ist eine einfach zu berechnende aber "schwer" umzukehrende Funktion, z.B. aus dem Produkt zweier Zahlen (einfach zu berechnen) wieder auf die Faktorisierung zu schliessen. Damit die Umkehrung eindeutig ist, betrachtet man Produkte zweier "grosser" Primzahlen. Also:

2.4.1 Faktorisierung

Gegeben eine Zahl n. Gesucht seien p und q Zahlen >1 mit

$$n = p \cdot q \tag{2.142}$$

also eine nicht-triviale Faktorisierung. Um eine solche Zerlegung zu finden, gibt

es verschiedene algorithmische Ansätze:

1. Untersuche für alle Zahlen $m \leq \sqrt{n}$ ob diese Zahl n teilt oder nicht.
2. Führe diesen Algorithmus nur für Primzahlen $\leq \sqrt{n}$ durch

3. Fermat: Existiert eine Zerlegung $n = a^2 - b^2$ dann ist eine Zerlegung gefunden durch $n = (a+b) \cdot (a-b)$ Es gilt dann auch $b^2 = a^2 - n$. Berechnen

nun für die Zahlen $a \geq \sqrt{n}$ den Term $a^2 - n$. Ist das Ergebnis eine Quadratzahl b^2,so ist die Zerlegung gefunden. Dieses Verfahren funktioniert gut für Faktoren nahe bei $\sqrt{n}$. Bsp: n=851 $\Longrightarrow \sqrt{n} = 29, ...$ Also: Starte mit $a = 30$:

$$30^2 - 851 = 49 = 7^2 \tag{2.143}$$

Damit $a = 30, b = 7$ und $n = (30+7) \cdot (30-7) = 37 \cdot 23$

2.5 Diskrete Logarithmen

Während es in jeder Gruppe einfach ist, Potenzen auszruechnen, ist die Umkehrung wiederum schwierig. Zur Berechnung der Potenzen wird mit dem square-and-multiply-Algorithmus die Zerlegung in Zweierpotenzen vorgenommen, also

$$a^{21} = a^{16} \cdot a^4 \cdot a^1 \tag{2.144}$$

Dann werden die Quadrate gebildet:

$$\begin{aligned} a^0 &= 1_G \\ a^1 &= a \\ a^2 &= (a)^2 \\ a^4 &= (a^2)^2 \\ a^8 &= (a^4)^2 \\ a^{16} &= (a^8)^2 \end{aligned}$$

und dann die benötigten Ergebnisse von a^{16}, a^4 und a eingesetzt. Die Umkehrung besteht nun darin zu einer vorgebenen Zahl h eine Potenz x der Zahl g (aus der Gruppe G) zu finden, so dass

$$h = g^x \tag{2.145}$$

(bzw. zu zeigen, dass keine solche Zahl x existiert). Hierzu wird aus der Anzahl der Elemente in G die Zahl m^2 mit $m^2 \geq |G|$ gewählt. Dann werden zwei Listen erzeugt: Giant-Step:Berechne zunächst g^m und dann

$$g^m, (g^m)^2 = g^{2m}, g^{3m}, ..., g^{m \cdot m} \tag{2.146}$$

Baby-Step:Berechne zunächst g^{-1} und dann

$$h, hg^{-1}, hg^{-1} \cdot g^{-1} = hg^{-2}, ..., hg^{-m} \tag{2.147}$$

und vergleiche die beiden Listen ob ein gemeinsamer Eintrag existiert. Falls ja ist

$$g^{k \cdot m} = hg^{-i} \tag{2.148}$$

und damit

$$g^{k \cdot m + i} = h \tag{2.149}$$

Dieses liefert wiederum den Wert $x = k \cdot m + i$.

2.6 Graphentheorie

2.6.1 Ungerichtete Graphen

Ein Graph besteht aus einer Menge Knoten (Punkte; auch als Ecken bezeichnet) E und einer Menge Kanten K. Jede Kante verbindet 2 Knoten. Knoten müssen jedoch nicht zwingenderweise durch Kanten verbunden werden.

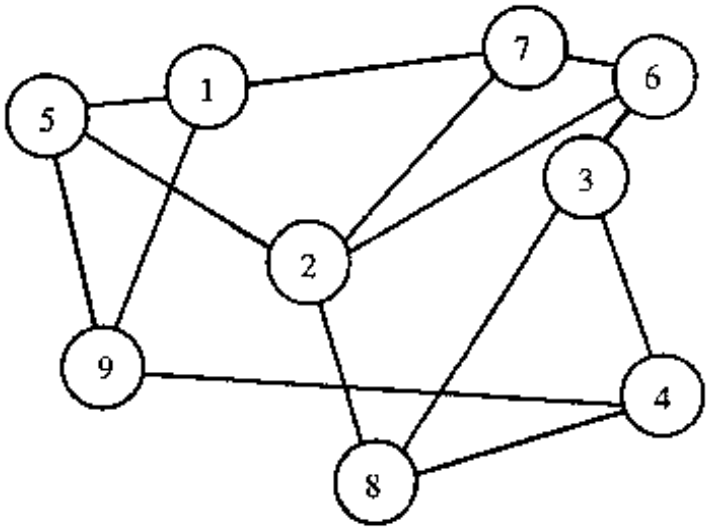
Beispiel:

Jeder Graph wird somit durch

$$G = (E, K) \tag{2.150}$$

identifiziert.

