2 Zahlen

Schon früh führte die vage gehaltene Mengendefinition Cantors zu Widersprüchen. Besonders bekannt sind die Russel'schen Antinomien (Bertrand Russell, 1872–1970), vor allem die Geschichte vom Barbier:

> Es war einmal ein Dorfbarbier, der hängte in sein Fenster ein Schild mit folgender Aufschrift:
>
> „Ich rasiere jeden Mann im Ort, der sich nicht selbst rasiert!“
>
> Das ging so lange gut, bis ein Fremder in den Ort kam und ihn fragte, ob er sich denn selbst rasiere. „Ja“, wollte der Barbier sagen, als ihm plötzlich Bedenken kamen. Rasierte er sich wirklich selbst, so dürfte er sich — des Schildes wegen — nicht rasieren. Rasierte er sich aber nicht selbst, so müsste er sich eben doch rasieren.
>
> Seit der Zeit vernachlässigte der Barbier sein Geschäft immer mehr, und wenn er nicht gestorben ist, dann grübelt er noch immer darüber nach, ob er sich nun rasieren soll oder nicht.

Was hat das mit der Mengenlehre zu tun? Wir setzen

$$U := \{x \mid x \notin x\}.$$

Ist $U \notin U$ wahr, so muss U ein Element von U sein, also auch $U \in U$. Ist dagegen $U \notin U$ falsch, so kann U nicht in U liegen, es ist $U \notin U$. In jedem Fall erhält man einen Widerspruch. U ist keine Menge, sondern eher eine *Unmenge*.

Derartige Widersprüche wurden zunächst nur provisorisch durch das Verbot, allzu wilde Mengen zu bilden, aus der Welt geschafft. Erst 1908 stellte Ernst Zermelo, ein Schüler Cantors, ein Axiomensystem vor, das die Antinomien vermeidet – soweit man bis jetzt weiß. Im Detail wird das Zermelo'sche Axiomensystem im Anhang zu Abschnitt 1 vorgestellt. Wir wollen hier nicht näher darauf eingehen.

Definition.
Ist M eine Menge, so kann man deren *Potenzmenge*

$$\boxed{P(M) := \{T \mid T \subset M\}}$$

bilden, also die Menge aller Teilmengen von M.

Beispiele.

1. Sei $M := \{1, 2, 3\}$. Wir wollen sämtliche Teilmengen von M bestimmen. Zunächst gehört die leere Menge dazu! Denn die Aussageform

$$„\, x \in \varnothing \implies x \in M\, “$$

ist immer wahr, weil die Aussageform „$x \in \varnothing$“ immer falsch ist. Wie gut, dass die logische Implikation auch falsche Prämissen zulässt. Mit dem „gesunden Menschenverstand“ allein kämen wir bei solchen Spitzfindigkeiten nicht weit.

Geht man systematisch vor, so sucht man als nächstes am besten nach den 1-elementigen Teilmengen, das sind $\{1\}$, $\{2\}$ und $\{3\}$. Die 2-elementigen Teilmengen sind $\{1,2\}$, $\{1,3\}$ und $\{2,3\}$. Und schließlich ist M auch Teilmenge von sich selbst. Damit gilt:

$$P(M) = \{\varnothing, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}.$$

2. Hat auch die leere Menge eine Potenzmenge?

   Die Aussage „$\varnothing \subset \varnothing$“ ist wahr, weil die leere Menge aus formal–logischen Gründen in jeder Menge enthalten ist. Andere Teilmengen kann es nicht geben, also gilt:

   $$P(\varnothing) = \{\varnothing\}.$$

   Aus der leeren Menge haben wir durch Übergang zur Potenzmenge eine Menge mit einem Element konstruiert! Nun wollen wir es auf die Spitze treiben: Was ist denn die Potenzmenge der Potenzmenge der leeren Menge? Das Ergebnis lautet:

   $$P(P(\varnothing)) = \{\varnothing, \{\varnothing\}\}.$$

   Das ist nun eine Menge mit 2 Elementen! Und wenn wir das Verfahren noch einmal durchführen, so bekommen wir eine Menge mit 4 Elementen. Es ist offensichtlich, dass wir auf diesem Wege beliebig lange weiterschreiten können.

   Wir wollen jetzt einen ähnlichen, aber etwas anderen Weg einschlagen, um eine unendliche Folge von Mengen zu konstruieren. Dabei geben wir diesen Mengen provisorische Namen:

   $$\begin{aligned} 0 &:= \varnothing, \\ 1 &:= \{0\} = \{\varnothing\}, \\ 2 &:= \{0,1\} = \{\varnothing, \{\varnothing\}\}, \\ 3 &:= \{0,1,2\} = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}, \\ &\dots \end{aligned}$$

   Aus Nichts können wir so eine ganze Welt erschaffen, eine *unendliche Menge*, die als Modell für die Menge der *natürlichen Zahlen* dienen kann.

   Natürlich ist das ein ziemlich abstrakter Unsinn. Niemand soll sich von seiner gewohnten Vorstellung vom Zählen und von den natürlichen Zahlen verabschieden. Es ist sogar eher gefährlich, die leere Menge mit 0 zu bezeichnen. Vergessen wir also besser diese seltsame Konstruktion. Nur ein Aspekt sollte im Gedächtnis bleiben: Durch die Zuordnung

   $$n \to n^+ := n \cup \{n\}$$

wird jeder natürlichen Zahl n auf eindeutige Weise ein *Nachfolger* n^+ zugeordnet. Diese Tatsache ist unabhängig davon, wie die natürlichen Zahlen realisiert werden, ob als merkwürdige Mengen, als Dezimalzahlen 1, 2, 3 usw., oder – wie in der Steinzeit – durch Abzählen von Fingern oder Holzstöckchen. Darauf werden wir an späterer Stelle zurückkommen.

Was sind nun Zahlen wirklich?

Jede Zahl x, die einem bis zum Abitur begegnet, kann man folgendermaßen aufschreiben:

$$x = \pm v_m v_{m-1} \dots v_0 \,.\, n_1 n_2 n_3 \dots .$$

Es gibt ein *Vorzeichen* + oder −, eine endliche Anzahl von *Vorkomma-Stellen* und unendlich viele *Nachkomma-Stellen*. An jeder dieser Stellen steht eine *Ziffer* zwischen 0 und 9 (weil wir im Dezimalsystem arbeiten). Das Komma schreiben wir als Dezimalpunkt. Alle so darstellbaren Zahlen nennt man *reelle Zahlen*. Die Menge aller reellen Zahlen bezeichnet man mit $\mathbb{R}$.

Die Darstellung ist übrigens nicht eindeutig. Wir werden später sehen, dass die Zahlen $13.547000\dots$ und $13.546999\dots$ gleich sind!

Man kann mit den reellen Zahlen rechnen. Die Rechenoperationen könnte man über die Dezimal-Darstellung definieren, aber das wäre recht kompliziert. Wir können uns in der Mathematik auf einen anderen Standpunkt stellen: Jeder kennt die Zahlen und die Rechenoperationen. Wir stellen ein Axiomensystem für $\mathbb{R}$ auf und verabreden, dass alle weiteren Aussagen über reelle Zahlen aus diesen Axiomen hergeleitet werden müssen. Wir verlassen uns aber darauf, dass das kluge Leute schon gemacht haben und beschränken uns auf Stichproben und zweifelhafte Fälle.

[R-1] Axiome der Addition. *Je zwei Elementen $x, y \in \mathbb{R}$ ist eindeutig eine reelle Zahl $x + y$ (ihre* Summe*) zugeordnet. Es gilt:*

1. **Assoziativgesetz:** $\forall\, x, y, z \in \mathbb{R}$ *ist* $(x + y) + z = x + (y + z)$.
2. **Kommutativgesetz:** $\forall\, x, y \in \mathbb{R}$ *ist* $x + y = y + x$.
3. **Existenz der Null:** *Es gibt ein Element* $0 \in \mathbb{R}$*, so dass gilt:* $\forall\, x \in \mathbb{R}$ *ist* $x + 0 = x$.
4. **Existenz des Negativen:** $\forall\, x \in \mathbb{R}\, \exists\, y \in \mathbb{R}$ *mit* $x + y = 0$.

Das Assoziativgesetz besagt, dass man beliebig klammern kann. Deshalb sind auch Ausdrücke der Gestalt $x_1 + x_2 + \ldots + x_n$ sinnvoll.

Das Kommutativgesetz besagt, dass die Reihenfolge von Summanden keine Rolle spielt. Dabei dürfen es aber immer nur endlich viele Summanden sein. Man beschäftigt sich in der Mathematik auch mit der Addition von unendlich vielen Summanden. Das geht aber nicht mehr mit Hilfe unserer bekannten Rechenoperation. Man braucht dafür ganz andere Techniken, und es stellt sich heraus, dass

es dann sehr wohl auf Reihenfolge und Klammerung ankommt, d.h. Kommutativ- und Assoziativgesetz gelten nicht universell, sondern nur in dem obigen Sinne.

Axiom 4 ist erst recht nicht selbstverständlich. Ist x eine Zahl, so ist $x+(-x)=0$. Durch das Axiom wird sichergestellt, dass $-x$ wieder eine reelle Zahl ist. Bei den natürlichen Zahlen ist diese Eigenschaft nicht gegeben! Außerdem gilt zu beachten, dass „das Negative einer Zahl“ etwas anderes ist als „eine negative Zahl“. -7 ist eine negative Zahl. Das Negative von -7 ist die Zahl 7 (das Vorzeichen + lässt man meistens weg), also eine positive Zahl. Bei konkreten Zahlen kann das jeder erkennen. Schwieriger wird es, wenn man die konkrete Zahl durch eine Variable ersetzt. Ist $-x$ (das Negative von x) nun selbst negativ oder positiv? Wir können es ohne weitere Informationen nicht wissen!

Axiom 4 besagt übrigens nicht, dass die Lösung y der Gleichung $x+y=0$ eindeutig bestimmt ist. Das werden wir aber gleich beweisen.

Satz. *Für alle reellen Zahlen a, b besitzt die Gleichung*

$$a+x=b$$

eine eindeutig bestimmte Lösung.

Beweis: 1) Zunächst zeigen wir die Existenz einer Lösung. Dafür reicht es, die Lösung anzugeben und die Probe zu machen.

