Primzahlen und ihre Bedeutung in der Kryptographie

Einbindungsmöglichkeiten im Unterricht

Diplomarbeit

Im Lehramtsstudium

Mathematik - Biologie und Umweltkunde

zur Erlangung des akademischen Grades

Magistra der Naturwissenschaften

eingereicht an der

Fakultät für Mathematik, Informatik und Physik der Universität Innsbruck

von

Daniela Aichner

Betreuer der Diplomarbeit: Univ.-Prof. Dr. Tim Netzer

Innsbruck, Februar 2022

Inhaltsverzeichnis

Abbildungsverzeichnis

Einleitung

Primzahlen nehmen eine besondere Stellung innerhalb der ganzen Zahlen ein. Sie faszinieren die Menschheit bereits seit der Antike. Ihnen werden sogar übernatürliche und magische Fähigkeiten zugesprochen. So gilt die Dreizehn als Unglückszahl und es wird gesagt, Katzen hätten sieben Leben. Aber auch in der wissenschaftlichen Forschung sind Primzahlen heute noch von Bedeutung.
Waren die Primzahlen früher ein fixer Bestandteil in den Lehrplänen, so sind sie heute fast vollständig daraus verschwunden. Ihre Anwendung lag in der Berechnung des größten gemeinsamen Teilers mit Hilfe der Primfaktorzerlegung. Mathematisch gesehen spricht einiges gegen diese Anwendung, zumal es eine weitere Berechnungsweise gibt. Deshalb wurden sie wohl zu Recht aus den Lehrplänen der Unterstufe gestrichen.
Nichtsdestotrotz lässt sich eine Einführung der Primzahlen im Mathematikunterricht rechtfertigen. Ihr Einsatz im Bereich der Kryptographie in der modernen Datensicherheit ist auch im Alltag der Schüler zu finden und deshalb durchaus von Relevanz.
Die Arbeit ist in zwei Teilen Aufgebaut. Im ersten Teil finden sich die wichtigsten Definitionen und Sätze, die im Zusammenhang mit den Primzahlen von Bedeutung sind. Im zweiten Teil werden mögliche Anwendungen der Primzahlen und Kryptographie im Schulunterricht vorgestellt. Mit Hilfe einer kurzen Schulbuchanalyse wird ein Blick auf die derzeitige Situation an den Schulen geworfen. Den Hauptteil bilden die vier selbst entwickelten Arbeitsmaterialien zur Einführung der Teilbarkeit und der Primzahlen, sowie zwei Anwendungsbeispiele im Bereich der Kryptographie.

Teil I.

Mathematische Hintergründe

1. Was ist eine Primzahl?

Ganze Zahlen können addiert und subtrahiert werden und wir erhalten wieder eine ganze Zahl. Sie können auch problemlos miteinander multipliziert werden. Beim Dividieren stoßen die ganzen Zahlen jedoch an ihre Grenze. Wir erhalten nicht bei jeder beliebigen Division wieder eine ganze Zahl. So zum Beispiel ist $15 \div 3 = 5$ eine ganze Zahl, $15 \div 2$ lässt sich innerhalb der ganzen Zahlen aber nicht lösen. Die Division kann auf den ganzen Zahlen somit nicht definiert werden. Eine dazu entsprechende Eigenschaft, die definiert werden kann ist die Teilbarkeit. Die Definitionen, Sätze und Beweise sind an denen von Rempe & Waldecker (2009) angelehnt.

Definition: Teiler und Vielfache

Seien a und b ganze Zahlen.
*Dann gilt a teilt b in $\mathbb{Z}$ genau dann, wenn es ein k aus $\mathbb{Z}$ gibt mit $a \cdot k = b$. Damit ist a ein **Teiler** von b und b ist ein **Vielfaches** von a. Für a teilt b schreiben wir kurz $a \mid b$.*

Aus dieser Definition lassen sich einige Teilbarkeitsregeln ableiten. Kennen wir bereits Teiler von zwei Zahlen a und b, so lassen sich daraus einige Teiler der Summe, der Differenz, dem Produkt und beliebiger Vielfache der beiden Zahlen herleiten.

Satz 1.1 (Teilbarkeitsregeln)**.** Seien $a, b, c \in \mathbb{Z}$
Wenn c sowohl a als auch b teilt, dann teilt c auch $a + b$, $a - b$ und $a \cdot b$. Zudem gilt, dass jeder Teiler von a auch jedes beliebige Vielfache von a teilt, also aus $c \mid a$ folgt $c \mid m \cdot a$ für $m \in \mathbb{Z}$.

Beweis. Wir nehmen an, dass c sowohl a als auch b teilt. Das heißt, es gibt $k_1, k_2 \in \mathbb{Z}$ so, dass $a = k_1 \cdot c$ und $b = k_2 \cdot c$. Daraus folgt $a + b = k_1 \cdot c + k_2 \cdot c = (k_1 + k_2) \cdot c$. Wir setzen $k = k_1 + k_2$ und damit folgt aus der Definition des Teilers, dass c Teiler von $a + b$ ist. Dasselbe Beweisverfahren können wir auch auf $a - b$ und $a \cdot b$, sowie auf die beiden weiteren Aussagen anwenden und werden deshalb hier nicht weiter ausgeführt. □

Im Zusammenhang mit der Teilbarkeit lässt sich eine Menge der ganzen Zahlen abgrenzen, die sogenannten Primzahlen.

Definition: Primzahl

Eine ganze Zahl $p \in \mathbb{Z}$ heißt ***Primzahl****, wenn*

- $p \neq -1, 0, 1$ *und*
- $\{1, -1, p, -p\}$ *Menge der Teiler von p ist.*

Die Teiler 1, -1, p und $-p$ werden auch triviale Teiler von p genannt.

Hat eine Zahl zwei oder mehr nicht triviale Teiler, so spricht man von einer zusammengesetzten Zahl.

Für kleine Zahlen ist es noch verständlich, dass eine Zahl nur triviale Teiler besitzt. Umso spannender ist es, dass es auch sehr große Zahlen gibt, die diese Eigenschaft besitzen.

Bevor wir uns die Primzahlen genauer ansehen, betrachten wir noch einige wichtige Sätze und Definitionen über die Teilbarkeit von ganzen Zahlen die von Bedeutung sind.

Die Primzahlen machen noch deutlicher, dass das Dividieren in den ganzen Zahlen nicht beliebig durchführbar ist. Was aber möglich ist, ist die sogenannte Division mit Rest.

Satz 1.2 (Division mit Rest von ganzen Zahlen)**.** Zu je zwei ganzen Zahlen a und b, mit $b > 0$ gibt es zwei eindeutig bestimmte ganze Zahlen q und r mit $0 \leq r < b$ so, dass

$$a = q \cdot b + r$$

ist. q nennen wir Quotient und r den Rest von a nach Division durch b.