Üblicherweise numerieren wir die Ecken und Kanten durch. Beispiel:



E={1,2,3,4,5,6,7,8,9}
K={(1,5),(1,9),....}

Typische Probleme sind im Verkehrswesen Rundreiseprobleme, Flugoptimierung, Speditionseinsätze, aber auch in der Elektrotechnik (Ecken=Objekte, Kanten=Verbindungen) oder der Chemie (Strukturformeln: Ecken=Atome,Kanten=chemische Verbindungen)

Beispielsweise im Strassenverkehr exisitieren zu anzureisenden Punkten jedoch sehr viele Verbindungen.

Weitere Merkmale:
Kann man von jeder Ecke zu jeder anderen gelangen (Sind also je zwei Ecken miteinander verbunden), so heißt der Graph **vollständig**. Ein vollständiger Graph mit n Ecken wird mit K_n bezeichnet.

Bitte zeichnen Sie nun K_1 bis K_5.

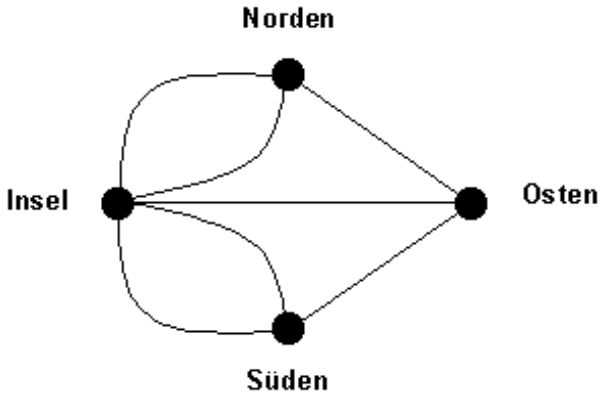
Ein Graph heißt **zusammenhängend**, wenn man von jeder Ecke über eine Folge von Kanten zu jeder anderen Ecke gelangen kann. Ist der Graph unterbrochen oder exisitieren isolierte Punkte, so ist der Graph nicht zusammenhängend.

Da durch ein Kante impliziert vorgegeben wird, von welcher Ecke zu welcher nachfolgenden Ecke man sich bewegt, wird bei einem Kantenzug durch den Graphen die Folge der Kanten angegeben. Verbindet die Kante k_i die Ecken e_i und e_{i-1}, so wird durch den Kantenzug $k_1, k_2, ..., k_n$ die Ecke e_0 mit e_n verbunden.Bei einem Kantenzug (siehe Haus vom Nikolaus) darf sich eine Ecke durchaus wiederholen und sogar eine Kante mehrfach verwendet werden.

Der Kantenzug heißt **geschlossen,** wenn $e_n = e_0$ gilt. Betrachtet man den Graphen "Haus vom Nikolaus", so ist jede Kante nur einmal zu verwenden. Ein solcher Kantenzug, bei dem jede Kante (maximal) einmal verwendet wird, heißt **Weg**.

Ein geschlossener Weg heißt **Kreis** und die **Länge** eines Weges wird durch die Anzahl seiner Kanten definiert.

Schliesslich bezeichnet der **Grad** einer Ecke grad(e) die Anzahl der von ihm abgehenden Kanten.
Ist grad(e)=0, so heißt die Ecke **isoliert.**



Aufgabe: Bestimmen Sie zum Haus vom Nikolaus den Grad jeder Ecke. Ist der Graph zusammenhängend? Vollständig?

Das Problem beim Haus vom Nikolaus beruht auf dem Problem, welches Euler im 18 Jahrhundert in der Stadt Königsberg vorfand (und löste).

Königsberg liegt, wie jeder weiß, an der Pregel, die sich in der Stadt in einen nördlichen und einen südlichen Teil auftrennt. Dazu kommt eine Insel. Im Laufe der Zeit hatten die Königsberger insgesamt sieben Brücken gebaut, die die verschiedenen Ortsteile miteinander verbinden. Nach diesem anstrengenden Bau hatten sie genug Zeit, sich darüber zu streiten, ob es einen Rundweg durch Königsberg gebe, die jede der Brücken einmal überquert.