Wir sind auf's Raten angewiesen, und unsere Erfahrung sagt: Ist $-a$ eine der (eventuell zahlreichen) nach Axiom 4 existierenden Lösungen der Gleichung $a+y=0$, so sollten wir es mit $x:=b+(-a)$ versuchen. Tatsächlich gilt:

$$\begin{aligned} a+x &= a+(b+(-a)) && \text{(Einsetzen)} \\ &= a+((-a)+b) && \text{(Kommutativgesetz)} \\ &= (a+(-a))+b && \text{(Assoziativgesetz)} \\ &= 0+b && \text{(nach Wahl von } -a) \\ &= b. && \text{(Kommutativgesetz und Axiom 3)} \end{aligned}$$

2) Wie beweist man die Eindeutigkeit der Lösung? Ein direkter Weg würde vielleicht sogar die Lösung frei Haus liefern, aber dieser direkte Weg erweist sich hier als nicht gangbar. Dann bleibt noch folgendes Standardverfahren:

Wir zeigen: Sind x und y zwei Lösungen, so ist zwangsläufig $x=y$.
Sei also $a+x=b$ und $a+y=b$. Dann gilt:

$$a+x=a+y \qquad \text{(Gleichsetzen der linken Seiten).}$$

Das setzen wir in der folgenden Gleichungskette ein:

$$\begin{aligned} y &= 0 + y \\ &= (a + (-a)) + y \\ &= (a + y) + (-a) \\ &= (a + x) + (-a) \\ &= (a + (-a)) + x \\ &= 0 + x \quad = \quad x. \end{aligned}$$

Das war's! ∎

Es folgt insbesondere, dass die Null und das Negative eindeutig bestimmt sind. Die eindeutig bestimmte Lösung $x := b + (-a)$ der Gleichung $a + x = b$ bezeichnet man auch mit dem Symbol $b - a$ und nennt sie *die Differenz* von a und b.

Als nächstes wollen wir die altbekannten Vorzeichenregeln beweisen:

Satz. *Es ist* $-(-a) = a$ *und* $-(a + b) = (-a) + (-b)$.

Beweis: Nach Axiom 4 ist

$$\begin{aligned} (-a) + (-(-a)) &= 0 \\ \text{und} \qquad (-a) + a &= 0. \end{aligned}$$

Wegen der eindeutigen Lösbarkeit von Gleichungen muss dann $a = -(-a)$ sein.

Genauso beweist man die 2. Behauptung: $-(a + b)$ und $(-a) + (-b)$ sind beides Lösungen der Gleichung $(a + b) + x = 0$. Also müssen sie gleich sein. ∎

[R-2] Axiome der Multiplikation. *Je zwei Elementen* $x, y \in \mathbb{R}$ *ist eindeutig eine reelle Zahl* $x \cdot y$ *(ihr* Produkt*) zugeordnet. Es gilt:*

1. **Assoziativgesetz:** $\forall\, x, y, z \in \mathbb{R}$ *ist* $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.
2. **Kommutativgesetz:** $\forall\, x, y \in \mathbb{R}$ *ist* $x \cdot y = y \cdot x$.
3. **Existenz der Eins:** *Es gibt ein Element* $1 \in \mathbb{R} \setminus \{0\}$*, so dass gilt:* $\forall\, x \in \mathbb{R}$ *ist* $x \cdot 1 = x$.
4. **Existenz des Inversen:** $\forall\, x \in \mathbb{R}$ *mit* $x \neq 0$ $\exists\, y \in \mathbb{R}$*, so dass* $x \cdot y = 1$ *ist.*

Man beachte, dass die Aussage $1 \neq 0$ ein Axiom ist! Und auch Axiom (4) der Multiplikation sieht anders aus als das entsprechende Axiom der Addition. Es gibt eine **Ausnahme**, x darf nicht die Null sein. Warum nicht? Jeder weiß, dass stets $0 \cdot x = 0$ ist, und dass deshalb nie die 1 als Vielfaches von 0 herauskommen kann.

Das muss natürlich bewiesen werden, und es lässt sich auch beweisen, sofern wir noch folgendes Axiom hinzufügen:

[R-3] Axiom vom Distributivgesetz.

$\forall\, x, y, z \in \mathbb{R}$ *ist* $x \cdot (y + z) = x \cdot y + x \cdot z$.

Man beachte, dass man beim Distributivgesetz Addition und Multiplikation nicht vertauschen darf! Im allgemeinen ist

$$a + (b \cdot c) \neq (a + b) \cdot (a + c),$$

wie man sich an Hand einfacher Zahlenbeispiele leicht überlegt. Bei den Mengenoperationen $\cup$ und $\cap$ ist das anders.

Satz. $\forall\, x \in \mathbb{R}$ *ist* $x \cdot 0 = 0$.

Beweis: Es ist $x \cdot 0 = x \cdot (0 + 0) = x \cdot 0 + x \cdot 0$ und $x \cdot 0 = 0 + x \cdot 0$. Wegen der eindeutigen Lösbarkeit der Gleichung $y + x \cdot 0 = x \cdot 0$ (als Gleichung für y) muss $x \cdot 0 = 0$ sein. ∎

Deshalb ist die Gleichung $0 \cdot y = 1$ nie lösbar!

Für Zahlen $x \neq 0$ hat aber die Gleichung $x \cdot y = 1$ stets eine Lösung, die mit x^{-1} bezeichnet wird, und man nennt diese Zahl *das Inverse* zu x. Die Bruchschreibweise $1/x$ führen wir erst später ein!

Satz. $\forall\, a, b \in \mathbb{R}$ *mit* $a \neq 0$ *ist die Gleichung*

$$a \cdot x = b$$

stets eindeutig lösbar.

Beweis: Wie bei der Addition. Man setzt $x := b \cdot a^{-1}$, dazu braucht man, dass $a \neq 0$ ist. ∎

Entsprechend gilt:

Satz. $\forall\, a, b \in \mathbb{R}$ *mit* $a \neq 0$ *und* $b \neq 0$ *gilt:*

$$(a^{-1})^{-1} = a \quad \text{und} \quad (a \cdot b)^{-1} = a^{-1} \cdot b^{-1}.$$

Neue Aspekte ergeben sich dort, wo additive und multiplikative Struktur zusammenspielen:

Satz. *Es ist* $(-1) \cdot (-1) = 1$.

Beweis:

$$\begin{aligned} \text{Es ist} \quad (-1) + (-1) \cdot (-1) &= (-1) \cdot 1 + (-1) \cdot (-1) \\ &= (-1) \cdot (1 + (-1)) \\ &= (-1) \cdot 0 \quad = \quad 0 \\ \text{und} \quad (-1) + 1 &= 1 + (-1) \quad = \quad 0. \end{aligned}$$

Wegen der eindeutigen Lösbarkeit der Gleichung $(-1) + x = 0$ folgt der Satz. ∎

In ähnlicher Weise zeigt man allgemein: $(-a) \cdot (-b) = a \cdot b$.

Wir wissen, dass die Multiplikation einer reellen Zahl mit Null immer Null ergibt. Kann die Null auch noch auf andere Weise als Ergebnis einer Multiplikation erscheinen?

Satz. *Es seien a, b reelle Zahlen mit $a \cdot b = 0$.*
Dann ist $a = 0$ oder $b = 0$.

BEWEIS: Sei $a \cdot b = 0$. Was nun?
Wenn man in einem Beweis nicht weiter kommt, gibt es ein paar Tricks: Zunächst frage man sich, ob man schon alle Voraussetzungen benutzt hat. Das ist hier der Fall, hilft also nicht weiter. Danach überlege man sich, was es denn überhaupt für Möglichkeiten gibt. Das führt ganz automatisch zur Methode der Fallunterscheidung, die einem zusätzliche Voraussetzungen an die Hand gibt:

Ist $b = 0$, so ist schon alles klar.

Ist $b \neq 0$, so existiert das Inverse b^{-1}. Diese Information können wir zusammen mit der Voraussetzung $a \cdot b = 0$ verwerten:

$$0 = 0 \cdot b^{-1} = (a \cdot b) \cdot b^{-1} = a \cdot 1 = a,$$

und damit ist alles gezeigt, denn andere Möglichkeiten gibt es nicht. ∎

Definition.
Sind a und b reelle Zahlen, $b \neq 0$, so wird die reelle Zahl $a \cdot b^{-1}$ mit dem Symbol $\frac{a}{b}$ oder a/b bezeichnet. Man spricht dann von einem *Bruch*. Die Zahl a heißt *Zähler* des Bruches, und die Zahl b heißt *Nenner* des Bruches.

Die Regeln der Bruchrechnung ergeben sich ganz einfach aus den Rechenregeln für reelle Zahlen:

Satz.

1. $\frac{a}{b} + \frac{c}{d} = \frac{a \cdot d + b \cdot c}{b \cdot d}$ *für $b \neq 0$ und $d \neq 0$.*
2. $\frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}$ *für $b \neq 0$ und $d \neq 0$.*
3. $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$ *für $a \neq 0$ und $b \neq 0$.*

BEWEIS: **Den Multiplikations-Punkt lässt man meist weg!**
1) $(ad + cb)(bd)^{-1} = (ad)(bd)^{-1} + (cb)(bd)^{-1} = ab^{-1} + cd^{-1}$.

2) $(ab^{-1})(cd^{-1}) = (ac)(bd)^{-1}$.

3) $(ab^{-1})^{-1} = (a^{-1})((b^{-1})^{-1}) = ba^{-1}$. ∎

Beispiele.

1. Sei x eine beliebige reelle Zahl $\neq 0$ und $\neq 1$. Dann gilt:

$$\frac{x}{1 - 1/(1-x)} \quad = \quad \frac{x}{-x/(1-x)} \quad = \quad x \cdot \frac{1-x}{-x} \quad = \quad x - 1.$$

2. Sei $x \neq 1$ und $x \neq -1$. Dann gilt:

$$\frac{1}{x-1} - \frac{1}{x+1} \quad = \quad \frac{(x+1)-(x-1)}{(x-1)(x+1)} \quad = \quad \frac{2}{x^2-1}.$$

Wir wollen nun die natürlichen Zahlen als Elemente von $\mathbb{R}$ wiederfinden. Dabei dürfen wir uns aber nur auf die Axiome beziehen. Zunächst eine Festlegung: Die natürlichen Zahlen sollen bei 1 starten, und die Null soll nicht zu $\mathbb{N}$ gehören. Und nun erinnern wir uns an die Geschichte vom Nachfolger.

Definition.
Eine Teilmenge $M \subset \mathbb{R}$ heißt *induktiv*, falls gilt:

1. $1 \in M$.
2. $\forall\, x \in \mathbb{R} : \big((x \in M) \implies ((x+1) \in M) \big)$.

Jede induktive Menge enthält die Zahlen 1, 2, 3, 4, ..., aber offensichtlich ist auch $\mathbb{R}$ selbst induktiv, und das ist zu viel des Guten. Der Durchschnitt von zwei induktiven Mengen ist wieder induktiv, dabei wird die Menge höchstens kleiner. Also suchen wir nach der „kleinsten“ induktiven Menge!