Das Verfahren zur Berechnung von q und r entspricht dem schriftlichen Dividieren, welches bereits in der Grundschule eingeführt wird. Dieses meist abgekürzte Verfahren lässt sich auf mehrfache Subtraktion zurückführen.

Beispiel. *Wir dividieren* 158 *mit Rest durch* 6*.*
Die einfachste Möglichkeit ist, 6 *so lange von* 158 *zu subtrahieren, bis wir eine Zahl erhalten, die kleiner ist als* 6*. Diese Zahl ist dann der Rest r und q ist die Anzahl der Subtraktionen. Schneller funktioniert dagegen die schriftliche Division, die wir aus der Grundschule kennen:*

$$\begin{array}{l} \overline{158}\dot{} : 6 = 26 \\ 38 \\ \quad 2 \ \textit{Rest} \end{array}$$

Die ursprüngliche Aufgabe wird hiermit vereinfacht, sodass die Aufgabe mit Hilfe des kleinen Ein-mal-Eins bzw. bei Divisionen durch größere Zahlen nach maximal zehn Subtraktionen je Schritt gelöst werden kann.

158 *lässt sich schreiben als* $150+8$. 150 *wiederum lässt sich aufspalten in* $15 \cdot 10$. *Anstatt* 150 *mit Rest durch* 6 *zu teilen, teilen wir nun* 15 *mit Rest durch* 6 *und erhalten* $15 = 2 \cdot 6 + 3$. *Davon können wir auf* $150 = (2 \cdot 6 + 3) \cdot 10$ *schließen und nach ausmultiplizieren und einsetzen wieder zurück auf* $158 = 2 \cdot 6 \cdot 10 + 3 \cdot 10 + 8$. *Weiteres Umformen führt uns zur Lösung:*

$$
\begin{aligned}
158 &= 2 \cdot 10 \cdot 6 + 3 \cdot 10 + 8 \\
158 &= 20 \cdot 6 + 38 \\
158 &= 20 \cdot 6 + 6 \cdot 6 + 2 \\
158 &= (20 + 6) \cdot 6 + 2 \\
158 &= 26 \cdot 6 + 2
\end{aligned}
$$

1.1. Der Euklidische Algorithmus

Eine Eigenschaft von ganzen Zahlen, die besonders beim Rechnen mit Brüchen Anwendung findet, ist der größte gemeinsame Teiler (ggT) und das kleinste gemeinsame Vielfache (kgV).

Definition: ggT und kgV, teilerfremd

Der ***größte gemeinsame Teiler*** *zweier ganzer Zahlen a und b mit $a, b \neq 0$, ist die größte ganze Zahl, die sowohl a als auch b teilt.*
Das ***kleinste gemeinsame Vielfache*** *zweier ganzer Zahlen a und b mit $a, b \neq 0$, ist die kleinste positive ganze Zahl, die sowohl Vielfaches von a als auch von b ist.*
Zwei ganze Zahlen a und b sind ***teilerfremd****, wenn sie keinen gemeinsamen Teiler besitzen, insbesondere gilt $ggT(a, b) = 1$.*

Zur Berechnung des ggT und kgV gibt es mehrere Möglichkeiten. Die einfachste ist dabei wohl der sogenannte Euklidische Algorithmus. Dieser ist leicht verständlich und für beliebige, insbesondere auch große ganze Zahlen einfach durchzuführen. Die einzige Rechenoperation die dafür benötigt wird ist die Division mit Rest.
Um zu verstehen, wie der Euklidische Algorithmus funktioniert, benötigen wir noch eine Eigenschaft des ggT.

Satz 1.3. Seien a, b und m ganze Zahlen. Dann gilt

$$ggT(a, b) = ggT(a, b + m \cdot a)$$

.

Beweis. Wir müssen zeigen, dass jeder gemeinsame Teiler von a und b auch Teiler von a und $b + m \cdot a$ und umgekehrt ist. Wenn alle gemeinsamen Teiler identisch sind, muss somit laut Definition auch der größte gemeinsame Teiler derselbe sein und die Aussage ist gezeigt.
Sei k_1 Teiler von a und b. Aus Satz 1.1 wissen wir, dass k_1 auch Teiler von $m \cdot a$. Damit ist k_1 aber auch Teiler der Summe $a + m \cdot a$. Umgekehrt sei k_2 Teiler von a und $b + m \cdot a$, dann ist nach demselben Satz k_2 auch Teiler von $m \cdot a$ und damit auch Teiler der Differenz $b + m \cdot a - m \cdot a = b$, also auch Teiler von b. □

Wir wissen jetzt, dass der ggT zweier Zahlen derselbe bleibt, wenn man zu einer der beiden Zahlen die andere beliebig oft addiert oder auch subtrahiert. Mit diesem Wissen ist es möglich die beiden Zahlen geschickt zu verkleinern, bis der größte gemeinsame Teiler einfach ablesbar ist. Diesem Prinzip folgt der Euklidische Algorithmus.

Satz 1.4 (Der Euklidische Algorithmus)**.** Seien a, b positive ganze Zahlen. Falls $a > b$ setze $r_0 = a$ und $r_1 = b$, andernfalls setze $r_0 = b$ und $r_1 = a$. Setze $i = 1$

Schritt 1: Sei r_{i+1} der Rest nach Division von r_{i-1} durch r_i:

$$r_{i-1} = q_i \cdot r_i + r_{i+1}$$

(*Für* $i = 1$ *berechen wir* r_2 *mit* $a = q_1 \cdot b + r_2$.)

Schritt 2: Falls $r_{i+1} = 0$ ist $ggT(a, b) = r_i$ und wir sind fertig.
Ansonsten setze $i := i + 1$ und wiederhole Schritt 1.

Für negative ganze Zahlen ersetze a und b mit $|a|$ und $|b|$.

Der Algorithmus funktioniert für beliebige ganze Zahlen a und b. Da nach Satz 2 der Rest nach jeder Division kleiner ist als sein Vorgänger, kommt der Algorithmus nach endlich vielen Schritten zu einem Ergebnis.

Beispiel. *Berechne den ggT von* 396 *und* 156.
Wir dividieren 396 *mit Rest durch* 156*:*

$$396 = 2 \cdot 156 + 84$$

Es gilt also $ggT(396, 156) = ggT(156, 84)$.