Euler übersetzte dies nun in die Sprache der Graphentheorie, in dem er die Landgebiete als Ecken und die Brücken als Kanten definierte:

Und die Frage stellt sich nun, ob es einen Kreis gibt, der jede Kante verwendet. Ein solcher Kreis heißt eulerscher Kreis und ein Graph mit eulerschem Kreis heißt ebenfalls eulersch. Insbesondere ist die Frage beim Haus vom Nikolaus ähnlich: Gibt es dort einen eulerschen Kreis?

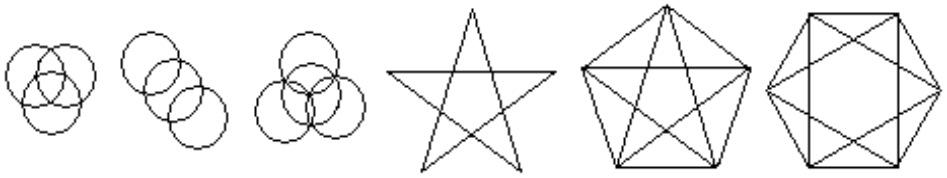
Frage: Welche der vollständigen Graphen K_2 bis K_5 ist eulersch?

Ist das Haus vom Nikolaus eulersch? Falls nicht: 1. Wo muss Start und Ziel sein, damit sie durchzeichnen können? Gibt es einen "fast-eulerschen (oder offenen eulerschen) Kreis", d.h. durch Hinzufügen einer Kante wird der Graph ein Kreis. Wo?

Grundlage ist der von Euler festgestellte Zusammenhang:

Satz 97 *Wenn G eulersch ist, so muss jede Ecke geraden Grad haben.*

Ist also eine Ecke ungeraden Grades, so kann der Graph nicht eulersch sein.



Beweis: Wir betrachten eine beliebige Ecke e eines Eulerschen Graphens. Der Kreis durchläuft den Punkt (ausser dem Start/Endpunkt) diesen n mal.Da jede Kante nur einmal benutzt werden darf muss der Graph an e mindestens 2n Kanten haben. Da aber auch jede Kante verwendet wird, muss gelten, dass der Grad(e)=2n ist. Im Start-Endpunkt wird dieser 2(n-1)- mal durchlaufen sowie je einmal zu Beginn und Ende. Auch diese Ecke hat somit geraden Grad.

Wir sehen:

1. Beim Haus vom Nikolaus: 2 Ecken haben ungeraden Grad, die anderen sind gerade: Nicht eulersch !

2. Königsberg: Eine Ecke hat Grad 5, die anderen Grad 3: Nicht eulersch!

3. K_n hat grad(e)=n-1 für alle Ecken: Kann also nur eulersch sein für n ungerade!

Euler hat ebenfalls die Umkehrung gezeigt: Wenn alle Ecken ein geraden Grad haben, dann existiert ein eulerscher Kreis. Also: Insbesondere bei K_{2n} existiert dieser also.

Diese Umkehrung kann nun auch bei fast-eulerschen Kreisen angewendet werden:

Haben nur zwei Ecken einen ungeraden Grad, so lassen sich die beiden Ecken durch eine zusätzliche Kante l verbinden und es existiert ein eulerscher Weg von $s = k_0, k_1, ..., k_r, l, k_s, ..., k_n = s$

Nun sortieren wir die Kantenreihenfolge um: $k_s, ..., k_n, k_0, ..., k_r, l$ und lassen die letzte hinzugefügte Kante wieder weg. Da nun alle Kanten verwendet werden, gibt es einen fast-eulerschen Weg (nur die letzte Kante, um den Weg zu schliessen, fehlt), bei dem es einen geschlossenen Streckenzug, welcher alle Kanten verwendet, gibt.

z.B. Haus des Nikolaus: Nur zwei Ecken haben ungeraden Grad und damit existiert ein fast-eulerscher Kreis. Insbesondere müssen Start und Ziel somit in den beiden Ecken mit ungeradem Grad liegen.

Welche der folgenden Figuren lassen sich in einem Strich durchzeichnen?

Planare und plättbare Graphen

Wir bezeichnen einen Graphen als planar, wenn er ohne Überschneidungen gezeichnet werden kann. Dies bedeutet, dass sich je zwei Kanten höchstens in einer Ecke schneiden können.

Frage: Ist das Haus vom Nikolaus planar? Oder plättbar?

Wir sehen also, dass der Graph links nicht planar ist, durch Umzeichnen einer Kante jedoch planar gezeichnet werden kann und somit plättbar ist. Planare Graphen zerlegen die Ebene in Gebiete (oder Länder). Dabei wir die Umgebung auch als ein Gebiet betrachtet. Das obige (rechte) Haus vom Nikolaus mit seinen n=5 Ecken und m=8 Kanten umschliesst somit g=5 Länder.

