Vorlesung 1: Eine Tafel Schokolade in Quadrate schneiden

Problem 1. Sei X ein Rechteck mit Seitenlängen n, m, wobei n und m natüliche Zahlen sind $(n, m \in \mathbb{N})$. Bestimmen Sie die größtmögliche Seitenlänge $k \in \mathbb{N}$ sodass sich das Rechteck vollständig in Quadrate der Größe $k \times k$ zerlegen lässt.

Man kann sich das Rechteck als eine Schokoladentafel vorstellen, die bereits in kleine Quadrate der Größe 1×1 unterteilt ist. Nun möchten wir die Tafel vollständig in größere, quadratische Stücke einteilen, sodass keine Schokolade übrig bleibt.

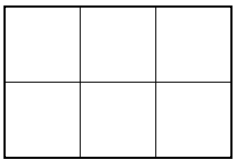
Ich nehme an, dass im Problem gemeint ist, das Rechteck zu zerlegen, indem man jede Seite in gleich große Teile unterteilt und das Rechteck dann entlang von Linien schneidet, die parallel zu den Seiten verlaufen. Es ist wahrscheinlich die einzige Möglichkeit, das gegebene Ergebnis zu erreichen, aber wir werden dies nicht beweisen.

Wenn man auf ein Problem stößt, bei dem eine allgemeine Aussage bewiesen werden – also eine Aussage, die viele mögliche Fälle umfasst –, ist es oft hilfreich, diese zunächst an einem konkreten Beispiel zu überprüfen.

Beispiel 1. Sei $m = 2, n = 1$. Dann müssen wir die längere Seite des Rechtecks schneiden, und die Antwort ist offensichtlich: $k = 1$.

2×1

Beispiel 2. Sei $m = 3, n = 2$. Wenn wir probieren das Rechteck in Quadraten der Größe $k = 2$ zu schneiden, bleibt der Rest des Rechtecks kein Quadrat. Und größere k is unmöglich, da k kann nicht größer als n sein. Also muss $k = 1$ gelten.



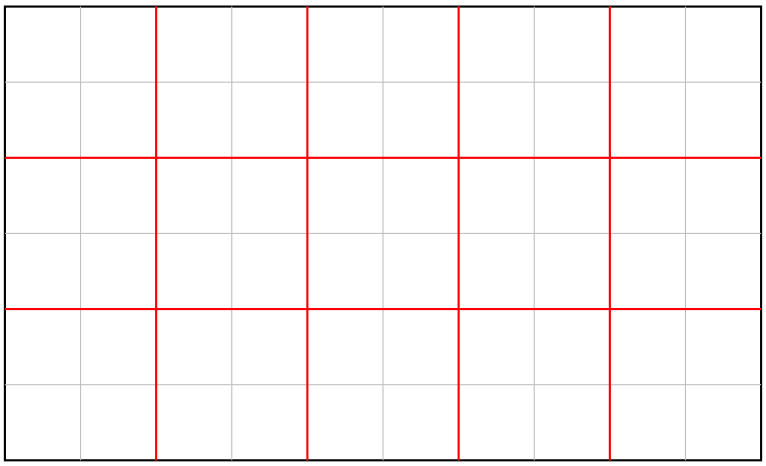
2×3

Vielleicht muss das Rechteck immer in 1×1-Quadrate zerteilt werden, aber das klingt nicht sehr realistisch. Um diese Hypothese zu widerlegen, brauchen wir nun ein Beispiel.

Beispiel 3. Sei $m = n$. In diesem Fall ist das Rechteck schon ein Quadrat, und wir müssen nichts weiter tun. Die Antwort ist also $k = m = n$.

Das hier ist nicht nur ein Beispiel, sondern eine ganze Reihe von Beispielen mit dem Parameter $m = n$. Es kann sehr nützlich sein, das Problem in solche Reihen zu unterteilen und für jede Reihe einen eigenen Beweis zu liefern.

Beispiel 4. Sei $m = 10, n = 6$. Man betrachtet nun $k = 1, 2, \ldots, 6$ und stellt fest, dass nur $k = 1$ und $k = 2$ funktionieren. Also ist die Antwort $k = 2$.



6×10: wir können das Rechteck in rote 2×2 Quadraten zerschneiden

Beispiel 4 ist wahrscheinlich das einzige nicht ganz triviale Beispiel bisher. Deshalb sollten wir genau hinschauen und verstehen, was dabei passiert – das könnte der Schlüssel zur Lösung des Problems sein.

Vielleicht merkt man schon: Damit man das Rechteck in $k \times k$-Quadraten aufteilen kann, muss jede Seite des Rechtecks ein Vielfaches von k sein. Warum? Ganz einfach – wenn man das Rechteck in Quadrate zerschneidet, muss jede Seite genau von den Seiten der Quadrate aufgefüllt werden. Also, muss sowie m als auch n durch k teilbar sein.

Satz 1.0.1. *Seien m, n natürliche Zahlen. Es gibt dann eine maximale natürliche Zahl k, durch die sowohl m als auch n teilbar sind. Diese Zahl nennt man den größten gemeinsamen Teiler von m und n, und sie ist die Lösung von Problem 1.*

Beweis. Wir brauchen zu zeigen die folgende Aussagen:

(1) Die Zahl k existiert.
(2) Man kann das Rechteck in $k \times k$-Quadraten zerteilen.
(3) Wenn man kann das Rechteck in $k' \times k'$-Quadraten zerteilen, dann ist $k' \leq k$.

(1) Wir betrachten die Menge M von natürlichen Zahlen, durch die sowohl m als auch n teilbar sind. Diese Menge ist endlich, da jede Zahl in M höchstens so groß wie m und n sein kann. Außerdem ist M nicht leer, denn $1 \in X$. Daraus folgt, dass M eine maximale Zahl k enthält.

(2) Sei k der größte gemeinsame Teiler von n und m, also, $n = s \cdot k$, $m = l \cdot k$. Zuerst schneiden wir das Rechteck entlang der Seite mit Länge m in l gleich große Teile – also senkrecht zur Seite mit Länge n. Dabei entstehen Streifen der Größe $k \times n$. Diese Streifen schneiden wir nun entlang der Seite mit Länge n in s gleiche Teile, also waagerecht. Am Ende erhalten wir Rechtecke der Größe $k \times k$, also genau die gewünschten Quadrate.

(3) Angenommen, dass das Rechteck wurde in Quadrate der Größe $k' \times k'$ zerteilt, so müssen beide Seitenlängen des Rechtecks in gleich lange Abschnitte der Länge k' unterteilt worden sein. Daraus folgt, dass sowohl n als auch m durch k' teilbar sind. Mit anderen Worten: k' gehört zur Menge X aus Punkt 1. Daher ist k' nicht größer als k. □

Vorlesung 2

2.1. Teilbarkeit von Zahlendifferenzen.

> **Problem 2.** Sei $X \subset \{1, 2, 3, \dots, 10\}$ eine Menge aus 6 verschiedenen Zahlen.
> Zeigen Sie, dass es in X mindestens zwei Zahlen gibt, deren Differenz durch 5 teilbar ist.

Wie in der ersten Vorlesung versuchen wir zunächst, den Schlüssel zu diesem Problem anhand von Beispielen zu finden.

Beispiel 1. Sei $X = \{1, 2, 3, 4, 5, 6\}$. In diesem Fall stimmt die Behauptung: $6 - 1 = 5$, und diese Diefferenz ist durch 5 teilbar.

Was passiert, wenn wir eine Zahl in dieser Menge – zum Beispiel die 6 – durch eine andere ersetzen?

Beispiel ?. Sei $X = \{1, 2, 3, 4, 5, ?\}$, wobei ? ist $6, 7, 8, 9$ oder 10.

Genau genommen handelt es sich hierbei nicht um ein einzelnes Beispiel, sondern um eine ganze Reihe von Beispielen mit einem freien Parameter, den wir mit dem Symbol ? bezeichnet haben.

Dieses Symbol könnte auch durch ein anderes wie x oder n ersetzt werden – je nachdem, was gerade besser passt. Es gibt keine feste Regel für die Wahl der Notation; theoretisch könnten wir auch ζ oder sogar $\square$ verwenden.

In manchen Problemen lässt sich eine Lösung finden, indem man alle möglichen Fälle systematisch in eine Reihe von Beispielen einteilt und für jede dieser Reihen einen eigenen Beweis führt.
Hier könnten wir zum Beispiel zehn Fälle untersuchen: Für jedes n zwischen 1 und 10 betrachten wir nur die Mengen X, die n enthalten. Da X mindestens eine dieser Zahlen enthalten muss, haben wir damit alle Möglichkeiten erfasst.
Allerdings sind Beweise, die auf einer Vielzahl einzelner Fälle beruhen, oft schwerer zu verstehen – und möglicherweise wollen wir solche Beweisführungen lieber vermeiden.

In der Beispielreihe für ? stimmt die Behauptung, da die Zahl $? - 5$ zwischen 1 und 5 liegt. Bezeichnen wir diese Zahl mit x, also $x :=? - 5$, so gilt $x \in \{1, 2, 3, 4, 5\}$.

Mit dem Symbol $:=$ zeigt man an, dass man etwas definiert. Wenn man schreibt $x := y$, dann heißt das: Wir führen x ein und setzen es gleich y. Zum Beispiel: $a := 2 + 2$ bedeutet, dass a einfach 4 ist.

Man könnte dieses Problem auch durch vollständige Fallunterscheidung lösen: Es gibt lediglich 210 mögliche Mengen X, und für jede davon könnte man alle Zahlenpaare betrachten, deren Differenz durch 5 teilbar ist. Das würde das Problem formal lösen – aber würde man dadurch wirklich etwas verstehen?.. Wir müssen also einen anderen Ansatz wählen – wir brauchen eine neue Idee.

Idee. Wir konstruieren aus X eine neue, einfachere Menge, mit der sich die Frage, ob X zwei Zahlen enthält, deren Differenz durch 5 teilbar ist, leichter beantworten lässt.

Zum Beispiel, sei $Diff(X)$ die Menge aller Differenzen zwischen von Zahlen aus X. Wir können dies kurz mathematisch so schreiben:

$$Diff(X) := \{ \underbrace{a - b}_{\text{Bezeichnung/Gestalt eines Elements}} \mid \underbrace{a, b \in X}_{\text{Eigenschaft, welche ein solches Element haben soll}} \}$$

Um die Behauptung zu zeigen, genügt es nachzuweisen, dass $Diff(X)$ eine Zahl enthält, die durch 5 teilbar ist. Dazu brauchen wir aber nicht die vollständige Information über $Diff(X)$: es reicht, sich anzuschauen, welche Reste die Zahlen in $Diff(X)$ bei Division durch 5 haben. Um das zu berechnen, reicht es, nur die Reste die Zahlen in X bei Division durch 5 anzuschauen, denn daraus lassen sich auch die Reste der Differenzen ableiten.

Ich führe die folgende Notation ein: Wenn n und m natürlichen Zahlen sind, dann schreibe ich $n \mod m$ für den Rest der Division von n durch m. Das bedeutet, $n \mod m$ ist eine Zahl zwischen 0 und $m-1$, und es gilt $n = k \cdot m + (n \mod m)$ für eine natürliche Zahl k. Zum Beispiel, $11 \mod 3 = 2$.

Sei Y die Menge von Resten bei der Division durch 5 von Zahlen in X:

$$Y := \{ \underbrace{x \mod 5}_{\text{Bezeichnung/Gestalt eines Elements}} \mid \underbrace{x \in X}_{\text{Eigenschaft, welche ein solches Element haben soll}} \}$$

Beispiel 1. In diesem Beispiel $X = \{1, 2, 3, 4, 5, 6\}$ und wir können Y berechnen:

$$\begin{aligned} 1 &\mod 5 = 1 \\ 2 &\mod 5 = 2 \\ 3 &\mod 5 = 3 \\ 4 &\mod 5 = 4 \\ 5 &\mod 5 = 0 \\ 6 &\mod 5 = 1 \end{aligned}$$

Also $Y = \{0, 1, 2, 3, 4\}$. (In der Mathematik gilt: Eine Menge enthält entweder ein Element oder nicht – die Häufigkeit wird nicht gezählt. Zum Beispiel enthält Y die Zahl 1 aus zwei verschiedenen Gründen (als Rest von 1 und von 6), aber die Mengen $\{0, 1, 2, 3, 4\}$ und $\{0, 1, 2, 3, 4\}$ sind **gleich**.)

Beachten Sie hier, dass ich nicht mehr := schreibe, sondern =, weil es keine Definition von Y ist, sondern die Berechnung von Y.

Das Symbol := wurde aber nicht überall in der Mathematik verwendet, manchmal macht man keinen Unterschied zwischen Berechnungen und Definitionen.

Man erkennt hier, dass 6 und 1 denselben Rest bei der Division durch 5 haben. Genau diese beiden Zahlen, 6 und 1, sind diejenigen, deren Differenz durch 5 teilbar ist. Aus diesem Beispiel lässt sich die folgende Vermutung ableiten, die ich nun beweisen werde. Daher bezeichne ich sie als Satz.

Satz 2.1.1. *Wenn natürliche Zahlen a, b gleiche Reste bei der Division durch 5 haben, dann ist $a - b$ durch 5 teilbar.*

Beweis. Wir wissen, dass $a = 5 \cdot k + r$, wobei $k \in \mathbb{N}_0$, $0 \leq r < 5$, und $b = 5 \cdot m + r$, wobei $m \in \mathbb{N}_0$ und r ist dieselbe Zahl wie für a.

Dann $a - b = 5 \cdot k + r - (5 \cdot m + r) = 5 \cdot (k - m)$. Es folgt daraus, dass $k - m$ ist auch eine ganze Zahl, dass $a - b$ durch 5 teilbar ist. □

Jetzt können wir das ursprungliche Probem mithilfe dieses Satzes umformulieren. Wir brauchen zu zeigen, dass mindestens zwei Elemente in der Menge X denselben Rest bei Division durch 5 haben. Und jetzt können wir den Grund für die Behauptung sehen: es gibt nur 5 verschiededn Resten bei Division durch 5, und wenn wir 6 Zahlen betrachten werden wir ein von Resten zweimal bekommen, wegen des "Schubfachprinzips".

Satz 2.1.2. *Gegeben seien* 6 *natürlichen Zahlen (nicht unbedingt verschieden und nicht notwendigerweise zwischen* 1 *und* 10*. Dann existieren zwei Zahlen unter diesen* 6*, die denselben Rest bei Division durch* 5 *haben.*

Beweis. Es gibt nur 5 mögliche Reste bei der Division durch 5: $0, 1, 2, 3, 4$. Die 6 gegebenen Zahlen liefern jeweils einen Rest, also entstehen 6 Reste. Da es aber nur 5 verschiedene mögliche Reste gibt, muss nach dem Schubfachprinzip mindestens ein Rest doppelt auftreten. Nach dem oben bewiesenen Satz folgt daraus, dass die Differenz zweier solcher Zahlen durch 5 teilbar ist. □

Wir haben damit nicht nur Problem 2 gelöst, sondern auch verstanden, was dabei passiert, und die Aussage des Problems verallgemeinert. Gerade diese Verallgemeinerung zeigt, dass wir das Problem auf eine mathematische Weise betrachtet haben.

2.2. **Vollständige Induktion.**

Hat man eine (möglicherweise unendliche) Liste von Aussagen

Aussage 1
Aussage 2
Aussage 3
⋮

die sich nur dadurch unterscheiden, dass an bestimmten Stellen der Aussagen eine *natürliche Zahl* vorkommt, die von Aussage zu Aussage jeweils um 1 größer wird, ist die *vollständige Induktion* eine mögliche Methode, alle diese Aussagen auf einen Schlag zu beweisen.

Ein Induktionsbeweis besteht aus einer *Induktionsverankerung* und dem *Induktionsschritt*. In der Induktionsverankerung wird die erste Aussage (von den unendlich vielen) bewiesen.

Induktionsverankerung.
Aussage 1 *ist wahr.*

Im Induktionsschritt beweist man Folgendes:

Induktionsschritt.
Falls Aussage n *wahr ist,*
dann ist auch Aussage $n+1$ *wahr.*

Hier ist zu beachten, dass der Induktionsschritt für *jede* natürliche Zahl n funktionieren soll, unabhängig davon, welche Zahl n ist. *Außerdem behauptet der Induktionsschritt nicht, dass Aussage* n *wahr sei* und auch nicht, dass Aussage $n+1$ bedingungslos wahr sei – sondern nur, dass, *falls* Aussage n wahr ist, auch Aussage $n+1$ wahr ist.

Erst wenn die Induktionsverankerung und der Induktionsschritt kombiniert werden, haben wir einen Beweis dafür, dass alle Aussagen in der Liste wahr sind. Die Idee dabei ist Folgende: Wollen wir beispielsweise wissen, ob Aussage 512 wahr ist, betrachten wir zuerst die Induktionsverankerung, welche den Beweis von Aussage 1 enthält. Wir wissen nun, dass Aussage 1 wahr ist. Der Induktionsschritt für $n = 1$ beweist nun, dass Aussage 2 wahr ist (denn die Prämisse, dass Aussage 1 wahr sei, ist ja bereits eine überprüfte Tatsache und keine bloße Annahme mehr). Der Induktionsschritt für $n = 2$ beweist jetzt, dass Aussage 3 wahr ist. So wenden wir den Induktionsschritt immer wieder an, bis wir (nach 511 sukzessiven Anwendungen des Induktionsschritts) zur 512. Aussage gelangen.

Das Prinzip der vollständigen Induktion ist sozusagen ein "meta"-Beweis: Ein Induktionsbeweis zeigt letztlich, dass man für jede einzelne der unendlich vielen Aussagen in endlicher Zeit einen tatsächlichen Beweis angeben könnte.

Problem 3. Beweisen Sie, dass für jede natürliche Zahl n die Zahl $5^n - 1$ durch 4 teilbar ist.

Wir verwenden vollständige Induktion:

Induktionsverankerung. Die Aussage 1 ist: $5^1 - 1$ ist durch 4 teilbar. Diese Aussage ist offensichtlich wahr.

Induktionsschritt. Wenn die Aussage n wahr ist, so gilt: $5^n - 1$ ist durch 4 teilbar ist, das heißt, es existiert eine natürliche Zahl k, sodass $5^n - 1 = 4k$.
Nun möchten wir zeigen, dass daraus folgt, dass auch die Aussage $n + 1$ wahr ist. Die Zahl $5^{n+1} - 1$ können wir so umschreiben:

$$5 \cdot 5^n - 1 = 5 \cdot (4k + 1) - 1 = 20k + 5 - 1 = 20k + 4 = 4(5k + 1).$$

Das zeigt, dass auch $5^{n+1} - 1$ durch 4 teilbar ist, vorausgesetzt, dass $5^n - 1$ durch 4 teilbar war.

Mit diesen Schritten haben wir die Grundlage für den vollständigen Induktionsbeweis gelegt und können nun abschließend sagen, dass die Behauptung des Problems 3 durch vollständige Induktion bewiesen ist.

2.3. **Mengen.**

Praktisch die gesamte moderne Mathematik ist in der "Sprache" der Mengen formuliert. Die Menge selbst ist jedoch ein grundlegendes Konzept, das keiner Definition im engeren Sinne bedarf – denn man kann nichts aus dem Nichts definieren. Stattdessen muss man grundlegende mathematische Objekte indirekt durch ein Axiomsystem definieren. Die Axiome sagen uns nicht, was genau diese Objekte sind, sondern wie man mit diesen Objekten umgehen kann. Wir werden die Axiome der Mengenlehre in dieser Vorlesung jedoch nicht behandeln, da sich die intuitive Vorstellung einer Menge für unsere Zwecke gut verwenden lässt.

Eine *Menge* ist eine Zusammenfassung oder Sammlung von wohlunterschiedenen Objekten, die man als *Elemente* der Menge bezeichnet.

Mengen werden mit geschweiften Klammern $\{\}$ notiert und oft mit Großbuchstaben bezeichnet. Dabei gibt es zwei Möglichkeiten:

(1) Die Elemente werden als Liste beschrieben; zum Beispiel $A = \{2, 3, 5\}$.

(2) Die Elemente werden durch ihre Eigenschaften festgelegt; zum Beispiel für die Menge A oben: $A = \{n \mid n < 6 \text{ und } n \text{ ist eine Primzahl}\}$.

Eine Menge ist selbst auch ein Objekt – wir können also auch Mengen als Objekte einer anderen Menge betrachten; zum Beispiel ist $\{\{2, 3, 5\}, \{7\}\}$ eine Menge mit zwei Elementen, die ihrerseits Mengen sind.

Die *leere Menge* $\emptyset$ oder $\{\}$ hat keine Elemente.

Zwei Mengen sind *gleich*, wenn sie dieselben Elemente haben. Um die Gleichheit zweier Mengen A und B zu beweisen, müssen wir also zeigen, dass jedes Element von A auch ein Element von B ist und dass jedes Element von B auch ein Element von A ist.

Zum Beispiel $\{2, 3, 5\} = \{2, 2, 3, 5, 3\} = \{3, 5, 2\} = \{n \mid n \text{ Primzahl}, \ n < 6\}$, aber $\{2, 3, 5\} \neq \{2, 3\}$.

2.3.1. *Einige wichtige Notationen.*

$a \in A$ bedeutet: a ist ein Element der Menge A.
z.B. $2 \in \{2, 3, 5\}$, $5 \in \{2, 3, 5\}$, $4 \notin \{2, 3, 5\}$

$A \subseteq B$ bedeutet: A ist eine *Teilmenge* der Menge B,
das heißt, jedes Element von A ist auch ein Element von B.
z.B. $\{2, 3\} \subseteq \{2, 3, 5\}$, $\{2, 5\} \subseteq \{2, 3, 5\}$,
$\{2, 3\} \not\subseteq \{4, 3\}$, $\{4, 3\} \not\subseteq \{2, 3\}$, $\{\} \subseteq \{2, 3\}$

$A \cup B$ ist die Menge, die aus allen Elementen von A und allen Elementen von B besteht (*Vereinigung* von A und B).
Mit anderen Worten: $A \cup B = \{x \mid x \in A \text{ oder } x \in B\}$.
z.B. $\{2, 3\} \cup \{3, 4\} = \{2, 3, 4\}$, $\{2, 3\} \cup \{\} = \{2, 3\}$,
$\{2, 3\} \cup \{2, 3, 4\} = \{2, 3, 4\}$.

$A \cap B$ ist die Menge, die aus allen Elementen besteht, die sowohl Elemente von A als auch Elemente von B sind (*Durchschnitt* von A und B).
Mit anderen Worten: $A \cap B = \{x \mid x \in A \text{ und } x \in B\}$.
z.B. $\{2, 3\} \cap \{3, 4\} = \{3\}$, $\{2, 3\} \cap \{4, 5\} = \{\}$,
$\{2, 3\} \cap \{2, 3, 5\} = \{2, 3\}$

$A \setminus B$ ist die Menge, die aus allen Elementen von A besteht, die nicht Elemente von B sind.
Mit anderen Worten: $A \setminus B = \{x \mid x \in A \text{ und } x \notin B\}$.
z.B. $\{2, 3\} \setminus \{3, 4\} = \{2\}$, $\{2, 3, 5\} \setminus \{5\} = \{2, 3\}$

$A \times B$ ist das (cartesische) *Produkt* der Mengen A und B.
Das ist die Menge, die aus allen Paaren der Form (a, b) besteht,
wobei $a \in A$ und $b \in B$, also $A \times B = \{(a, b) \mid a \in A \text{ und } b \in B\}$.
z.B. $\{2, 3\} \times \{3, 4\} = \{(2, 3), (2, 4), (3, 3), (3, 4)\}$
Falls $A = \{2, 3\}$ und $B = \{4, 5\}$, gilt $(3, 4) \in A \times B$.

A^n Falls A eine Menge und $n \geq 1$ eine natürliche Zahl sind,
bezeichnet A^n die Menge, deren Elemente von der Form
$(a_1, a_2, \ldots, a_n)$ sind, wobei $a_1 \in A, a_2 \in A, \ldots, a_n \in A$.
z.B. $(2, 2, 5) \in \mathbb{N}^3$, $(-1, 9, -1, 0) \in \mathbb{Z}^4$, $A^2 = A \times A$.

Vorlesung 3

3.1. Schubfachprinzip.

Satz 3.1.1 (Schubfachprunzip)**.** *Falls man n Objekte auf m Mengen (mit $m > 0$) verteilt und n größer als m ist, dann wird mindestens eine Menge mehrere Objekte enthalten.*

Beweis durch Widerspruch (Indirekter Beweis). Falls das Prinzip nicht stimmt, dann enthält jedes Schubfach höchstens ein Objekt. Damit gibt es höchstens so viele Objekte wie Schubfächer. Das steht aber im Widerspruch zur Voraussetzung, dass es mehr Objekte als Schubfächer gibt. □

Obwohl das Schubfachprinzip sehr einfach klingt, taucht es häufig in Problemen und Aufgaben auf, in denen endliche Mengen betrachtet werden. Ein Beispiel dafür haben wir bereits in der letzten Vorlesung gesehen – hier ist ein weiteres.