In den weiteren Schritten ersetzen wir die größere der beiden Zahlen mit dem Rest und führen die Division mit Rest erneut durch, bis der Rest Null ist.

$$\begin{aligned} 156 &= 1 \cdot 84 + 72 \\ 84 &= 1 \cdot 72 + 12 \\ 72 &= 6 \cdot 12 + 0 \end{aligned}$$

und damit $ggT(396, 156) = ggT(156, 84) = ggT(72, 12) = 12$.

Anstelle der Division mit Rest, kann jeder Schritt durch eine Subtraktion der jeweils größeren von der kleineren Zahl ausgeführt werden. Im nächsten Schritt wird die größere Zahl durch die Differenz ersetzt. Das Verfahren benötigt dadurch zwar mehr Schritte, ist aber noch leichter durchführbar.

Beispiel. $ggT(225, 144) = ggT(81, 144) = ggT(81, 63) = ggT(18, 63) = ggT(18, 45) = ggT(18, 27) = ggT(18, 9) = ggT(9, 9) = 9$

Aus dem Euklidischem Algorithmus lässt sich eine spezielle Darstellung des ggT ableiten, die später für einige Beweise wichtig wird. Der ggT(a,b) lässt sich nämlich als Linearkombination von a und b darstellen.

Satz 1.5 (Lemma von Bézout)**.** Seien $a, b \in \mathbb{Z}$.
Dann gibt es ganze Zahlen u und v so, dass

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

ist.

Bevor wir diesen Satz beweisen, betrachten wir nochmals das vorherige Beispiel zur Berechnung des ggT mit der Division mit Rest und versuchen die Aussage des Lemmas zu erhalten.

Beispiel. *Wir betrachten die Berechnung des ggT von* 396 *und* 156*. Durch Umformen und rückwärts Einsetzen, dass*

$$\begin{aligned} 12 &= 84 - 1 \cdot 72 \\ &= 84 - 1 \cdot (156 - 84) = 2 \cdot 84 - 156 \\ &= 2 \cdot (396 - 2 \cdot 156) - 156 = 2 \cdot 396 - 6 \cdot 156 \end{aligned}$$

Dieses Lemma ist auch als **erweiterter euklidischer Algorithmus** bekannt, da es sich aus dem euklidischen Algorithmus herleiten lässt. Der Beweis des Lemmas verwendet

dieselbe Strategie, mit der wir das Beispiel gelöst haben.

Beweis. Seien $r_0, r_1, ..., r_j$ aus dem euklidischen Algorithmus zur Berechnung von ggT(a,b). Wir müssen zeigen, dass für alle $i \in \{0, \dots j\}$ gilt, dass $r_i = u_i \cdot a + v_i \cdot b$. Da $r_j = ggT(a, b)$ ist, wäre die Aussage damit bewiesen. Der Beweis folgt durch vollständige Induktion über i.

IA Für $i = 0$ und $i = 1$ ist die Behauptung erfüllt, da

$$r_0 = a = 1 \cdot a + 0 \cdot b \text{ und } r_1 = b = 0 \cdot a + 1 \cdot b$$

ist. Unser Induktionsanfang (IA) ist gemacht. Ausgehend davon, möchten wir die Aussage für jedes weitere i zeigen.

IV Für ein fest gewähltes $i \geq 1$ können wir annehmen, dass $r_i = u_i \cdot a + v_i \cdot b$ und $r_{i-1} = u_{i-1} \cdot a + v_{i-1} \cdot b$. Das ist unsere Induktionsvoraussetzung (IV).

IS Wir schließen nun von i auf das nächstgrößere, also $i+1$. Zu zeigen ist, dass es u_{i+1} und v_{i+1} gibt, mit $r_{i+1} = u_{i+1} \cdot a + v_{i+1} \cdot b$.

Es gilt, dass $r_i = q_i \cdot r_{i-1} + r_{i+1}$ ist, also $r_{i+1} = r_i - q_i \cdot r_{i-1}$. Durch Einsetzen der IV für r_i und r_{i-1}, Umformen und erneutem Faktorisieren erhalten wir:

$$\begin{aligned} r_{i+1} &= r_i - q_i \cdot r_{i-1} = \\ &= u_i \cdot a + v_i \cdot b - q_i \cdot (u_{i-1} \cdot a + v_{i-1} \cdot b) = \\ &= u_i \cdot a + v_i \cdot b - q_i \cdot u_{i-1} \cdot a - q_i v_{i-1} \cdot b = \\ &= (u_i - q_i \cdot u_{i-1}) \cdot a + (v_i - q_i v_{i-1}) \cdot b \end{aligned}$$

Wir setzen $u_{i+1} := u_i - q_i \cdot u_{i-1}$ und $v_{i+1} = v_i - q_i \cdot v_{i-1}$ und die Aussage ist bewiesen.

□

Eine weitere Möglichkeit zur Berechnung des ggT, nämlich die Primfaktorzerlegung, lernen wir im nächsten Abschnitt kennen. Zuvor schauen wir uns die Primzahlen aber noch genauer an, wobei wir uns in den nun folgenden Abschnitten auf die natürlichen Primzahlen beschränken, da die Aussagen für negative Primzahlen im Schulunterricht nicht von Relevanz sind.

2. Die Entdeckung der Primzahlen

Bereits im antiken Griechenland haben sich Mathematiker mit den Primzahlen auseinandergesetzt. Ihre besonderen Eigenschaften, insbesondere ihre Unregelmäßigkeiten innerhalb der natürlichen Zahlen haben das Interesse der Mathematiker geweckt.

2.1. Das Sieb des Eratosthenes

Welche Eigenschaft eine natürliche Zahl erfüllen muss, um eine Primzahl zu sein, ist bereits klar. Alle Teiler einer Zahl herauszufinden, ist sehr aufwendig und langwierig. Darum war es schon früh von Interesse ein Verfahren zu entwickeln, um Primzahlen zu finden.

Ein Verfahren zur Auflistung der ersten Primzahlen gibt das Sieb des Eratosthenes, welches bereits im 3. Jahrhundert v.Chr. von Eratosthenes entwickelt wurde.

Eratosthenes von Kyrene (273 - 192 v. Chr.) war ein griechischer Mathematiker, der gemeinsam mit Archimedes wirkte. Er beschäftigte sich nicht nur mit naturwissenschaftlichen Fächern wie Mathematik, Astronomie und Geographie, sondern auch mit geisteswissenschaftlichen Fächern wie der Philosophie, Geschichte und der Dichtkunst. Er arbeitete auch als Chef-Bibliothekar in der Bibliothek von Alexandria. Seine eigenen Werke wie beispielsweise „ Über Plato “ sind nicht überliefert (Vgl. Hermann, 2020).