Definition.
Ein Element $n \in \mathbb{R}$ heißt *natürliche Zahl*, falls n zu **jeder** induktiven Teilmenge von $\mathbb{R}$ (also zum Durchschnitt aller induktiven Teilmengen) gehört.

Mit $\mathbb{N}$ wird die Menge der natürlichen Zahlen in $\mathbb{R}$ bezeichnet.

Hilfssatz. *$\mathbb{N}$ ist selbst induktiv.*

Beweis: Es müssen zwei Eigenschaften überprüft werden:

1) Da 1 in jeder induktiven Menge liegt, ist 1 eine natürliche Zahl.

2) Sei n eine beliebige reelle Zahl, die in $\mathbb{N}$ liegt. Dann gehört n definitionsgemäß zu jeder induktiven Menge $M \subset \mathbb{R}$, und wegen der induktiven Eigenschaft von M muss auch die reelle Zahl $n+1$ in M liegen. Das bedeutet, dass auch $n+1$ eine natürliche Zahl ist. ∎

Damit haben wir gezeigt, dass $\mathbb{N}$ die kleinste Teilmenge von $\mathbb{R}$ ist, die alle uns vom Zählen her bekannten „natürlichen“ Zahlen 1, 2, 3, ... enthält. Also ist $\mathbb{N}$ genau das, was wir uns unter der Menge $\{1, 2, 3, \ldots\}$ vorstellen. Nun lässt sich eine sehr wichtige Folgerung ziehen:

Induktionsprinzip. *Es sei $M \subset \mathbb{N}$ eine Teilmenge, und es gelte:*

1. $1 \in M$.
2. $\forall\, n \in \mathbb{N} : n \in M \implies (n+1) \in M$.

Dann ist bereits $M = \mathbb{N}$.

Beweis: Nach Voraussetzung ist M eine induktive Teilmenge von $\mathbb{N}$. Weil aber $\mathbb{N}$ schon die kleinste induktive Menge ist, muss sogar $M = \mathbb{N}$ gelten. ∎

Warum ist das Induktionsprinzip wichtig? Es führt zu einem völlig neuen Beweisverfahren, dem „Beweis durch vollständige Induktion“. Man kann dieses Verfahren immer dann benutzen, wenn natürliche Zahlen im Spiel sind:

Sei $A(n)$ eine Aussageform, bei der die natürlichen Zahlen einen zulässigen Objektbereich für die Variable n bilden. Dann kann man versuchen, die Aussage

$$\boxed{\forall\, n \in \mathbb{N} : A(n)}$$

durch vollständige Induktion zu beweisen. Und das geht so:

Sei $M := \{n \in \mathbb{N} \mid A(n)\}$. Dann ist die gewünschte Aussage äquivalent zu der Aussage „ $M = \mathbb{N}$ “. Der Beweis besteht – so er denn möglich ist – aus 2 Teilen.

1) **Induktionsanfang:** Man zeige, dass die Aussage $A(1)$ wahr ist. Das bedeutet, dass $1 \in M$ ist.

2) **Induktionsschluss:** Man beweise, dass für beliebiges $n \in \mathbb{N}$ die folgende Implikation wahr ist:

$$A(n) \quad \Longrightarrow \quad A(n+1).$$

Beachte: Die *Implikation* muss wahr sein, nicht die Aussage $A(n+1)$! Das bedeutet dann: Wenn n in M liegt, so liegt auch $n+1$ in M. Mit dem Induktionsprinzip folgt daraus, dass $M = \mathbb{N}$ ist.

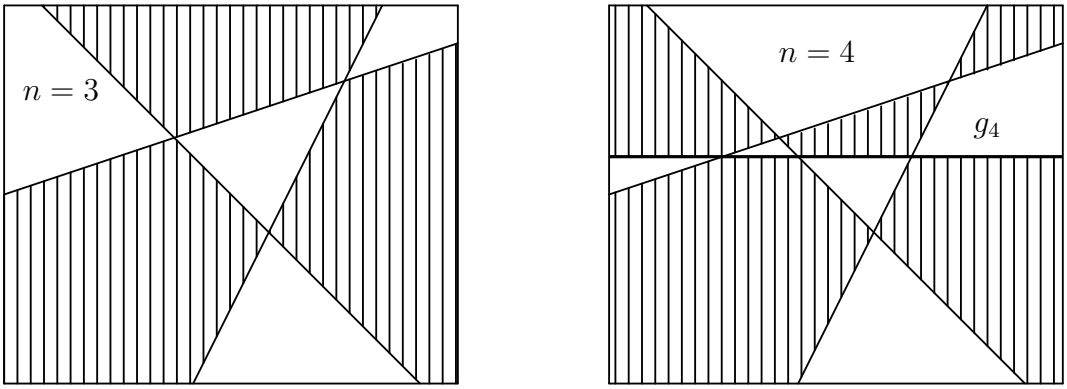
Genaugenommen ist ein Induktionsbeweis ein Beweis mit unendlich vielen Schritten. Man zeigt zunächst den Fall $n = 1$. Dann benützt man diesen schon bewiesenen Fall, um den Fall $n = 2 = 1+1$ zu zeigen. Und dann benützt man wiederum diesen Fall, um den Fall $n = 3 = 2+1$ zu zeigen. Und so fährt man fort. Unendlich viele Schritte kann man nicht aufschreiben, aber wenn die einzelnen Schritte formal alle gleich sind, dann kann man sie mit variablem n alle auf einen Schlag durchführen.

Beispiel.

In einer Ebene seien n paarweise verschiedene Geraden gegeben. Diese teilen die Ebene in verschiedene Gebiete auf und erzeugen so eine „Landkarte“ mit

endlich vielen (zum Teil unendlich weit ausgedehnten) Ländern. Diese Landkarte soll so eingefärbt werden, dass zwei Länder, deren Grenzen wenigstens ein Geradenstück gemeinsam haben, mit verschiedenen Farben versehen sind. Mit wie vielen Farben kommt man aus? Erste Experimente mit wenigen Geraden legen den Verdacht nahe, dass es in einfachen Fällen mit 2 Farben geht.

Behauptung: Man kommt **immer** mit 2 Farben aus.



Beweis: Die einzige natürliche Zahl, die vorkommt, ist die Anzahl n der Geraden. $A(n)$ sei nun die folgende Aussageform:

> Eine von n Geraden erzeugte Landkarte kann mit 2 Farben in der gewünschten Weise eingefärbt werden.

Der Beweis soll durch Induktion nach n geführt werden.

$\underline{n = 1}$: **Eine** Gerade teilt die Ebene in zwei Gebiete, und dann kommt man natürlich mit 2 Farben aus.

$\underline{n \to n + 1}$: Die Behauptung sei schon für die Zahl n bewiesen. Betrachten wir nun eine von $n + 1$ Geraden $g_1, g_2, \ldots, g_{n+1}$ erzeugte Landkarte. Da $n \geq 1$ ist, ist $n + 1 \geq 2$. Lassen wir zunächst die Gerade g_{n+1} weg. Nach Induktionsvoraussetzung kann man die verbliebene Karte mit zwei Farben einfärben. Dann fügen wir g_{n+1} wieder hinzu. Jetzt sind die Regeln verletzt, aber wenn wir auf einer der beiden Seiten von g_{n+1} die vorhandenen Farben vertauschen, dann bekommen wir eine gültige Einfärbung. Also haben wir die Behauptung auch für die Zahl $n + 1$ bewiesen. ∎

Im Oktober 1852 entdeckte der Engländer Francis Guthrie, dass er beim Färben einer Landkarte immer mit vier Farben auskam, auch wenn Länder mit gemeinsamer Grenzlinie verschieden gefärbt sein sollten. Die Frage nach dem Grund dieser erstaunlichen Tatsache wurde durch seinen Bruder Frederick Guthrie und dessen Lehrer de Morgan (dessen Name uns schon bei den

logischen Verneinungsregeln begegnet ist) als *Vierfarbenproblem* bekannt gemacht.

Jahre später verfasste Arthur Cayley eine gründliche mathematische Analyse des Problems, und 1879 veröffentlichte der Jurist Sir Alfred Bray Kempe einen Beweis, der von dem Mathematiker Charles Sanders Peirce noch etwas verbessert wurde. 1890 zeigte Percy John Heawood, dass Kempes Beweis einen Trugschluss enthielt! Gleichzeitig bewies er, dass *fünf* Farben immer genügen.

Immer wieder gab es nun Beiträge zum Vierfarbenproblem, und Ende der sechziger Jahre benutzten Heinrich Heesch und Karl Dürre zum ersten Mal Computer als Hilfsmittel. Ihre Ideen wurden in Amerika bekannt, wo dann schließlich auch das Rennen gewonnen wurde:

Wolfgang Haken und Kenneth Appel konnten 1976 bekanntgeben: Vier Farben genügen! Mit Hilfe einer IBM 360 war es ihnen möglich, tausende von Spezialfällen in vernünftiger Zeit zu behandeln. Dieser intensive Einsatz eines Computers beim Beweis eines mathematischen Theorems hat übrigens in der Fachwelt heftige Grundsatzdiskussionen ausgelöst.

Definition.
Unter der Menge der *ganzen Zahlen* versteht man die Menge

$$\mathbb{Z} = \mathbb{N} \cup \{0\} \cup \{x \in \mathbb{R} : -x \in \mathbb{N}\}.$$

Ist $p \in \mathbb{Z}$ und $q \in \mathbb{N}$, so nennt man den Bruch $\frac{p}{q}$ eine *rationale Zahl*. Die Menge aller rationalen Zahlen wird mit $\mathbb{Q}$ bezeichnet.

Bisher haben wir uns wenig um die Unterscheidung zwischen positiven und negativen Zahlen gekümmert.

[R-4] Axiome der Anordnung. *In $\mathbb{R}$ gibt es eine Teilmenge P (die Menge der* positiven reellen Zahlen*), so dass gilt:*

1. *Ist $a \in P$ und $b \in P$, so ist auch $a + b \in P$ und $a \cdot b \in P$.*
2. *Jede reelle Zahl gehört zu genau einer der drei Mengen P, $\{0\}$ oder $-P := \{x \in \mathbb{R} \mid -x \in P\}$.*

Ist $a \in P$, so schreibt man: $a > 0$.

Die Axiome der Anordnung kann man nun auch folgendermaßen formulieren:
Sind $a, b > 0$, so ist auch $a + b > 0$ und $a \cdot b > 0$. Ist x eine beliebige reelle Zahl, so ist entweder $x = 0$, $x > 0$ oder $-x > 0$, und diese drei Eigenschaften schließen sich gegenseitig aus.