> **Aufgabe.** Auf dem Kopf eines Menschen wachsen höchstens 200.000 Haare. In München leben mehr als 1,5 Millionen Menschen. Zeigen Sie, dass es mindestens zwei Münchner gibt, die genau gleich viele Haare auf dem Kopf haben.

Wir stellen uns vor, dass wir alle Münchner nach der Anzahl ihrer Haare in "Schubfächer" einteilen. Da es nur 200001 Schubfächer gibt, aber mehr als 200001 Münchner, müssen zwangsläufig mindestens zwei Personen im selben Schubfach landen. Diese haben nach Definition der Schubfächer dieselbe Anzahl Haare auf dem Kopf.

3.2. Division mit Rest: Existenz und Eindeutigkeit.

Die Menge aller natürlichen Zahlen wird mit dem Symbol $\mathbb{N}$ bezeichnet. Oft ist es zweckmäßig, die Zahl 0 ebenfalls dazu zu zählen; das werden wir in dieser Vorlesung tun:

$$\mathbb{N} := \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, \ldots\}$$

Die Menge der ganzen Zahlen bezeichnet man mit dem Symbol $\mathbb{Z}$:

$$\mathbb{Z} := \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

und die Menge der rationalen Zahle wird mit dem Symbol $\mathbb{Q}$ bezeichnet:

$$\mathbb{Q} = \{\frac{p}{q} \mid p, q \in \mathbb{Z},\ q \neq 0\}.$$

Wenn wir die Notation der letzten Vorlesung verwenden, können wir auch schreiben:

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q}.$$

In der letzten Vorlesung haben wir bereits die Division mit Rest anhand von Beispielen verwendet. Nun möchte ich zeigen, dass der Rest bei einer Division wohldefiniert ist. Auch wenn man dies in der Schule oft ohne Beweis lernt, lässt es sich mathematisch problemlos und korrekt begründen.

Satz 3.2.1 (Division mit Rest)**.** *Seien a und b zwei ganzen Zahlen mit $b > 0$. Dann existieren eindeutig bestimmte ganze Zahlen q und r mit den Eigenschaften:*

$$a = qb + r \quad \textit{und} \quad 0 \leq r < b.$$

Wir nennen q den *Quotienten* und r den *Rest* der Division von a durch b. Bereits beim letzten Mal haben wir den Rest mit $a \mod b$ bezeichnet.

Die Notation $\mod$ unterscheidet sich in einem wichtigen Punkt von anderen Operationen und Symbolen in der Zahlentheorie. Wenn $a \mod b = r$ gilt und man die Zahlen b und r kennt, ist die Zahl a nicht eindeutig bestimmt. Zum Beispiel: $12 \mod 5 = 2$ und $2 \mod 5 = 2$. Im Gegensatz dazu ist etwa bei der Division von rationalen Zahlen $\frac{a}{b} = r$ die Zahl a eindeutig bestimmt, wenn b und r gegeben sind.

Beweis. Um den Satz zu beweisen, müssen wir zwei unterschiedliche Aussagen zeigen: Zum einen ist zu zeigen, dass es für gegebene Zahlen a und b tatsächlich passende Zahlen q und r gibt; zum anderen müssen wir begründen, warum diese Zahlen eindeutig bestimmt sind. Wir beginnen mit dem zweiten Teil.

(Beweis der Eindeutigkeit) Angenommen, es existieren zwei unterschiedliche Paare (q, r) und (q', r'), die die Gleichungen:

$$a = qb + r = q'b + r', \quad \text{und} \quad 0 \leq r, r' < b.$$

erfüllen. Dies führt zu der Gleichung $qb - q'b = r' - r$. Nun betrachten wir den Betrag beider Seiten:

$$b|q - q'| = |r' - r|. \tag{1}$$

Die Zahl $b|q - q'|$ ist entweder Null, wenn $q = q'$, oder größer als b. Da jedoch $|r' - r| < b$ gilt,muss $b|q - q'|$ sein, was $q = q'$ impliziert. Aber dann folgt es aus der Gleichung (1), dass $r' - r = 0$, also $r' = r$. Somit sind die Paare (q, r) und (q', r') gleich.

(Beweis der Existenz) Die Existenz der Zahlen q und r kann durch vollständige Induktion bewiesen werden. Es ist jedoch wichtig, vorsichtig zu sein, da der Satz für eine ganze Zahl a formuliert wurde und nicht für eine natürliche Zahl. Daher konzentrieren wir uns zunächst auf den Fall $a \geq 0$.

Aussage 1: Für jede $a : 0 \leq a < b$ existiert ein Zahlenpaar (q, r), das die gefordeten Eigenschaften erfüllt. Ich nehme als Aussage k für $k < b$ auch die Aussage 1.

Aussage n (für $n \geq b$): Für jede Zahl $a \leq n$ existiert die Paare (q, r) die benötigte Eigenschaften erfüllt.

(Induktionsverankerung) Wenn $a < b$ dann gilt $a = 0 \cdot b + a$, also $q = 0, r = a$ ist die Paare, die benötigte Eigenschaften erfüllt.

(Induktionsschritt) Falls Aussage n wahr ist, dann ist auch Aussage $n + 1$ wahr.

Für $n \leq b-2$ gibt es nichts zu beweisen, da die Aussage n und die Aussage $n+1$ identisch sind. Wir nehmen also an, dass $n \geq b-1$. Wir wollen zeigen, dass für alle $a \leq n+1$ ein Paar (q, r) existiert, das die geforderten Bedingungen erfüllt. Für alle $a \leq n$ gilt dies bereits aufgrund der Induktionsvoraussetzung. Betrachten wir nun den Fall $a = n + 1$. Dann ist auch $a - b \geq 0$, da $n \geq b - 1$. Zudem gilt $a - b \leq n$, sodass erlaubt uns die Induktionsvoraussetzung, ein Paar (q', r') zu finden mit $a-b = q' \cdot b+r'$. Daraus ergibt sich $a = (q' + 1) \cdot b + r'$, wobei $0 \leq r' < b$ weiterhin erfüllt ist. Also erfüllt das Paar $(q' + 1, r')$ die geforderten Bedingungen.

Damit ist der Beweis für den Fall $a \geq 0$ abgeschlossen. Nun betrachten wir den Fall $a < 0$. Sei $a' := -a$, also ist $a' > 0$. Nach dem bereits bewiesenen Fall für nichtnegative Zahlen existieren ganze Zahlen q, r, sodass $a' = q \cdot b + r$ mit $0 \leq r < b$.

Das bedeutet:

$$-a = q \cdot b + r \Rightarrow a = (-q) \cdot b - r.$$

Diese Darstellung lässt sich umformen zu

$$a = (-q - 1) \cdot b + (b - r).$$

Da $0 \leq r < b$, folgt $0 \leq b - r \leq b$, sodass das Paar $(-q - 1, b - r)$ die gefordeten Bedingungen erfüllt. □

Zwar diente die vollständige Induktion im Wesentlichen dem Existenzbeweis, dennoch zeigt der Aufbau des Beweises auch, wie man den Quotienten und den Rest in der Division tatsächlich berechnen kann. Wir starten mit der Zahl $a \geq 0$, die wir durch b teilen wollen. Der Induktionsschritt legt nahe, die Zahl $a - b$ zu betrachten und dann schrittweise weiterzugehen zu $a - 2b$, $a - 3b$ usw., bis man eine Zahl im Bereich zwischen 0 und $b - 1$ erreicht.

Beispiel. Teilen Sie $a = 77$ mit Rest durch $b = 20$. Da 77 größer ist als 20, abziehen wir b von a:

$$\begin{aligned} a - b &= 77 - 20 = 57, \\ a - 2b &= 57 - 20 = 37, \\ a - 3b &= 37 - 20 = 17. \end{aligned}$$

Da 17 größergleich 0 und kleiner als b ist, ist $r = 17$ der gesuchte Rest. Da wir dreimal b von a abgezogen haben, ist $q = 3$ der Quotient.

$$77 = 3 \cdot 20 + 17, \quad \text{und } 0 \leq 17 < 20.$$

3.3. **Euklidischer Algorithmus.**

Definition 3.3.1 (Teiler)**.** *Seien a, b zwei ganze Zahlen. Wir sagen, dass b ein* Teiler *von a ist, wenn eine ganze Zahl m mit der Eigenschaft $a = b \cdot m$ existiert.*

Synonyme Ausdrucksweisen sind: "*b teilt a*", "a ist durch b *teilbar*" und "a ist ein Vielfaches von b". Als Symbol verwendet man einen senkrechten Strich:

$$b|a \qquad \text{“}b \text{ teilt } a\text{”}$$

Natürlich ist es nicht verboten, 3 durch 17 zu dividieren; man erhält dabei die weithin bekannte rationale Zahl $\frac{3}{17} = 0.176\ldots$ Trotzdem ist 3 nicht durch 17 *teilbar*, denn es existiert keine ganze Zahl m mit der Eigenschaft $3 = 17 \cdot m$. Der Begriff der Teilbarkeit im Kontext der ganzen Zahlen ist also nicht zu verwechseln mit der Möglichkeit, in $\mathbb{Q}$ oder in $\mathbb{R}$ eine Division durchzuführen.

Definition 3.3.2. *Seien $a, b \in \mathbb{Z}$. Eine Zahl $c \in \mathbb{Z}$ mit den Eigenschaften $c|a$ und $c|b$ nennen wir einen* gemeinsamen Teiler *von a und b.*

Definition 3.3.3 (größter gemeinsamer Teiler – ggT)**.** *Seien a und b zwei ganze Zahlen, die nicht beide Null sind. Den* größten gemeinsamen Teiler *von a und b bezeichnen wir mit $ggT(a, b)$.*

Die Existenz vom größten gemeinsamen Teiler haben wir in der Vorlesung 1 schon bewiesen.

Definition 3.3.4 (Teilerfremd)**.** *$a, b \in \mathbb{Z}$ sind* teilerfremd*, wenn $ggT(a, b) = 1$.*

0 ist durch jede ganze Zahl teilbar. Es gibt also keinen größten gemeinsamen Teiler von 0 und 0. Jede andere ganze Zahl hat endlich viele Teiler.

Definition 3.3.5 (kleinstes gemeinsames Vielfaches – kgV)**.** *Seien a und b zwei ganze Zahlen, die nicht beide Null sind. Das* kleinste gemeinsame Vielfache *von a und b ist die kleinste natürliche Zahl $c \geq 1$ mit der Eigenschaft $a|c$ und $b|c$. Es wird mit $kgV(a, b)$ bezeichnet.*

Lemma 3.3.6. *Falls $c|a$ und $c|b$ gilt, dann auch $c|(au + bv)$, für alle $u, v \in \mathbb{Z}$.*

Beweis. Angenommen, c teilt sowohl a als auch b, also $c|a$ und $c|b$. Dann gibt es ganze Zahlen α und β, sodass $a = c\alpha$ und $b = c\beta$ gilt. Setzt man dies in die Linearkombination $au + bv$ ein, so ergibt sich:

$$au + bv = c(\alpha u + \beta v).$$

Da $\alpha u + \beta v$ eine ganze Zahl ist, folgt daraus, dass $c|(au + bv)$. □

Satz 3.3.7. *Seien a, b ganze Zahlen.*
Wenn $a = qb + r$, dann ist $ggT(a, b) = ggT(b, r)$.

Bemerken Sie, dass wir nehmen nicht an, dass r der Rest bei Division von a durch b ist. Zum Beispiel: $12 = 1 \cdot 5 + 7$.

Beweis. Sei c ein gemeinsamer Teiler von a und b. Nach dem Lemma gilt dann auch: $c|(a - q \cdot b) = r$. Daher ist jeder gemeinsame Teiler von a und b auch ein gemeinsamer Teiler von b und r.

Sei d ein gemeinsamer Teiler von b und r. Nach dem Lemma gilt dann auch: $d|(q \cdot b + r) = a$. Daher ist jeder gemeinsame Teiler von b und r auch ein gemeinsamer Teiler von a und b.

Damit ist gezeigt, dass die Zahlenpaare (a, b) und (b, r) dieselbe Menge gemeinsamer Teiler besitzen. Insbesondere folgt daraus, dass auch ihre größten gemeinsamen Teiler übereinstimmen. □

Dieser Satz erlaubt uns, eine effektive Methode zu entwickeln, die den gemeinsamen größten Teiler berechnet. Die Methode heißt **Euklidischer Algorithmus**. Wir folgen zuerst den Algorithmus anhand eines Beispiels.

Beispiel. Seien $a = 39$, $b = 21$.

$$\begin{aligned} 39 &= 1 \cdot 21 + 18 \quad \text{ggT}(39, 21) = \text{ggT}(21, 18) \\ 21 &= 1 \cdot 18 + 3 \quad \text{ggT}(21, 18) = \text{ggT}(18, 3) \\ 18 &= 6 \cdot 3 + 0 \quad \text{ggT}(18, 3) = 3. \end{aligned}$$

Wir haben somit berechnet: $\text{ggT}(39, 21) = 3$.

Beispiel. Seien $a = 1617$, $b = 915$.

$$\begin{aligned}
1617 &= 1 \cdot 915 + 702 && \text{ggT}(1617, 915) = \text{ggT}(915, 702)\\
915 &= 1 \cdot 702 + 213 && \text{ggT}(915, 702) = \text{ggT}(702, 213)\\
702 &= 3 \cdot 213 + 63 && \text{ggT}(702, 213) = \text{ggT}(213, 63)\\
213 &= 3 \cdot 63 + 24 && \text{ggT}(213, 63) = \text{ggT}(63, 24)\\
63 &= 2 \cdot 24 + 15 && \text{ggT}(63, 24) = \text{ggT}(24, 15)\\
24 &= 1 \cdot 15 + 9 && \text{ggT}(24, 15) = \text{ggT}(15, 9)\\
15 &= 1 \cdot 9 + 6 && \text{ggT}(15, 9) = \text{ggT}(9, 6)\\
9 &= 1 \cdot 6 + 3 && \text{ggT}(9, 6) = \text{ggT}(6, 3)\\
6 &= 2 \cdot 3 + 0 && \text{ggT}(6, 3) = 3.
\end{aligned}$$

Wir haben somit berechnet: $\text{ggT}(1617, 915) = 3$.

Dieses Beispiel zeigt, dass der Euklidische Algorithmus in bestimmten Fällen nur sehr langsam zum Ergebnis führt.

Euklidischer Algorithmus

Seien $a, b \in \mathbb{Z}$, nicht beide Null. Falls $a = 0$, ist $\text{ggT}(a, b) = |b|$, und wenn $b = 0$, dann ist $\text{ggT}(a, b) = |a|$. Wir können uns also auf den Fall konzentrieren, wo weder a noch b Null ist. Ausserdem gilt

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

und falls $a = b$ ist $\text{ggT}(a, b) = |a| = |b|$. Es genügt also, den Fall $a > b > 0$ anzuschauen.
Nach dem Satz über die Division mit Rest können wir a schreiben als

$$a = q_1 b + r_1 \quad \text{und} \quad 0 \leq r_1 < b.$$

Wenn $r_1 = 0$, dann ist b ein Teiler von a und damit $\text{ggT}(a, b) = b$.
Falls $r_1 \neq 0$, teilen wir b mit Rest durch r_1:

$$b = q_2 r_1 + r_2 \quad \text{mit} \quad 0 \leq r_2 < r_1.$$

Aus Lemma folgt dann $\text{ggT}(a, b) = \text{ggT}(b, r_1)$, und wenn $r_2 = 0$, dann ist $\text{ggT}(a, b) = r_1$. Andernfalls:

$$r_1 = q_3 r_2 + r_3 \quad \text{mit} \quad 0 \leq r_3 < r_2,$$

und so weiter. Weil $b > r_1 > r_2 > \ldots \geq 0$, erhalten wir zwangsläufig einmal $r_n = 0$ (nämlich nach höchstens b solcher Schritte), und es gilt dann

$$\text{ggT}(a, b) = \text{ggT}(b, r_1) = \text{ggT}(r_1, r_2) = \ldots = \text{ggT}(r_{n-2}, r_{n-1}) = r_{n-1}.$$

Vorlesung 4

4.1. **Eine graphische Darstellung des Euklidischen Algorithmus.** Erinnern Sie sich, dass wir in der ersten Vorlesung das folgende Problem betrachtet haben.

> **Problem 1.** Wir betrachten eine Schokoladentafel, die in Quadrate unterteilt ist und eine Größe von $n \times m$ Quadraten hat.
> Bestimmen Sie die größtmögliche Seitenlänge $k \in \mathbb{N}$ sodass sich die Schokoladentafel vollständig in Quadrate der Größe $k \times k$ zerlegen lässt.

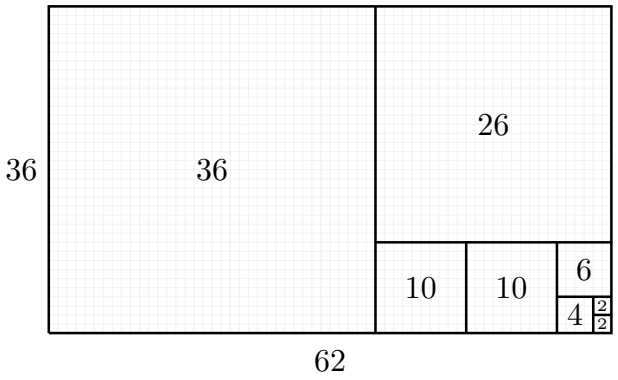
Ich habe dann erklärt, dass die Lösung dieses Problems dem größten gemeinsamen Teiler von n und m entspricht: $\mathrm{ggT}(n, m)$. Tatsächlich lässt sich in diesem Zusammenhang der euklidische Algorithmus auch grafisch anwenden.

Wir können ohne Einschränkung der Allgemeinheit annehmen, dass $n \geq m$ gilt (ansonsten drehen wir die Schokoladentafel einfach und vertauschen n und m). Um n durch m mit Rest zu teilen, versuchen wir, die Schokoladentafel mit Quadraten der Größe $m \times m$ auszufüllen. Dabei decken wir einen Teil der Seite der Länge n vollständig mit q solchen Quadraten ab, also eine Länge von $q \cdot m$. Der verbleibende Rest ist $r := n - q \cdot m$ — die ungedeckte Länge dieser Seite. Entfernt man die q $m \times m$-Quadrate, so bleibt eine Resttafel der Größe $m \times r$.

Dies stellt den ersten Schritt des euklidischen Algorithmus dar, nämlich die Gleichung $n = q \cdot m + r$.

Mit der Resttafel $m \times r$ führen wir denselben Vorgang fort. Nach einer endlichen Anzahl von Schritten (entsprechend der Anzahl der Divisionen im euklidischen Algorithmus) gelangen wir schließlich zu einer Tafel ohne Rest. Das bedeutet, im letzten Schritt wurde ein Quadrat der Größe $k \times k$ gefunden, mit dem sich die gesamte Ausgangstafel vollständig überdecken lässt. Dabei ist $k = \mathrm{ggT}(n, m)$.

Auf dem untenstehenden Bild ist eine solche grafische Darstellung des euklidischen Algorithmus für $n = 62$ und $m = 36$ zu sehen.



$$62 = 1 \cdot 36 + 26$$
$$36 = 1 \cdot 26 + 10$$
$$26 = 2 \cdot 10 + 6$$
$$10 = 1 \cdot 6 + 4$$
$$6 = 1 \cdot 4 + \boxed{2}$$
$$4 = 2 \cdot 2 + 0$$
$$\mathrm{ggT}(62, 36) = 2$$

4.2. **Lineare diophantische Gleichungen:** Ziel dieses Abschnitts ist es, eine allgemeine Methode zu entwickeln, mit der sich das folgende Problem lösen lässt.

> **Problem.**
> Gegeben seien ganze Zahlen a, b, c. Bestimmen Sie alle ganzzahligen Lösungen der Gleichung
> $$ax + by = c,$$
> d.h. alle Zahlenpaare (x, y) mit $x, y \in \mathbb{Z}$, die die Gleichung erfüllen.

Beispiel. Seien $a = 2, b = 3$ und $c = 1$. Es lässt sich leicht erkennen, dass $x = -1$ und $y = 1$ eine Lösung der Gleichung $2x + 3y = 1$ ist. Daraus folgt, dass für jedes beliebige c eine Lösung der Form $x = -c$ und $y = c$ existiert. Jedoch ist es nicht ganz so einfach, alle Lösungen für dieses Beispiel vollständig zu beschreiben.

Zuerst untersuchen wir, ob das Problem überhaupt eine Lösung hat. Eine notwendige Bedingung, die Sie bereits in der Übung gesehen haben, lautet: Wenn eine Lösung existiert, dann muss der größte gemeinsame Teiler $\mathrm{ggT}(a, b)$ die Zahl c teilen.

Satz 4.2.1 (Bézout)**.** *Seien $a, b \in \mathbb{Z}$ nicht beide Null. Dann existieren $u, v \in \mathbb{Z}$, die die folgende Gleichung erfüllen:*

$$a \cdot u + b \cdot v = ggT(a, b).$$

Da es um die Existenz einer Lösung geht, wäre es sinnvoll, bereits im Beweis eine Methode zur Bestimmung dieser Lösung zu erkennen. Glücklicherweise liefert uns der Euklidische Algorithmus genau eine solche Methode.

Beweis. Errinern Sie sich, dass wenn wir den Euklidischen Algorithmus anwenden, bekommen wir eine Liste von Gleichungen:

$$\begin{aligned} a &= q_1 \cdot b + r_1 \\ b &= q_2 \cdot r_1 + r_2 \\ r_1 &= q_3 \cdot r_2 + r_3 \\ &\dots \\ r_{n-2} &= q_n \cdot r_{n-1} + r_n \\ r_{n-1} &= q_{n+1} \cdot r_n + 0. \end{aligned}$$

Wir wissen also, dass $\mathrm{ggT}(a,b) = r_n$ gilt. Beachten Sie, dass sich r_n mithilfe der vorletzten Gleichung in der Form $r_n = r_{n-2} - q_n \cdot r_{n-1}$ schreiben lässt. Damit haben wir $\mathrm{ggT}(a,b) = r_n$ als ein Vielfaches von r_{n-2} plus ein Vielfaches von r_{n-1} ausgedrückt.

Man kann diese Umformungen der Zahlen schrittweise fortsetzen. Die vorherige Gleichung erlaubt es uns nämlich, auch r_{n-1} in der Form $r_{n-1} = r_{n-3} - q_{n-1} \cdot r_{n-2}$ auszudrücken. Setzen wir das in die Darstellung von r_n ein, erhalten wir:

$$\mathrm{ggT}(a,b) = r_n = r_{n-2} - q_n \cdot r_{n-1} = r_{n-2} - q_n(r_{n-3} - q_{n-1} \cdot r_{n-2}) = (1 - q_{n-1})r_{n-2} - q_n \cdot r_{n-3}.$$

Damit ist $\mathrm{ggT}(a,b)$ als als ein Vielfaches von r_{n-3} plus ein Vielfaches von r_{n-2} ausgedrückt. Wir setzen diesen Prozess Schritt für Schritt mit den vorhergehenden Gleichungen des Euklidischen Algorithmus fort, bis wir schließlich $\mathrm{ggT}(a,b)$ als Vielfaches von a plus ein Vielfaches von b dargestellt haben, also in der Form:

$$\mathrm{ggT}(a,b) = au + bv, \text{ mit } u, v \in \mathbb{Z}.$$

□

Beispiel. Seien $a = 7, b = 5$.
Der euklidische Algorithmus ergibt:

$$\begin{aligned} 7 &= 1 \cdot 5 + 2 \\ 5 &= 2 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0. \end{aligned}$$

Also ist $\mathrm{ggT}(7,5) = 1$. Nun formen wir die vorletzte Gleichung um:

$$1 = 5 - 2 \cdot 2.$$

Setzen wir nun $2 = 7 - 1 \cdot 5$ ein, so erhalten wir:

$$1 = 5 - 2 \cdot (7 - 5) = 5 + 2 \cdot 5 - 2 \cdot 7 = 3 \cdot 5 - 2 \cdot 7.$$

Damit haben wir 1 als eine Linearkombination von 7 und 5 dargestellt.

Fazit: Der Euklidische Algorithmus ermöglicht es uns, *eine* Lösung der Gleichung $ax+by = \mathrm{ggT}(a,b)$ zu finden. Bezeichnen wir eine solche Lösung mit $x = x_0, y = y_0$, so ist für jede Zahl c, die durch $\mathrm{ggT}(a,b)$ teilbar ist,

$$x = \frac{c}{\mathrm{ggT}(a,b)} x_0, \quad y = \frac{c}{\mathrm{ggT}(a,b)} y_0$$

eine ganzzahlige Lösung der Gleichung $ax + by = c$.

Aber wie können wir alle Lösungen finden, wenn wir schon eine gefunden haben? Der Schlüssel hier ist die Idee von Linearität, die einige von euch wahrscheinlich schon in Lineare Algebra 1 gesehen haben.