Wir beobachten für diesen Graphen n-m+g =5-8+5=2. Nehmen wir die Diagonale heraus: n-m+g=5-7+4=2 und löschen wir den Dachpunkt und verbinden die Dachhälften zu einer Kante n-m+g=4-6+4=2. Das die Summe immer zwei ergibt, besagt der Eulersche Polyedersatz:

Satz 98 *Für einen zusammenhängenden planaren Graphen mit n Ecken, m Kanten und g Gebieten gilt*

$$n - m + g = 2 \tag{2.151}$$

Beweis: Über die Kantenanzahl m

m=1: Wir betrachten einen planaren zusammenhängenden Graphen mit einer Kante. Daher ist g=1 und n=2 und insgesamt n-m+g=2-1+1=2

Sei nun die Aussage richtig für die Kantenzahl m.

Wir betrachten nun einen Graphen mit m+1 Kanten.(n Ecken und g Gebieten) und müssen zeigen $n - (m + 1) + g = 2$

Fall 1: es gibt eine Ecke, welche nur an einer Kante liegt. Wir schauen uns für einen Moment den Graphen an, welcher entsteht wenn wir die Ecke und die Kante entfernen:

n'=n-1, m'=m, g'=g

Dies ist ein Graph mit m Kanten und erfüllt nach Induktionsvorraussetzung

$$n' - m' + g' = n - 1 + m + g = 2 \tag{2.152}$$

Damit aber auch für den gesuchten Graphen

$$n - (m + 1) + g = 2 \tag{2.153}$$

Fall 2: Eine solche Kante existiert nicht: Damit hat jede Ecke mindestens grad 2 und damit existiert ein Kreis. (Gäbe es keinen Kreis, so existiert ein Endpunkt mit grad=1 im Widerspruch zu grad$\geq$ 2) Wir löschen wiederum eine Kante des Kreises und erhalten

n'=n,m'=m,g=g-1 und damit nach Induktionsvorraussetzung

$$n' - m' + g = n - m + g - 1 = 2 \tag{2.154}$$

und dies ist wiederum

$$n - (m + 1) + g = 2 \tag{2.155}$$

Folgerung: Ein planarer zusammenhängender Graph ohne doppelte Kanten erfüllt: $m \leq 3n - 6$ (Also: Ein planarer Graph hat wenige Kanten).

Wir betrachten für jedes Gebiet g die Anzahl der Kanten, die dieses Land umschliessen m(g). Da jedes Land mindestens 3 Kanten hat gilt

$$\sum m(g) \geq 3g \tag{2.156}$$

Da wir nun aber auch alle vorkommenden Kanten genau 2 mal gezählt haben, gilt

$$\sum m(g) = 2m \tag{2.157}$$

und damit $g \leq \frac{2}{3}m$ mit der Euler-Formel

$$2 = n - m + g \leq n - m + \frac{2}{3}m \tag{2.158}$$

$$= n - \frac{1}{3}m \tag{2.159}$$

Multiplikation mit 3 ergibt

$$6 \leq 3n - m \tag{2.160}$$

$$m \leq 3n - 6 \tag{2.161}$$

Anwendung: K_5 ist nicht plättbar: n=5, m=10. Wäre er planar so wäre $10 \leq 15 - 6 = 9$

Weiterhin:
In jedem planaren Graphen gibt es eine Ecke mit grad<6.

Beweis: Wir betrachten alle Ecken und deren angrenzende Kanten

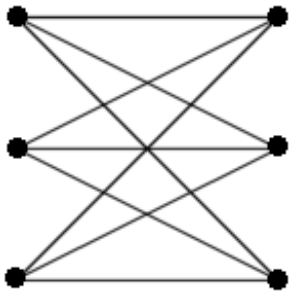
$$\sum grad(e) = 2m \tag{2.162}$$
$$\leq 6n - 12 \tag{2.163}$$

Nehmen wir an jede der n Ecken habe grad ≥ 6, dann wäre aber auch

$$\sum grad(e) \geq 6n \tag{2.164}$$

im Widerspruch zur vorigen Gleichung.

Weitere Anwendung:



Wir betrachten 3 Versorgungswerke (Strom v_1,Wasser v_2, Gas v_3) zu drei Haushalten v_4, v_5, v_6

Gibt es eine Möglichkeiten (2d) die m=9 Leitungen zwischen den 6 Ecken so zu legen, dass diese sich nicht überschneiden?

Beobachtungen: Wäre der Graph plättbar, so würde

1. nach Euler n-m+g=2 ergeben dass die Anzahl der Gebiete 2+9-6=5 Gebiete.

2. jedes Gebiet mind. 4 Kanten beinhalten (da man von einem Versorgungswerk nicht zu einem anderen kommt, und von einem Haus auch nicht zu einem anderen) und damit 2m$\geq 4g = 20$ bzw. m≥ 10 im Widerspruch zu m=9.