Definition.
Seien $a, b \in \mathbb{R}$. Dann sagt man:

$$\begin{aligned}
a < b &:\Longleftrightarrow b - a > 0 && (a \text{ kleiner als } b).\\
a > b &:\Longleftrightarrow b < a && (a \text{ größer als } b).\\
a \leq b &:\Longleftrightarrow (a < b) \vee (a = b) && (a \text{ kleiner oder gleich } b).\\
a \geq b &:\Longleftrightarrow (a > b) \vee (a = b) && (a \text{ größer oder gleich } b).
\end{aligned}$$

Für den Umgang mit Ungleichungen ist der folgende Satz nützlich:

Satz. *a, b, c seien stets reelle Zahlen. Dann gilt:*

1. *Ist $a < b$ und $b < c$, so ist auch $a < c$ (Transitivität).*
2. *Ist $a < b$ und c beliebig, so ist auch $a + c < b + c$.*
3. *Ist $a < b$ und $c > 0$, so ist $a \cdot c < b \cdot c$.*

Beweis: 1) Ist $a < b$, so ist definitionsgemäß $b - a > 0$. Ebenso folgt aus $b < c$, dass $c - b > 0$ ist. Damit sind die Voraussetzungen verarbeitet. Was haben wir noch zur Verfügung? Die Axiome! Wenden wir das erste Axiom der Anordnung auf $b - a$ und $c - b$ an, so folgt:

$$(b - a) + (c - b) > 0.$$

Es ist aber $(b - a) + (c - b) = c - a$. Also ist $a < c$.

2) Ist $a < b$, so ist $b - a > 0$. Für ein beliebiges c ist dann

$$(b + c) - (a + c) = b - a > 0, \quad \text{also } a + c < b + c.$$

3) Nach Voraussetzung ist $b - a > 0$ und $c > 0$, nach den Axiomen also

$$b \cdot c - a \cdot c = (b - a) \cdot c > 0.$$

∎

Satz. *Ist $x \in \mathbb{R}$ beliebig, $x \neq 0$, so ist $x^2 = x \cdot x > 0$.*
Insbesondere ist $1 > 0$.

Beweis: Wir führen eine Fallunterscheidung durch:

1) Ist $x > 0$, so ist $x^2 := x \cdot x > 0$, nach den Axiomen.

2) Ist $\neg(x > 0)$, so folgt (ebenfalls aus den Axiomen): entweder ist $x = 0$ (was nach Voraussetzung auszuschließen ist), oder es ist $(-x) > 0$.
In dem Fall ist aber $(-x) \cdot (-x) > 0$, und da $(-x) \cdot (-x) = x \cdot x$ ist, folgt die Behauptung.

Schließlich ist noch $1 = 1 \cdot 1 > 0$. ∎

In den Axiomen ist nicht ausdrücklich gefordert worden, dass die 1 zu den positiven Zahlen gehört. Um so befriedigender ist es, dass das automatisch herauskommt.

Behauptung. $\forall\, n \in \mathbb{N} : n \geq 1$.

Beweis:
$\underline{n = 1}$ (Induktionsanfang): Natürlich ist $1 \geq 1$.

$\underline{n \to n+1}$ (Induktionsschluss): Für die natürliche Zahl n sei schon bewiesen, dass $n \geq 1$ ist. Dann ist

$$n + 1 \geq 1 + 1 > 1 + 0 = 1,$$

also auch $n + 1 \geq 1$. ∎

Carl Friedrich Gauß (1777 - 1855) war sicher der bedeutendste Mathematiker seiner Zeit. Dabei stammte er aus sehr einfachen sozialen Verhältnissen. Als er noch in Braunschweig die Volksschule besuchte, trug sich nach seinen eigenen Worten folgendes zu:

Der Lehrer, der eine große Klasse mit Schülern verschiedener Altersstufen zu betreuen hatte, stellte diesen die Aufgabe, alle Zahlen von 1 bis 100 zu addieren, wohl um sie eine Weile zu beschäftigen. Doch nach kurzer Zeit trat der junge Gauß nach vorne an sein Pult und zeigte ihm sein Heft mit folgender Rechnung:

$$\begin{aligned} 1 + 2 + 3 + \ldots + 100 \quad &= \\ = \quad (1 + 100) + (2 + 99) + \ldots + (49 + 52) + (50 + 51) \\ = \quad 50 \cdot 101 \quad &= \quad 5050. \end{aligned}$$

Man kann das auch so schreiben:

$$1 + 2 + 3 + \ldots + 100 = \frac{100}{2} \cdot (100 + 1).$$

Das Verfahren klappt nicht nur bei $n = 100$, sondern mit einer kleinen Modifikation sogar für beliebiges $n \in \mathbb{N}$. Wir wollen hier jedoch noch einen anderen Weg einschlagen und die Formel mit *vollständiger Induktion* beweisen:

Behauptung.

$$1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}.$$

Beweis: Wir führen Induktion nach n.

$\underline{n = 1}$: Die linke Seite der Gleichung besteht nur aus der 1, und die rechte Seite ergibt

$$\frac{1 \cdot (1 + 1)}{2} = 1.$$

Also stimmt die Formel für $n = 1$.

$\underline{n \to n+1}$: Sei $n \in \mathbb{N}$ beliebig, die Formel stimme schon für dieses n. Wir müssen zeigen, dass sie auch für $n+1$ stimmt. Unter Verwendung der Induktionsvoraussetzung erhalten wir:

$$\begin{aligned} 1+2+3+\ldots+n+(n+1) &= \big(1+2+3+\ldots+n\big) + (n+1) \\ &= \frac{n(n+1)}{2} + (n+1) \\ &= \frac{n\cdot(n+1)+2\cdot(n+1)}{2} \\ &= \frac{(n+1)\cdot(n+2)}{2} = \frac{n\cdot(n+1)}{2}. \end{aligned}$$

∎

Solche Beweise werden oft als Inbegriff des Induktionsbeweises aufgefasst. In Wirklichkeit liefert jedoch der Weg zur Formel oft schon den Beweis, und die Induktion erweist sich dann als überflüssig.

Es ist etwas unbefriedigend, dass in solchen Formeln immer wieder die Pünktchen auftauchen. Sie lassen sich tatsächlich vermeiden:

Definition.
Sei $n \in \mathbb{N}$. Für jede natürliche Zahl i mit $1 \le i \le n$ sei eine reelle Zahl a_i gegeben. Dann bezeichnet man die Summe aller dieser Zahlen a_i mit dem Symbol

$$\boxed{\sum_{i=1}^{n} a_i}$$

In Worten: *Summe über a_i , i von 1 bis n.*

Induktiv wird das *Summenzeichen* erklärt durch:

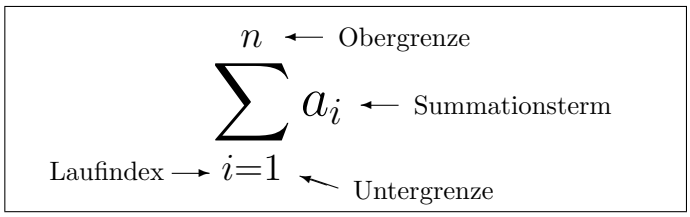
$$\sum_{i=1}^{1} a_i := a_1 \quad \text{und} \quad \sum_{i=1}^{n+1} a_i := \sum_{i=1}^{n} a_i + a_{n+1}.$$

Um die Definition besser zu verstehen, betrachten wir einige Spezialfälle:

$$\begin{aligned} \sum_{i=1}^{2} a_i &= a_1 + a_2. \\ \sum_{i=1}^{3} a_i &= (a_1 + a_2) + a_3. \\ &\vdots \\ \sum_{i=1}^{n} a_i &= (\ldots((a_1 + a_2) + a_3) + \ldots) + a_n. \end{aligned}$$

Wegen des Assoziativgesetzes kann man die Klammern weglassen.

Die Bestandteile des Summenzeichens haben im einzelnen folgende Bedeutung:



Der „Laufindex“ i kann durch ein beliebiges anderes Symbol ersetzt werden. Das muss dann allerdings gleichzeitig an allen Stellen geschehen, wo i auftritt, z.B.

$$\sum_{p=1}^{n} a_p \quad \text{oder} \quad \sum_{\nu=1}^{n} a_\nu \,.$$

Des weiteren sind folgende Manipulationen erlaubt:

1) **Beliebige Grenzen**: Sind $k, l \in \mathbb{Z}$, so ist

$$\sum_{i=k}^{l} a_i = a_k + a_{k+1} + a_{k+2} + \ldots + a_{l-1} + a_l.$$

Ist dabei $k > l$, so spricht man von der „leeren Summe“, und man vereinbart, dass diese immer $= 0$ ist.

2) **Aufteilung der Summe**: Ist $1 \leq m \leq n$, so ist

$$\sum_{i=1}^{n} a_i = \sum_{i=1}^{m} a_i + \sum_{i=m+1}^{n} a_i \quad \text{(Assoziativgesetz)}.$$

3) **Multiplikation mit einer Konstanten**: Ist $c \in \mathbb{R}$, so ist

$$c \cdot \sum_{i=1}^{n} a_i = \sum_{i=1}^{n} (c \cdot a_i) \quad \text{(Distributivgesetz)}.$$

4) **Summe von Summen**: Ist zu jedem i auch noch eine reelle Zahl b_i gegeben, so gilt:

$$\sum_{i=1}^{n} a_i \quad + \quad \sum_{i=1}^{n} b_i \quad = \quad \sum_{i=1}^{n} (a_i + b_i) \quad \text{(Kommutativgesetz)}.$$

5) **Umnummerierung der Indizes**: Ist $m \leq n$, so gilt:

$$\sum_{i=m}^{n} a_i = \sum_{j=1}^{n-m+1} a_{m-1+j}.$$

Diese Formel ist etwas schwerer zu verstehen. Die Terme a_m, a_{m+1}, ..., a_n sollen addiert werden. Wieviele Summanden ergibt das? Ich spreche gerne vom „Gartenzaun-Problem“[1]: Die Differenz aus Ober– und Untergrenze beträgt $n-m$, also sind es $n-m+1$ Summanden. Nun möchte man die Summe so umschreiben, dass der neue Laufindex j von 1 bis $n-m+1$ läuft. Dazu muss der Summationsterm einen Index der Form $k+j$ erhalten, wobei k so zu wählen ist, dass $k+1=m$ und $k+(n-m+1)=n$ ist. Das funktioniert mit $k := m-1$.

Ersetzt man $m-1$ durch ein beliebiges $k \in \mathbb{Z}$, so erhält man noch allgemeiner:

$$\sum_{i=m}^{n} a_i = \sum_{j=m-k}^{n-k} a_{j+k}.$$

Die Gaußsche Formel sieht jetzt z.B. so aus:

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}\,.$$

Zur Übung wollen wir noch eine weitere Summenformel beweisen:

Satz.

$$\sum_{i=1}^{n}(2i-1) = n^2.$$

Beweis: (durch vollständige Induktion nach n)

$\underline{n=1}$: Links ergibt sich $\sum_{i=1}^{1}(2i-1) = 2\cdot 1 - 1 = 1$, und rechts steht $1^2 = 1$.