Seien $x = x_0$, $y = y_0$ eine Lösung der Gleichung $ax+by = c$, also gilt: $ax_0+by_0 = c$. Nun betrachten wir eine weitere Lösung (x, y) der Gleichung $ax + by = c$ und subtrahieren die Gleichung für (x_0, y_0) davon:

$$ax + by - ax_0 - by_0 = c - c$$

was sich umformen lässt zu:

$$a(x - x_0) + b(y - y_0) = 0. \tag{2}$$

Mit anderen Worten: Die Differenz $(x - x_0, y - y_0)$ muss eine Lösung der Gleichung (2) sein.

Eine Gleichung der Form $a\tilde{x} + b\tilde{y} = 0$ heißt *homogene lineare Gleichung*, Ein wichtiges Merkmal solcher Gleichungen ist: Wenn $(\tilde{x}, \tilde{y})$ eine Lösung ist, dann ist auch jedes Vielfache $(k\tilde{x}, k\tilde{y})$ mit $k \in \mathbb{Z}$ wieder eine Lösung. Das liegt an der Linearität der Gleichung.

Die Gleichung (2) ist also eine homogene Gleichung in den Variablen

$$\tilde{x} := x - x_0, \quad \tilde{y} := y - y_0.$$

Wenn wir alle ganzzahligen Lösungen $(\tilde{x}, \tilde{y})$ dieser homogenen Gleichung finden, erhalten wir daraus alle Lösungen der ursprünglichen Gleichung $ax + by = c$, indem wir $(x, y) = (x_0 + \tilde{x},\ y_0 + \tilde{y})$ setzen.

Um alle Lösungen der Gleichung (2) zu finden, müssen wir die Gleichung $a\tilde{x} = -b\tilde{y}$ lösen.

Auf den ersten Blick ist vielleicht nicht ersichtlich, wie man diese Gleichung vollständig beschreibt. Um das systematisch tun zu können, müssen wir uns zunächst mit Primzahlen und der Primfaktorzerlegung von ganzen Zahlen beschäftigen.

4.3. **Primzahlen.**

Definition 4.3.1. *Eine Primzahl ist eine natürliche Zahl, die genau zwei natürliche Zahlen als Teiler hat (nämlich* 1 *und die Zahl selbst). Eine natürliche Zahl ist zusammengesetzt, falls sie mehr als zwei natürliche Zahlen als Teiler hat.*

Die erste 10 Primzahlen sind:

$$2; 3; 5; 7; 11; 13; 17; 19; 23; 29.$$

Ich will nun einen besonderen Fall der Gleichung $a \cdot x = b \cdot y$ betrachten, nämlich $p \cdot x = q \cdot y$, wobei p, q verschiedene Primzahlen sind. Dann weißt man wahrscheinlich aus der Schule, dass p die Zahl y teilen muss und q die Zahl x teilen muss. Aber warum ist das so?

Lemma 4.3.2. *Sei p eine Primzahl und $a, b \in \mathbb{Z}$ mit $p \mid a \cdot b$.*
Dann gilt: Entweder $p \mid a$ oder $p \mid b$.

Beweis. Falls $p \mid a$, sind wir fertig. Andernfalls ist $\mathrm{ggT}(p, a) = 1$, da p als Primzahl nur die Teiler 1 und p besitzt.

Nach dem Satz von Bézout existieren dann $u, v \in \mathbb{Z}$ mit

$$1 = u \cdot p + v \cdot a.$$

Multiplizieren wir diese Gleichung mit b, ergibt sich:

$$b = u \cdot b \cdot p + v \cdot a \cdot b.$$

Da p sowohl $p \cdot b$ als auch $a \cdot b$ teilt, teilt p auch die gesamte rechte Seite – und damit b selbst. □

Dieses Lemma mag auf den ersten Blick naiv oder einfach erscheinen. Wir werden es jedoch verwenden, um den Fundamentalsatz der Arithmetik zu beweisen.

Proposition 4.3.3. *Seien p, q verschiedene Primzahlen.*
Dann sind alle ganzzahlige Lösungen der Gleichung

$$p \cdot x = q \cdot y$$

von der Form $x = u \cdot q, y = u \cdot p$ mit $u \in \mathbb{Z}$.

Beweis. Es ist leicht zu überprüfen, dass jedes Zahlenpaar der Form $x = u \cdot q$, $y = u \cdot p$ eine Lösung der Gleichung liefert:

$$p \cdot x = p \cdot u \cdot q = q \cdot u \cdot p = q \cdot y.$$

Sei nun (x, y) eine ganzzahlige Lösung der Gleichung. Dann gilt nach Voraussetzung: $p \mid q \cdot y$. Da p und q verschiedene Primzahlen sind, folgt aus dem vorherigen Lemma, dass $p \mid y$. Nach Definition $p \mid q \cdot y$, und weil $p \nmid q$ gilt, folgt aus dem Lemma, dass $p \mid y$. Es existiert also $u \in \mathbb{Z}$ mit $y = u \cdot p$. Setzen wir dies in die ursprüngliche Gleichung ein, erhalten wir:

$$p \cdot x = q \cdot u \cdot p.$$

Kürzen wir beide Seiten der Gleichung durch $p \neq 0$, ergibt sich:

$$x = u \cdot q.$$

Damit gilt $x = u \cdot q$ und $y = u \cdot p$, wie behauptet. □

4.4. **BONUS: Luhn-Algorithmus und Kreditkarten.** Division mit Rest mag zunächst künstlich oder wenig nützlich erscheinen. Tatsächlich begegnet sie uns aber in vielen Bereichen des Alltags – oft, ohne dass wir es merken. Heute möchte ich euch von einer solchen Anwendung berichten: der Prüfziffer auf Kreditkarten.

Hier ist ein Beispiel der Kreditkartenummer:

5412 7512 3412 3452

Diese Ziffern enthalten verschiedene Informationen: Zum einen, zu welchem Kreditkartenanbieter die Karte gehört – etwa Visa oder MasterCard –, zum anderen, welche Bank die Karte ausgegeben hat und mit welchem Konto sie verknüpft ist. Die 16 Stellen einer Kreditkartennummer reichen aus, um all das zu codieren. Dabei dient jedoch die letzte Ziffer nicht der Information, sondern der Kontrolle: Sie ist die sogenannte Prüfziffer und wird ausschließlich aus den ersten 15 Ziffern berechnet.

Hier ist der Algorithmus zur Berechnung der letzten Ziffer (der Prüfziffer): Man beginnt damit, jede zweite Ziffer, ausgehend von der ersten Stelle, zu verdoppeln. Ist das Ergebnis größer als 9, ersetzt man es durch die Summe seiner Ziffern. Beispiele: $5 \cdot 2 = 10 \mapsto 1 + 0 = 1$; $1 \cdot 2 = 2 \mapsto 2$.

Wir schreiben diese Prüfziffer einfach anstelle der ursprünglichen 16. Ziffer in die Kreditkartennummer. Mit dem Beispiel oben bekommen wir damit eine vollständige Nummer:

1422 5522 6422 6412

Beachten Sie, dass wir die letzte Ziffer nicht verändert haben (man könnte sie bei allen Berechnungen auch einfach weglassen). Nun berechnen wir den Rest der Quersumme der bearbeiteten ersten 15 Ziffern bei Division durch 10.

Also, $1 + 4 + 2 + 2 + 5 + 5 + 2 + 2 + 6 + 4 + 2 + 2 + 6 + 4 + 1 = 48$ und hat den Rest 8 modulo 10. Die letzte Ziffer ist also diejenige, die man zu der Summe der ersten 15 bearbeiteten Ziffern addieren muss, damit die Gesamtsumme durch 10 teilbar ist. Im Beispiel ergibt sich: Die Summe der ersten 15 Ziffern ist 8, also muss die letzte Ziffer 2 sein, denn nur dann gilt $8 + 2 = 10$.

Vorlesung 5

5.1. Fundamentalsatz der Arithmetik.

Definition 5.1.1. *Sei $a \in \mathbb{Z}$. Ein Primteiler (oder ein Primfaktor) von a ist eine Primzahl, die a teilt.*

Beispiel. Sei $a = 10$, dann 2 und 5 sind alle Primteiler von a.

Satz 5.1.2 (Fundamentalsatz der Arithmetik)**.** *Jede natürliche Zahl $n \geq 2$ besitzt eine eindeutige Primfaktorzerlegung der Form*

$$n = p_1 \cdot p_2 \cdots p_k$$

wobei $k \geq 1$ eine natürliche Zahl und $p_1 \leq p_2 \leq \ldots \leq p_k$ Primzahlen sind.

Beispiel. Die Zahl $n = 600$ hat die Primfaktorzerlegung

$$600 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5 = 2^3 \cdot 3 \cdot 5^2.$$

Hier sind $k = 6$, $p_1 = p_2 = p_3 = 2$, $p_4 = 3$ und $p_5 = p_6 = 5$.

Von nun an bezeichnen wir die eindeutige Primfaktorzerlegung einer natürlichen Zahl n in der Form des Fundamentalsatzes einfach als die *Primfaktorzerlegung* von n.

Die Bedingung, dass die Primfaktoren $p_1, p_2, \ldots, p_k$ der Größe nach geordnet sind, stellt die Eindeutigkeit sicher. Andernfalls wäre zum Beispiel

$$2 \cdot 5 \cdot 2 \cdot 2 \cdot 3 \cdot 5$$

eine andere Primfaktorzerlegung derselben Zahl 600, nämlich mit $p_1 = 2$, $p_2 = 5$, $p_3 = p_4 = 2$, $p_5 = 3$ und $p_6 = 5$.

Der Fundamentalsatz der Arithmetik beschreibt die Primzahlen als die grundlegenden Bausteine aller natürlichen Zahlen in Bezug auf die Multiplikation. Sobald wir Eigenschaften betrachten, die auf der Multiplikation beruhen, ist die Anwendung des Fundamentalsatzes nicht nur nützlich, sondern unverzichtbar.

Was passiert mit den Primfaktorzerlegungen, wenn wir zwei Zahlen multiplizieren? Seien $a, b \in \mathbb{N}$, $a, b \geq 2$ und seien $p_1 \cdots p_k = a$, $q_1 \cdots q_l = b$ die Primfaktorzerlegung von a bzw. b. Dann gilt natürlich

$$a \cdot b = p_1 \cdots p_k \cdot q_1 \cdots q_l,$$

aber um die Primfaktorzerlegung von $a \cdot b$ zu bekommen, müssen wir die Primzahlen $p_1, \ldots, p_k, q_1, \cdots, q_l$ der Größe nach sortieren.

Beispiel. Seien $a = 21$, $b = 10$. Dann lauten die Primfaktorzerlegungen:

$$a = 3 \cdot 7, \quad b = 2 \cdot 5.$$

Die Primfaktorzerlegung des Produkts $a \cdot b = 21 \cdot 10 = 210$ ist wie folgt:

$$a \cdot b = 210 = 2 \cdot 3 \cdot 5 \cdot 7,$$

wobei die Primfaktoren von b in roter Farbe hervorgehoben sind.

Corollary 5.1.3 (Folgerung aus dem Fundamentalsatz der Arithemtik)**.** *Sei $a \geq 2$ eine natürliche Zahl.*

Eine Primzahl p erscheint genau dann in der Primfaktorzerlegung von a, wenn $p \mid a$.

Da die Aussage dieser Folgerung die Form "A gilt **genau dann, wenn** B gilt" hat, gliedert sich der Beweis in zwei Teile: Ein Teil zeigt "Wenn A gilt, gilt auch B", und der zweite Teil zeigt "Wenn B gilt, gilt auch A". Wir schreiben dies kurz als $A \Rightarrow B$ und $B \Rightarrow A$.

Beweis. 1. Die Primzahl p erscheint in der Primfaktorzerlegung von $a \Rightarrow p \mid a$.

Betrachten wir die Primfaktorzerlegung von a:

$$a = p_1 \cdots p_k,$$

wobei alle p_i Primzahlen sind. Dann folgt direkt aus der Definition der Teilbarkeit, dass $p_i \mid a$ für jedes i. Insbesondere gilt also $p \mid a$, wenn p unter den p_i vorkommt.

2. Für die Primzahl p gilt: $p \mid a \Rightarrow$ die Primzahl p erscheint in der Primfaktorzerlegung von a.

Nach Definition der Teilbarkeit bedeutet $p \mid a$, dass eine Zahl $u \in \mathbb{N}$ mit $a = p \cdot u$ existiert. Da auch u eine natürliche Zahl ist, besitzt u eine Primfaktorzerlegung:

$$u = q_1 \cdots q_l.$$

Setzen wir dies in die Darstellung von a ein, ergibt sich:

$$a = p \cdot q_1 \cdots q_k.$$

Dies ist eine Darstellung von a als Produkt von Primzahlen. Durch Sortieren der Faktoren erhalten wir eine Primfaktorzerlegung in der im Fundamentalsatz geforderten Form, in der p enthalten ist. □

Proposition 5.1.4. *Die ganze Zahlen a, b sind teilerfremd, genau dann, wenn in der Primfaktorzerlegung von a und b keine gemeinsame Primzahl erscheint.*

Beweis. 1. Die ganzen Zahlen a, b sind teilerfremd $\Rightarrow$ in der Primfaktorzerlegung von a und b erscheing keine gemeinsame Primzahl.

Wir führen den Beweis durch Widerspruch. Angenommen, in den Primfaktorzerlegungen von a und b tritt eine gemeinsame Primzahl p auf. Dann gilt nach Definition: $p \mid a$ und $p \mid b$. Also ist p ein gemeinsamer Teiler von a und b. Das bedeutet, dass $\mathrm{ggT}(a, b) \geq p \geq 2$, was im Widerspruch zur Annahme steht, dass $\mathrm{ggT}(a, b) = 1$.

2. In der Primfaktorzerlegung von a und b ercheint keine gemeinsame Primzahl $\Rightarrow a, b$ sind teilerfremd.

Sei $c := \mathrm{ggT}(a, b)$ der größte gemeinsame Teiler von a und b. Angenommen, $c \neq 1$. Dann besitzt c nach dem Fundamentalsatz der Arithmetik eine Primfaktorzerlegung. Sei p eine Primzahl in dieser Zerlegung. Dann gilt:

$$p \mid c, \quad c \mid a, \quad c \mid b \;\Rightarrow\; p \mid a \text{ und } p \mid b.$$

Nach dem vorigen Korollar muss p also in der Primfaktorzerlegung sowohl von a als auch von b erscheinen – ein Widerspruch zur Annahme. Also muss $c = 1$ sein, d.h. a und b sind teilerfremd. □

Corollary 5.1.5. *Seien $a, b \in \mathbb{Z}$ teilerfremde Zahlen.*
Wenn $a \mid (b \cdot y)$ für ein $y \in \mathbb{Z}$, gilt dann $a \mid y$.

Beweis. Die Annahme $a \mid (b \cdot y)$ bedeutet, dass es ein $x \in \mathbb{Z}$ gibt mit $a \cdot x = b \cdot y$.

Sei $p_1 p_2 \cdots p_k = a$ die Primfaktorzerlefung von a. Da a und b teilerfremd sind, folgt aus dem vorigen Satz, dass keine dieser Primzahlen in der Zerlegung von b erscheint. Somit müssen alle Primfaktoren von a in der Primfaktorzerlegung von y erscheinen, weil die Primfaktorzerlegung von $b \cdot y$ eindeutig ist und kann durch das Produkt von Primfaktorzerlegungen von a und x berechnet werden. Also folgt: $a \mid y$. □

Beweis des Fundamentalsatzes der Arithmetik. Der Fundamentalsatz der Arithmetik besagt, dass jede natürliche Zahl $n \geq 2$ eine eindeutige Primfaktorzerlegung besitzt. Dazu beweisen wir zwei Teile:

(i) **Existenz:** Jede natürliche Zahl $n \geq 2$ lässt sich als Produkt von Primzahlen schreiben.
(ii) **Eindeutigkeit:** Diese Zerlegung ist eindeutig, wenn die Primfaktoren der Größe nach geordnet sind.

(i) Existenz: Wir zeigen dies durch vollständige Induktion über $n \geq 2$.

Für jede $n \in \mathbb{N}$ nehme ich als die Aussage n: alle Zahlen $m : 2 \leq m \leq n + 1$ besitzen eine Primfaktorzerlegung. Zum Beispiel, besagt die Aussage 1: 2 besitzt eine Primfaktorzerlegung.

Induktionsverankerung (oder auch Induktionsanfang): Da 2 eine Primzahl ist, ist $2 = 2$ eine gültige Primfaktorzerlegung mit $k = 1$, $p_1 = 2$.

Induktionsschritt: Angenommen, alle Zahlen m mit $2 \leq m \leq n$ besitzen eine Primfaktorzerlegung. Wir möchten zeigen, dass die Zahl $n + 1$ auch eine Primfaktorzerlegung besitzt.

Für $n + 1$ unterscheiden wir zwei Fälle:

- Ist $n + 1$ eine Primzahl, so ist $n + 1$ bereits seine eigene Primfaktorzerlegung.
- Ist $n + 1$ keine Primzahl, so existieren $u, v \in \mathbb{N}$ mit $1 < u, v < n + 1$ und $n + 1 = u \cdot v$. Nach Induktionsannahme besitzen u und v Primfaktorzerlegungen. Dann erhält man eine Primfaktorzerlegung von $n + 1$ durch Multiplikation der Primfaktorzerlegungen von u und v und die Sortierung von Primfaktoren.

Damit ist die Existenz für alle $n \geq 2$ bewiesen.

(ii) Eindeutigkeit: Wir führen den Beweis durch Widerspruch.

Angenommen, es existiert eine natürliche Zahl $n \geq 2$ mit zwei verschiedenen Primfaktorzerlegungen. Sei n die kleinste solche Zahl. Dann existieren zwei Darstellungen:

$$n = p_1 \cdots p_k = q_1 \cdots q_l,$$

wobei p_i, q_j Primzahlen sind mit $p_1 \leq p_2 \leq \cdot \leq p_k$, $q_1 \leq q_2 \leq \cdots \leq q_l$.

Da $p_1 \mid n$, muss p_1 auch ein Teiler des Produkts $q_1 \cdots q_l$ sein. Nach einem Lemma der letzten Vorlesung (vergleiche: „eine Primzahl, die ein Produkt teilt, teilt einen der Faktoren“), gilt: $p_1 \mid q_i$ für ein i. Da q_i Primzahl ist, folgt $p_1 = q_i$. (Warum?).

Obwohl der letzte Satz trivial klingen kann, ist es eine gute Stelle, sich zu erinnern, was eine Primzahl ist und wie wir diesen Satz begründen können.

Wir können beide Seiten der Gleichung durch $p_1 = q_i$ kürzen:

$$p_2 \cdots p_k = q_1 \cdots q_{i-1} \cdot q_{i+1} \cdots q_l.$$

Damit haben wir zwei verschiedene Primfaktorzerlegungen einer kleineren Zahl als n – im Widerspruch zur Minimalität von n. (Bemerken Sie, dass wenn diese zwei Primfaktorzerlegungen gleich sind, sind auch die zwei Primfaktorzerlegungen von n gleich, da sie von diesen durch Multiplikation mit p_1 erhalten werden können.

□

Der Schlüssel zum Beweis des Fundamentalsatzes war das Lemma, das wir beim letzten Mal bewiesen haben. Ich möchte die Leser an dieser Stelle daran erinnern, dass wir für den Beweis dieses Lemmas den Euklidischen Algorithmus verwendet haben. Der Algorithmus spielt also nicht nur eine praktische Rolle bei der Berechnung des größten gemeinsamen Teilers und bei der Lösung diophantischer Gleichungen, sondern auch eine zentrale Rolle in der theoretischen Entwicklung der Zahlentheorie.

5.2. **Alle ganzzahlige Lösungen der Gleichung $ax = -by$.**

Proposition 5.2.1. *Seien $a, b \in \mathbb{Z}$, $a \neq 0$, $b \neq 0$. Schreibe $a = c \cdot a'$ und $b = c \cdot b'$.*
Dann sind alle ganzzahlige Lösungen der Gleichung

$$a \cdot x = -b \cdot y$$

von der Form $x = b' \cdot u, y = -a' \cdot u$, wobei $u \in \mathbb{Z}$.

Beweis. Es ist leicht zu überprüfen, dass die gegebenen Ausdrücke $x = b' \cdot u$, $y = -a' \cdot u$ tatsächlich Lösungen der Gleichung sind.

Seien nun $x, y \in \mathbb{Z}$ beliebige Lösungen der Gleichung $a \cdot x = -b \cdot y$. Da $c = \mathrm{ggT}(a, b)$, können wir beide Seiten durch c teilen und erhalten:

$$a' \cdot x = -b' \cdot y,$$

wobei die Zahlen a' und b' teilerfremd sind (Warum?).

Da a' und b' teilerfremd sind und b' den Ausdruck $a' \cdot x$ teilt, folgt aus der zuvor bewiesenen Folgerung, dass $b' \mid x$, also $x = b' \cdot u$ für ein $u \in \mathbb{Z}$.

Setzt man dies in die Gleichung ein, so ergibt sich:

$$a' \cdot b' \cdot u = -b' \cdot y.$$

Durch Kürzen mit b' (da $b' \neq 0$) erhalten wir:

$$a' \cdot u = -y \quad \Rightarrow \quad y = -a' \cdot u.$$

Damit sind alle ganzzahligen Lösungen beschrieben.

□

Letztendlich können wir das Problem aus der letzten Vorlesung vollständig lösen. Es war damals wie folgt formuliert:

> **Problem.**
> Gegeben seien ganze Zahlen a, b, c. Bestimmen Sie alle ganzzahligen Lösungen der Gleichung
> $$ax + by = c,$$
> d.h. alle Zahlenpaare (x, y) mit $x, y \in \mathbb{Z}$, die die Gleichung erfüllen.

Wenn $\mathrm{ggT}(a, b) \nmid c$, so besitzt die Gleichung keine Lösung. Andernfalls schreiben wir:

$$a = a' \cdot \mathrm{ggT}(a, b), \quad b = b' \cdot \mathrm{ggT}(a, b), \quad c = c' \cdot \mathrm{ggT}(a, b).$$

Dann können wir die Gleichung durch $\mathrm{ggT}(a, b)$ teilen und erhalten:

$$a'x + b'y = c',$$

wobei nun $\mathrm{ggT}(a', b') = 1$ gilt.

Wir finden zunächst **eine** Lösung der Gleichung

$$a'x + b'y = 1$$

mit Hilfe des (rückwärts angewendeten) Euklidischen Algorithmus. Sei (x_0, y_0) eine solche Lösung, also gilt $a'x_0 + b'y_0 = 1$. Dann ist $(x, y) = (c'x_0, c'y_0)$ eine Lösung der Gleichung $a'x + b'y = c'$, und somit auch eine Lösung des ursprünglichen Problems.

Sei nun (x, y) eine beliebige Lösung. Dann erfüllt das Zahlenpaar $(x - c'x_0,\ y - c'y_0)$ die Gleichung

$$a'(x - x_0) = -b'(y - y_0).$$

Nach dem obigen Satz folgt daraus, dass es ein $u \in \mathbb{Z}$ gibt mit

$$x = x_0 + b' \cdot u, \quad y = y_0 - a' \cdot u.$$

Damit sind alle ganzzahligen Lösungen des Problems beschrieben.

Beispiel. Angenommen, ein Automat akzeptiert nur Münzen im Wert von 5 und 7 Einheiten. Kann man an diesem Automaten genau 101 Einheiten einzahlen? Wenn ja, wie viele Münzen jeder Sorte benötigt man?

Bezeichnen wir die Anzahl der Münzen im Wert von 5 bzw. 7 Einheiten mit x bzw. y, so ergibt sich die folgende lineare Gleichung:

$$5x + 7y = 101.$$

Da 5 und 7 teilerfremd sind, versuchen wir zunächst, wie in der allgemeinen Theorie, eine Lösung der Gleichung

$$5x_0 + 7y_0 = 1$$

zu finden. Dies gelingt mit dem Euklidischen Algorithmus:

$$7 = 1 \cdot 5 + 2$$
$$5 = 2 \cdot 2 + 1$$
$$2 = 2 \cdot 1 + 0.$$

Durch Rückwärtseinsetzen erhalten wir: $1 = 5 \cdot 3 - 7 \cdot 2$, also ist $x_0 = 3, y_0 = -2$ eine Lösung der Gleichung $5x + 7y = 1$.

Multiplizieren wir diese Lösung mit 101, so erhalten wir eine Lösung der Gleichung $5x + 7y = 101$:

$$x = 101 \cdot 3 = 303, \quad y = 101 \cdot (-2) = -202.$$

Diese Lösung ist jedoch nicht praktikabel, da eine negative Anzahl von Münzen nicht möglich ist.