Abbildung 1: Eratosthenes
(Anonym, 2006)

Das Sieb des Eratosthenes ist ein sehr einfaches Verfahren zur Auflistung von Primzahlen, welches auch für Schüler aus der Unterstufe oder sogar für Schüler der Grundschule verständlich ist, da als Vorwissen nur die Multiplikation von natürlichen Zahlen Voraussetzung ist. Es nutzt die Multiplikation als Umkehrfunktion der Division, um Zahlen auszuschließen, die keine Primzahlen sein können.

Zunächst listen wir alle natürlichen Zahlen, beginnend mit der 2, bis zu einer vorgegebenen Grenze N, der Reihe nach auf. 2 ist unsere erste Primzahl. Nun streichen wir alle Vielfachen der 2. Diese Zahlen kommen nicht als Primzahlen in Frage. Die 3 ist unsere zweite Primzahl. Sie ist die kleinste Zahl, die nicht gestrichen wurde. Im nächsten Schritt streichen wir alle Vielfachen der 3 und wir erhalten die dritte Primzahl auf dieselbe Weise. Die kleinste Zahl die übrig geblieben ist, ist die 5. Dies führen wir weiter fort, bis wir bei der Wahl der nächsten Primzahl eine Zahl überschreiten, die zum Quadrat größer ist als die vorgegebene Grenze N. Die Zahlen, die wir bis zu diesem Zeitpunkt nicht gestrichen haben, sind alle Primzahlen die kleiner sind als N.

Ein Beispiel mit $N = 200$ *ist im zweiten Teil dieser Arbeit zu finden.*

Wir haben nun eine Methode, um Primzahlen aufzulisten. Es stellt sich die Frage, ob wir

irgendwann die letzte und damit größte Primzahl erreichen, wenn wir die vorgegebene Grenze dieses Verfahrens immer mehr erweitern.

2.2. Euklid und die Unendlichkeit der Primzahlen

Die Antwort auf die Frage nach der größten Primzahl wurde schon sehr früh geklärt. Egal wie groß wir N wählen, es gibt immer noch Primzahlen, die größer als N sind. Es gibt nämlich unendlich viele Primzahlen.

Einen Beweis für die Unendlichkeit der Primzahlen gibt der griechische Mathematiker Euklid in den *Elementen*. Euklid hat sich sehr stark mit den Primzahlen und allgemein mit der Arithmetik auseinandergesetzt und ist zu vielen wichtigen Erkenntnissen gekommen.

Euklid lebte um 360-260 v. Chr., wobei über sein Leben nicht sehr viel bekannt ist. Er wurde in Athen ausgebildet und wirkte laut Überlieferungen später in Alexandria. Sein wohl bekanntestes Werk sind die *Elemente*. Sie umfassen 13 Bücher über die Geometrie und Arithmetik (später 15), in denen er bisherige Erkenntnisse der griechischen Mathematik verständlicher angeordnet und neue Beweise entwickelt hat. Er erfüllt darin die Forderung von Aristoteles, dass das aus Beweisen neu erhaltene Wissen zunächst auf unbewiesenen Postulaten, den *Definitionen*, ruhen müssen (Vgl. Hermann, 2020).

Abbildung 2: Euklid (Wellcome Library, 2014)

Der Beweis von Euklid bedarf nicht vieler Voraussetzungen und ist leicht verständlich. Eine der Voraussetzungen ist eine weitere Teilbarkeitsregel, die unter dem Lemma von Euklid bekannt ist.

Lemma 2.1 (Lemma von Euklid)**.** Es sei p eine Primzahl und a,$b \in \mathbb{Z}$. Wenn p die Zahl $a \cdot b$ teilt, dann teilt p auch a oder b.

Beweis. Wir beweisen das Lemma, indem wir zeigen, wenn p die Zahl a nicht teilt, dann muss p die Zahl b teilen.

Wenn p die Zahl $a \cdot b$ teilt, dann gibt es ein $k \in \mathbb{Z}$ so, dass

$$k \cdot p = a \cdot b$$

. Wenn p die Zahl a nicht teilt, dann ist 1 der größte gemeinsame Teiler von a und p, kurz $ggt(a, p) = 1$. Nach dem Lemma von Bézout gibt es ganze Zahlen u und v so, dass $u \cdot a + v \cdot p = 1$. Nach Multiplikation mit b und duch Einsetzen der Voraussetzung, dass $a \cdot b = k \cdot p$

$$b = bua + bvp = u(ab) + bvp = ukp + bvp = (uk + bv)p$$

und damit ist b ein Vielfaches von p und es gilt $p \mid b$. □

2.2.1. Die Eindeutigkeit der Primfaktorzerlegung

Der Beweis des Lemmas von Euklid zeigt, dass wir mit Hilfe der Teiler weitere Faktoren der zusammengesetzten Zahl berechnen können. Kennen wir weitere Teiler der Zahl oder einer ihrer Faktoren, können wir die Zerlegung so lange fortführen, bis die einzelnen Faktoren die wir erhalten, nurmehr triviale Teiler besitzen.

Der Hauptsatz der Arithmetik zeigt, dass diese Zerlegung für jede beliebige natürliche Zahl existiert.

Satz 2.1 (Fundamentalsatz der Arithmetik)**.** Jede ganze Zahl $a \geq 2$ kann als Produkt von Primzahlen geschrieben werden. Diese Primzahlen nennt man Primfaktoren und den Vorgang Primfaktorzerlegung. Die Primfaktorzerlegung ist bis auf die Reihenfolge eindeutig bestimmt.

Beispielsweise lässt sich die Zahl 84 schreiben als $2 \cdot 2 \cdot 3 \cdot 7$. Für kleine Zahlen, ist diese Zerlegung mit Hilfe des Einmaleins und der Teilbarkeitsregeln schnell zu finden. Für große Zahlen ist diese Zerlegung jedoch mit einem großen Aufwand verbunden.
Allerdings lässt sich recht einfach beweisen, dass es diese Zerlegung für jede beliebige Zahl gibt.

Beweis. Sei $a \in \mathbb{Z}$ mit $a \geq 2$. Wir müssen zeigen, dass eine solche Primfaktorzerlegung für a existiert und falls sie existiert, dass sie eindeutig ist. Der Beweis der Existenz erfolgt durch Induktion über a.

IA Wir starten die Induktion mit $a = 2$. Damit ist a eine Primzahl und die Primfaktorzerlegung, die in diesem Fall aus nur einem Faktor besteht, existiert.

IV Wir nehmen nun an, dass jede Zahl die kleiner ist als ein festgelegtes a, in Primfaktoren zerlegt werden kann. Dies ist unsere Induktionsvoraussetzung.