$\underline{n \to n+1}$: Mit Hilfe der Induktionsvoraussetzung erhält man:

$$\sum_{i=1}^{n+1}(2i-1) = \sum_{i=1}^{n}(2i-1) + 2(n+1) - 1 = n^2 + 2n + 1 = (n+1)^2. \qquad \blacksquare$$

Definition.

Sei a eine beliebige reelle Zahl. Dann kann für jede natürliche Zahl n die Zahl a^n (die n-te *Potenz* von a) definiert werden. Man setzt

$$a^1 := a \quad \text{und} \quad a^{n+1} := a^n \cdot a.$$

Mit einfachen Induktionsbeweisen, die wir hier nicht ausführen wollen, zeigt man die folgenden Rechenregeln für Potenzen:

[1] An einer 30 m langen Grenze sollen Zaunpfähle im Abstand von je 1 m aufgestellt werden. Wieviele Pfähle braucht man?

Satz.

1. $a^{m+n} = a^m \cdot a^n$.
2. $(a^m)^n = a^{m \cdot n}$.

Definiert man noch

$$a^0 := 1 \quad \text{und} \quad a^{-n} := (a^n)^{-1} = (a^{-1})^n \quad \text{(letzteres nur für } a \neq 0),$$

so gelten die obigen Formeln auch für $m, n \in \mathbb{Z}$. Man beachte, dass $0^0 = 1$ ist!

Als nächstes wollen wir zwei kleine kombinatorische Probleme betrachten:

Das erste Problem lautet:

> **Auf wie viele verschiedene Weisen lassen sich die ersten n natürlichen Zahlen anordnen?**

Um die Antwort zu finden, betrachten wir zunächst einige Spezialfälle.

Im Falle $\mathbf{n = 2}$ gibt es 2 Möglichkeiten, nämlich: $\begin{matrix} 1 & 2 \\ 2 & 1 \end{matrix}$

Im Falle $\mathbf{n = 3}$ gibt es schon 6 Möglichkeiten, nämlich:

$$\begin{matrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{matrix} \qquad \begin{matrix} 2 & 1 & 3 \\ 2 & 3 & 1 \end{matrix} \qquad \begin{matrix} 3 & 1 & 2 \\ 3 & 2 & 1 \end{matrix}$$

Beim zweiten Mal sind wir so vorgegangen: Jede der 3 Zahlen kann vorne stehen. Ist diese erste Zahl festgelegt, so bleiben für die beiden restlichen Zahlen jedesmal genau so viele Möglichkeiten, wie sich im Falle $n = 2$ ergeben hatten. Insgesamt sind das $3 \cdot 2 = 6$ verschiedene Anordnungen.

Induktiv kann man nun weiterschließen: Bezeichnet $n!$ (in Worten: „n Fakultät“) die Anzahl der Möglichkeiten, die ersten n Zahlen (oder n beliebige paarweise verschiedene Objekte) anzuordnen, so gilt:

$$1! = 1 \qquad \text{und} \qquad (n+1)! = (n+1) \cdot n!$$

Offensichtlich ist $n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$ das Produkt der ersten n natürlichen Zahlen.

Die Fakultäten werden rasch größer:

$$\begin{aligned} 4! &= 24, \\ 5! &= 120, \\ 6! &= 720, \\ 7! &= 5040 \\ 8! &= 40320, \\ 9! &= 362\,880. \end{aligned}$$

Das nächste kombinatorische Problem lautet:

Wie viele verschiedene Teilmengen mit k Elementen gibt es in einer Menge mit n Elementen?

Am Beispiel der Menge $\{1, 2, 3, \ldots, n\}$ testen wir erst mal einige einfache Fälle:

Im Falle $\mathbf{k = 1}$ erhalten wir die n Teilmengen

$$\{1\},\ \{2\},\ \{3\},\ \ldots\ ,\{n\}.$$

Im Falle $\mathbf{k = 2}$ ergeben sich die folgenden Teilmengen:

$$\{1,2\},\ \{1,3\},\ \ldots\ ,\{1,n\},$$

$$\{2,3\},\ \ldots\ ,\{2,n\},$$

$$\vdots$$

$$\{n-1,n\}.$$

Das sind $(n-1)+(n-2)+\ldots+1 = \dfrac{(n-1)\cdot n}{2}$ Möglichkeiten.

Im Fallle $\mathbf{k = 3}$ erhalten wir die Teilmengen $\{n_1, n_2, m\}$, wobei für $\{n_1, n_2\}$ die Möglichkeiten des Falles $k = 2$ in Frage kommen und dann für m noch jeweils $n-2$ Möglichkeiten bleiben. Dabei tritt aber jede 3-elementige Menge $\{a, b, c\}$ insgesamt dreimal auf! Das sind die folgenden Fälle:

$$\begin{array}{lcll} \{a,b\} & = & \{n_1,n_2\}, & c = m, \\ \{a,c\} & = & \{n_1,n_2\}, & b = m \quad \text{und} \\ \{b,c\} & = & \{n_1,n_2\}, & a = m. \end{array}$$

So erhält man insgesamt $\dfrac{n(n-1)(n-2)}{2\cdot 3}$ Teilmengen.

Nun sieht man, wie es weitergeht: Im Falle der k-elementigen Teilmengen erwarten wir als Lösung die Zahl

$$N := \frac{n(n-1)(n-2)\cdots(n-k+1)}{2\cdot 3\cdots k}\,.$$

Tatsächlich gibt es $n(n-1)(n-2)\cdot\ldots\cdot(n-k+1)$ Möglichkeiten, k Elemente aus $\{1, 2, 3, \ldots, n\}$ herauszusuchen und auf bestimmte Weise anzuordnen. Aber jeweils $k!$ verschiedene Anordnungen ergeben die gleiche Menge. Das führt zu der Zahl

$$\binom{n}{k} := \frac{n(n-1)(n-2)\cdot\ldots\cdot(n-k+1)}{1\cdot 2\cdot\ldots\cdot k} = \frac{n!}{k!\,(n-k)!}.$$

Das neu eingeführte Symbol wird „n über k“ gesprochen. Man nennt diese Zahlen auch *Binomialkoeffizienten*, aus einem Grund, der bald klar werden wird.

Satz.

1. $\binom{n}{k} = \binom{n}{n-k}$.
2. $\binom{n}{1} = n$ *und* $\binom{n}{0} = 1$.
3. $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$.

BEWEIS: Hat $M \subset \{1, 2, \ldots, n\}$ k Elemente, so besitzt die Komplementärmenge M' genau $n - k$ Elemente. Daraus folgt die Aussage (1).

Die erste Aussage von (2) ist leicht zu sehen: Als 1-elementige Teilmengen kommen nur die n Mengen $\{1\}, \{2\}, \ldots, \{n\}$ in Frage. Die zweite Aussage von (2) ergibt sich aus der Tatsache, dass die leere Menge die einzige Menge mit 0 Elementen ist.

Die Aussage (3) muss man nachrechnen:

$$\begin{aligned}\binom{n-1}{k-1} + \binom{n-1}{k} &= \frac{(n-1)!}{(k-1)!(n-k)!} + \frac{(n-1)!}{k!(n-k-1)!} \\ &= \frac{k(n-1)! + (n-k)(n-1)!}{k!(n-k)!} \\ &= \frac{n(n-1)!}{k!(n-k)!} \quad = \quad \binom{n}{k}.\end{aligned}$$

■

Beispiele.

1. Auf einer Party treffen sich 25 Personen, und jeder möchte jedem die Hand geben. Dann werden $\binom{25}{2} = \frac{24 \cdot 25}{2} = 300$ mal Hände geschüttelt.
2. Beim Zahlenlotto werden aus 49 nummerierten Kugeln zufällig 6 Kugeln ausgewählt. Das ergibt $\binom{49}{6} = \frac{44 \cdot 45 \cdot \ldots \cdot 49}{720} = 13\ 983\ 816$ Möglichkeiten! Wenn Sie gerade dabei sind, Ihren Lottozettel auszufüllen, dann sollten Sie das noch einmal überdenken.

Die Regel (3) im obigen Satz ermöglicht es einem auf elegante Weise, Binomialkoeffizienten zu berechnen. Kennt man nämlich alle Koeffizienten der Gestalt $\binom{n-1}{i}$, so ergeben sich die Koeffizienten $\binom{n}{i}$ daraus durch einfache Additionen. Damit erspart man sich die Berechnung der Fakultäten, was bei etwas größeren Zahlen sowieso die Kapazität jedes Taschenrechners sprengen würde. Besonders übersichtlich wird

dieses Verfahren, wenn man die Koeffizienten in der Form des *Pascalschen Dreiecks* anordnet:

$$
\begin{array}{lccccccccccc}
n=0 & & & & & & 1 & & & & & \\
1 & & & & & 1 & & 1 & & & & \\
2 & & & & 1 & & 2 & & 1 & & & \\
3 & & & 1 & & 3 & & 3 & & 1 & & \\
4 & & 1 & & 4 & & 6 & & 4 & & 1 & \\
5 & 1 & & 5 & & 10 & & 10 & & 5 & & 1 \\
 & & & & & & \ldots & & & & &
\end{array}
$$

Nun kommen wir zu der Formel, der die Binomialkoeffizienten ihren Namen verdanken. Sie zeigt, wie man ein *Binom* (d.h die Potenz einer Summe zweier Zahlen) als Summe von *Monomen* (d.h. einfachen Potenzen) schreiben kann:

Die Binomische Formel. *Seien $a, b \in \mathbb{R}$ und $n \in \mathbb{N}$. Dann gilt:*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k.$$

Beweis: Wir könnten Induktion nach n führen, es lohnt aber, ein bisschen mehr nachzudenken.

Als erstes kann man ein paar einfache Fälle „zu Fuß“ berechnen:

1. $(a+b)^2 = a^2 + 2ab + b^2$.
2. $(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$.