Nach dem allgemeinen Lösungssatz für die lineare Diophantische Gleichung erhalten wir alle ganzzahligen Lösungen in der Form:

$$x = 303 + 7u, \quad y = -202 - 5u, \quad u \in \mathbb{Z}.$$

Zur Vereinfachung der Erklärung setze ich $v = -u$, die auch eine belibiege ganze Zahl sein kann.

$$x = 303 - 7v, \quad y = -202 + 5v.$$

Nun bestimmen wir alle ganzzahligen Werte von v, für die beide Ausdrücke nicht negativ sind: - Aus $y \geq 0$ folgt: $5v \geq 202 \Rightarrow v \geq 41$, - Aus $x \geq 0$ folgt: $7v \leq 303 \Rightarrow v \leq \left\lfloor \frac{303}{7} \right\rfloor = 43$.

Somit sind $v = 41, 42, 43$ die einzigen zulässigen Werte. Daraus ergeben sich drei Lösungen:

$$v = 41 \Rightarrow x = 303 - 287 = 16, \quad y = -202 + 205 = 3,$$
$$v = 42 \Rightarrow x = 303 - 294 = 9, \quad y = -202 + 210 = 8,$$
$$v = 43 \Rightarrow x = 303 - 301 = 2, \quad y = -202 + 215 = 13.$$

Antwort: Ja, man kann genau 101 Einheiten einzahlen, und es gibt genau drei Möglichkeiten:

$$(x, y) = (16, 3), \quad (9, 8), \quad (2, 13),$$

also mit 16 Fünfer- und 3 Siebener-Münzen, oder 9 Fünfer- und 8 Siebener-Münzen, oder 2 Fünfer- und 13 Siebener-Münzen.

Vorlesung 6

6.1. **Beispiele von Diophantischen Gleichungen.**

Erinnern wir uns daran, wie man eine allgemeine diophantische Gleichung der Form $ax + by = c$ lösen kann.

Schritt 0. Zunächst überprüfen wir, ob überhaupt Lösungen existieren: Eine notwendige Bedingung ist, dass c durch den größten gemeinsamen Teiler $\mathrm{ggT}(a, b)$ teilbar ist. Ist dies nicht der Fall, besitzt die Gleichung keine ganzzahlige Lösung. Andernfalls teilen wir die gesamte Gleichung durch $\mathrm{ggT}(a, b)$ und erhalten eine Gleichung derselben Form:

$$a'x + b'y = c', \tag{3}$$

wobei nun $\mathrm{ggT}(a', b') = 1$ gilt.

Schritt 1. Wir bestimmen eine Lösung der Gleichung $a'x + b'y = 1$. Dies ist möglich, da nach dem vorherigen Schritt a' und b' teilerfremd sind. Eine solche Lösung (x_0, y_0) kann man mithilfe des erweiterten Euklidischen Algorithmus finden, sodass

$$a'x_0 + b'y_0 = 1.$$

Wir erhalten eine Lösung der Gleichung (3), indem wir beide Seiten mit c' multiplizieren:

$$a'(c'x_0) + b'(c'y_0) = c',$$

also ist $(x, y) = (c'x_0, c'y_0)$ eine Lösung.

Schritt 2. Alle ganzzahligen Lösungen lassen sich dann durch folgende Parameterdarstellung angeben:

$$x = c' \cdot x_0 + b'u, \quad y = c' \cdot y_0 - a'u, \quad \text{wobei } u \in \mathbb{Z}.$$

> *Beispiel 1.* Angenommen, ein Automat akzeptiert nur Münzen im Wert von 5 und 7 Einheiten. Kann man an diesem Automaten genau 101 Einheiten einzahlen? Wenn ja, wie viele Münzen jeder Sorte benötigt man?

Bezeichnen wir die Anzahl der Münzen im Wert von 5 bzw. 7 Einheiten mit x bzw. y, so ergibt sich die folgende lineare Gleichung:

$$5x + 7y = 101.$$

Da 5 und 7 teilerfremd sind, versuchen wir zunächst, wie in der allgemeinen Theorie, eine Lösung der Gleichung

$$5x_0 + 7y_0 = 1$$

zu finden. Dies gelingt mit dem Euklidischen Algorithmus:

$$7 = 1 \cdot 5 + 2$$
$$5 = 2 \cdot 2 + 1$$
$$2 = 2 \cdot 1 + 0.$$

Durch Rückwärtseinsetzen erhalten wir: $1 = 5 \cdot 3 - 7 \cdot 2$, also ist $x_0 = 3, y_0 = -2$ eine Lösung der Gleichung $5x + 7y = 1$.

Multiplizieren wir diese Lösung mit 101, so erhalten wir eine Lösung der Gleichung $5x + 7y = 101$:

$$x = 101 \cdot 3 = 303, \quad y = 101 \cdot (-2) = -202.$$

Diese Lösung ist jedoch nicht praktikabel, da eine negative Anzahl von Münzen nicht möglich ist.

Nach dem allgemeinen Lösungssatz für die lineare Diophantische Gleichung erhalten wir alle ganzzahligen Lösungen in der Form:

$$x = 303 + 7u, \quad y = -202 - 5u, \quad u \in \mathbb{Z}.$$

Zur Vereinfachung der Erklärung setze ich $v = -u$, die auch eine belibiege ganze Zahl sein kann.

$$x = 303 - 7v, \quad y = -202 + 5v.$$

Nun bestimmen wir alle ganzzahligen Werte von v, für die beide Ausdrücke nicht negativ sind:
Aus $y \geq 0$ folgt: $5v \geq 202 \Rightarrow v \geq \frac{202}{5} = 40 + \frac{2}{5} \Rightarrow v \geq 41$;
Aus $x \geq 0$ folgt: $7v \leq 303 \Rightarrow v \leq \frac{303}{7} = 43 + \frac{2}{7} \Rightarrow u \leq 43$.

Somit sind $v = 41, 42, 43$ die einzigen zulässigen Werte. Daraus ergeben sich drei Lösungen:

$$v = 41 \Rightarrow x = 303 - 287 = 16, \quad y = -202 + 205 = 3,$$
$$v = 42 \Rightarrow x = 303 - 294 = 9, \quad y = -202 + 210 = 8,$$
$$v = 43 \Rightarrow x = 303 - 301 = 2, \quad y = -202 + 215 = 13.$$

Antwort: Ja, man kann genau 101 Einheiten einzahlen, und es gibt genau drei Möglichkeiten:

$$(x, y) = (16, 3), \quad (9, 8), \quad (2, 13),$$

also mit 16 Fünfer- und 3 Siebener-Münzen, oder 9 Fünfer- und 8 Siebener-Münzen, oder 2 Fünfer- und 13 Siebener-Münzen.

> *Beispiel 2.*
> Ein Transportunternehmen verfügt über zwei Lkw-Typen:
> - Der erste Lkw kann 3 Tonnen transportieren,
> - der zweite Lkw kann 5 Tonnen transportieren.
>
> Es sollen genau 63 Tonnen transportiert werden. Welche Kombinationen der beiden Lkw-Typen sind möglich, um die gesamte Last zu befördern, vorausgesetzt, die Transporte sollen voll ausgelastet sein?

Dies führt zur linearen diophantischen Gleichung:

$$3x + 5y = 63, \tag{4}$$

wobei x die Anzahl der 3-Tonnen-Lkw und y die Anzahl der 5-Tonnen-Lkw bezeichnet.
Zuerst finden wir eine ganzzahlige Lösung der Gleichung

$$3x + 5y = 1.$$

Es gibt eine systematische Methode, um eine solche Lösung zu finden, aber es ist oft nicht nötig, diese anzuwenden, wenn man eine Lösung durch Ausprobieren erraten kann. Hier zum Beispiel erkennt man durch Einsetzen kleiner Werte von x und y, dass $x = -3, y = 2$ eine Lösung ist.
Daraus ergibt sich durch Multiplikation mit 63 die Lösung der Gleichung 4:

$$x_0 = -3 \cdot 63 = -189, \quad y_0 = 2 \cdot 63 = 126.$$

Die allgemeine Lösung kann dann wie folgt beschrieben werden:

$$x = -189 + 5u, y = 126 - 3u, \quad \text{wobei } u \in \mathbb{Z}.$$

Man könnte auch direkt eine Lösung der Gleichung 4 durch Ausprobieren finden. Da 63 durch 3 teilbar ist, sieht man leicht, dass $x = 21, y = 0$ eine Lösung ist. Die allgemeine Lösung lässt sich dann alternativ als

$$x = 21 + 5u, y = -3u$$

darstellen. Beachten Sie, dass dies lediglich eine andere Parametrisierung der gleichen Lösungsmenge ist.

Nun sollen wir alle $u \in \mathbb{Z}$ finden, für die $x, y \geq 0$ gilt. Das bedeutet, wir müssen folgendes Ungleichungssystem lösen:

$$-189 + 5u \geq 0$$
$$126 - 3u \geq 0.$$

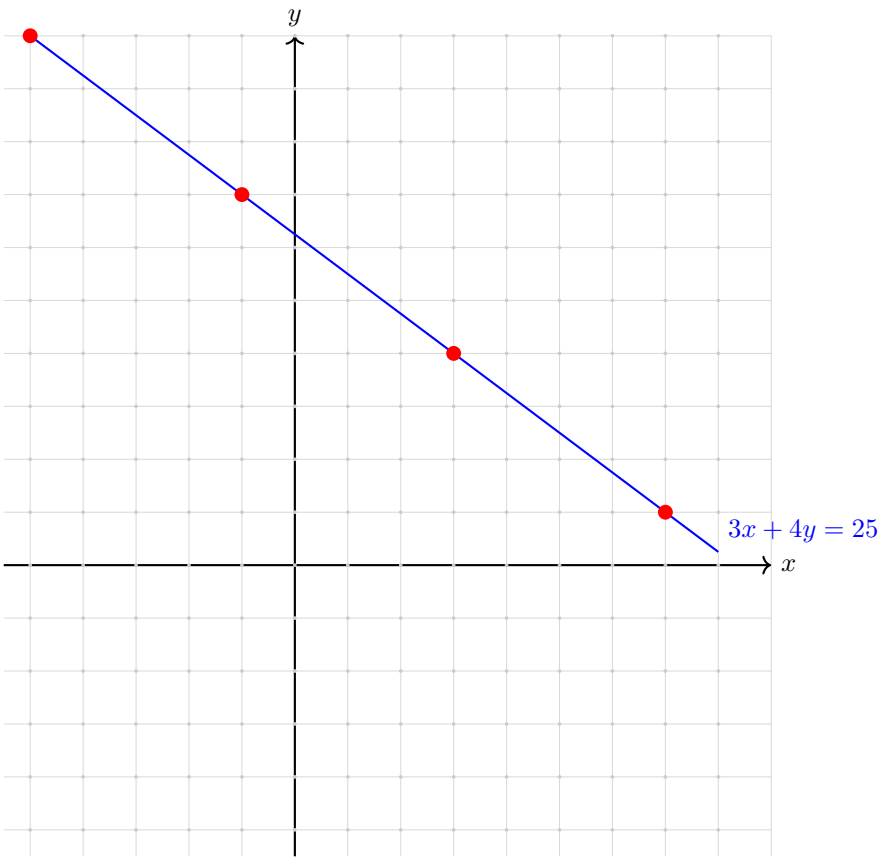
Es folgt daraus, dass $u \geq \frac{189}{5} = 38 - \frac{1}{5} = 37,8$ und $u \leq \frac{126}{3} = 42$ gilt. Da u ganzzahlig sein muss, ergibt sich:

$$u \in \{38, 39, 40, 41, 42\}.$$

Also alle Lösungen des Problems sind

$$u = 38 \Rightarrow x = 1, y = 12$$
$$u = 39 \Rightarrow x = 6, y = 9$$
$$u = 40 \Rightarrow x = 11, y = 6$$
$$u = 41 \Rightarrow x = 16, y = 3$$
$$u = 42 \Rightarrow x = 21, y = 0.$$

Man kann die Lösungen der diophantischen Gleichung auch graphisch darstellen.
Wie man vielleicht aus der Schule weiß, beschreibt die Gleichung $ax + by = c$ eine Gerade in der Ebene mit den Koordinaten x und y. (Man kann sie auch in die Form $y = -\frac{a}{b}x + \frac{c}{b}$ umformen, sofern $b \neq 0$.)
Die ganzzahligen Lösungen entsprechen den Schnittpunkten dieser Geraden mit dem Gitter der ganzzahligen Punkte in der Ebene.
Ein Beispiel ist die Gerade $3x + 4y = 25$, die durch die Punkte $x = 7$, $y = 1$ und $x = 3$, $y = 4$ läuft.



6.2. **Unendlichkeit von Primzahlen.** In dem Fundamentalsatz der Arithmetik haben wir gesehen, dass die Primzahlen eine zentrale Rolle in der Zahlentheorie spielen. Dies führt zur Frage, ob es möglicherweise nur endlich viele Primzahlen gibt. Diese Frage wurde bereits von Euklid mit dem folgenden Beweis verneint:

Satz 6.2.1. *Es gibt unendlich viele Primzahlen.*

Beweis. Der Beweis erfolg durch Widerspruch. Angenommen, es gäbe nur endlich viele Primzahlen. Dann könnten wir sie vollständig aufzählen und bezeichnen mit $p_1, p_2, \ldots, p_n$.

Betrachten wir nun die Zahl

$$N := p_1 \cdot p_2 \cdot p_3 \cdots p_n + 1.$$

Diese Zahl ist ju jeder Primzahl p_i teilerfremd, denn

$$N = u \cdot p_i + 1,$$

wobei u das Produkt aller Primzahlen außer p_i ist. (Errinern Sie sich daran, dass wenn $a = u \cdot b + r$, dann gilt $\mathrm{ggT}(a, b) = \mathrm{ggT}(b, r)$.)

Daraus folgt, dass keine der Primzahlen $p_1, \ldots, p_n$ in der Primfaktorzerlegung von N erscheint. Also muss in der Primfaktorzerlegung von N eine weitere Primzahl auftreten, die nicht in der Liste $p_1, \ldots, p_n$

enthalten ist. Das steht im Widerspruch zur Annahme, dass alle Primzahlen bereits aufgezählt wurden. □

Obwohl wir wissen, dass es unendlich viele Primzahlen gibt, kann man ihre Liste nicht einfach vollständig aufschreiben. Sobald die Zahlen relativ groß werden, ist es schwierig zu überprüfen, ob eine Zahl eine Primzahl ist, und die Berechnung der Primfaktorzerlegung ist in der Praxis oft nur theoretisch möglich.
Die derzeit größte bekannte Primzahl ist

$$2^{136279841} - 1.$$

Sie wurde am 12. Oktober 2024 mithilfe eines Computers entdeckt.

Aus dem Beweis ergeben sich zwei wichtige Bemerkungen.
Erstens: obwohl der Beweis durch Widerspruch geführt wurde, kann man ihn tatsächlich zur Konstruktion neuer Primzahlen verwenden. Wenn man die ersten n Primzahlen $p_1, \dots, p_n$ kennt, dann enthält die Primfaktorzerlegung der Zahl $N = p_1 \cdots p_n + 1$ mindestens eine neue Primzahl, die nicht in der Liste enthalten ist. Diese Methode ist jedoch praktisch wenig effizient, da das Produkt N sehr schnell sehr groß wird, und die Primfaktorzerlegung von N rechenintensiv ist und viele Ressourcen benötigt.
Zweitens: Beim Betrachten der Zahl N war das Entscheidende, dass sie zu jeder Primzahl p_i teilerfremd ist. Man hätte also statt $N = p_1 \cdot p_2 \cdot \dots \cdot p_n + 1$ auch z. B. $N = 2 \cdot p_1 \cdot p_2 \cdot \dots \cdot p_n + 1$ oder $N = 4 \cdot p_1 \cdot p_2 \cdot \dots \cdot p_n + 3$ betrachten können.
Dies führt zu weiteren Beweisen interessanter Eigenschaften von Primzahlen – siehe unten.

Satz 6.2.2. *Es gibt unendlich viele Primzahlen der Form $4q + 3$, wobei q eine natürliche Zahl ist.*

Eine natürliche Zahl n hat genau dann die Form $4q + 3$, wenn sie bei Division durch 4 den Rest 3 hat.

Beweis. Der Beweis erfolgt durch Widerspruch.
Angenommen, es gäbe nur endlich viele Primzahlen der Form $4q+3$ und bezeichne sie mit $p_1, p_2, \dots, p_n$.
Betrachten wir nun die Zahl

$$N := 4 \cdot p_1 \cdot p_2 \cdot p_3 \cdots p_n - 1.$$

Diese Zahl ist ju jeder Primzahl p_i teilerfremd (wie im obenen Beweis von Unendlichkeit der Primzahlen). Also müssen in der Primfaktorzerlegung von N andere Primzahlen vorkommen.
Nun beachten wir, dass eine natürliche Zahl entweder die Form $4q$, $4q + 1$, $4q + 2$ oder $4q + 3$ hat. Zahlen der Form $4q$ und $4q + 2$ sind gerade, also durch 2 teilbar. Da N ungerade ist (da das Produkt $4 \cdot p_1 \cdots p_n$ gerade ist, und $4 \cdot \text{gerade} - 1$ ergibt eine ungerade Zahl), kann N nicht durch 2 teilbar sein. Also kann keine der Primzahlen in seiner Zerlegung die Form $4q$ oder $4q + 2$ haben.
Es folgt, dass alle Primzahlen in der Zerlegung von N die Form $4q + 1$ haben. Dann hätte auch ihr Produkt die Form $4q + 1$. Denn:

$$(4a + 1)(4b + 1) = 16ab + 4a + 4b + 1 = 4(4ab + a + b) + 1,$$

also wieder eine Zahl der Form $4q + 1$.
Aber:

$$N = 4 \cdot p_1 \cdot p_2 \cdots p_n - 1 = 4 \cdot (p_1 \cdot p_2 \cdots p_n - 1) + 3,$$

also hat N die Form $4q + 3$, nicht $4q + 1$. Das ist ein Widerspruch.
Daraus folgt, dass in der Primfaktorzerlegung von N mindestens eine Primzahl vorkommen muss, die die Form $4q + 3$ hat — aber diese steht nicht in unserer Liste $p_1, \dots, p_n$. Das widerspricht der Annahme, dass es nur endlich viele solcher Primzahlen gibt. □

Wir schließen die Diskussion über Primzahlen mit dem folgenden Satz ab, dessen Beweis jedoch den Rahmen dieser Vorlesung übersteigt.

Satz 6.2.3 (Dirichlet, 1837)**.** *Seien a, b teilerfremde natürliche Zahlen.*
Dann gibt es unendlich viele Primzahlen unter den Zahlen der arithmetischen Folge

$$n \cdot a + b, \quad n \in \mathbb{N}.$$

6.3. **Das Problem mit zwei Rädern.**

Bevor wir das nächste Thema beginnen, lassen Sie uns ein Problem aus dem Übungsblatt ausführlich lösen.

> **Aufgabe 5 aus Übungsblatt 4.**
> Stellen Sie sich vor, ein kleines Rad mit einem Radius von 18 rollt ohne zu rutschen an der Außenseite eines größeren Rads mit dem Radius 40 entlang (s. die Abbildung unten). In das kleine Rad ist ein Nagel eingeschlagen. Jedes Mal, wenn der Nagel das große Rad berührt, hinterlässt er eine Markierung auf dessen Rand.
>
> (1) Wie viele verschiedene Markierungen entstehen auf dem großen Rad, wenn das kleine Rad beliebig oft umläuft?
> (2) Nach wie vielen vollständigen Umdrehungen des kleinen Rads kehrt der Nagel genau zur ersten Markierung zurück?

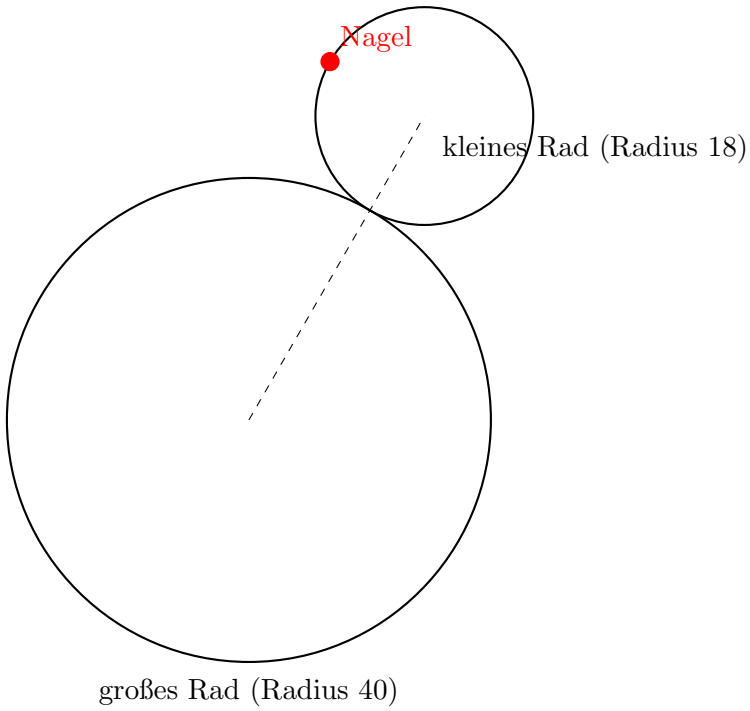
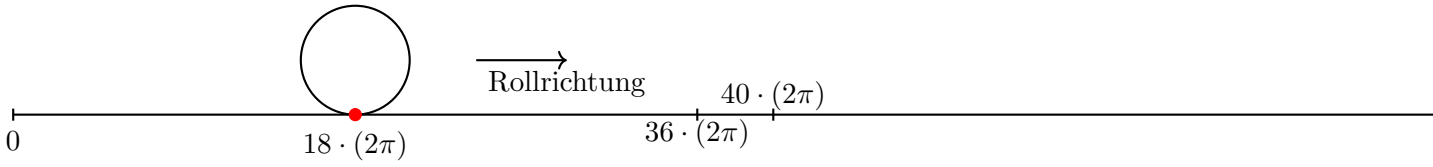


Abbildung 1. Kleines Rad rollt ohne zu rutschen außen am großen Rad entlang

Um das Problem zu verstehen, visualisieren wir, wie die Markierungen auf dem größeren Rad entstehen. Stellen wir uns vor, dass wir die Außenseite des größeren Rads zu einer geraden Linie abrollen: Wir setzen den Punkt 0 an die Stelle der ersten Markierung. Die zweite Markierung entsteht dann bei $18 \cdot (2\pi)$ Einheiten Entfernung (denn der Umfang eines Kreises ist 2π mal Radius). Die dritte Markierung liegt bei $36 \cdot (2\pi)$.



Wenn wir die vierte Markierung bezeichnen möchten, haben wir zwei Möglichkeiten:

1. Direkte Mehthode: Wir markieren einfach den Punkt $3 \cdot 18(2\pi) = 54(2\pi)$ auf der Linie.

2. Periodische Methode: Wir errinern uns, dass diese Markierungen auf dem Rad entstehen, das heißt, dass die Punkten $40(2\pi)$ mit 0 zusammengeklebt sind. Wenn das kleine Rad den Punkt $40(2\pi)$ erreicht hat, bleibt noch eine Strecke von $(18 - (40 - 36))(2\pi)$ zu rollen. Also entsteht die vierte Markierung auf dem Punkt $14 \cdot (2\pi)$.

Beide Sichtweisen sind nützlich. Die zweite Methode zeigt uns: Wenn wir das Rad auf diese Weise immer weiter rollen, dann erscheinen die Markierungen nur an bestimmten Stellen der Länge des großen Rads, also an Positionen:

$$0, 1 \cdot (2\pi), 2 \cdot (2\pi), \ldots, 39 \cdot (2\pi).$$

Das bedeutet, dass nur endlich viele verschiedene Markierungen auf dem großen Rad entstehen können — höchstens 40.

Diese Beobachtung erlaubt eine wichtige Argumentation:

Angenommen, es entstehen insgesamt N verschiedene Markierungen. Dann wird die letzte Markierung genau dann entstehen, wenn der Nagel das erste Mal zur ursprünglichen Markierung bei 0 zurückkehrt. Tatsächlich gilt: Immer wenn der Nagel eine Markierung auf dem großen Rad setzt, wiederholt sich genau die geometrische Situation, die bereits bei der ersten Markierung vorlag.

Das bedeutet, dass die Anzahl der Markierungen und die Anzahl der vollständigen Umdrehungen des kleinen Rads bis zur Rückkehr zur ersten Markierung fast gleich sind. Wenn die Anzahl der verschiedenen Markierungen N ist, dann kehrt der Nagel nach $N + 1$ vollständigen Umdrehungen zur ersten Markierung zurück.

Wir kommen nun zur ersten Methode zurück. Die Nagel markiert die Punkte mit Koordinaten $n \cdot 18(2\pi)$, wobei n eine natürliche Zahl ist. Denn jedes Mal muss das Rad um genau $18(2\pi)$ Einheiten entlang der Linie rollen, damit eine vollständige Umdrehung erfolgt.

Wann wiederholen sich diese Markierungen? Auf dieser Linie wiederholen sie sich nicht, denn das Rad rollt ständig nach rechts und kehrt nie zurück.

Wir erinnern uns jedoch daran, dass diese Linie nur eine hypothetische Darstellung ist. Zum Beispiel, die Punkte mit Koordinaten 0 und $40 \cdot (2\pi)$ auf der Linie entsprechen demselben Punkt auf dem größeren Rad.