IS Für $a > 2$ gilt

- a ist Primzahl und die Primfaktorzerlegung existiert, oder
- a ist zusammengesetztes, das heißt es gibt ganze Zahlen b und c mit $0 < b, c < a$ so, dass $a = b \cdot c$. Da nach Induktionsvoraussetzung b und c in Primfaktoren zerlegt werden können, kann a ebenfalls als Produkt von Primzahlen geschrieben werden.

Nun gilt es noch die Eindeutigkeit zu beweisen. Wir zeigen, falls zwei Zerlegungen von a existieren, so sind diese gleich.
Seien $k, l \in \mathbb{N}$ und $a = p_1 \cdot p_2 \cdot ... \cdot p_k$ und $a = q_1 \cdot q_2 \cdot \ldots \cdot q_l$ zwei Zerlegungen von a.

Wir führen den Beweis durch Induktion über die größere Anzahl an Primfaktoren der beiden Zerlegungen $(max(k, l))$:

IA Für $max(k, l) = 1$ gilt $a = p_1, a = q_1$ und somit $p_1 = q_1$. Die beiden Primfaktoren sind gleich und damit ist die Primfaktorzerlegung für $max(k, l) = 1$ eindeutig.

IV Wir nehmen nun an, dass für eine maximale Zerlegungsgröße von n die beiden Zerlegungen identisch sind: Für ein festgelegtes $n \in \mathbb{N}$ mit $max(k, l) = n$ gilt $p_1 \cdot p_2 \cdot \ldots \cdot p_k = q_1 \cdot q_2 \cdot \ldots \cdot q_l$ mit $k = l$ und für alle $i \in \{1, ..., n\}$ gilt $p_i = q_i$.

IS Wir nutzen hier eine Variante des Induktionsbeweises, in der wir von einer maximalen Zerlegungsgröße von $n - 1$ auf jede weitere schließen $(n - 1 \mapsto n)$: Da p_1 laut Definition Teiler von a ist, muss p_1 auch Teiler von $q_1 \cdot q_2 \cdot \ldots \cdot q_l$ sein. Nach dem Lemma von Euklid teilt p_1 einen der Faktoren $q_1, q_2, \ldots, q_l$. Da alle Faktoren Primzahlen sind, gibt eine Zahl $j \in 1, \ldots, l$ so, dass $p_1 = q_j$.

Damit gilt, dass

$$p_1 \cdot p_2 \cdot \ldots \cdot p_k = p_1 \cdot q_1 \cdot \ldots \cdot q_{j-1} \cdot q_{j+1} \cdot \ldots \cdot q_l$$

Da innerhalb der ganzen Zahlen gekürzt werden darf, gilt

$$p_2 \cdot \ldots \cdot p_k = q_1 \cdot \ldots \cdot q_{j-1} \cdot q_{j+1} \cdot \ldots \cdot q_l$$

. Nach Induktionsvoraussetzung ist die erhaltene Primfaktorzerlegung mit maximaler Zerlegungsgröße von $n - 1$ eindeutig und damit ist auch jene mit maximaler Zerlegungsgröße von n eindeutig und der Beweis vollständig.

□

Es lässt sich folglich jede beliebige ganze Zahl in ihre Primfaktoren zerlegen. Diese Eigenschaft nützt Euklid in seinem Beweis über die Unendlichkeit der Primzahlen.

2.2.2. Der Beweis von Euklid

Es gibt viele Beweise, die zeigen, dass es unendlich viele Primzahlen gibt. Hier möchte ich mich auf den Beweis von Euklid bzw. einer seiner Abwandlungen beschränken.

Beweis. Um zu beweisen, dass es unendlich viele Primzahlen gibt, nehmen wir das Gegenteil an und versuchen zu einem Wiederspruch zu kommen. Wir nehmen also an, es gibt nur endlich viele Primzahlen. Diese Primzahlen sind $p_1 = 2 < p_2 = 3 < ... < p_n$. Sei nun N jene natürliche Zahl, die wir erhalten, wenn wir alle Primzahlen $p_1, p_2, ..., p_n$ miteinander multiplizieren und 1 addieren.

$$N = p_1 \cdot p_2 \cdot ... \cdot p_n + 1 = 1 + \prod_{i=1}^{n} p_i$$

Wir können zwei Fälle unterscheiden:

Fall 1: N ist eine Primzahl.
Da $N \neq p_1, p_2, ..., p_n$ ist, muss N eine neue, die $n+1$-te Primzahl sein. $p_1, p_2, ..., p_n$ sind also nicht alle Primzahlen und damit wäre unsere Annahme falsch. N kann keine Primzahl sein, es muss also Fall 2 gelten.

Fall 2: N ist keine Primzahl.
Da nach dem Fundamentalsatz der Arithmetik jede zusammengesetzte Zahl in ihre Primfaktoren zerlegt werden kann, gibt es mindestens eine Primzahl q, die N teilt. Da wir alle Primzahlen kennen, muss q eine der n Primzahlen $p_1, p_2, \ldots, p_n$ sein. Damit teilt q sowohl die Summe $p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$ als auch den Summanden $p_1 \cdot p_2 \cdot \ldots \cdot p_n$. Nach den Teilbarkeitsregeln muss q auch die Differenz $p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1 - p_1 \cdot p_2 \cdot \ldots \cdot p_n = 1$ teilen und damit folgt $q = 1$. Damit ist q aber keine Primzahl und wir haben erneut einen Wiederspruch erhalten. Es gibt also mit unserer Annahme keine Primzahl die N teilt und damit ist N auch nicht zusammengesetzt.

Beide Fälle führen zu einem Wiederspruch unserer Annahme es gäbe nur endlich viele Primzahlen und damit ist gezeigt, es gibt unendlich viele Primzahlen. □

Die größte Primzahl die bis heute (Oktober 2021) entdeckt wurde ist $2^{82.589.933} - 1$. Sie wurde von Patrick Laroche 2018 im Rahmen des internationalen Projekts „The GIMPS“ („Great Internet Mersenne Prime Search“) gefunden und hat 24.862.048 Stellen. Würden wir die Zahl ausschreiben, würde sie in etwa 6.673 A4 Seiten füllen. Im Kapitel Primzahltests wird kurz ausgeführt, wie solche Primzahlen gefunden werden.

Die besonderen Eigenschaften der Primzahlen finden im Bereich der Modularrechnung eine wichtige Anwendung wie Rempe & Waldecker (2009) in Kapitel 3 aufzeigen.

3. Restklassen und Modularrechnung

Wenn wir beliebige Zahlen mit Rest durch 7 dividieren, können wir erkennen, dass sich immer wieder dieselben Reste ergeben. Um genau zu sein, gibt es sieben verschiedene Reste, nämlich $0, 1, 2, 3, 4, 5$ und 6. Nach einer kurzen Überlegung leuchtet das auch ein, denn würde der Rest 7 oder mehr ergeben, könnten wir die Zahl ein weiteres Mal durch 7 dividieren und wir müssten den Quotienten um eins erhöhen.