Dann überlegt man sich, dass das Produkt $(a+b)\cdots(a+b)$ eine Summe von Termen der Gestalt $a^i b^{n-i}$ ergibt. Jeder dieser Terme taucht genau so oft auf, wie man aus den n Faktoren i auswählen kann. Und das ergibt schon die gewünschte Formel. ∎

Folgerung. *Eine Menge A von n Elementen besitzt genau 2^n verschiedene Teilmengen (inkl. A und $\varnothing$).*

Beweis: Die Anzahl ist

$$= \binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{n}$$

$$= \sum_{k=0}^{n} \binom{n}{k} = \sum_{k=0}^{n} \binom{n}{k} 1^{n-k} \cdot 1^k = (1+1)^n = 2^n.$$

∎

Geometrische Summationsformel. *Ist $a \in \mathbb{R}$, $a \neq 1$ und $n \in \mathbb{N}$, so gilt:*

$$\sum_{i=0}^{n} a^i = \frac{a^{n+1} - 1}{a - 1}.$$

Beweis: Wir verwenden einen Trick, den man sich unbedingt für sein späteres Leben merken sollte:

$$\begin{aligned} \text{Es ist nämlich} \quad \left(\sum_{i=0}^{n} a^i \right) \cdot (a-1) &= \sum_{i=0}^{n} a^{i+1} - \sum_{i=0}^{n} a^i \\ &= \sum_{i=1}^{n+1} a^i - \sum_{i=0}^{n} a^i \\ &= a^{n+1} - a^0 \quad = \quad a^{n+1} - 1. \end{aligned}$$

Da $a \neq 1$ vorausgesetzt wurde, darf man durch $(a-1)$ dividieren. ∎

Sissa, der legendäre Erfinder des Schachspiels, erbat sich von dem indischen König Shirham nur wenig als Belohnung: Er wollte 1 Weizenkorn für das erste Feld, 2 für das zweite, $2^2 = 4$ für das dritte, u.s.w. Insgesamt ergab das

$$1 + 2 + 4 + 8 + \ldots + 2^{63} = \frac{2^{64} - 1}{2 - 1} = 2^{64} - 1$$

Körner, eine Zahl mit 20 Stellen, und auf der ganzen Welt gab es nicht genug Getreide, um die Belohnung auszuzahlen.

Das bei der geometrischen Summenformel benutzte Beweisverfahren lässt sich übrigens auch bei folgender Aussage verwenden:

Satz. *Sind $a, b \in \mathbb{R}$, $n \in \mathbb{N}$, so ist*

$$a^{n+1} - b^{n+1} = (a - b) \cdot \sum_{i=0}^{n} a^i b^{n-i}.$$

Zum Beweis muss man nur die rechte Seite ausmultiplizieren. Es ergibt sich eine Wechselsumme, von der mit Ausnahme des ersten und des letzten Gliedes alles wegfällt.

Beispiel.

Es ist $a^2 - b^2 = (a - b) \cdot (a + b)$.

Erweitertes Induktionsprinzip. *Es sei $M \subset \mathbb{N}$ eine Teilmenge, $k \in \mathbb{N}$ und es gelte:*

1. $k \in M$.

2. $\forall\, n \geq k : n \in M \implies (n+1) \in M$.

Dann ist bereits $M = \{n \in \mathbb{N} : n \geq k\}$.

Die Induktion braucht also nicht unbedingt bei 1 **zu beginnen.**

BEWEIS: Man beweist durch Induktion die Aussage: „$n < k$ oder $n \in M$“. ∎

Wir müssen nun noch ein paar ganz einfache Aussagen beweisen.

Hilfssatz 1. *Ist* $n \in \mathbb{N}$ *und* $n \neq 1$*, so gibt es einen „Vorgänger“* $m \in \mathbb{N}$ *mit* $m + 1 = n$.

BEWEIS: Wir beweisen die Aussage des Satzes durch Induktion nach n.

$\underline{n = 1:}$ Da hier die Prämisse „$n \neq 1$“ schon falsch ist, ist nichts zu zeigen.

$\underline{n \to n+1:}$ Ist die Aussage für ein $n \geq 1$ schon bewiesen, so folgt, dass $n + 1$ die natürliche Zahl n als Vorgänger hat. ∎

Bemerkung: Beim Induktionsanfang gilt die Implikation, weil die Prämisse falsch ist, beim Induktionsschluss gilt sie, weil dann die Behauptung auf jeden Fall wahr ist. Inhaltlich haben wir garnicht geschlossen!

Hilfssatz 2. *Seien* $n, m \in \mathbb{N}$*. Ist* $m < n$*, so ist* $n - m \in \mathbb{N}$.

BEWEIS: Wir führen Induktion nach m. Der Induktionsanfang wurde durch Hilfssatz 1 erledigt. Ist die Behauptung für ein $m \geq 1$ bewiesen und $m + 1 < n$, so hat $n - m$ einen Vorgänger k, d.h. es ist $n - m = k + 1$ und damit $n - (m + 1) = n - m - 1 = k \in \mathbb{N}$. ∎

Hilfssatz 3. *Ist* $n \in \mathbb{N}$*, so gibt es keine natürliche Zahl* x *mit* $n < x < n + 1$.

BEWEIS: Auch hier benutzen wir Induktion nach n.

Ist x eine natürliche Zahl mit $1 < x < 1 + 1$, so ist $x - 1 \in \mathbb{N}$ (nach Hilfssatz 1) und $0 < x - 1 < (1 + 1) - 1 = 1$. Das kann aber nicht sein.

Nun sei die Behauptung für ein $n \geq 1$ bewiesen. Gibt es ein $x \in \mathbb{N}$ mit $n + 1 < x < n + 2$, so ist $x > 1$, besitzt also einen Vorgänger $x - 1 \in \mathbb{N}$. Es muss dann auch $n < x - 1 < n + 1$ sein, und das ist nicht möglich, nach Induktionsvoraussetzung. ∎

Definition.

Sei $M \subset \mathbb{R}$ eine beliebige Teilmenge. Ein Element $a \in M$ heißt *kleinstes Element* (bzw. *größtes Element*) von M, falls gilt:

$$\forall\, x \in M \,:\, a \leq x \quad (\text{bzw. } a \geq x\,).$$

Beispiele.

1. 5 ist kleinstes Element der Menge $\{5, 7, 89/7, 100\}$.
2. 0 ist kleinstes Element der Menge $\{m \in \mathbb{Z} \mid m > -1/3\}$.
3. Die Menge $\{x \in \mathbb{R} \mid x > 0\}$ besitzt kein kleinstes Element. (Warum nicht?)

Fundamental für das Arbeiten mit natürlichen Zahlen ist die folgende Tatsache:

Wohlordnungs–Satz.
Jede ***nicht leere*** *Menge M von natürlichen Zahlen besitzt ein kleinstes Element.*

Beweis: Wir würden gerne Induktion benutzen, aber es fehlt eine Variable dafür. Der Trick dieses Beweises besteht darin, dass wir künstlich eine Variable einführen. Wir beweisen nämlich die folgende Aussage $A(n)$:

> Jede Teilmenge $M \subset \mathbb{N}$, die die Zahl n enthält, besitzt ein kleinstes Element.

Haben wir die Aussage $A(n)$ durch vollständige Induktion für jedes $n \in \mathbb{N}$ bewiesen, so haben wir auch den Satz bewiesen.

A(1): Ist $1 \in M$, so ist natürlich 1 das kleinste Element.

A(n) $\Longrightarrow$ **A(n+1)**: Es sei $M \subset \mathbb{N}$ eine Teilmenge, die die Zahl $n+1$ enthält. Die Aussage $A(n)$ sei schon bewiesen.

Wir müssen die Aussage $A(n)$ irgendwie benutzen. Da wir nicht wissen, ob n in M liegt, machen wir eine Fallunterscheidung:

a) Ist $n \in M$, so hat M nach Induktionsvoraussetzung ein kleinstes Element, und wir sind fertig.

b) Ist $n \notin M$, müssen wir uns einen weiteren Trick einfallen lassen. Wir basteln uns eine neue Menge, die n enthält: Sei $H := M \cup \{n\}$ unsere „Hilfsmenge“. Offensichtlich ist $H \subset \mathbb{N}$ und $n \in H$. Nach Induktionsvoraussetzung besitzt H ein kleinstes Element a, und es muss dann $a \leq n$ sein.

Ist $a < n$, so muss a schon in M liegen und dort erst recht das kleinste Element sein. So bleibt nur noch der Fall zu betrachten, dass $a = n$ ist. Aber dann kommt a in M nicht vor, und es muss $a < m$ für alle $m \in M$ gelten. Da die Ungleichung $m - 1 < a < m$ nicht gelten kann, muss $m - 1 \geq a$ sein, also $n + 1 = a + 1 \leq m$ für alle $m \in M$. Das bedeutet, dass $n + 1$ das kleinste Element von M ist. ∎

Manch einer wird nicht verstanden haben, dass man den Satz überhaupt beweisen muss. Aber wer glaubt, dass ihm schon der gesunde Menschenverstand sagt, dass der Wohlordnungssatz richtig ist, der möge versuchen, die Erklärung dafür zu Papier zu bringen. Außerdem sollte einem der folgende Satz zu denken geben:

Satz. *Die Menge $\mathbb{N}$ besitzt kein größtes Element.*

BEWEIS: Wir führen einen Widerspruchsbeweis: Wäre $a \in \mathbb{N}$ ein größtes Element von $\mathbb{N}$, so wäre $n \leq a$, für jede natürliche Zahl n. Aber mit a liegt auch $a+1$ in $\mathbb{N}$, und es ist $a+1 > a+0 = a$. Das ist ein Widerspruch! ∎

Der Wohlordnungssatz liefert uns nun eine weitere Variante des Induktionsprinzips:

Zweites Induktionsprinzip. *Es sei $M \subset \mathbb{N}$, und es gelte:*

1. $1 \in M$.
2. *Ist $n \in \mathbb{N}$ und $k \in M$ für alle $k < n$, so ist auch $n \in M$.*

Dann ist $M = \mathbb{N}$.

BEWEIS: Es sei eine Menge $M \subset \mathbb{N}$ mit den Eigenschaften (1) und (2) gegeben.
Annahme: $M \neq \mathbb{N}$.
Dann ist die Menge $T := \mathbb{N} \setminus M$ nicht leer, sie besitzt also ein kleinstes Element n. Dieses muss größer als 1 sein (da die 1 in M liegt). Für alle Zahlen $k < n$ gilt offensichtlich: $k \in M$. Wegen Bedingung (2) ist dann auch $n \in M$. Aber das ist ein Widerspruch! ∎

Als nächstes wollen wir uns mit der Frage beschäftigen, wie es in $\mathbb{Z}$ mit der Multiplikation und Division aussieht. Dafür brauchen wir noch ein Ergebnis über Ungleichungen.

Hilfssatz. *Sind a, b reelle Zahlen mit $0 < a < b$, so ist $a^{-1} > b^{-1} > 0$.*

BEWEIS: Allgemein gilt: Ist $x \in \mathbb{R}$, $x > 0$, so ist auch $x^{-1} > 0$, denn es ist ja $x \cdot x^{-1} = 1 > 0$.

Ist nun $0 < a < b$, so ist $1 = aa^{-1} < ba^{-1}$, also $b^{-1} = b^{-1} \cdot 1 < b^{-1}(ba^{-1}) = a^{-1}$. ∎

Satz.