Welchem Punkt auf dem größeren Rad entspricht dann ein Punkt mit Koordinate $x \geq 0$ auf der Linie? Um das herauszufinden, müssen wir von x die Zahl $40 \cdot (2\pi)$ so oft wie möglich abziehen, bis wir eine Zahl zwischen 0 und $40 \cdot (2\pi)$ erhalten.

Mit dieser Darstellung im Kopf ist die folgende Frage leicht zu beantworten: Nach wie vielen Umdrehungen kehrt der Nagel zur ursprünglichen Markierung zurück?

Nach n Umdrehungen erreichen wir den Punkt $n \cdot 18 \cdot (2\pi)$, und dieser Punkt muss dieselbe Position auf dem größeren Rad haben wie ein Punkt der Form $m \cdot 40 \cdot (2\pi)$, also:

$$18 \cdot n = 40 \cdot m.$$

Die kleinste mögliche ganze Zahl $n > 0$, die diese Gleichung erfüllt, liefert die Antwort auf unsere Frage.

Letztes Mal haben wir Gleichungen dieser Form gelöst: Zuerst berechnen wir, dass $\mathrm{ggT}(18, 40) = 2$ ist, und dann hat die Gleichung $9n = 20m$ ganzzahlige Lösungen der Form

$$n = 20u, \quad m = 9u, \quad u \in \mathbb{Z}.$$

Die kleinste mögliche positive Lösung für n ist also 20, das bedeutet: Der Nagel kehrt nach 20 Umdrehungen zur ersten Markierung zurück, und es entstehen insgesamt 19 verschiedene Markierungen.

Vorlesung 8[1]

8.1. **Kongruenzen.**

8.1.1. *Definition von "modulo n".* In Vorlesung 3 wurde die folgende Notation eingeführt:
($a \mod b$) ist der Rest bei Division von a durch b, d. h. $a = m \cdot b + (a \mod b)$, wobei m und ($a \mod b$) ganze Zahlen sind und $0 \leq (a \mod b) < b$ gilt.

Das Ziel nächstes Themas ist eine Arithmetik von Resten zu entwickeln. Diese Arithmetik wird auch modulare Arithmetik genannt.

Definition 8.1.1. *Sei n eine positive natürliche Zahl. Zwei ganze Zahlen a, b heißen* **kongruent modulo** *n, wenn sie bei Division durch n denselben Rest lassen.*
Notation: $a \equiv b \mod n$.

Die Notation $a \equiv b \mod n$ bedeutet genau dasselbe wie $(a \mod n) = (b \mod n)$, man kann sie also als eine vereinfachte Schreibweise dieser Gleichung verstehen.

Beispiel 8.1.2.

$$\begin{aligned} 9 &\equiv 1 \mod 4 && \text{denn } 9 = 2 \cdot 4 + 1 \\ -3 &\equiv 7 \mod 5 && \text{denn } -3 = -1 \cdot 5 + 2,\ 7 = 1 \cdot 5 + 2 \\ 1 &\equiv 1 \mod n && \text{für jedes } n \in \mathbb{N}. \end{aligned}$$

Lemma 8.1.3. *Sei n eine positive natürliche Zahl. Ganze Zahlen a und b sind genau dann kongruent modulo n, wenn n die Differenz $a - b$ teilt:*

$$a \equiv b \mod n \ \Leftrightarrow\ n \mid (a - b).$$

Beweis. 1. $a \equiv b \mod n \ \Rightarrow\ n \mid (a - b)$.
Da a und b bei Division durch n denselben Rest haben, existieren $m, k, r \in \mathbb{Z}$ mit $0 \leq r < n$, sodass

$$a = m \cdot n + r, \quad b = k \cdot n + r.$$

Dann gilt:

$$a - b = (m \cdot n + r) - (k \cdot n + r) = (m - k) \cdot n.$$

Also teilt n die Differenz $a - b$.
2. $n \mid (a - b) \ \Rightarrow\ a \equiv b \mod n$.
Seien r_1, r_2 die Reste bei Division von a bzw. b durch n, d. h.:

$$a = m \cdot n + r_1, \quad b = k \cdot n + r_2, \quad \text{mit } 0 \leq r_1, r_2 < n.$$

Dann gilt:

$$a - b = (m - k) \cdot n + (r_1 - r_2).$$

Da $n \mid (a - b)$, muss n auch $(r_1 - r_2)$ teilen. Da aber $|r_1 - r_2| < n$ ist, kann $r_1 - r_2$ nur dann durch n teilbar sein, wenn $r_1 - r_2 = 0$, also: $r_1 = r_2$. Somit haben a und b denselben Rest bei Division durch n, also gilt $a \equiv b \mod n$. □

Wir haben im Lemma gezeigt, dass die Aussage „a und b sind kongruent modulo n" äquivalent dazu ist, dass n die Differenz $a - b$ teilt. Diese Äquivalenz erlaubt es, letztere Eigenschaft als Definition zu verwenden — eine Formulierung, die man in vielen Quellen findet.

Dieses Lemma erlaubt es uns zu verstehen, wie sich die Reste bei Division durch n verhalten, wenn man zwei Zahlen addiert oder multipliziert.

Satz 8.1.4. *Sei n eine positive natürliche Zahl. Seien a_1, a_2 zwei ganzen Zahlen mit demselben Rest modulo n haben, also: $a_1 \equiv a_2 \mod n$. Sei b eine weitere ganze Zahl. Dann gilt:*

(1) *$a_1 \cdot b$ und $a_2 \cdot b$ haben gleiche Reste modulo n, also: $a_1 \cdot b \equiv a_2 \cdot b \mod n$;*
(2) *$a_1 + b$ und $a_2 + b$ haben gleiche Reste modulo n, also: $a_1 + b \equiv a_2 + b \mod n$.*

Wir zeigen zunächst anhand eines Beispiels, wie der oben genannte Satz verwendet werden kann, um Rechnungen mit großen Zahlen zu vereinfachen.

[1] Vorlesung 7 fiel aus, stattdessen gab es eine Repetitoriumstunde.

Beispiel 8.1.5. *Welchen Rest hat die Zahl* $35 \cdot 40 \cdot 374$ *bei Division durch* 37*?*

Um die Antwort zu erhalten, ist es nicht notwendig, die Zahlen vollständig zu multiplizieren. Es genügt, nur die Reste zu multiplizieren.

Wir bestimmen zunächst die Reste der einzelnen Faktoren modulo 37*:*

$$40 = 1 \cdot 37 + 3, \quad \textit{also } 40 \equiv 3 \mod 37$$
$$374 = 10 \cdot 37 + 4, \quad \textit{also } 374 \equiv 4 \mod 37$$

Man erkennt auch, dass $35 \equiv -2 \mod 37$*, denn* $35 - (-2) = 37$ *ist durch* 37 *teilbar.*

Nach dem oben genannten Satz gilt somit:

$$35 \cdot 40 \cdot 374 \equiv (-2) \cdot 3 \cdot 4 \mod 37.$$

Wir rechnen weiter:

$$(-2) \cdot 3 \cdot 4 = -24.$$

Und da $-24 \equiv 13 \mod 37$*, ergibt sich*

$$35 \cdot 40 \cdot 374 \equiv 13 \mod 37.$$

Die Zahl $35 \cdot 40 \cdot 374$ *hat somit denselben Rest wie* 13 *bei Divison durch* 37*. Da* $0 \leq 13 < 37$ *ist der Rest also genau* 13*.*

Beweis vom Satz. Nach dem obigen Lemma wissen wir, dass $n \mid (a_1 - a_2)$. Es genügt also zu zeigen, dass n auch die Differenz $a_1 \cdot b - a_2 \cdot b$ teilt – eine Anwendung des Lemmas.

Diese Differenz lässt sich wie folgt umschreiben:

$$a_1 \cdot b - a_2 \cdot b = (a_1 - a_2) \cdot b.$$

Da n die Zahl $(a_1 - a_2)$ teilt, folgt unmittelbar, dass n auch $(a_1 - a_2) \cdot b$ teilt. Nach dem Lemma ergibt sich somit:

$$a_1 \cdot b \equiv a_2 \cdot b \mod n.$$

Hier sieht man, wie nützlich das obige Lemma ist. Würde man versuchen, die Aussage direkt über die Definition von Kongruenz zu beweisen, müsste man zum Beispiel schreiben:

$$a_1 = m_1 \cdot n + r, \quad a_2 = m_2 \cdot n + r, \quad b = k \cdot n + r_b,$$

und dann $a_1 \cdot b$ und $a_2 \cdot b$ ausmultiplizieren, nur um am Ende zu sehen, dass beide Zahlen denselben Rest modulo n haben. Das Lemma erspart uns diese Rechnung.

Für die Addition argumentiert man ganz ähnlich: Es genügt zu zeigen, dass n die Differenz

$$(a_1 + b) - (a_2 + b) = a_1 - a_2$$

— was bereits bekannt ist. Also folgt:

$$a_1 + b \equiv a_2 + b \mod n.$$

□

8.1.2. *Die Menge von Restklassen* $\mathbb{Z}/n\mathbb{Z}$ *und ihre Arithmetik.* Der oben genannte Satz zeigt, dass sich die Reste bei Division durch n in gewisser Weise so verhalten, als wären sie selbst Zahlen. Genau das möchten wir nun präziser formulieren.

Sei $n \geq 1$. Ein Rest bei Division durch n ist eine der folgenden Zahlen:

$$0, 1, 2, \ldots, n - 1.$$

Die Menge dieser Reste wird mit $\mathbb{Z}/n\mathbb{Z}$ bezeichnet, und ihre Elemente schreibt man mit einem Überstrich:

$$\mathbb{Z}/n\mathbb{Z} := \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}.$$

Die Elemente von $\mathbb{Z}/n\mathbb{Z}$ nennt man auch *Restklassen modulo* n, und später wird klar werden, warum dieser Begriff sinnvoll ist.

Wie die Restklasse $\overline{a}$ definiert ist, hängt vom "Modulus" n ab. Wenn wir also $\overline{a}$ schreiben, setzen wir voraus, dass aus dem Kontext klar ist, auf welche Zahl n sich die Notation bezieht.

Es gibt eine Abbildung

$$\begin{array}{rcl} \pi_n \colon \mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ a & \longmapsto & \overline{a \bmod n} \end{array}$$

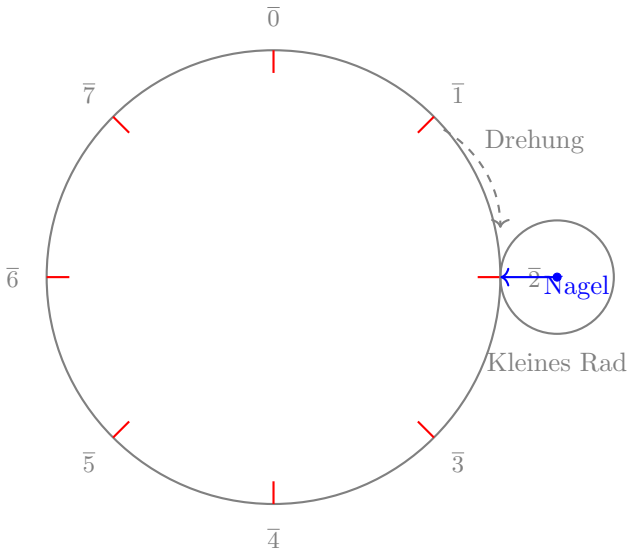
die jeder ganzen Zahl a **ihre Restklasse** modulo n zuordnet, also den Rest von a bei Division durch n.

Beispiel 8.1.6. *Sei $n = 5$, dann bildet diese Abbildung die folgende Zahl wie folgt ab:*

$$\begin{array}{rcl} -1 & \longmapsto & \overline{4} \\ 0 & \longmapsto & \overline{0} \\ 1 & \longmapsto & \overline{1} \\ 2 & \longmapsto & \overline{2} \\ & \dots & \\ 13 & \longmapsto & \overline{3} \\ 14 & \longmapsto & \overline{4} \end{array}$$

Beachten Sie: Zwei Zahlen $a_1, a_2 \in \mathbb{Z}$ werden genau dann in dieselbe Restklasse abgebildet, wenn sie kongruent modulo n sind, also $a_1 \equiv a_2 \mod n$. Nach dem obigen Lemma ist das genau dann der Fall, wenn n die Differenz $a_1 - a_2$ teilt.

Erinnern wir uns an die Aufgabe mit den zwei Rädern, so lässt sich die Abbildung $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ anschaulich visualisieren.
Stellen wir uns ein kleines Rad mit Umfang 1 vor, das — ohne zu rutschen — außen an einem größeren Rad mit Umfang n entlangrollt. In das kleine Rad ist ein Nagel eingeschlagen. Jedes Mal, wenn der Nagel das große Rad berührt, hinterlässt er dort eine Markierung.
So entstehen auf dem Rand des großen Rads insgesamt n Markierungen, die wir mit $\overline{0}, \overline{1}, \dots, \overline{n-1}$ bezeichnen. Steht der Nagel anfangs bei der Markierung $\overline{0}$, so befindet er sich nach m vollständigen Umdrehungen des kleinen Rads bei der Markierung $\overline{m \bmod n}$. Das entspricht genau dem Bild, das durch die Abbildung $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ entsteht: Jede ganze Zahl wird auf ihre Restklasse modulo n abgebildet.



Großes Rad (Umfang $n = 8$)

Ein ähnliches Prinzip kennt man von Uhren: Nach S Stunden zeigt der Stundenzeiger auf $\overline{S \bmod 12}$, nach M Minuten zeigt der Minutenzeiger auf $\overline{M \bmod 60}$.

Das Interessante an der Menge $\mathbb{Z}/n\mathbb{Z}$ ist, dass sich auf ihr eine Addition und Multiplikation definieren lässt — und zwar so, dass die natürliche Abbildung $\pi_n \colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ diese Operationen erhält.

Anders ausgedrückt: Wenn a bei Division durch n den Rest r_a und b den Rest r_b hat, dann ist $\overline{r_a} \cdot \overline{r_b}$ genau die Restklasse von $a \cdot b$ modulo n. Also, wir *definieren*:

$$\overline{r_a} \cdot \overline{r_b} := \overline{r_a \cdot r_b \mod n} \quad \text{und} \quad \overline{r_a} + \overline{r_b} := \overline{(r_a + r_b) \mod n}.$$

Addition und Multiplikation auf $\mathbb{Z}/n\mathbb{Z}$ erfüllen die üblichen Rechengesetze. Bevor wir dies formulieren, betrachten wir einige Beispiele.

Beispiele. Sei $n = 5$, dann ist

$$\mathbb{Z}/5\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}.$$

Es gelten folgende Rechenregeln:

$$\overline{2} \cdot \overline{2} = \overline{4} \qquad \text{denn } 2 \cdot 2 = 4 \text{ und 4 hat den Rest 4 modulo 5}$$
$$\overline{3} \cdot \overline{2} = \overline{1} \qquad \text{denn } 3 \cdot 2 = 6 \text{ und 6 hat den Rest 1 modulo 5}$$
$$\overline{1} + \overline{4} = \overline{0} \qquad \text{denn } 1 + 4 = 5 \text{ und 5 hat den Rest 0 modulo 5.}$$

Satz. *Die Addition und die Multiplikation auf dem Restklassenring $\mathbb{Z}/n\mathbb{Z}$ erfüllen die folgenden Eigenschaften:*

(1) *für jede $x, y \in \mathbb{Z}/n\mathbb{Z}$ gilt $x + y = y + x$, $x \cdot y = y \cdot x$;*
(2) *für jedes $x \in \mathbb{Z}/n\mathbb{Z}$ gilt $x + \overline{0} = x$, $x \cdot \overline{1} = x$;*
(3) *für jede $x, y, z \in \mathbb{Z}/n\mathbb{Z}$ gilt $x \cdot (y + z) = x \cdot y + x \cdot z$ und $x \cdot (y \cdot z) = (x \cdot y) \cdot z$;*
(4) *für jede $x \in \mathbb{Z}/n\mathbb{Z}$ existiert $y \in \mathbb{Z}/n\mathbb{Z}$ mit $x + y = \overline{0}$.*

Für Gleichungen mit ganzen Zahlen kann man immer kürzen. Das heißt: Wenn $a \cdot b = a \cdot c$ und $a \neq 0$, dann folgt $b = c$. Diese Eigenschaft gilt jedoch nicht in allen Restklassenringen $\mathbb{Z}/n\mathbb{Z}$!
Hier ist ein Beispiel: In $\mathbb{Z}/6\mathbb{Z}$ gilt

$$\overline{2} \cdot \overline{3} = \overline{2} \cdot \overline{0} = \overline{0},$$

aber natürlich sind $\overline{3}$ und $\overline{0}$ verschiedene Elemente von $\mathbb{Z}/6\mathbb{Z}$.

Der Beweis dieses Satzes ist eher formeller Natur und wird hier weggelassen. Die Struktur, bestehend aus Addition und Multiplikation auf der Menge $\mathbb{Z}/n\mathbb{Z}$, wird in der Algebra als *kommutativer Ring* bezeichnet. Die korrekte mathematische Definition von $\mathbb{Z}/n\mathbb{Z}$ umfasst daher nicht nur die Menge $\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ mit ihren n Elementen, sondern auch die beiden Operationen sowie die Abbildung

$$\pi \colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z},$$

welche diese Operationen erhält.

Im Folgenden bezeichnen wir $\mathbb{Z}/n\mathbb{Z}$ als **Restklassenring**.

8.1.3. *Das Rechnen mit Restklassen und mit ganzen Zahlen.* Nun zeigen wir, wie das Rechnen im Restklassenring $\mathbb{Z}/n\mathbb{Z}$ uns hilft, Rechnungen mit Zahlen zu vereinfachen.

Beispiel 8.1.7. *Was ist der Rest der Zahl 3^{51} bei Division durch 5?*

Da die Abbildung $\mathbb{Z} \to \mathbb{Z}/5\mathbb{Z}$ die Multiplikation erhält, wird die Zahl $3 \cdot 3 \cdots 3$ (insgesamt 51 Faktoren) ins Element $\overline{3} \cdot \overline{3} \cdots \overline{3}$ (insgesamt 51 Faktoren) abgebildet. Wir müssen also die 51-te Potenz des Elements $\overline{3}$ in $\mathbb{Z}/5\mathbb{Z}$ berechnen. Da dieser Ring nur 5 Elemente enthält, lässt sich das einfach durch Ausprobieren machen. Wir bestimmen die ersten Potenzen von $\overline{3}$:

$$(\overline{3})^2 = \overline{3} \cdot \overline{3} = \overline{4}, \quad \text{da } 9 = 1 \cdot 5 + 4,$$
$$(\overline{3})^3 = \overline{3} \cdot \overline{3} \cdot \overline{3} = \overline{4} \cdot \overline{3} = \overline{2}, \quad \text{da } 12 = 2 \cdot 5 + 2,$$
$$(\overline{3})^4 = \overline{3} \cdot \overline{3} \cdot \overline{3} \cdot \overline{3} = \overline{2} \cdot \overline{3} = \overline{1}, \quad \text{da } 6 = 1 \cdot 5 + 1.$$

Wir sehen also, dass $(\overline{3})^4 = \overline{1}$, was sehr nützlich ist, denn die Multiplikation mit $\overline{1}$ ändert das Element nicht.

Damit können wir schreiben:

$$(\overline{3})^{51} = (\overline{3})^{4 \cdot 12 + 3} = (\overline{3})^{4 \cdot 12} \cdot (\overline{3})^3 = ((\overline{3})^4)^{12} \cdot (\overline{3})^3 = (\overline{1})^{12} \cdot (\overline{3})^3 = (\overline{3})^3 = \overline{2}.$$

Wir haben also berechnet, dass 3^{51} bei Division durch 5 den Rest 2 hat.

Vorlesung 9

9.1. **Widerholung von Kongruenzen.**

Wann haben zwei Zahlen denselben Rest bei Division durch n? Diese Frage haben wir beim letzten Mal mit dem folgenden Lemma beantwortet. Ich nenne es nun das "Kongruenz-Lemma", um später darauf verweisen zu können.

Lemma 9.1.1 ("Kongruenz-Lemma")**.** *Seien a, b ganze Zahlen. Dann haben a und b genau dann denselben Rest bei Division durch n, wenn n die Differenz $a - b$ teilt.*

Wenn die Bedingungen des Lemmas für a und b erfüllt sind, schreibt man:

$$a \equiv b \mod n$$

Man sagt: "a ist kongruent zu b modulo n", oder kürzer: "a kongruent b modulo n".

Es ist nützlich zu bemerken: Wenn $a \equiv b \mod n$ und $b \equiv c \mod n$, dann gilt auch $a \equiv c \mod n$. Die Begründung ist klar: Wenn a und b denselben Rest bei Division durch n haben und b und c ebenfalls, dann haben auch a und c denselben Rest bei Division durch n.

Das Kongruenz-Lemma hilft uns, die Arithmetik mit Restklassen zu entwickeln. Ein erstes wichtiges Resultat lautet: Seien a, b, c ganze Zahlen und sei n eine positive natürliche Zahl. Dann gilt:

$$\text{wenn } a \equiv b \mod n \quad \text{dann } ac \equiv bc \mod n \text{ und } a + c \equiv b + c \mod n.$$

Wir werden diese Aussagen "Rechenregeln der Kongruenzarithmetik" oder gelegentlich "Rechenregeln der Resten" nennen, um auf diese Formeln zu verweisen.

Beachten Sie auch die folgende Aussage:

$$a \equiv b \mod n,\ c \equiv d \mod n \Rightarrow a \cdot c \equiv d \cdot b \mod n.$$

Diese Aussage lässt sich aus der vorherigen in zwei Schritten ableiten: Zunächst folgt aus $a \equiv b \mod n$, dass $a \cdot c \equiv b \cdot c \mod n$. Dann ergibt sich aus $c \equiv d \mod n$, dass $b \cdot c \equiv b \cdot d \mod n$ (bei Multiplikation mit b). Wie es oben beobachtet wurde, folgt die Aussage daraus.

Hier ein Beispiel: Betrachten wir folgende Aussage:

Wenn zwei Zahlen von der Form $4q + 1$ sind,
dann ist auch ihr Produkt von dieser Form.

Diese Aussage haben wir in Vorlesung 6 im Beweis verwendet, dass es unendlich viele Primzahlen der Form $4q + 3$ gibt. Mit Hilfe der Kongruenzarithmetik können wir diesen Beweis nun besser verstehen: Die Bedingung, dass eine Zahl x von der Form $4q + 1$ ist, entspricht genau der Aussage über den Rest von x bei Division durch 4:

$$a = 4q + 1 \Longleftrightarrow a \equiv 1 \mod 4$$

Wenn also $a \equiv 1 \mod 4$ und $b \equiv 1 \mod 4$, dann folgt aus den Rechenregeln der Kongruenzarithmetik:

$$a \cdot b \equiv 1 \cdot 1 \mod 4.$$

Da $1 \cdot 1 = 1$, ergibt sich:

$$a \cdot b \equiv 1 \mod 4$$

Das Produkt zweier Zahlen der Form $4q + 1$ ist also ebenfalls von dieser Form.

Bei ganzen Zahlen gibt es neben der Addition auch die Subtraktion – man kann also Zahlen voneinander abziehen. Natürlich funktioniert das auch in der Kongruenzarithmetik:

$$a \equiv b \mod n \Longrightarrow a - c \equiv b - c \mod n.$$

Wir fassen die Rechenregeln der Kongruenzarithmetik in der folgenden Tabelle:

- $a \equiv b \mod n$ und $b \equiv c \mod n \Longrightarrow a \equiv c \mod n$.
- $a \equiv b \mod n \Longrightarrow ac \equiv bc \mod n$, $a + c \equiv b + c \mod n$, $a - c \equiv b - c \mod n$.
- $a \equiv b \mod n$ und $c \equiv d \mod n \Longrightarrow ab \equiv cd \mod n$.

9.2. **Einige Teilbarkeitsregeln.**

Ich führe die folgende Notation ein: Wenn eine natürliche Zahl eine Dezimaldarstellung mit $n+1$ Ziffern $a_n, a_{n-1}, \ldots, a_0$ hat, dann schreiben wir $[a_n a_{n-1} \cdots a_1 a_0]_{10}$.

Beispiel: Wenn $n = 3$ und $a_2 = 4$, $a_1 = 2$, $a_0 = 0$, ist diese Zahl $420 = [420]_{10}$.

Es ist klar, dass man diese Notation nur braucht, wenn die Ziffer in einer gewissen Weise unbekannt sind, da es keinen Sinn macht anstatt 420 immer $[420]_{10}$ zu schreiben. Wenn wir aber die Zahl $[a_n a_{n-1} \cdots a_1 a_0]_{10}$ mit dem Produkt $a_n \cdot a_{n-1} \cdot a_1 \cdot a_0$ nicht verwirren möchten, ist irgendwelche neue Notation unvermeidbar.