Da es nur endlich viele Reste gibt ist es möglich, Zahlen in Bezug auf ihren Rest nach Division durch eine vorgegebene Zahl zusammenzufassen. Beispielsweise haben $8, 15$ und 22 alle den Rest 1 nach Division durch 7.

Dass es sinnvoll sein kann, Zahlen nach ihrem Rest zusammenzufassen, zeigt ein Beispiel aus dem Alltag. Eine Familie fährt mit dem Auto in den Urlaub und benötigt sechs Stunden bis sie am Ziel ankommt. Startet sie um 8 Uhr los, sind sie um 14 Uhr am Ziel. Wenn sie hingegen um 21 Uhr mit dem Auto losstarten, kommen sie um 3 Uhr an. Wir berechnen im Grunde den Rest von $21 + 6 = 27$ nach Division durch 24. Im 12-Stunden-Format wäre es die Division durch 12. Eine fortlaufende Uhrzeit könnte sich wohl niemand mehr vorstellen.

Ein weiteres Beispiel wären die Wochentage. Wenn heute Montag ist, dann wäre in sieben Tagen auch wieder Montag. In acht Tagen wäre dann Dienstag und in 100 Tagen wäre Mittwoch, da $100 = 14 \cdot 7 + 2$ ist. Wir können also mit Hilfe der Division mit Rest durch 7 die Wochentage bestimmen.

Zahlen, die nach Division durch eine Zahl n denselben Rest besitzen, werden in sogenannte Restklassen zusammengefasst.

Definition: Restklasse

Sei n eine ganze Zahl mit $n \geq 2$. Für eine ganze Zahl a heißt die Menge

$$\overline{a} = \{a + z \cdot n \mid z \in \mathbb{Z}\} = \{a, a + n, a + 2 \cdot n, a + 3 \cdot n, \ldots\}$$

***Restklasse von** a **modulo** n. Die Menge aller Restklassen*

$$\{\overline{a} \mid a \in \mathbb{Z}\} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$$

wird mit $\mathbb{Z}_n$ (Sprich "$\mathbb{Z}$ modulo n") bezeichnet.

Beispiel. *Wir wählen $n = 5$. Dann gibt es in $\mathbb{Z}_5$ die fünf Restklassen $\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}$.*
$\overline{3}$ beinhaltet alle Zahlen, die dividiert durch 5 den Rest 3 haben, also $3, 8, 13, 18, 23, \ldots$

Eine alternative Darstellung zu den Restklassen bietet die Kongruenz modulo n.

Definition: Kongruenz

Es sei $n \geq 2$ eine natürliche Zahl. a und b sind ***kongruent modulo*** *n, wenn sie den selben Rest nach Division durch n haben, also in derselben Restklasse liegen. Wir schreiben*

$$a \equiv b \,(mod\, n).$$

Beispiel. $48 \equiv 23 \equiv 3 \;(mod\, 5)$,
48 *und* 23 *befinden sich somit in der Restklasse* $\overline{3}$ *modulo* 5.

Wir können Zahlen nicht nur Restklassen zuordnen, sondern auch mit den Restklassen rechnen.

3.1. Addition und Multiplikation auf $\mathbb{Z}_n$

Wir können auf $\mathbb{Z}_n$ zwei Operationen definieren:

$$+ : \quad \mathbb{Z}_n \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_n, (\overline{a}, \overline{b}) \longmapsto \overline{a} + \overline{b} := \overline{a + b}$$

und

$$\cdot : \quad \mathbb{Z}_n \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_n, (\overline{a}, \overline{b}) \longmapsto \overline{a} \cdot \overline{b} := \overline{a \cdot b}$$

$\mathbb{Z}_n$ bildet mit diesen Rechenoperationen einen kommutativen Ring. In kommutativen Ringen können Elemente addiert, subtrahiert und multipliziert werden. Allerdings kann ein Element nicht von einem anderen Dividiert werden, es gibt also kein inverses Element bezüglich der Multiplikation.

Beispiel. *Für* $n = 8$ *ist* $\overline{2} + \overline{3} = \overline{2 + 3} = \overline{5}$.
Dass diese Rechenoperation sinnvoll ist, können wir mit den beiden beliebigen Vertretern $2 + k_1 \cdot 8$ *und* $3 + k_2 \cdot 8$ *der beiden Restklassen zeigen:*

$$2 + k_1 \cdot 8 + 3 + k_2 \cdot 8 = 2 + 3 + (k_1 + k_2) \cdot 8 = 5 + (k_1 + k_2) \cdot 8$$

Die Summe ist ein Vertreter der Restklasse $\overline{5}$.

Mit einer zusätzlichen Bedingung können wir in $\mathbb{Z}_n$ auch dividieren und somit $\mathbb{Z}_n$ zu einem Körper machen.

Satz 3.1. Seien $a \neq 0$ und $n \geq 2$ ganze Zahlen.
Die Restklasse $\overline{a} \in \mathbb{Z}_n$ besitzt genau dann ein inverses Element bezüglich der Multiplikation, wenn 1 der größte gemeinsame Teiler von a und n ist ($ggT(a, n) = 1$).

Das inverse Element $\overline{a}^{-1}$ lässt sich mit Hilfe des erweiterten euklidischen Algorithmus berechnen. Ist $ggT(a,n) = 1$, gibt es ganze Zahlen u und v, sodass $u \cdot a + v \cdot n = 1$ gilt. Es muss also $\overline{u \cdot a + v \cdot n} = \overline{1}$ gelten und da $\overline{v \cdot n} = \overline{0}$ folgt

$$\begin{aligned} \overline{u \cdot a} + \overline{v \cdot n} &= \overline{1} \\ \overline{u \cdot a} + \overline{0} &= \overline{1} \\ \overline{u \cdot a} &= \overline{1} \end{aligned}$$

Aus $\overline{u \cdot a} = \overline{1}$ folgt $\overline{u} \cdot \overline{a} = \overline{1}$ und damit $\overline{a^{-1}} = \overline{u}$.

Umgekehrt lässt sich zeigen, wenn $\overline{a}$ ein inverses Element $\overline{a}^{-1}$ mit $\overline{a} \cdot \overline{a}^{-1}$ besitzt, so gibt es eine ganze Zahl v mit $a \cdot a^{-1} = 1 + v/cdotn$ und damit $a \cdot a^{-1} - v \cdot n = 1$. Nach dem Lemma von Bézout folgt $ggT(a,n) = 1$.