1. *Sind $a, b \in \mathbb{Z}$, so ist auch $a \cdot b \in \mathbb{Z}$.*
2. *Ist $a \in \mathbb{Z}$, $a \neq 0$ und $a \notin \{1, -1\}$, so ist $a^{-1} \notin \mathbb{Z}$.*

BEWEIS: 1) Ist $a = 0$ oder $b = 0$, so ist $a \cdot b = 0 \in \mathbb{Z}$. Wegen der Formeln $(-a) \cdot (-b) = a \cdot b$ und $(-a) \cdot b = -(a \cdot b)$ genügt es zu zeigen: Sind $m, n \in \mathbb{N}$, so ist auch $m \cdot n \in \mathbb{N}$.

Sei m fest gewählt. Dann ist $m \cdot 1 = m \in \mathbb{N}$. Ist $n \in \mathbb{N}$ beliebig und $m \cdot n \in \mathbb{N}$, so ist $m \cdot (n+1) = m \cdot n + m$ offensichtlich auch in $\mathbb{N}$.

2) Es reicht zu zeigen: Ist $n \in \mathbb{N}$ und $n > 1$, so ist $n^{-1} \notin \mathbb{N}$. Angenommen, n^{-1} liegt doch in $\mathbb{N}$. Da $(n^{-1})^{-1} = n$ ist, kann n^{-1} nicht $= 1$ sein. Also muß $n^{-1} > 1$ sein, aber das ist nach dem vorigen Hilfssatz unmöglich. ∎

Die Division ist also in $\mathbb{Z}$ i.a. nicht möglich. Trotzdem ist die Situation besser, als es nach dem letzten Satz aussieht. Es kann nämlich passieren, daß $a \in \mathbb{Z}$, $b \in \mathbb{Z}$ und $b > 1$ ist, aber dennoch $a \cdot b^{-1} \in \mathbb{Z}$. Zum Beispiel ist $12 \cdot 3^{-1} = 4$. Diese Situation ist so wichtig, daß man dafür eine neue Bezeichnung eingeführt hat:

Definition.
Seien $a, b \in \mathbb{Z}$. b heißt *Teiler* von a, falls es eine ganze Zahl q gibt, so daß $a = q \cdot b$ ist.

Man schreibt dann: $\boxed{b \mid a}$ („b teilt a“).

Beispiele.

1. $3 \mid 12, \quad (-7) \mid 49, \quad (-5) \mid (-20)$.
2. $b \mid 0$ gilt für jede ganze Zahl b.
3. $1 \mid a$ gilt für jede ganze Zahl a.

Ist b **kein** Teiler von a, so schreibt man: $b \nmid a$.

Satz. *Für $a, b, c, d \in \mathbb{Z}$ gelten folgende Teilbarkeitsregeln:*

1. $a \mid b \implies a \mid bc$,
2. $(a \mid b) \wedge (b \mid c) \implies a \mid c$,
3. $(a \mid b) \wedge (a \mid c) \implies a \mid (b + c)$.

Beweis: 1) $b = q \cdot a \implies bc = (qc) \cdot a$.
2) $(b = q \cdot a) \wedge (c = p \cdot b) \implies c = (pq) \cdot a$.
3) $(b = q \cdot a) \wedge (c = r \cdot a) \implies b + c = (q + r) \cdot a$. ∎

Definition.
Sei $a \in \mathbb{Z}$. Dann heißen die Zahlen 1, -1, a und $-a$ die *trivialen Teiler* von a. Alle anderen Teiler von a nennt man *echte Teiler* von a.

Eine natürliche Zahl $p > 1$ heißt *Primzahl*, falls sie keine echten Teiler besitzt.

In der Schule wird oft die Frage gestellt, warum 1 keine Primzahl sei. Aus Gründen, die erst in der höheren Algebra verständlich werden, definiert man das einfach so!

Hilfssatz. *Seien $a, b \in \mathbb{N}$. Ist $a \mid b$, so ist $a \leq b$.*

BEWEIS: Sei $b = q \cdot a$ mit einer ganzen Zahl q. Da a und b positiv sind, muß auch q positiv sein, also $q \in \mathbb{N}$. Aber dann ist $q \geq 1$ und $b = q \cdot a \geq 1 \cdot a = a$. ∎

Satz. 2 *ist die kleinste Primzahl.*

BEWEIS: a) Zwischen 1 und $2 = 1 + 1$ kann es keine weitere natürliche Zahl geben. Also ist 2 die zweit-kleinste natürliche Zahl.

b) Sei jetzt $a \in \mathbb{N}$ ein Teiler von 2. Dann muß $a \leq 2$ sein und dafür kommen nur die trivialen Teiler 1 und 2 in Frage. ∎

Wir wollen jetzt eine Tabelle der Primzahlen unter 100 erstellen:

Das ist viel leichter, als man zunächst annehmen könnte. Ist $n \leq 100$ und $n = a \cdot b$ mit echten Teilern a und b, so muß wenigstens einer der beiden Faktoren < 10 sein. Und wie wir uns im Folgenden noch überlegen werden, muß n dann sogar Vielfaches einer Primzahl $p < 10$ sein.

Alle *geraden Zahlen*, also alle Vielfachen der 2, kommen — mit Ausnahme der 2 selbst — nicht als Primzahlen in Frage. Streichen wir sie in der Multiplikationstabelle der Zahlen von 1 bis 10, so bleiben nur noch die 2 und alle *ungeraden Zahlen* zwischen 1 und 100 übrig. Die 3 bleibt als Primzahl stehen und alle echten Vielfachen von 3 können wir ebenfalls streichen. Die nächste Primzahl ist die 5, ihre Vielfachen lassen wir weg. Nun ist von den Zahlen unter 10 nur noch die 7 übrig geblieben. Die muß ebenfalls eine Primzahl sein (denn wir haben ja schon die Vielfachen aller kleineren Primzahlen entfernt), und wenn wir noch die Vielfachen von 7 aus unserer Tabelle streichen, so bleiben genau die Primzahlen unter 100 stehen.

	2	3	5	7	
11		13		17	19
		23			29
31				37	
41		43		47	
		53			59
61				67	
71		73			79
		83			89
				97	

Dieses Verfahren nennt man das *Sieb des Eratosthenes* (Eratosthenes von Cyrene war etwa um 240 v.Chr. Direktor der Bibliothek von Alexandria). Es benutzt keinerlei Division, was für die alten Griechen angesichts ihres komplizierten Zahlensystems sehr wertvoll war.

Jede natürliche Zahl ist Summe von endlich vielen Einsen. Multiplikativ gesehen bilden jedoch die Primzahlen die elementaren Bausteine der natürlichen Zahlen.

Das wollen wir in den nächsten Sätzen vertiefen:

Satz. *Jede natürliche Zahl $a > 1$ besitzt mindestens einen Primteiler (also eine Primzahl p mit $p \mid a$), und zwar ist der kleinste Teiler $p > 1$ von a eine Primzahl.*

Beweis: Sei $M := \{n \in \mathbb{N} \mid (n > 1) \wedge (n \mid a)\}$. Da a selbst in M liegt, ist M nicht leer. Also gibt es in M ein kleinstes Element p. Nach Konstruktion ist $p > 1$. Hätte p einen echten Teiler, so wäre dieser auch ein Teiler von a. Das kann aber nicht sein, also ist p eine Primzahl. ∎

Satz von der eindeutigen Primfaktorzerlegung.
Jede natürliche Zahl $a > 1$ besitzt eine Darstellung

$$a = p_1 \cdots p_n$$

als Produkt von endlich vielen Primzahlen.
Die Primzahlen $p_1, \ldots, p_n$ brauchen nicht alle verschieden zu sein. Bis auf die Reihenfolge sind sie jedoch eindeutig bestimmt.

Dieser Satz wird auch als *Fundamentalsatz der Elementaren Zahlentheorie* bezeichnet. Zum ersten Mal klar formuliert und bewiesen wurde er 1801 von C. F. Gauß.

Auf den Beweis müssen wir hier verzichten.

Es folgt:

Satz. *Seien $a, b \in \mathbb{N}$, p eine Primzahl. Dann gilt:*

$$p \mid (a \cdot b) \implies (p \mid a) \vee (p \mid b).$$

Beweis: Ist p ein Teiler von ab, so gibt es eine natürliche Zahl q mit $ab = qp$. Sind $a = p_1 \cdots p_s$ und $b = q_1 \cdots q_r$ Primfaktorzerlegungen, so muss p in diesen Primfaktoren vorkommen. ∎

Wenn wir eine Primfaktorzerlegung praktisch durchführen, versuchen wir meist, etwas Ordnung zu schaffen, indem wir die Primzahlen der Größe nach ordnen und gleiche Primzahlen zu Primzahlpotenzen zusammenfassen. Dadurch können wir auch die Eindeutigkeit der Zerlegung herstellen:

> *Zu jeder natürlichen Zahl $a > 1$ gibt es eine eindeutig bestimmte Zahl $k \in \mathbb{N}$, Primzahlen $p_1 < p_2 < \ldots < p_k$ und Exponenten $n_1, n_2, \ldots, n_k$, so daß gilt:*
>
> $$a = p_1^{n_1} \cdot p_2^{n_2} \cdots p_k^{n_k}.$$

Z.B. ist $44 = 2^2 \cdot 11$ oder $120 = 2^3 \cdot 3 \cdot 5$.

Wenn zwei Zahlen a und b die selben Primfaktoren enthalten,

$$a = p_1^{n_1} \cdot p_2^{n_2} \cdot \cdots \cdot p_k^{n_k} \quad \text{und} \quad b = p_1^{m_1} \cdot p_2^{m_2} \cdot \cdots \cdot p_k^{m_k},$$

so gilt:

$$a \,\Big|\, b \iff n_1 \leq m_1,\, n_2 \leq m_2, \ldots, n_k \leq m_k.$$

Um dieses Kriterium immer anwenden zu können, fügt man gerne fehlende Primfaktoren mit dem Exponenten 0 ein.

Gesetzmäßigkeiten zur Verteilung der Primzahlen zu finden, gehört zu den schwersten Problemen in der Mathematik. Ob die Folge der Primzahlen eventuell sogar ganz abbricht, beantwortet der folgende Satz:

Satz von Euklid. *Es gibt unendlich viele Primzahlen.*

Beweis: Genau genommen wird gezeigt, dass die Folge der Primzahlen nicht abbricht. Wir nehmen an, es gibt nur endlich viele Primzahlen, etwa $p_1, p_2, \ldots, p_n$, und bilden die Zahl $P := p_1 p_2 \cdots p_n$. Dann besitzt die Zahl $P + 1$ einen kleinsten Primteiler q, der natürlich unter den Zahlen $p_1, \ldots, p_n$ vorkommen muß, also auch ein Teiler von P ist. Wenn jedoch q ein Teiler von P und von $P + 1$ ist, dann muß q auch Teiler von 1 sein. Das ist unmöglich! ∎

Leider gibt es keine Formel, die automatisch Primzahlen liefert.