Satz 9.2.1. *Sei x eine natürliche Zahl mit Dezimaldarstellung: $x = [a_n a_{n-1} \cdots a_0]_{10}$.*
Dann haben x und die zweistellige Zahl $[a_1 a_0]_{10}$ denselben Rest bei Division durch 4.

Beweis. Nach dem Kongruenz-Lemma genügt es, die Differenz

$$x - [a_1 a_0]_{10}$$

zu betrachten und zu zeigen, dass sie durch 4 teilbar ist. Diese Differenz ist eine Zahl, deren letzte zwei Ziffern 00 sind, also ein Vielfaches von 100. Genauer:

$$x - [a_1 a_0]_{10} = [a_n a_{n-1} \cdot a_2 00]_{10} = 100 \cdot [a_n a_{n-1} \cdot a_2]_{10}.$$

Da 100 durch 4 teilbar ist, ist auch die ganze Differenz durch 4 teilbar:

$$x - [a_1 a_0]_{10} = 4 \cdot (25 \cdot [a_n a_{n-1} \cdot a_2]_{10}).$$

□

Corollary 9.2.2. *Die Zahl $[a_n a_{n-1} \cdots a_0]_{10}$ ist genau dann durch 4 teilbar, wenn die Zahl $[a_1 a_0]_{10}$ durch 4 teilbar ist.*

Nun betrachten wir eine andere, aber konkrete Frage, um zu zeigen, wie die Kongruenzarithmetik verwendet werden kann.

> Ist die Zahl 22051946 ein Quadrat?

Eine mögliche Lösung: Wäre 22051946 ein Quadrat, so gäbe es eine ganze Zahl x mit $x^2 = 22051946$. Wir untersuchen den Rest dieser Zahl bei Division durch 4.

Nach dem obigen Satz genügt es, die letzten zwei Ziffern zu betrachten:

$$22051946 \equiv 46 \mod 4.$$

Da $46 = 4 \cdot 11 + 2$, ergibt sich:

$$22051946 \equiv 2 \mod 4.$$

Um daraus zu schließen, dass 22051946 kein Quadrat ist, verwenden wir folgenden Satz:

Satz 9.2.3. *Für jede ganze Zahl x ist der Rest von x^2 bei Division durch 4 entweder 0 oder 1:*

$$x^2 \equiv 0 \mod 4 \quad \textit{oder } x^2 \equiv 1 \mod 4.$$

Da $22051946 \equiv 2 \mod 4$ gilt, folgt daraus, dass diese Zahl kein Quadrat sein kann.

Beweis. Der Rest von x bei Division durch 4 kann nur 0, 1, 2 oder 3 sein. Wir prüfen jeweils x^2 in diesen Fällen:

- Wenn $x \equiv 0 \mod 4$, dann $x^2 \equiv 0 \mod 4$ (da $0 \cdot 0 \equiv 0 \mod 4$).
- Wenn $x \equiv 1 \mod 4$, dann $x^2 \equiv 1 \mod 4$ (da $1 \cdot 1 \equiv 1 \mod 4$).
- Wenn $x \equiv 2 \mod 4$, dann $x^2 \equiv 0 \mod 4$ (da $2 \cdot 2 \equiv 0 \mod 4$).
- Wenn $x \equiv 3 \mod 4$, dann $x^2 \equiv 1 \mod 4$ (da $3 \cdot 3 \equiv 1 \mod 4$).

□

An dieser Stelle erinnern wir uns an die Definition der Menge der Restklassen modulo n:

$$\mathbb{Z}/n\mathbb{Z} := \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}.$$

Diese Menge ist mit einer natürlichen Abbildung $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ versehen und besitzt eine wohldefinierte Addition und Multiplikation. Man nennt $\mathbb{Z}/n\mathbb{Z}$ den Restklassenring modulo n.

Mit dieser Struktur lässt sich der obige Beweis auch eleganter formulieren: Sei $y \in \mathbb{Z}/4\mathbb{Z}$ der Rest von x bei Division durch 4. Dann betrachten wir die möglichen Werte von y^2 in diesem Ring:

- $\overline{0}^2 = \overline{0}$
- $\overline{1}^2 = \overline{1}$
- $\overline{2}^2 = \overline{0}$
- $\overline{3}^2 = \overline{1}$

Also kann ein Quadrat modulo 4 nur den Rest $\overline{0}$ oder $\overline{1}$ haben — nicht jedoch $\overline{2}$. Daher ist 22051946 kein Quadrat.

Im Restklassenring gibt es nicht nur Addition und Multiplikation, aber auch Subtraktion. Um $\overline{a} - \overline{b}$ in $\mathbb{Z}/n\mathbb{Z}$ zu berechnen, können wir einfach den Rest von $a - b$ bei Division durch n bestimmen. Es gilt also:

$$\overline{a} - \overline{b} = \overline{(a-b) \mod n}.$$

Beispiele:

$$\text{in } \mathbb{Z}/10\mathbb{Z}: \quad \overline{0} - \overline{1} = \overline{9}$$
$$\text{in } \mathbb{Z}/12\mathbb{Z}: \quad \overline{5} - \overline{7} = \overline{10}$$

Die Subtraktion ist keine "neue" Operation im Restklassenring, sondern sie ergibt sich aus der Addition. Für zwei Elemente $x, y \in \mathbb{Z}/n\mathbb{Z}$ gibt es ein eindeutiges Element z mit $z + y = x$. Dieses Element z ist dann die Differenz $x - y$, da gilt: $(x - y) + y = x$.

Satz 9.2.4 (Quersummeregel)**.** *Die Zahl mit Dezimaldarstellung $[a_n a_{n-1} \cdots a_0]_{10}$ hat denselben Rest bei Divison durch 3 wie die Zahl $a_n + a_{n-1} + \ldots + a_1 + a_0$ (auch* **Quersumme** *genannt).*

Insbesondere, ist die Zahl $[a_n a_{n-1} \cdots a_0]_{10}$ genau dann durch 3 teilbar, wenn die Quersumme $a_n + a_{n-1} + \ldots + a_1 + a_0$ durch 3 teilbar ist.

Beispiele:

(1) Für die Zahl $123 = [123]_{10}$ ist die Quersumme $1 + 2 + 3 = 6$, also:
$$123 \equiv 6 \mod 3 \Rightarrow 123 \equiv 0 \mod 3.$$

(2) Für die Zahl 2026 ist die Quersumme $2 + 0 + 2 + 6 = 10$:
$$2026 \equiv 10 \mod 3 \Rightarrow 2026 \equiv 1 \mod 3.$$

Beweis. Die Zahl $[a_n a_{n-1} \cdots a_0]_{10}$ ist nichts anderes als die Summe $a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \ldots + a_1 \cdot 10 + a_0$. Wir interessieren uns für den Rest dieser Zahl bei Division durch 3. Dazu bietet sich die Anwendung der Rechenregeln der Kongruenzrechnung an.

Betrachten wir zunächst einen Summanden der Form $x \cdot 10^k$. Da $10 = 3 \cdot 3 + 1$, gilt:

$$10 \equiv 1 \mod 3.$$

Diese Kongruenz können wir mit sich selbst multiplizieren:

$$10 \cdot 10 \equiv 1 \cdot 1 \mod 3,$$

und tatsächlich können wir dies k-mal wiederholen:

$$10^k \equiv 1 \mod 3.$$

Natürlich ist dies nicht der einzige Weg, um die Aussage "10^k hat den Rest 1 bei Division durch 3" zu beweisen. Man kann auch beobachten, dass $10^k - 1$ eine Zahl mit Dezimaldarstellung $[999\ldots9]_{10}$ ist und somit durch 3 teilbar:

$$[9999\ldots9]_{10} = 3 \cdot [3333\ldots3]_{10}.$$

Multiplizieren wir nun die letzte Kongruenz mit x, ergibt sich:

$$x \cdot 10^k \equiv x \mod 3.$$

Insbesondere gilt für die Summanden $a_k \cdot 10^k$:

$$a_k \cdot 10^k \equiv a_k \mod 3.$$

Summieren wir diese Kongruenzen für $k = 0, 1, \ldots, n$, ergibt sich die Behauptung des Satzes:

$$a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \ldots + a_1 \cdot 10 + a_0 \equiv a_n + a_{n-1} + \ldots + a_1 + a_0 \mod 3.$$

□

9.3. **Affine Chiffre.** Das nächste Thema auf unserer kleinen Reise durch die Kongruenzarithmetik sind Verschlüsselungsverfahren. Tatsächlich wurde die Kongruenzarithmetik schon vor Tausenden von Jahren für diesen Zweck eingesetzt.

9.3.1. *Caesar-Verschlüsselung.* Das einfachste Beispiel ist die *Caesar-Verschlüsselung* (auch *Caesar-Chiffre* genannt). Dabei wird eine Zuordnung zwischen den Buchstaben des lateinischen Alphabets und Zahlen hergestellt – genauer gesagt: zu Restklassen modulo 26:

$$A \mapsto \overline{0}, \quad B \mapsto \overline{1}, \quad \ldots, \quad Z \mapsto \overline{25}.$$

Wenn wir diese Zuordnung als Tabelle darstellen, erhalten wir:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{12}$	$\overline{13}$	$\overline{14}$	$\overline{15}$	$\overline{16}$	$\overline{17}$	$\overline{18}$	$\overline{19}$	$\overline{20}$	$\overline{21}$	$\overline{22}$	$\overline{23}$	$\overline{24}$	$\overline{25}$

In mathematischer Sprache konstruieren wir hier eine bijektive Abbildung zwischen der Menge der Buchstaben und der Menge $\mathbb{Z}/26\mathbb{Z}$.

Statt Buchstaben verwenden wir also die entsprechenden Restklassen:

$$HALLO \longrightarrow \overline{7}\,\overline{0}\,\overline{11}\,\overline{11}\,\overline{14}$$

In diesem Schritt handelt es sich lediglich um eine *Substitution*; es ist dafür nicht notwendig, die Symbole $\overline{0}$, $\overline{1}$ usw. als Elemente eines Rings zu betrachten. Gaius Iulius Caesar ging jedoch weiter: Er verschob die Buchstaben zyklisch um 3 Stellen nach rechts. In der Kongruenzarithmetik entspricht das einer Addition von $\overline{3}$:

$$HALLO \longrightarrow \overline{7}\,\overline{0}\,\overline{11}\,\overline{11}\,\overline{14} \xrightarrow{+\overline{3}} \overline{10}\,\overline{3}\,\overline{14}\,\overline{14}\,\overline{17} \longrightarrow KDOOR$$

Wir fassen die Caesar-Verschlüsselung zusammen:

Die Caesar-Verschlüsselung.
*Schritt 1.*Die Buchstaben der Nachricht in Restklassen umwandeln.
Schritt 2. Die Restklassen jeweils mit $\overline{3}$ addieren.
Schritt 3. Die resultierenden Restklassen wieder in Buchstaben zurückverwandeln.

Die erste Frage bei jedem Verschlüsselungsverfahren lautet: Lässt sich die verschlüsselte Nachricht eindeutig entschlüsseln? Und wenn ja – wie?

Im Fall der Caesar-Chiffre ist die Antwort einfach: Wenn wir eine Nachricht **entschlüsseln** möchten, schieben wir die Buchstaben um 3 Stellen nach links – oder rechnen mit $-\overline{3}$ in $\mathbb{Z}/26\mathbb{Z}$.

Beispiel von Entschlüsselung.

$$KDOOR \longrightarrow \overline{10}\,\overline{3}\,\overline{14}\,\overline{14}\,\overline{17} \xrightarrow{-\overline{3}} \overline{7}\,\overline{0}\,\overline{11}\,\overline{11}\,\overline{14} \longrightarrow HALLO$$

Die Zahl 3 bei diesem Vefahren muss natürlich nicht fest sein – man kann jede beliebige Restklasse $\overline{n}$ in $\mathbb{Z}/26\mathbb{Z}$ verwenden. So erhält man eine Verschlüsselung von Caesar-Art.

9.3.2. *Multiplikation statt Addition: affine Chiffre.* Wir haben bisher nur Addition mit Restklassen verwendet. Was aber, wenn wir stattdessen die Multiplikation benutzen?

Ein dummes Beispiel ist die Multiplikation mit $\overline{0}$: Dann wird jede Restklasse auf $\overline{0}$ abgebildet, und alle Buchstaben werden in denselben Buchstaben A verschlüsselt. Das ist natürlich keine sinnvolle Verschlüsselung.

Das Problem bei der Verschlüsselung tritt eigentlich nur bei der Multiplikation mit $\overline{0}$, $\overline{2}$ oder $\overline{13}$ auf, wie wir uns beim nächsten Mal genauer ansehen werden.

Wenn wir hingegen die Multiplikation mit $\overline{3}$ verwenden, funktioniert die Verschlüsselung wie folgt:

$$HALLO \longrightarrow \overline{7}\,\overline{0}\,\overline{11}\,\overline{11}\,\overline{14} \xrightarrow{\cdot\overline{3}} \overline{21}\,\overline{0}\,\overline{7}\,\overline{7}\,\overline{16} \longrightarrow VAHHQ$$

Wir können beide Methoden, die Addition wie bei der Caesar-Verschlüsselung und die Multiplikation, zusammen verwenden. Somit erhalten wir eine sogenannte affine Chiffre.

Die affine Chiffre.
Dieses Verschlüsselungsverfahren hat zwei Parameter: a und b aus $\mathbb{Z}/26\mathbb{Z}$. Für jede gültige Wahl von a und b ergibt sich ein eigenes Verfahren.
Wähle $a, b \in \mathbb{Z}/26\mathbb{Z}$, wobei $a = \overline{k}$ mit $0 \leq k \leq 25$ eine ungerade Zahl, $k \neq 13$.
Schritt 1. Die Buchstaben der Nachricht in Restklassen umwandeln.
Schritt 2. Die Restklassen mit a multiplizieren.
Schritt 3. Die Restklassen mit b addieren.
Schritt 3. Die resultierenden Restklassen wieder in Buchstaben umwandeln.

Die Schritte 2 und 3 können zusammen als eine Operation beschrieben werden:

$$x \mapsto a \cdot x + b,$$

wobei $x \in \mathbb{Z}/26\mathbb{Z}$ eine Restklasse ist.

Beispiel. Seien $a = \overline{3}$, $b = \overline{1}$.

$$HALLO \longrightarrow \overline{7}\,\overline{0}\,\overline{11}\,\overline{11}\,\overline{14} \xrightarrow{\cdot\overline{3}} \overline{21}\,\overline{0}\,\overline{7}\,\overline{7}\,\overline{16} \xrightarrow{+\overline{1}} \overline{22}\,\overline{1}\,\overline{8}\,\overline{8}\,\overline{17} \longrightarrow WBIIR$$

Wir werden das nächste Mal erklären, warum die affine Chiffre mit $a \neq \overline{0}, \overline{2}, \overline{13}$ eindeutig entschlüsselbar ist. Für das Rechnen von Beispielen zur Verschlüsselung und Entschlüsselung ist dieser Nachweis jedoch nicht erforderlich!

Vorlesung 10

10.1. **Widerholung von Rechnen in Restklassenringen.**

Erinnern Sie sich daran, dass der Restklassenring $\mathbb{Z}/n\mathbb{Z}$ die Menge der Elemente $\overline{0}, \overline{1}, \ldots, \overline{n-1}$ ist, auf der Addition und Multiplikation wie folgt definiert sind:

$$\overline{a} + \overline{b} = \overline{(a+b) \mod n},$$
$$\overline{a} \cdot \overline{b} = \overline{(a \cdot b) \mod n},$$

wobei $(x \mod n)$ den Rest bei Division von x durch n bezeichnet.

Wir beginnen die heutige Vorlesung mit den folgenden Fragen, die eine Wiederholung der Rechnung in Restklassenringen darstellen:

- In $\mathbb{Z}/13\mathbb{Z}$: $\overline{2} \cdot \overline{7} + \overline{3} =$?
- In $\mathbb{Z}/26\mathbb{Z}$: $\overline{4} \cdot \overline{11} =$? $\quad \overline{5} \cdot \overline{21} =$?

  In einem Restklassenring zu multiplizieren, kann es hilfreich sein, die Kongruenzarithmetik zu verwenden. Hier gilt zum Beispiel:

  $$21 \equiv -5 \mod 26,$$

  woraus folgt:

  $$5 \cdot 21 \equiv 5 \cdot (-5) \mod 26.$$

  Da $-25 \equiv 1 \mod 26$, erhalten wir $5 \cdot 21 \equiv 1 \mod 26$, also ist $\overline{5} \cdot \overline{21} = \overline{1}$.
- Finden Sie ein x in $\mathbb{Z}/95\mathbb{Z}$ mit $x + \overline{5} = \overline{0}$.

10.2. **Affine Chiffre (Fortsetzung).**

Wir interessieren uns für eine Verschlüsselung, die mithilfe von Addition und Multiplikation in Restklassenringen beschrieben werden kann. Um diese Verschlüsselung auf natürliche Sprachen (z. B. Englisch) anzuwenden, verwenden wir die folgende Tabelle, die eine Zuordnung zwischen den Buchstaben des lateinischen Alphabets und Zahlen herstellt.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{12}$	$\overline{13}$	$\overline{14}$	$\overline{15}$	$\overline{16}$	$\overline{17}$	$\overline{18}$	$\overline{19}$	$\overline{20}$	$\overline{21}$	$\overline{22}$	$\overline{23}$	$\overline{24}$	$\overline{25}$

Die affine Chiffre. Dieses Verschlüsselungsverfahren hat zwei Parameter: a und b aus $\mathbb{Z}/26\mathbb{Z}$. Für jede gültige Wahl von a und b ergibt sich ein eigenes Verfahren.

Wähle $a, b \in \mathbb{Z}/26\mathbb{Z}$, wobei $a = \overline{k}$ mit $0 \leq k \leq 25$ eine ungerade Zahl, $k \neq 13$.
Schritt 1. Die Buchstaben der Nachricht in Restklassen umwandeln.
Schritt 2. Die Restklassen mit a multiplizieren.
Schritt 3. Die Restklassen mit b addieren.
Schritt 4. Die resultierenden Restklassen wieder in Buchstaben umwandeln.

Die Schritte 1 und 4 dienen nur dem Zweck, Nachrichten, die in Buchstaben geschrieben sind, verschlüsseln zu können. Für das Verständnis der Verschlüsselung und der entsprechenden Entschlüsselung sind sie nicht notwendig. Wir werden diese Schritte daher ab sofort ignorieren und stattdessen direkt über die Verschlüsselung von Restklassen sprechen.

Die affine Verschlüsselung erzeugt somit eine Permutation der Restklassen. Hier ein Beispiel.

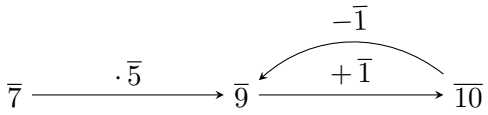
Beispiel 10.2.1. *Seien $a = \overline{5}$ und $b = \overline{1}$. Wir können die Verschlüsselung aller Restklassen durch die Schritte 2 und 3 berechnen:*

$$\overline{x} \longmapsto \overline{x} \cdot \overline{5} \longmapsto \overline{x} \cdot \overline{5} + \overline{1}$$

$$
\begin{array}{lll}
\overline{0} & \longmapsto & \overline{0} \longmapsto \overline{1} \\
\overline{1} & \longmapsto & \overline{5} \longmapsto \overline{6} \\
\overline{2} & \longmapsto & \overline{10} \longmapsto \overline{11} \\
\overline{3} & \longmapsto & \overline{15} \longmapsto \overline{16} \\
\overline{4} & \longmapsto & \overline{20} \longmapsto \overline{21} \\
\overline{5} & \longmapsto & \overline{25} \longmapsto \overline{0} \\
\overline{6} & \longmapsto & \overline{4} \longmapsto \overline{5} \\
\overline{7} & \longmapsto & \overline{9} \longmapsto \overline{10} \\
\overline{8} & \longmapsto & \overline{14} \longmapsto \overline{15} \\
\overline{9} & \longmapsto & \overline{19} \longmapsto \overline{20} \\
\overline{10} & \longmapsto & \overline{24} \longmapsto \overline{25} \\
\overline{11} & \longmapsto & \overline{3} \longmapsto \overline{4} \\
\overline{12} & \longmapsto & \overline{8} \longmapsto \overline{9} \\
\overline{13} & \longmapsto & \overline{13} \longmapsto \overline{14} \\
\overline{14} & \longmapsto & \overline{18} \longmapsto \overline{19} \\
\overline{15} & \longmapsto & \overline{23} \longmapsto \overline{24} \\
\overline{16} & \longmapsto & \overline{2} \longmapsto \overline{3} \\
\overline{17} & \longmapsto & \overline{7} \longmapsto \overline{8} \\
\overline{18} & \longmapsto & \overline{12} \longmapsto \overline{13} \\
\overline{19} & \longmapsto & \overline{17} \longmapsto \overline{18} \\
\overline{20} & \longmapsto & \overline{22} \longmapsto \overline{23} \\
\overline{21} & \longmapsto & \overline{1} \longmapsto \overline{2} \\
\overline{22} & \longmapsto & \overline{6} \longmapsto \overline{7} \\
\overline{23} & \longmapsto & \overline{11} \longmapsto \overline{12} \\
\overline{24} & \longmapsto & \overline{16} \longmapsto \overline{17} \\
\overline{25} & \longmapsto & \overline{21} \longmapsto \overline{22}
\end{array}
$$

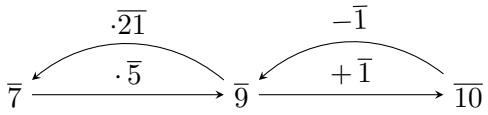
Wenn man die Ergebnisse dieser Verschlüsselung im obigen Beispiel genau betrachtet, kann man feststellen, dass kein Element des Restklassenrings in der rechten Spalte doppelt erscheint. Das bedeutet genau, dass diese Verschlüsselung im Prinzip entschlüsselbar ist: Für jedes verschlüsselte Element in $\mathbb{Z}/26\mathbb{Z}$ lässt sich ein eindeutiges ursprüngliches Element finden. Aber wie gelingt uns das? Und wie können wir das mithilfe der Kongruenzarithmetik durchführen?

Der erste Schritt besteht darin, mit einem Element aus $\mathbb{Z}/26\mathbb{Z}$ zu beginnen und das entsprechende Element in der mittleren Spalte zu ermitteln. Dies erreicht man durch Subtraktion von $b = \overline{1}$, zum Beispiel:



Der zweite Schritt besteht darin, das Element in der mittleren Spalte durch $\overline{5}$ zu "teilen". Ist das überhaupt möglich? Und wenn ja – wie?

Glücklicherweise haben wir bereits zuvor berechnet, dass $\overline{5} \cdot \overline{21} = \overline{1}$. Das bedeutet: Wenn wir eine Restklasse zuerst mit $\overline{5}$ und dann mit $\overline{21}$ multiplizieren, erhalten wir wieder die ursprüngliche Restklasse. In der Zeile mit $\overline{7}$ funktioniert das wie folgt:



Fazit. Um die affine Chiffre mit den Parametern a, b zu entschlüsseln, müssen wir eine Restklasse z finden, für die $a \cdot z = \overline{1}$ gilt.
Um eine verschlüsselte Restklasse y zu entschlüsseln, verwenden wir dann die folgende Formel:

$$y \mapsto z \cdot (y - b).$$

Beispiel 10.2.2. *Für $a = \overline{5}$ gilt $\overline{5} \cdot \overline{21} = \overline{1}$ und die Entschlüsselung der affinen Chiffre $x \mapsto \overline{5} \cdot x + \overline{1}$ kann mit der Formel $y \mapsto \overline{21} \cdot (y - \overline{1})$ erledigt werden.*

Da das Element z mit der Eigenschaft $a \cdot z = \overline{1}$ eine zentrale Rolle spielt, führen wir für solche Elemente eine Bezeichnung ein und definieren den Begriff des Inversen.

Definition 10.2.3. *Sei n eine positive natürliche Zahl und $a \in \mathbb{Z}/n\mathbb{Z}$.*
Ein Element $z \in \mathbb{Z}/n\mathbb{Z}$ heißt invers zu a (bezüglich der Multiplikation), *wenn $a \cdot z = \overline{1}$ gilt. Besitzt ein Element ein solches Inverses, so nennt man es* invertierbar.

Beispiel 10.2.4.