Beispiel. *Sei $n = 7$. Wir berechnen das Inverse Element von $\overline{5}$. Da $ggT(5,7) = 1$ können wir das Inverse berechnen. Mit dem erweiterten Euklidischem Algorithmus berechnen wir u und v so, dass $u \cdot 5 + v \cdot 7 = 1$ ist:*

$$\begin{aligned} 7 &= 1 \cdot 5 + 2 \\ 5 &= 2 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned} \qquad \begin{aligned} 1 &= 5 - 2 \cdot 2 \\ 1 &= 5 - 2 \cdot (7 - 5) \\ 1 &= 5 + 2 \cdot 5 - 2 \cdot 7 \\ 1 &= 3 \cdot 5 - 2 \cdot 7 \end{aligned}$$

Wir haben das Inverse $\overline{u} = \overline{3}$ gefunden. Probe: $\overline{3} \cdot \overline{5} = \overline{3 \cdot 5} = \overline{15} = \overline{1}$

Daraus lässt sich schließen, dass ein Inverses insbesondere dann berechnet werden kann, wenn n eine Primzahl ist. Für eine Primzahl p besitzt in $\mathbb{Z}_p$ jede Restklasse $\overline{a} \neq \overline{0}$ ein inverses Element, da für alle $a \in \mathbb{Z}$ gilt, a ist teilerfremd zu p. Somit ist $\mathbb{Z}_p$ ein Körper.

3.2. Chinesischer Restsatz

Ist n keine Primzahl sondern eine zusammengesetzte Zahl, ist das Rechnen modulo n erschwert. Mit Hilfe des Chinesischen Restsatzes können wir das Rechnen modulo $n := n_1 \cdot n_2$ auf jenes modulo n_1 und n_2 zurückführen.

Satz 3.2 (Chinesischer Restsatz)**.** Seien n_1 und n_2 zwei teilerfremde ganze Zahlen mit $n_1, n_2 \geq 2$ und $n := n_1 \cdot n_2$. Zwei ganze Zahlen b und c sind genau dann kongruent zueinander modulo n, wenn $b \equiv c \pmod{n_1}$ und $b \equiv c \pmod{n_2}$ gilt. Zudem gibt es zu zwei ganzen Zahlen s und t immer ein $x \in \mathbb{Z}$ mit $x \equiv s \pmod{n_1}$ und $x \equiv t \pmod{n_2}$.

Beweis. Wir beweisen die Äquivalenz der ersten Aussage des Satzes zunächst von links nach rechts. Wir nehmen an $b \equiv c \pmod{n}$. Das bedeutet, b und c haben denselben Rest r nach Division durch n:

$$b = u_1 \cdot n + r \text{ und } c = u_2 \cdot n + r \text{ daraus folgt}$$

$$b = u_1 \cdot n + (c - u_2 \cdot n) = c + n \cdot (u_1 - u_2).$$

Wir setzen $u := u_1 - u_2$. Durch Umformen erhalten wir

$$b = c + u \cdot n = c + u(n_1 \cdot n_2) = c + un_2 \cdot n_1 = c + un_1 \cdot n_2.$$

Damit ist $b \equiv c \pmod{n_1}$ und $b \equiv c \pmod{n_2}$.

Für die andere Richtung nehmen wir an $b \equiv c \pmod{n_1}$ und $b \equiv c \pmod{n_2}$. Dann gibt es v_1 und $v_2 \in \mathbb{Z}$ so, dass $b = c + v_1 \cdot n_1$ und $b = c + v_2 \cdot n_2$. Daraus folgt

$$b - c = c + v_1 \cdot n_1 - c = v_1 n_1 = c + v_2 \cdot n_2 - c = v_2 n_2.$$

Wir haben gezeigt, dass $b - c$ durch n_1 und n_2 teilbar ist. Da n_1 und n_2 teilerfremd sind, muss $b - c$ auch durch $n_1 \cdot n_2$ und damit durch n teilbar sein. Somit gibt es ein $v \in \mathbb{Z}$ mit

$$b - c = v \cdot n \text{ und also } b = v \cdot n + c,$$

also $b \equiv c \pmod{n}$.

Den zweiten Teil beweisen wir mit Hilfe des erweiterten euklidischen Algorithmus.
Da n_1 und n_2 teilerfremd sind gibt es eindeutig bestimmte ganze Zahlen u und v so, dass $u \cdot n_1 + v \cdot n_2 = 1$. Da $v \cdot n_2 \equiv 0 \pmod{n_2}$ und $u \cdot n_1 \equiv 0 \pmod{n_1}$ muss $u \cdot n_1 \equiv 1 \pmod{n_2}$ und $v \cdot n_2 \equiv 1 \pmod{n_1}$ gelten.
Setzen wir $x := t \cdot u \cdot n_1 + s \cdot v \cdot n_2$, dann gilt

$$x \equiv s \cdot v \cdot n_2 \equiv s \cdot 1 \equiv s \pmod{n_1} \text{ und}$$
$$x \equiv t \cdot u \cdot n_1 \equiv t \cdot 1 \equiv t \pmod{n_2}.$$

□

Damit können wir mit Hilfe der Kongruenz bezüglich der Primfaktoren einer Zahl n auf die Kongruenz modulo n schließen und dabei auf die Vorteile der Rechenregeln eines Körpers zurückgreifen.

3.3. Der kleine Satz von Fermat

Wir haben uns die wichtigsten Rechenoperationen in der Modularrechnung angesehen. Eine letzte Rechenoperation, nämlich das Potenzieren schauen wir uns noch an.

Potenzieren ist nichts anderes als mehrfach Multiplizieren und ist daher ohne Probleme möglich. Von Interesse ist, ob es eine Möglichkeit gibt, die Potenz einer Zahl modulo n schnell zu berechnen.

Wir betrachten zunächst am Beispiel modulo 7, zu welchen Restklassen die Potenzen von 4 gehören:

$$4^0 = 1, \qquad 4^1 = 4, \qquad 4^2 = 16 \equiv 2, \qquad 4^3 = 64 \equiv 1, \qquad 4^4 = (4^2)^2 \equiv 2^2 = 4$$
$$4^5 = 4^{4+1} = 4^4 \cdot 4 \equiv 4 \cdot 4 = 4^2 \equiv 2, \qquad 4^6 = 4^{3\cdot 2} = (4^3)^2 \equiv 1^2 = 1$$

Wir bemerken, dass ab einer bestimmten Potenz sich die Restklassen wiederholen. Dass dies immer der Fall sein muss, ergibt sich daraus, dass es nur endlich viele mögliche Reste modulo n gibt und zwar die Reste $0, 1, \ldots n-1$. Nach spätestens der $n-1$-ten Potenz kommt es zu einer Wiederholung. In unserem Beispiel passiert dies bereits nach der dritten Potenz.