Definition.
Sei $M \subset \mathbb{R}$ eine beliebige Teilmenge. Eine Zahl $a \in \mathbb{R}$ heißt *obere Schranke* (bzw. *untere Schranke*) von M, falls gilt:

$$\forall\, x \in M \,:\, x \leq a \quad (\text{bzw. } x \geq a).$$

Die Menge M heißt *nach oben* (bzw. *nach unten*) *beschränkt*, falls sie eine obere (bzw. untere) Schranke besitzt.

Das größte Element einer Menge muss also in der Menge enthalten sein, eine obere Schranke nicht. Bei einer groben Überschlagsrechnung wird man sicher viel schneller eine obere Schranke als das (sogar eindeutig bestimmte) größte Element finden.

Satz. *Sei $M \subset \mathbb{N}$ nicht leer. Wenn es eine* ***natürliche Zahl*** *s gibt, die obere Schranke von M ist, so besitzt M ein größtes Element.*

Beweis: Jede Menge natürlicher Zahlen besitzt die 1 als untere Schranke und auch tatsächlich ein kleinstes Element. Es scheint eine gewisse Symmetrie zwischen diesem Sachverhalt und der Behauptung zu geben, und das wollen wir ausnutzen. Wir spiegeln die Menge M an der Null in die negativen ganzen Zahlen hinein und verschieben sie dann so weit „nach rechts“, daß sie wieder in $\mathbb{N}$ liegt:

Sei $s \in \mathbb{N}$ eine obere Schranke von M. Ist $m \in M$, so ist $m \leq s$, also $s - m + 1 > 0$ und damit ein Element von $\mathbb{N}$. Die Menge

$$M^* := \{s - m + 1 \mid m \in M\} \subset \mathbb{N}$$

ist nicht leer (weil M nicht leer ist) und besitzt daher ein kleinstes Element a.

Es gibt ein $m_0 \in M$, so daß $a = s - m_0 + 1$ ist. Damit gilt:

$$\forall\, m \in M \text{ ist } s - m_0 + 1 \leq s - m + 1,$$

also $m_0 \geq m$ für alle $m \in M$. Die Zahl m_0 ist größtes Element von M. ∎

Ist $a \in \mathbb{N}$, so ist $T_a := \{n \in \mathbb{N} : n \,\Big|\, a\}$ die Menge aller positiven Teiler von a. Sind a, b zwei natürliche Zahlen, so ist $T_a \cap T_b$ die Menge der gemeinsamen Teiler. Diese Menge wird durch natürliche Zahlen nach oben beschränkt, denn jeder Teiler von a muß $\leq a$ sein. Außerdem ist sie nicht leer, denn sie enthält immer die 1. Also besitzt sie ein größtes Element.

Definition.
Für je zwei natürliche Zahlen a, b ist der *größte gemeinsame Teiler* von a und b (in Zeichen: $\mathrm{ggT}(a, b)$) definiert als das (eindeutig bestimmte) größte Element von $T_a \cap T_b$.

Ist $\mathrm{ggT}(a, b) = 1$, so nennt man a und b *teilerfremd*.

Die Menge $V_a := \{n \in \mathbb{N} : a \,\Big|\, n\} = \{a, 2a, 3a, \ldots\}$ ist die Menge aller (positiven) Vielfachen von a. Sind $a, b \in \mathbb{N}$, so enthält $V_a \cap V_b$ die gemeinsamen Vielfachen von a und b. Auch diese Menge ist nicht leer, denn sie enthält ja die Zahl $a \cdot b$. Allerdings ist sie unbeschränkt!

Definition.
Für je zwei natürliche Zahlen a, b ist das *kleinste gemeinsame Vielfache* von a und b (in Zeichen: $\mathrm{kgV}(a, b)$) definiert als das (eindeutig bestimmte) kleinste Element von $V_a \cap V_b$.

Das folgende Verfahren zur Bestimmung von ggT und kgV dürfte jedem aus der Schule bekannt sein:

Sind a und b mit ihrer Primfaktorzerlegung gegeben,

$$a = p_1^{n_1} \cdot p_2^{n_2} \cdot \cdots \cdot p_k^{n_k} \quad \text{und} \quad b = p_1^{m_1} \cdot p_2^{m_2} \cdot \cdots \cdot p_k^{m_k},$$

so gilt offensichtlich:

$$\begin{aligned} \mathrm{ggT}(a, b) &= p_1^{\min(n_1, m_1)} \cdot \ldots \cdot p_k^{\min(n_k, m_k)}, \\ \mathrm{kgV}(a, b) &= p_1^{\max(n_1, m_1)} \cdot \ldots \cdot p_k^{\max(n_k, m_k)}. \end{aligned}$$

Sind $n, m \in \mathbb{N}$, so ist $\min(n, m)$ die kleinere und $\max(n, m)$ die größere der beiden Zahlen. Offensichtlich ist

$$\min(n, m) + \max(n, m) = n + m.$$

Daraus folgt:

Satz. *Sind* $a, b \in \mathbb{N}$*, so ist* $\mathrm{ggT}(a,b) \cdot \mathrm{kgV}(a,b) = a \cdot b$.

Wenn die Zahlen allerdings groß werden, dann kann sich ihre Zerlegung in Primfaktoren als sehr schwierig erweisen.

Satz von der Division mit Rest. *Seien* $a, b \in \mathbb{N}$, $1 \leq b \leq a$. *Dann gibt es eindeutig bestimmte Zahlen* $q, r \in \mathbb{N}_0$*, so daß gilt:*

1. $a = q \cdot b + r$.
2. $0 \leq r < b$.

Beweis: Das Verfahren ist ganz simpel. b wird so oft von a subtrahiert, bis nur noch ein Rest $r < b$ übrig bleibt:

$$\begin{aligned} \text{Sei } S &:= \{a,\, a-b,\, a-2b,\, \ldots\} \cap \mathbb{N}_0 \\ &= \{n \in \mathbb{N}_0 \,:\, \exists\, x \in \mathbb{N}_0 \text{ mit } n = a - x \cdot b\}. \end{aligned}$$

Da $a = a - 0 \cdot b$ in S liegt, ist $S \neq \varnothing$. Als Teilmenge von $\mathbb{N}_0$ besitzt S ein kleinstes Element r. Sei $q \in \mathbb{N}_0$ so gewählt, daß $r = a - q \cdot b$ ist. Damit haben wir schon die gewünschte Darstellung, und wir müssen nur noch nachprüfen, ob alle Eigenschaften erfüllt sind.

Nach Konstruktion ist $r \geq 0$. Wäre $r \geq b$, so wäre auch noch $r - b = a - (q+1) \cdot b \in S$, im Widerspruch zur Minimalität von r. Das bedeutet, daß $r < b$ ist.

Nun fehlt noch die Eindeutigkeit: Es gebe Zahlen $q_1, q_2 \in \mathbb{N}_0$ und $r_1, r_2 \in \mathbb{N}_0$, so daß $a = q_1 \cdot b + r_1 = q_2 \cdot b + r_2$ ist, mit $0 \leq r_1 < b$ und $0 \leq r_2 < b$. Dann ist $(q_1 - q_2) \cdot b = r_2 - r_1$. Ist $r_1 = r_2$, so ist die rechte Seite der Gleichung $= 0$, und es muß auch $q_1 = q_2$ sein. Dann ist man fertig. Ist $r_1 \neq r_2$, so muß eine der beiden Zahlen größer sein. O.B.d.A. (also „Ohne Beschränkung der Allgemeinheit“) sei $r_2 > r_1$. Dann ist die rechte Seite der Gleichung positiv, und $q_1 - q_2$ muß ebenfalls > 0 sein.

Da $r_2 < b$ und $r_1 \geq 0$ ist, ist auch $r_2 - r_1 < b$ und damit $b \cdot (q_1 - q_2) < b$. Das geht nur, wenn $q_1 - q_2 < 1$ ist, aber für eine positive ganze Zahl ist das nicht möglich. ∎

Die Division mit Rest ist aus der Schulmathematik gut bekannt. Man schreibt dort auch:

$$a \,:\, b = q \text{ Rest } r, \qquad \text{oder} \qquad a \,:\, b = q + \frac{r}{q}\,.$$

Hier wollen wir die Division mit Rest benutzen, um einen Algorithmus zur Bestimmung des ggT zweier Zahlen zu gewinnen.

Der euklidische Algorithmus:

Gegeben seien zwei natürliche Zahlen a, b mit $a \geq b$. Dann führt man sukzessive Divisionen mit Rest aus:

$$\begin{aligned}
a &= q \cdot b + r, \quad \text{mit } 0 \leq r < b. \\
b &= q_1 \cdot r + r_2, \quad \text{mit } 0 \leq r_2 < r. \\
r &= q_2 \cdot r_2 + r_3, \quad \text{mit } 0 \leq r_3 < r_2. \\
&\vdots \\
r_{n-2} &= q_{n-1} \cdot r_{n-1} + r_n, \quad \text{mit } 0 \leq r_n < r_{n-1}. \\
r_{n-1} &= q_n \cdot r_n.
\end{aligned}$$

Das Verfahren muß auf jeden Fall abbrechen, weil $b > r > r_2 > r_3 > \ldots \geq 0$ ist. Weiter ist $T_a \cap T_b = T_b \cap T_r = T_r \cap T_{r_2} = \ldots = T_{r_{n-1}} \cap T_{r_n} = T_{r_n}$. Die letzte Gleichung gilt, weil $T_{r_n} \subset T_{r_{n-1}}$ ist. Daraus folgt:

$$\mathrm{ggT}(a, b) = \mathrm{ggT}(b, r) = \mathrm{ggT}(r, r_2) = \ldots = \mathrm{ggT}(r_{n-1}, r_n) = r_n.$$

Beispiel.

Es soll $\mathrm{ggT}(12378, 3054)$ berechnet werden:

$$\begin{aligned}
12378 &= \underbrace{4 \cdot 3054}_{12216} + 162. \\
3054 &= \underbrace{18 \cdot 162}_{2916} + 138. \\
162 &= 1 \cdot 138 + 24. \\
138 &= 5 \cdot 24 + 18. \\
24 &= 1 \cdot 18 + 6. \\
18 &= 3 \cdot 6.
\end{aligned}$$

Also ist $\mathrm{ggT}(12378, 3054) = 6$.

Der euklidische Algorithmus ist besonders bei großen Zahlen nützlich.