- *$\overline{5}$ in $\mathbb{Z}/26\mathbb{Z}$ ist invertierbar mit dem Inversen Element $\overline{21}$.*
- *$\overline{5}$ in $\mathbb{Z}/10\mathbb{Z}$ ist nicht invertierbar: Angenommen, es gäbe ein x mit $x \cdot \overline{5} = \overline{1}$. Multiplizieren wir diese Gleichung mit $\overline{2}$, so ergibt sich:*
$$x \cdot \overline{5} \cdot \overline{2} = \overline{1} \cdot \overline{2} \quad \Rightarrow \quad \overline{0} = \overline{2},$$
da $\overline{5} \cdot \overline{2} = \overline{0}$ in $\mathbb{Z}/10\mathbb{Z}$. Dies ist ein Widerspruch.
- *$\overline{1}$ in $\mathbb{Z}/n\mathbb{Z}$ ist für alle $n > 1$ invertierbar mit dem inversen Element $\overline{1}$, denn $\overline{1} \cdot \overline{1} = \overline{1}$.*
- *$\overline{0}$ in $\mathbb{Z}/n\mathbb{Z}$ ist für alle $n > 0$ nicht invertierbar, da $\overline{0} \cdot x = \overline{0}$ für alle $x \in \mathbb{Z}/n\mathbb{Z}$.*

Für die Entschlüsselung affiner Chiffren ist es daher entscheidend zu verstehen, welche Elemente $a \in \mathbb{Z}/26\mathbb{Z}$ invertierbar sind. Diese Frage lässt sich im Allgemeinen für beliebige Restklassenringe beantworten:

Satz 10.2.5. *Sei n eine positive natürliche Zahl und m eine natücliche Zahl mit $0 < m < n$.*
Dann ist das Element $\overline{m} \in \mathbb{Z}/n\mathbb{Z}$ genau dann invertierbar, wenn m und n teilerfremd sind.
Anders gesagt: Ein Element $z \in \mathbb{Z}/n\mathbb{Z}$ mit $z \cdot \overline{m} = \overline{1}$ existiert genau dann, wenn $ggT(m, n) = 1$.

Beispiel 10.2.6. *Im Restklassenring $\mathbb{Z}/26\mathbb{Z}$ besitzt ein Element $\overline{m}$ genau dann ein Inverses, wenn m weder durch 2 noch durch 13 teilbar ist, also $ggT(m, 26) = 1$.*

Eine interessante Folgerung dieses Satzes ist die Existenz von inversen Elementen in $\mathbb{Z}/p\mathbb{Z}$, wenn p eine Primzahl ist.

Corollary 10.2.7. *Sei p eine Primzahl. Dann besitzt jedes von $\overline{0}$ verschiedene Element in $\mathbb{Z}/p\mathbb{Z}$ ein multiplikatives Inverses.*

Beweis der Folgerung. Für jedes m mit $0 < m < p$ gilt $\mathrm{ggT}(m, p) = 1$, da p eine Primzahl ist. Nach dem obigen Satz existiert daher ein $z \in \mathbb{Z}/p\mathbb{Z}$ mit $z \cdot \overline{m} = \overline{1}$. Da $\mathbb{Z}/p\mathbb{Z}$ die Elemente $\overline{0}, \overline{1}, \ldots, \overline{p-1}$ enthält, sind also alle Elemente außer $\overline{0}$ invertierbar. □

Beweis des Satzes. Wir untersuchen, wann die Gleichung
$$\overline{x} \cdot \overline{m} = \overline{1}$$
in $\mathbb{Z}/n\mathbb{Z}$ eine Lösung besitzt. Da $\overline{x} \cdot \overline{m} = \overline{x \cdot m \bmod n}$, suchen wir also ein x mit
$$x \cdot m \equiv 1 \mod n,$$
also eine Lösung der Gleichung
$$x \cdot m = y \cdot n + 1$$
für geeignete ganze Zahlen x, y.

Wir möchten herausfinden, wenn die Gleichung in $\mathbb{Z}/n\mathbb{Z}$
$$\overline{x} \cdot \overline{m} = \overline{1}$$
eine Lösung mit $x : 0 \leq x < n$ hat. Da $\overline{x} \cdot \overline{m}$ nach der Definition gleich $\overline{x \cdot m \mod n}$ gleich ist, müssen wir x finden, sodass der Rest von $x \cdot m$ bei Division durch n gleich 1 ist. Das heißt:
$$x \cdot m = y \cdot n + 1.$$

Wir erkennen diese Gleichung an: Dies ist eine sogenannte diophantische Gleichung, die wir lösen können, wenn und nur wenn $\mathrm{ggT}(m, n) = 1$.

Fall 1: $\mathrm{ggT}(m, n) = 1$.

Dann existieren ganze Zahlen x, y' mit
$$x \cdot m + y' \cdot n = 1.$$

Dies bedeutet

$$x \cdot m = -y' \cdot n + 1,$$

also wie gewünscht:

$$x \cdot m \equiv 1 \mod n.$$

Falls x nicht im Bereich $0 \leq x < n$ liegt, nehmen wir den Rest x' von x bei Division durch n, also $x = z \cdot n + x'$ mit $0 \leq x' < n$. Dann ist

$$x' \cdot m = (x - z \cdot n) \cdot m = x \cdot m - z \cdot m \cdot n = (-y') \cdot n + 1 - z \cdot m \cdot n.$$

Da beide zusätzlichen Terme Vielfache von n sind, bleibt $x' \cdot m \equiv 1 \pmod{n}$. Also ist $\overline{x'} \cdot \overline{m} = \overline{1}$ in $\mathbb{Z}/n\mathbb{Z}$.

Den **Fall 2** – $\mathrm{ggT}(m, n) = k \neq 1$ – betrachten wir bei nächster Sitzung. □

Beispiel 10.2.8. *Der Beweis liefert nicht nur eine theoretische Aussage über die Existenz von Inversen, sondern erlaubt uns auch, diese konkret zu berechnen.*

Betrachten wir den Ring $\mathbb{Z}/21\mathbb{Z}$. Ein Element $\overline{m}$ ist genau dann invertierbar, wenn $ggT(m, 21) = 1$. Da $21 = 3 \cdot 7$, ist z. B. $m = 8$ teilerfremd zu 21, weil 8 durch 3 oder 7 nicht teilbar ist.

Wir suchen also x mit:

$$\overline{x} \cdot \overline{8} = \overline{1} \quad \text{in } \mathbb{Z}/21\mathbb{Z}.$$

Das entspricht der diophantischen Gleichung:

$$8 \cdot x + 21 \cdot y = 1.$$

Der erweiterte Euklidische Algorithmus liefert die Lösung $x = 8$, $y = -3$. Da der Rest von x bei Division durch 21 gleich 8 ist, erhalten wir:

$$\overline{8} \cdot \overline{8} = \overline{1} \quad \text{in } \mathbb{Z}/21\mathbb{Z}.$$

Also ist $\overline{8}$ sein eigenes Inverses.

Vorlesung 11

11.1. **Invertierbare Elemente in Restklassenringen.**

Erinnern Sie sich daran, dass Element x der Restklassenring $\mathbb{Z}/n\mathbb{Z}$ **invertierbar** heißt, wenn es Element $y \in \mathbb{Z}/n\mathbb{Z}$ mit $x \cdot y = \overline{1}$ gibt. Das Element y heißt **invers** zu x. Man sagt auch, dass y **das Inverse** von x ist.

Beispiel 11.1.1. *In $\mathbb{Z}/17\mathbb{Z}$ gilt es:*

$$\overline{4} \cdot \overline{13} = \overline{1},$$

und $\overline{13}$ ist invers zu $\overline{4}$ (und $\overline{4}$ ist invers zu $\overline{13}$).

Wir haben in der letzten Sitzung den folgenden Satz teilweise bewiesen:

Satz 11.1.2. *Sei n eine positive natürliche Zahl und m eine natürliche Zahl mit $0 < m < n$.*
Dann ist das Element $\overline{m} \in \mathbb{Z}/n\mathbb{Z}$ genau dann invertierbar, wenn m und n teilerfremd sind.
Anders gesagt: Ein Element $y \in \mathbb{Z}/n\mathbb{Z}$ mit $y \cdot \overline{m} = \overline{1}$ existiert genau dann, wenn $ggT(m, n) = 1$.

Fortsetzung des Beweises. **Fall 2.** Sei m mit $\mathrm{ggT}(m, n) = k \neq 1$. Wir müssen zeigen, dass $\overline{m}$ nicht invertierbar ist.

Dann gibt es natürliche Zahlen r, ℓ mit $m = k \cdot r$, $n = k \cdot \ell$ und $r, \ell < n$. Betrachte dann:

$$\overline{m} \cdot \overline{\ell} = \overline{k \cdot r} \cdot \overline{\ell} = \overline{k \cdot r \cdot \ell} = \overline{r \cdot n} = \overline{0}.$$

Nehmen wir nun an, $\overline{m}$ sei invertierbar, es gäbe also $z \in \mathbb{Z}/n\mathbb{Z}$ mit $z \cdot \overline{m} = \overline{1}$. Multiplizieren wir beide Seiten dieser Gleichung mit $\overline{\ell}$:

$$z \cdot \overline{m} \cdot \overline{\ell} = \overline{\ell},$$

aber links steht $\overline{0}$, denn $\overline{m} \cdot \overline{\ell} = \overline{0}$. Also gilt $\overline{\ell} = \overline{0}$ — ein Widerspruch. Folglich ist $\overline{m}$ nicht invertierbar. □

Beispiel 11.1.3. *Sei $n = 26$. Dann sind die Elemente $\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}, \overline{12}, \overline{13}, \overline{14}, \overline{16}, \overline{18}, \overline{20}, \overline{22}, \overline{24}$ in $\mathbb{Z}/26\mathbb{Z}$ nicht invertierbar.*

Die inverse Elemente ermöglichen es uns, die lineare Gleichungen in Restklassenringen zu lösen.

Beispiel 11.1.4. *Finden Sie alle Lösungen der Gleichung*

$$\overline{5} \cdot x + \overline{2} = \overline{0},$$

wobei $\overline{5}, \overline{2}, \overline{0}, x$ Elemente des Restklassenrings $\mathbb{Z}/17\mathbb{Z}$ sind.

Wir bestimmen zunächst das inverse Element zu $\overline{5}$. Dazu suchen wir ein $z \in \mathbb{Z}/17\mathbb{Z}$ mit $\overline{5} \cdot z = \overline{1}$. Dies entspricht (s. Vorlesung 10) der ganzzahligen Gleichung

$$5 \cdot x = 1 + 17y,$$

also einer linearen Diophantischen Gleichung in den Unbekannten x, y. Wir wenden den Euklidischen Algorithmus an:

$$17 = 3 \cdot 5 + 25 = 2 \cdot 2 + 1,$$

Rückwärtseinsetzen ergibt:

$$1 = 5 - 2 \cdot 2 = 5 - 2 \cdot (17 - 3 \cdot 5) = 7 \cdot 5 - 2 \cdot 17.$$

Nun können wir die Reste aller Zahlen bei Division durch 17 in der letzten Gleichung betrachten und erhalten damit:

$$\overline{1} = \overline{7} \cdot \overline{5}.$$

Das heißt, $\overline{7}$ ist das Inverse von $\overline{5}$ ist.

Wir kehren zur ursprunglichen Gleichung $\overline{5} \cdot x + \overline{2} = \overline{0}$ zurück. Multiplizieren wir beide Seiten mit $\overline{7}$:

$$\overline{7}(\overline{5} \cdot x + \overline{2}) = \overline{7} \cdot \overline{07} \cdot \overline{5} \cdot x + \overline{7} \cdot \overline{2} = \overline{01} \cdot x + \overline{14} = \overline{0}x + \overline{14} = \overline{0}$$

Da $-\overline{14} = \overline{3}$, erhalten wir die Lösung dieser Gleichung: $x = \overline{3}$.

Man muss sich fragen, warum wir alle Lösungen gefunden haben!

Fazit. Seien $a, b \in \mathbb{Z}/n\mathbb{Z}$, wobei a invertierbar ist.
Um die Gleichung

$$a \cdot x + b = 0$$

zu lösen, bestimmt man zunächst das Inverse zu a – sei es z.
Dann lautet die Lösung der Gleichung:

$$x = -z \cdot b.$$

11.2. **Eulersche ϕ-Funktion.**

Die nächste Frage, die man zu inversen Elementen stellen kann, lautet:

Wie viele invertierbare Elemente gibt es in $\mathbb{Z}/n\mathbb{Z}$?

Da wir die invertierbaren Elemente im obigen Satz bereits beschrieben haben, ist die Antwort auf diese Frage: Es sind genau die Zahlen m mit $0 \leq m < n$, die teilerfremd zu n sind. Die Anzahl dieser Zahlen bezeichnet man mit $\phi(n)$; dabei steht ϕ für die sogenannte *Eulersche ϕ-Funktion*.

Beispiel 11.2.1.

(1) $\phi(26) = 12$.
Um $\phi(26)$ zu berechnen, zählt man einfach die Zahlen m mit $0 < m < 26$, die zu 26 teilerfremd sind.
Da $26 = 2 \cdot 13$, können wir aus der Liste $0, 1, 2, \ldots, 25$ die Zahlen streichen, die durch 2 oder durch 13 teilbar sind. Durch 13 ist in dieser Liste nur die Zahl 13 teilbar, und durch 2 sind alle geraden Zahlen: $0, 2, \ldots, 24$, es gibt genau 13 davon.
Es bleiben also $26 - 13 - 1 = 12$ Zahlen übrig.

(2) $\phi(4) = 2$.
Die Zahlen 1 und 3 sind teilerfremd zu 4, aber $ggT(2, 4) = 2 \neq 1$. Es gibt also genau 2 Zahlen m mit $0 \leq m < 4$, die zu 4 teilerfremd sind. Daher ist $\phi(4) = 2$.

Satz 11.2.2. *Sei p eine Primzahl.*

(1) $\phi(p) = p - 1$;
(2) $\phi(p^k) = p^k - p^{k-1}$.

Beweis.

(1) Die Primzahl p hat nur zwei Teiler: 1 und p. Für jede ganze Zahl m ist also $\mathrm{ggT}(m, p)$ entweder 1 oder p. Aber $\mathrm{ggT}(m, p) = p$ bedeutet, dass m durch p teilbar ist, also ein Vielfaches von p. Keine Zahl m mit $0 < m < p$ kann durch p teilbar sein, daher sind sie alle zu p teilerfremd.

Das heißt: $\overline{1}, \ldots, \overline{p-1}$ sind die invertierbaren Elemente des Restklassenrings $\mathbb{Z}/p\mathbb{Z}$, und es gibt genau $p - 1$ davon.

(2) Die Zahl p^k hat als Teiler: $1, p, p^2, \ldots, p^{k-1}, p^k$. Für jede ganze Zahl m ist also $\mathrm{ggT}(m, p^k)$ einer dieser Werte.

Wenn m durch p teilbar ist, dann ist $\mathrm{ggT}(m, p^k) \geq p$, und m und p^k sind nicht teilerfremd. Wenn m nicht durch p teilbar ist, dann ist m auch durch kein p^s teilbar (für $s > 0$), also ist $\mathrm{ggT}(m, p^k) = 1$.

Die Zahlen m mit $0 < m < p^k$, die zu p^k teilerfremd sind, sind also genau die Zahlen, die nicht durch p teilbar sind. Um $\phi(p^k)$ zu berechnen, zählen wir diese Zahlen.

Es ist einfacher, zuerst die Zahlen zu zählen, die durch p teilbar sind. Diese sind genau die Vielfachen von p in der Liste

$$0, p, 2p, 3p, \ldots$$

Wie viele davon liegen zwischen 0 und $p^k - 1$? Die letzte Zahl dieser Form, die noch kleiner als p^k ist, ist $(p^{k-1} - 1) \cdot p$. Das nächste Vielfache von p wäre $p^{k-1} \cdot p = p^k$ und fällt schon raus. Wenn wir die Vielfache, die kleiner als p^k sind, nummerieren – 0 als "nullte", $1 \cdot p$ als die erste, $2 \cdot p$ als die zweite, usw. – gibt es die Nummern von 0 bis zu $p^{k-1} - 1$. Also gibt es p^{k-1} Vielfache von p mit $0 \leq m < p^k$.

Die Anzahl von m mit $0 \leq m < p^k$ und $\mathrm{ggT}(m, p^k) = 1$ kann also als die Differenz von der Anzahl aller Zahlen m mit $0 \leq m < p^k$ (es gibt genau p^k davon) und die Anzahl der Vielfache von p (es gibt genau p^{k-1} davon) berechnet werden.

Daher gilt:

$$\phi(p^k) = p^k - p^{k-1}.$$

□

11.3. **Der Satz von Euler.** In zukünftigen Vorlesungen werden wir eine einfache Methode kennenlernen, mit der sich $\phi(n)$ anhand der Primfaktorzerlegung von n berechnen lässt. Schon jetzt erkennen wir jedoch, welche zentralle Rolle die Zahl $\phi(n)$ für die invertierbare Elemente spielt.

Satz 11.3.1 (Satz von Euler)**.** *Sei x ein invertierbares Element des Restklassenrings $\mathbb{Z}/n\mathbb{Z}$, und sei $\phi(n)$ die Anzahl aller invertierbaren Elementen in $\mathbb{Z}/n\mathbb{Z}$.*

Dann gilt:

$$x^{\phi(n)} = \overline{1}.$$

Beispiel 11.3.2. *Sei $n = 4$, dann ist $\phi(4) = 2$, und die invertierbaren Elemente von $\mathbb{Z}/4\mathbb{Z}$ sind $\overline{1}, \overline{3}$.*

Es gilt $\overline{3}^2 = \overline{1}$ (und natürlich auch $\overline{1}^2 = \overline{1}$).

Beispiel 11.3.3 (Der kleine Satz von Fermat)**.** *Sei p eine Primzahl. Dann ist $\phi(p) = p - 1$, und alle Elemente außer $\overline{0}$ in $\mathbb{Z}/p\mathbb{Z}$ sind invertierbar.*

Für jedes $a \in \mathbb{Z}/p\mathbb{Z}$, $a \neq \overline{0}$, gilt:

$$a^{p-1} = \overline{1}.$$

Vorlesung 12

12.1. **Potenzen von Elementen in Restklassenringen.**

Was sind die Potenzen des Elements $\overline{2}$ im Restklassenring $\mathbb{Z}/5\mathbb{Z}$, also

$$\overline{2}^2 = \overline{4}, \quad \overline{2}^3 = \overline{3}, \quad \overline{2}^4 = \overline{1}, \quad \overline{2}^5 = \overline{2}, \quad \overline{2}^6 = \overline{4} \ldots$$

Und was sind die Potenzen von $\overline{4}$ in $\mathbb{Z}/5\mathbb{Z}$?

$$\overline{4}^2 = \overline{1}, \quad \overline{4}^3 = \overline{4}, \quad \overline{4}^4 = \overline{4}, \quad \ldots$$

Man kann hier zwei interessante Bemerkungen machen. Die erste ist, dass für ein Element $x \in \mathbb{Z}/n\mathbb{Z}$ die Folge $x, x^2, x^3, \ldots, x^k, \ldots$ nicht unendlich viele verschiedene Werte annimmt, sondern sich wiederholt. Die zweite: Es gibt eine natürliche Zahl k, sodass $x^k = \overline{1}$.

Können wir diese Bermerkungen im Allgemeinen beweisen?

Lemma 12.1.1. *Sei $x \in \mathbb{Z}/n\mathbb{Z}$.*
Dann existieren verschiedene natürliche Zahlen k, m, sodass $x^k = x^m$.

Beweis. Die Menge der Potenzen $x, x^2, x^3, \ldots$ scheint unendlich zu sein, aber alle diese Elemente liegen in $\mathbb{Z}/n\mathbb{Z}$, das nur endlich viele Elemente besitzt (genau n).

Da es nur endlich viele verschiedene Elemente in $\mathbb{Z}/n\mathbb{Z}$ gibt, müssen sich in der Folge $x, x^2, x^3, \ldots$ irgendwann Wiederholungen ergeben. □

Um die zweite Bemerkung näher zu betrachten, berechnen wir ein weiteres Beispiel.

Beispiel 12.1.2. *Was sind die Potenzen von $\overline{2}$ in $\mathbb{Z}/6\mathbb{Z}$?*

$$\overline{2}^2 = \overline{4}, \quad \overline{2}^3 = \overline{2}, \quad \overline{2}^4 = \overline{4}, \quad \overline{2}^5 = \overline{2}, \quad \ldots$$

Wir sehen also, dass es für $\overline{2}$ keine natürliche Zahl m gibt, sodass $\overline{2}^m = \overline{1}$. Der Grund dafür ist, dass $\overline{2}$ in $\mathbb{Z}/6\mathbb{Z}$ nicht invertierbar ist.

> **Erinnerung.** Sei n eine positive natürliche Zahl.
> Ein Element $x \in \mathbb{Z}/n\mathbb{Z}$ heißt **invertierbar**, wenn es y gibt mit $x \cdot y = \overline{1}$.

Tatsächlich, wäre $\overline{2}^m = \overline{1}$, dann würde

$$\overline{2} \cdot (\overline{2})^{m-1} = \overline{1}$$

gelten. Also wäre $\overline{2}$ invertierbar. Aber sie ist nicht: Wenn wir die Gleichung $\overline{2} \cdot z = \overline{1}$ mit $\overline{3}$ multiplizieren, ergibt sich:

$$\overline{0} = \overline{3},$$

was zum Widerspruch führt.

Lemma 12.1.3. *Sei $x \in \mathbb{Z}/n\mathbb{Z}$ ein nicht-invertierbares Element. Dann gilt $x^k \neq \overline{1}$ für jedes k.*

Beweis durch Widerspruch. Angenommen, es existiert ein k, sodass $x^k = \overline{1}$ gilt. Wir schreiben diese Gleichung um:

$$x \cdot x^{k-1} = \overline{1}.$$

Das heißt, x^{k-1} ist das Inverse von x, und x wäre invertierbar – im Widerspruch zur Annahme des Lemmas. □

Sei nun x ein invertierbares Element in $\mathbb{Z}/n\mathbb{Z}$. Sind alle Elemente in der Folge $x, x^2, x^3, \ldots$ ebenfalls invertierbar?

Lemma 12.1.4. *Seien x_1, x_2 invertierbare Elemente des Restklassenrings $\mathbb{Z}/n\mathbb{Z}$. Dann ist $x_1 \cdot x_2$ auch invertierbar.*

Wenn y_1 das Inverse von x_1 und y_2 das Inverse von x_2 ist, dann ist $y_1 \cdot y_2$ das Inverse von $x_1 \cdot x_2$.

Beweis. Da $x_1 \cdot y_1 = \overline{1}$ und $x_2 \cdot y_2 = \overline{1}$ gilt, können wir beide Gleichungen multiplizieren und erhalten:

$$(x_1 \cdot x_2) \cdot (y_1 \cdot y_2) = \overline{1}.$$

Somit ist $y_1 \cdot y_2$ ein Inverses zu $x_1 \cdot x_2$. □

Corollary 12.1.5. *Sei x ein invertierbares Element des Restklassenrings $\mathbb{Z}/n\mathbb{Z}$. Dann gilt:*

(1) *Für jede positive ganze Zahl $k > 0$ ist auch x^k invertierbar.*
(2) *Es existiert eine positive ganze Zahl $m > 0$ mit $x^m = \overline{1}$.*

Beweis. Sei x invertierbar in $\mathbb{Z}/n\mathbb{Z}$ und sei z das Inverse von x, also $z \cdot x = \overline{1}$. Dann gilt auch:

$$z^k \cdot x^k = (z \cdot x)^k = (\overline{1})^k = \overline{1},$$

womit z^k ein Inverses zu x^k ist. Also ist x^k für jedes $k > 0$ invertierbar und somit (1) bewiesen.

(2). Nach dem ersten Lemma existieren es natürliche Zahlen $k > m$ mit $x^k = x^m$. Multiplizieren wir beide Seiten dieser Gleichung mit z^k (dem Inversen von x^k), ergibt sich:

$$x^r \cdot z^k = x^k \cdot z^k \Longrightarrow x^{r-k} \cdot x^k \cdot z^k = x^k \cdot z^k \Longrightarrow x^{r-k} = \overline{1}.$$

Dabei haben wir verwendet, dass $x^k \cdot z^k = \overline{1}$.

Damit existiert also ein $s = r - k > 0$ mit $x^s = \overline{1}$. □

Wir sehen also: Für jedes invertierbare Element x in $\mathbb{Z}/n\mathbb{Z}$ existiert eine natürliche Zahl m, sodass $x^m = \overline{1}$.

Diese Zahl m kann von x abhängen, wir werden aber bald sehen, dass es eine Zahl $\phi(n)$ gibt, sodass die Gleichung

$$x^{\phi(n)} = \overline{1}$$

für alle invertierbaren x erfüllt ist.

12.2. **Die Eulersche Phi-Funktion (Erinnerung).**

Die Anzahl der invertierbaren Elemente in $\mathbb{Z}/n\mathbb{Z}$ wird als $\phi(n)$ bezeichnet,
und die Funktion $\phi(n)$ heißt die **Eulersche Phi-Funktion**.

Fragen zur Errinerung:

(1) Ist $\overline{1}$ ein invertierbares Element in $\mathbb{Z}/n\mathbb{Z}$? Was ist das Inverse zu $\overline{1}$?
Ja, $\overline{1}$ ist in $\mathbb{Z}/n\mathbb{Z}$ für jedes $n \geq 2$ invertierbar, denn $\overline{1} \cdot \overline{1} = \overline{1}$. Damit ist $\overline{1}$ sein eigenes Inverses.
(2) Welche Elemente sind in $\mathbb{Z}/6\mathbb{Z}$ invertierbar?
Die invertiebaren Elemente sind $\overline{1}$ und $\overline{5}$, und $\overline{5} \cdot \overline{5} = \overline{1}$, damit ist $\overline{5}$ sein eigenes Inverse. Da $\overline{2} \cdot \overline{3} = \overline{0}$ und $\overline{4} \cdot \overline{3}$ ebenfalls, sind die Elemente $\overline{2}, \overline{3}, \overline{4}$ nicht invertierbar (s. Vorlesung 11). Außerdem ist $\overline{0}$ in $\mathbb{Z}/n\mathbb{Z}$ für jedes $n \geq 2$ nicht invertierbar.
(3) Wie kann man entscheiden, ob $\overline{m}$ in $\mathbb{Z}/n\mathbb{Z}$ invertierbar ist?

Satz 12.2.1 (siehe Vorlesungen 10–11)**.** *Sei n eine positive natürliche Zahl und m eine natürliche Zahl mit $0 < m < n$.*
Dann ist das Element $\overline{m} \in \mathbb{Z}/n\mathbb{Z}$ genau dann invertierbar, wenn m und n teilerfremd sind.

Beispiel 12.2.2. *Sei $n = 6$. Dann ist $\phi(6) = 2$, da es genau zwei invertierbare Elemente in $\mathbb{Z}/6\mathbb{Z}$ gibt: $\overline{1}$ und $\overline{5}$.*

Beispiel 12.2.3 (s. Vorlesung 11)**.** *Sei p eine Primzahl. Dann gilt:*

(1) $\phi(p) = p - 1$;
Begründung: Da jede Zahl m mit $0 < m < p$ zu p teilerfremd ist, ist $\overline{m}$ in $\mathbb{Z}/p\mathbb{Z}$ invertierbar.
(2) $\phi(p^k) = p^k - p^{k-1}$.

12.3. **Der Satz von Euler (Fortsetzung).**

Satz 12.3.1 (Satz von Euler)**.** *Sei n eine natürliche Zahl.*
Erste Formulierung: Sei x ein invertierbares Element des Restklassenrings $\mathbb{Z}/n\mathbb{Z}$, und sei $\phi(n)$ die Anzahl aller invertierbaren Elementen in $\mathbb{Z}/n\mathbb{Z}$.
Dann gilt:

$$x^{\phi(n)} = \overline{1}.$$

Zweite Formulierung: Sei $m \in \mathbb{Z}$ eine Zahl, die zu n teilerfremd ist. Dann hat $m^{\phi(n)}$ den Rest 1 bei Division durch n.

Erinnerung: Die Notation

$$a \equiv b \mod n$$

bedeutet, dass a und b denselben Rest bei Division durch n haben.
Es gibt die folgende Rechenregel der Kongruenzarithmetik (für beliebige a, b, n und m):

$$a \equiv b \mod n \Longrightarrow a^m \equiv b^m \mod n$$

Wenn m zu n teilerfremd ist, ist auch $r := m \mod n$ zu n teilerfremd. Tatsählich gilt

$$m = q \cdot n + r$$

und gäbe es einen gemeinsamen Teiler von r und n, so wäre auch m durch diese Zahl teilbar, und somit nicht zu n teilerfremd.
Also ist nach dem Satz über invertierbare Elemente von $\mathbb{Z}/n\mathbb{Z}$ $\overline{r}$ invertierbar. Nach dem Satz von Euler gilt dann:

$$\overline{r}^{\phi(n)} = \overline{1}.$$

Das bedeutet genau, dass der Rest von $r^{\phi(n)}$ bei Division durch n gleich 1 ist. Das bedeutet genau, dass der Rest von $r^{\phi(n)}$ bei Division durch n gleich 1 ist.

Nun betrachten wir, wie der Satz von Euler angewendet werden kann, um die Reste von höheren Potenzen ganzer Zahlen zu berechnen. Dazu verwenden wir die zweite Formulierung dieses Satzes.

Beispiel 12.3.2. *Was ist der Rest von* 3^{4825} *bei Division durch* 5*?*
Es gilt nach dem Satz von Euler:

$$3^4 \equiv 1 \mod 5,$$

da $\phi(5) = 4$.
Es folgt daraus, dass für jedes a

$$(3^4)^a \equiv 1 \mod 5.$$

Also:

$$3^{4a} \equiv 1 \mod 5.$$

Wenn wir nun den Rest von 4825 *bei Division durch* 4 *berechnen, ergibt sich:*

$$4825 = 4a + 1.$$

denn $4825 = 4824 + 1$ *und* 4824 *durch* 4 *teilbar ist, da* $24 = 4 \cdot 6$.
Dann gilt: $3^{4825} = (3^4)^a \cdot 3^1$ *und*

$$3^{4825} \equiv 3^1 \mod 5.$$

$$3^{4825} \equiv 3 \mod 5.$$

Beispiel 12.3.3. *Sei* $n = 25$*, dann ist* $\phi(25) = 5^2 - 5 = 20$.
Sei $m \in \mathbb{Z}$*. Dann ist* m *genau dann zu* 25 *teilerfremd, wenn* m *nicht durch* 5 *teilbar ist. Zum Beispiel ist* 97 *zu* 25 *teilerfremd. Wir können nun* $97^{102} \mod 25$ *berechnen.*
Der Satz von Euler ergibt:

$$97^{20} \equiv 1 \mod 25.$$

Wie im obigen Beispiel betrachten wir den Rest von 102 *bei Division durch* $20 = \phi(25)$*:*

$$102 = 5 \cdot 20 + 2.$$

Es gilt dann:

$$97^{102} = (97^{20})^5 \cdot 97^2$$

$$97^{102} \equiv 97^2 \mod 25$$

Da $97 \equiv -3 \mod 25$*, ergibt sich:*

$$97^2 \equiv (-3)^2 \mod 25.$$

Der Rest von 97^{102} *bei Division durch* 25 *ist somit* 9*:*

$$97^{102} \equiv 9 \mod 25.$$

Berechnung des Restes von m^a bei Division durch n (Fazit).
Sei n eine natürliche Zahl und sei m eine ganze Zahl, die zu n teilerfremd ist. Sei $a \in \mathbb{N}$.
Um den Rest von m^a bei Division durch n zu berechnen, kann man folgende Schritte durchführen:

(1) Die Eulersche Phi-Funktion $\phi(n)$ berechnen.

Bisher hatten wir nur eine Methode, um $\phi(p^k)$ zu berechnen, wobei p eine Primzahl ist. Beim nächsten Mal werden wir eine allgemeinere Methode kennenlernen.

(2) Den Rest von a bei Division durch $\phi(n)$ bestimmen:

$$a = k \cdot \phi(n) + r, \quad \text{wobei } 0 \leq r < \phi(n).$$

(3) Nach dem Satz von Euler erhalten wir dann:

$$m^a \equiv m^r \mod n.$$

(4) Die Berechnung von $m^r \mod n$ ggf. vereinfachen.
(Z. B. wenn s der Rest von m bei Division durch n ist, dann gilt $m^r \mod n = s^r \mod n$.)

Vorlesung 13

13.1. **Potenzen von Elementen in Restklassenringen (Widerholung).** Sei n eine positive natürliche Zahl und sei $x \in \mathbb{Z}/n\mathbb{Z}$.

In Vorlesung 12 haben wir bewiesen, dass die Folge $1, x, x^2, \ldots, x^k, \ldots$ sich widerholt. Außerdem, wenn x invertierbar ist, sind alle Elemente in dieser Folge invertierbar und die Folge widerholt sich, indem sie mit 1 erneut anfängt. Also, für jedes invertierbare x gibt es k, sodass $x^k = \overline{1}$.

Beispiel 13.1.1. *Sei $p = 5$. Dann ist $\phi(5) = 5 - 1 = 4$, da 5 eine Primzahl ist.*

Wir berechnen $\overline{2}^4$ in $\mathbb{Z}/5\mathbb{Z}$:

$$\overline{2}^2 = \overline{4}, \quad \overline{2}^3 = \overline{3}, \quad \overline{2}^4 = \overline{1}.$$

Wir berechnen $\overline{4}^4$ in $\mathbb{Z}/5\mathbb{Z}$:

$$\overline{4}^2 = \overline{1}, \quad \overline{4}^3 = \overline{4}, \quad \overline{4}^4 = \overline{1}.$$

13.2. **Der Satz von Euler mit dem Beweis.**

Satz 13.2.1 (Satz von Euler)**.** *Sei n eine natürliche Zahl.*

Erste Formulierung: Sei x ein invertierbares Element des Restklassenrings $\mathbb{Z}/n\mathbb{Z}$, und sei $\phi(n)$ die Anzahl aller invertierbaren Elementen in $\mathbb{Z}/n\mathbb{Z}$.

Dann gilt:

$$x^{\phi(n)} = \overline{1}.$$

Zweite Formulierung: Sei $m \in \mathbb{Z}$ eine Zahl, die zu n teilerfremd ist. Dann hat $m^{\phi(n)}$ den Rest 1 bei Division durch n.

Man sieht in dem Beispiel oben: Es kann vorkommen, dass für ein invertierbares Element x in $\mathbb{Z}/n\mathbb{Z}$ bereits $x^m = \overline{1}$ für ein $m < \phi(n)$ gilt. Zum Beispiel ist für $n = 5$ und $x = \overline{4}$ bereits $x^2 = \overline{1}$.
Die eulersche Phi-Funktion $\phi(5) = 4$ ist jedoch durch diese Zahl 2 teilbar. Genau dieses Verhalten werden wir im Allgemeinen im Verlauf des Beweises des Satzes von Euler zeigen.

Idee des Beweises. Sei I die Menge der invertierbaren Elemente in $\mathbb{Z}/n\mathbb{Z}$. Diese Menge hat $\phi(n)$ Elemente, gemäß Definition der Phi-Funktion.

Wir veranschaulichen die Beweismethode an einem konkreten Beispiel, das mit farbigem Text geschrieben wurde. Sei $n = 9$, dann ist $\phi(9) = 9 - 3 = 6$ und die Menge I der invertierbaren Elementen in $\mathbb{Z}/9\mathbb{Z}$ besitzt Elementen $\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{7}, \overline{8}$. Dies sind genau die $\overline{m}$ mit $0 < m < 9$ und $\mathrm{ggT}(m, 9) = 1$.

Sei $x \in I$ und m die kleinste positive Zahl mit $x^m = \overline{1}$.

Sei $x = \overline{8}$ in $\mathbb{Z}/9\mathbb{Z}$. Dann ist $x^2 = \overline{1}$ und $m = 2$.

(Diese Zahl wird als *Ordnung* des Elements x in der multiplikativen Gruppe von $\mathbb{Z}/n\mathbb{Z}$ bezeichnet. Wir verwenden diese Terminologie hier jedoch nicht weiter.)

Erste Bemerkung. Es genügt zu zeigen, dass m ein Teiler von $\phi(n)$ ist, also dass ein $l \in \mathbb{N}$ existiert mit

$$\phi(n) = l \cdot m.$$

Dann folgt direkt:

$$x^{\phi(n)} = x^{l \cdot m} = (x^m)^l = \overline{1}^l = \overline{1}.$$

Für das oben gewählte $x = \overline{8}$ in $\mathbb{Z}/9\mathbb{Z}$ gilt $m = 2$, $\phi(9) = 6$ und $2 \mid 6$.

Diese erste Bemerkung ist für den Aufbau des Beweises sehr wichtig, weil sie verdeutlicht, was genau gezeigt werden muss.

Wir müssen erklären, warum die Anzahl der invertierbaren Elemente (also $\phi(n)$) durch die Zahl m (die Ordnung von x) teilbar ist. Was könnte ein solcher Grund sein? Ideal wäre es, wenn wir die Menge I in Teilmengen aufteilen könnten, die jeweils genau m Elemente haben und keine gemeinsamen Elemente besitzen. Gibt es davon k Stück, so gilt $\phi(n) = m \cdot k$, also $m \mid \phi(n)$.

Was könnten diese Teilmengen sein? Es ist interessant, dass diese Teilmengen von Potenzen von x konstruiert werden können. Dies ist der Schlüssel zum Beweis und wird in folgendem Lemma formuliert:

Lemma 13.2.2 (zweite Bemerkung des Beweises)**.** *Sei $x \in I$ und m wie oben, also $x^m = \overline{1}$ und m minimal mit dieser Eigenschaft.*

(1) *Die Elemente $\overline{1}, x, \ldots, x^{m-1}$ sind paarweise verschieden. Insbesondere besitzt die Menge $J := \{\overline{1}, x, \ldots, x^{m-1}\}$ genau m Elemente.*

(2) *Für jedes $a \in I$ besitzt die Menge $a \cdot J := \{a, a \cdot x, \dots, a \cdot x^{m-1}\}$ ebenfalls genau m Elemente und ist eine Teilmenge von I.*
(3) *Wenn $b \in I$ und $b \notin a \cdot J$, dann schneiden sich $b \cdot J$ und $a \cdot J$ nicht.*
Insbesondere gilt: Wenn $b \in I$ und $b \notin J = 1 \cdot J$, dann schneiden sich $b \cdot J$ und J nicht.

Der Beweis dieses Lemmas ist nicht kompliziert. Wir verzichten jedoch darauf.
Wir illustrieren dieses Lemma mit einem Beispiel:
Sei $n = 9$, $I = \{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{7}, \overline{8}\}$. Sei $x = \overline{8} \in I$, $m = 2$: $x^2 = \overline{1}$ und $J = \{\overline{1}, \overline{8}\}$.
Sei $a = \overline{2}$, dann gilt $a \notin J$ und $a \in I$. Die Menge $a \cdot J$ berechnen wir, indem wir alle Elemente der Menge J durch a multiplizieren:

$$a \cdot J = \{\overline{2}, \overline{7}\}.$$

Die Mengen J und $a \cdot J$ schneiden sich also nicht.
Der Hauptschritt des Beweises.
Die Menge $J = \{1, x, x^2, \dots, x^{m-1}\}$ hat m Elemente und ist Teilmenge von I mit $\phi(n)$ Elementen. Nun zerlegen wir I in Teilmengen der Form $a \cdot J$, die sich alle paarweise nicht schneiden.

- Beginne mit J. Wenn $J = I$, sind wir fertig (und $m = \phi(n)$).
  Für $x = \overline{8}$ ist $J = \{\overline{1}, \overline{8}\} \neq I$ und $m = 2$ ungleich zu $\phi(9) = 6$ ist.
- Sonst existiert ein $a_1 \in I$, das nicht in J liegt. Dann ist $a_1 \cdot J$ eine neue Teilmenge mit m Elementen, die sich mit J nicht schneidet.
  Wie oben können wir als a_1 das Element $\overline{2}$ nehmen. Dann ist $a_1 \cdot J = \{\overline{2}, \overline{7}\}$.
- Wenn $J \cup a_1 \cdot J = I$ – also jedes Element von I entweder in J oder $a_1 \cdot J$ behalten ist, dann ist $\phi(n) = 2 \cdot m$ und wir sind fertig.
  Wir haben $J \cup a_1 \cdot J = \{\overline{1}, \overline{2}, \overline{7}, \overline{8}\}$, also nicht alle Elemente von I schon in J oder in $a_1 \cdot J$ enthalten sind.
- Falls nicht, wählen wir $a_2 \in I$, das weder in J noch in $a_1 \cdot J$ liegt. Wir betrachten dann $a_2 \cdot J$, eine Teilmegne mit m Elementen, die sich mit J und $a_1 \cdot J$ nicht schneidte, usw.
  Wir können also $a_2 = \overline{5}$ betrachten, $a_2 \in I$, $a_2 \notin J$. Dann ist $a_2 \cdot J = \{\overline{5}, \overline{4}\}$.
  In diesem Beispiel ist die Menge I in 3 Teilemengen zerlegt: J, $a_1 \cdot J$, $a_2 \cdot J$. Da jede diese Teilemnge 2 Elemente hat und sie sich paarweise nicht schneiden, bekommen wir, dass $\phi(9) = 3 \cdot 2$ gilt.

Dieser Prozess endet nach endlich vielen Schritten, da I endlich ist. So erhalten wir eine Zerlegung von I in k Teilmengen, die sich nicht schneiden, jede mit m Elementen, und somit $\phi(n) = k \cdot m$, also $m \mid \phi(n)$. □

13.3. **Die Berechnung der eulerschen Phi-Funktion.**

Die Anzahl der invertierbaren Elemente in $\mathbb{Z}/n\mathbb{Z}$ wird mit $\phi(n)$ bezeichnet,
und die Funktion $\phi(n)$ heißt die **Eulersche Phi-Funktion**.

Beispiel 13.3.1 (s. Vorlesung 11)**.** *Sei p eine Primzahl. Dann gilt:*
(1) $\phi(p) = p - 1$;
(2) $\phi(p^k) = p^k - p^{k-1}$.

Satz 13.3.2. *Seien k, m teilerfremde natürliche Zahle.*
Dann gilt

$$\phi(k \cdot m) = \phi(k) \cdot \phi(m).$$

Anhand eines Beispiels schauen wir an, wie dieser Satz zur Berechnung von $\phi(n)$ angewendet werden kann.

Beispiel 13.3.3. *Sei $n = 200$. Wir können n als Produkt $2^3 \cdot 5^2$ schreiben, wobei 2^3 und 5^2 teilerfremd sind. Dann gilt:*

$$\phi(200) = \phi(2^3) \cdot \phi(5^2) = (2^3 - 2^2) \cdot (5^2 - 5) = 4 \cdot 20 = 80.$$

Beispiel 13.3.4. *Sei $n = 7^3 \cdot 11^5 \cdot 13^{10}$. Die Zahlen $7^3 \cdot 11^5$ und 13^{10} sind teilerfremd, daher gilt nach dem obigen Satz:*

$$\phi(n) = \phi(7^3 \cdot 11^5) \cdot \phi(13^{10}).$$

Da auch 7^3 und 11^5 teilerfremd sind, gilt weiter: $\phi(7^3 \cdot 11^5) = \phi(7^3) \cdot \phi(11^5)$.

Wir erhalten somit:

$$\phi(7^3 \cdot 11^5 \cdot 13^{10}) = \phi(7^3) \cdot \phi(11^5) \cdot \phi(13^{10}) = (7^3 - 7^2) \cdot (11^5 - 11^4) \cdot (13^{10} - 13^9).$$

Dieses Beispiel führt zur folgenden allgemeinen Formel:

Formel für die Berechnung der Eulerschen Phi-Funktion.
Sei n eine positive natürliche Zahl.
Sei $n = p_1^{r_1} \cdot p_2^{r_2} \cdots p_k^{r_k}$ eine Zerlegung in Potenzen verschiedener Primzahlen.
Dann gilt

$$\phi(n) = (p_1^{r_1} - p_1^{r_1-1}) \cdot (p_2^{r_2} - p_2^{r_2-1}) \cdots (p_k^{r_k} - p_k^{r_k-1}).$$

Beispiel 13.3.5. *Sei* $n = 400 = 16 \cdot 25 = 2^4 \cdot 5^2$.
Dann gilt $\phi(400) = (2^4 - 2^3) \cdot (5^2 - 5) = (16 - 8) \cdot (25 - 5) = 8 \cdot 20 = 160$.

Beweise des Satzes in einem Spezialfall. Wir werden den Satz in dieser Vorlesung nicht vollständig beweisen, sondern einen Spezialfall betrachten. Der allgemeine Beweis folgt jedoch derselben Idee wie in diesem Fall.

Sei $n = p \cdot q$, wobei p, q verschiedene Primzahlen sind. Dann ist zu zeigen:

$$\phi(p \cdot q) = \phi(p) \cdot \phi(q) = (p-1)(q-1) = pq - p - q + 1.$$

Erinnern wir uns, wie wir in Vorlesung 11 den Wert von $\phi(p^k)$ berechnet haben: Die eulersche Phi-Funktion zählt die Anzahl der Zahlen zwischen 0 und n, die zu n teilerfremd sind. Ist $n = p^k$, so ist eine Zahl m genau dann teilerfremd zu n, wenn sie nicht durch p teilbar ist. Die durch p teilbaren Zahlen zwischen 0 und $n = p^k$ sind:

$$0, p, 2p, 3p, \ldots, (p^{k-1} - 1)p.$$

Diese Liste enthält genau p^{k-1} Zahlen.

Somit ist:

$$\phi(p^k) = p^k - p^{k-1}.$$

Im Fall $n = p \cdot q$ ist eine Zahl m genau dann teilerfremd zu n, wenn sie weder durch p noch durch q teilbar ist.

Die durch p teilbaren Zahlen zwischen 0 und $pq - 1$ sind:

$$0, p, 2p, \ldots, (q-1)p \qquad \text{(insgesamt } q \text{ Zahlen.)}$$

Die durch q teilbaren Zahlen sind:

$$0, q, 2q, \ldots, (p-1)q \qquad \text{(insgesamt } p \text{ Zahlen.)}$$

Die einzige gemeinsame Zahl in beiden Listen ist 0, denn alle anderen Vielfachen von p und q sind erst ab pq gemeinsame Vielfache.

Daher ist die Anzahl der Zahlen zwischen 0 und $pq - 1$, die nicht teilerfremd zu pq sind, genau:

$$p + q - 1.$$

Die Anzahl von Zahlen $m\colon 0 \leq m < p \cdot q$, die zu $p \cdot q$ teilerfremd sind, ist somit:

$$\phi(p \cdot q) = p \cdot q - (p + q - 1) = p \cdot q - p - q + 1 = (p-1)(q-1) = \phi(p)\phi(q).$$

□

Der nächste Abschnitt wurde in der Vorlesung ausgelassen, ist aber zur Information hier aufgeführt.

13.4. **Der kleine Satz von Fermat.** Der Satz von Euler ermöglicht uns, die Inverse in Restklassenringen zu rechnen, ohne den Euklidischen Algorithmus zu verwenden.

Corollary 13.4.1 (Berechnung des Inversen mittels Potenzen)**.** *Sei n eine positive natürliche Zahl. Sei $x \in \mathbb{Z}/n\mathbb{Z}$ ein invertierbares Element.*

Dann gilt: $x \cdot x^{\phi(n)-1} = \overline{1}$, also ist $x^{\phi(n)-1}$ das Inverse von x.

Beispiel 13.4.2. *Sei $n = 11$.*

Dann gilt $\phi(11) = 10$, da 11 eine Primzahl ist. Ein Element $\overline{m} \in \mathbb{Z}/11\mathbb{Z}$ ist genau dann invertierbar, wenn $m \neq 0$.

Dann gilt:

$$m \cdot (m^9) = \overline{1}.$$

Insbesondere, für $m = 2$ können wir berechnen:

$$\overline{2}^2 = \overline{4}, \quad \overline{2}^4 = (\overline{4})^2 = \overline{5}, \quad \overline{2}^8 = (\overline{5})^2 = \overline{3}$$
$$\overline{2}^9 = \overline{2}^8 \cdot \overline{2} = \overline{3} \cdot \overline{2} = \overline{6}.$$

Also ist $\overline{6}$ das Inverse von $\overline{2}$ in $\mathbb{Z}/11\mathbb{Z}$.

Hier ist eine weitere Folgerung aus dem Satz von Euler.

Corollary 13.4.3 (Der kleine Satz von Fermat)**.** *Sei p eine Primzahl, sei a eine ganze Zahl.*

Dann gilt:

$$a^p \equiv a \mod p.$$

Erinnerung: Das heißt, dass a^p und a gleiche Reste bei Division durch p haben.

Beweis. Wir unterscheiden zwei Fälle.

Fall 1. Die Zahlen a und p sind nicht teilerfremd.

Dann muss p die Zahl a teilen, da p nur 2 Teiler hat. Wenn $p \mid a$, dann gilt $a \equiv 0 \mod p$, und auch $a^p \equiv 0 \mod p$. Weil a und a^p gleiche Reste (nämlich 0) bei Division durch p haben, folgt: $a^p \equiv a \mod p$.

Fall 2. Die Zahlen a und p sind teilerfremd.

Dann können wir den Satz von Euler anwenden. Da $\phi(p) = p - 1$, gilt:

$$a^{p-1} \equiv 1 \mod p.$$

Wenn wir beide Seiten dieser Kongruenz mit a multiplizieren, ergibt sich:

$$a^p \equiv a \mod p.$$

□

Eine Folgerung dieser Aussage ist die Formel für die p-te Potenz einer Summe.

Corollary 13.4.4. *Sei p eine Primzahl, seien $a, b \in \mathbb{Z}$.*

Dann gilt:

$$(a + b)^p \equiv a^p + b^p \mod p.$$

Beweis. Nach dem kleinen Satz von Fermat gilt:

$$(a + b)^p \equiv a + b \mod p,$$
$$a^p \equiv a \mod p, \quad b^p \equiv b \mod p.$$

□

Genau diesen Fehler macht man manchmal, wenn man in der Schule lernt, wie Potenzen funktionieren, und fälschlicherweise $(a + b)^n = a^n + b^n$ schreibt. Nun kann man sagen, dass diese Formel tatsächlich richtig ist – aber nur, wenn n eine Primzahl ist und man die Gleichheit modulo n versteht.