Satz 3.3 (Ordnung modulo n)**.** Sei $n \geq 2$, $a \in \mathbb{Z}$ und a teilerfremd zu n. Die kleinste Zahl k für die $a^k \equiv 1 \pmod{n}$ gilt, nennt man **Ordnung** von a modulo n. Für $k_1, k_2 \geq 1$ gilt $a^{k_1} \equiv a^{k_2}$ genau dann, wenn die Differenz $k_2 - k_1$ ein Vielfaches der Ordnung von a modulo n ist.

Beweisskizze. Mit Hilfe der Potenzregeln für ganze Zahlen können wir a^k geschickt erweitern:

$$a^{k_2} = a^{k_2+k_1-k_1} = a^{k_1} \cdot a^{k_2-k_1}$$

Da a und n teilerfremd sind, können wir die Umformungen problemlos auf die Modularrechnung übertragen. Ist $a^{k_2-k_1} \equiv 1 \pmod{n}$, dann gilt $a^{k_2} = a^{k_1} \cdot a^{k_2-k_1} \equiv a^{k_1} \cdot 1 = a^{k_1} \pmod{n}$. Das ist genau dann der Fall, wenn $k_2 - k_1$ ein Vielfaches der Ordnung von a modulo n ist.

Wenn wir die Ordnung einer Zahl modulo n kennen, können wir somit das Potenzieren auf das Potenzieren mit Zahlen zurückführen, die kleiner als die Ordnung sind. Dazu müssen wir aber erst die Ordnung finden, was uns vor ein erneutes Problem stellt. Mit welchen anderen Voraussetzungen die Potenzierung noch weiter vereinfacht wird, zeigt uns der kleine Satz von Fermat.

Satz 3.4 (Kleiner Satz von Fermat)**.** Seien a eine ganze Zahl und p eine positive Primzahl. Es ist

$$a^p \equiv a \pmod{p}.$$

Zudem gilt, wenn a kein Vielfaches von p ist, dann ist

$$a^{p-1} \equiv 1 \pmod{p}$$

Für den Beweis des kleinen Satzes von Fermat benötigen wir noch einen Hilfssatz, der besagt, dass für $a \in \mathbb{Z}$ und eine positive Primzahl p gilt

$$(a+b)^p \equiv a^p + b^p \pmod{p}.$$

Dies lässt sich mit Hilfe des Binomischen Lehrsatzes beweisen. Nehmen wir diesen Satz als bekannt voraus, lässt sich der kleine Satz von Fermat recht einfach mittels vollständiger Induktion über a beweisen.

Beweis. Beweis vom kleinen Satz von Fermat mittels Induktion über a.

IA Für $a = 0$ ist $0^p = 0$.

IV Für festes $a \geq 0$ gelte $a^p \equiv a \pmod{p}$.

IS Wir schließen nun von a auf $a+1$, so erhalten wir induktiv die Aussage für jedes beliebige $a \geq 0$. Nach dem Hilfssatz gilt $(a+1)^p \equiv a^p + 1^p = a^p + 1 \pmod{p}$. Setzen wir nun noch die Induktionsvoraussetzung ein, erhalten wir

$$(a+1)^p \equiv a^p + 1 \equiv a + 1 \pmod{p}$$

und damit ist der erste Teil bewiesen.
Der zweite Teil des Satzes setzt voraus, dass a und p teilerfremd sind. Wir können also nach Satz 3.1 die erste Aussage durch a dividieren und erhalten

$$\begin{aligned} a^p &\equiv a && \mid \cdot a^{-1} \\ a^p \cdot a^{-1} &\equiv a \cdot a^{-1} \\ a^{p-1} &\equiv 1 && \pmod{p} \end{aligned}$$

und somit unsere Behauptung $a^{p-1} \equiv 1 \pmod{p}$. □

Beispiel. $2^{175} (mod\, 7)$. *Da* 2 *und* 7 *teilerfremd sind, wissen wir aus dem kleinen Satz von Fermat, dass* $2^6 \equiv 1 (mod\, 7)$ *ist. Dividieren wir die Potenz mit Rest durch* 6 *erhalten wir*

$175 = 6 \cdot 29 + 1$ *und damit*

$$2^{175} = 2^{6 \cdot 29 + 1} = (2^6)^{29} \cdot 2 \equiv 1^{29} \cdot 2 = 2 \qquad (mod\ 7)$$

4. Primzahltests

Eine Frage, die im Zusammenhang mit der Primfaktorzerlegung noch offen bleibt, ist, wie diese Primfaktoren berechnet werden können.

Im Grunde gibt es einen sehr einfachen Weg, wie man mit endlich vielen Schritten herausfinden kann, ob eine natürliche Zahl N eine Primzahl ist, oder im Falle der Zerlegbarkeit, wie ihre Primfaktoren lauten.

Wir überprüfen für jede natürliche Zahl $2 \leq n \leq \lfloor \sqrt{N} \rfloor$, ob sie Teiler von N ist. Haben wir eine Zahl n_0 gefunden, die Teiler von N, so gilt $N = n_0 \cdot n_1$ mit $n_1 < N$ und wir führen das Verfahren nun für n_1 anstelle von N bis $n < \lfloor \sqrt{n_1} \rfloor$ fort. Nach endlich vielen Schritten (maximal $\lfloor \sqrt{N} \rfloor - 1$ falls N prim) erhalten wir die vollständige Primfaktorzerlegung von N. Das Verfahren ist zwar sehr einfach, jedoch nimmt es bei sehr großen Zahlen doch einiges an Zeit in Anspruch. Daher war es schon sehr früh für die Mathematiker ein Anliegen, ein möglichst effizientes Verfahren zu finden.

4.1. Der Fermat-Primzahltest

Wir möchten prüfen ob eine natürliche Zahl n mit $n \geq 3$ eine Primzahl oder eine zusammengesetzte Zahl ist. Die folgende Ausführung des Fermat-Primzahltest findet sich vergleichbar in Stroth & Waldecker (2019) im Kapitel Primzahltests.

1. Wir wählen eine natürliche Zahl $a \in \{2, ..., n-1\}$ die teilerfremd zu n ist als Basis für den Test.

2. Im zweiten Schritt berechnen wir a^{n-1} mod n.

3. Wir unterscheiden zwei Fälle:
   Falls $a^{n-1} \equiv 1$ mod n ist, ist die Antwort des Test: „n ist prim"
   Falls $a^{n-1} \not\equiv 1$ mod n ist, ist die Antwort des Test: „n ist zusammengesetzt"

Aus dem kleinen Satz von Fermat lässt sich vermuten, dass es sich leicht überprüfen lässt, ob eine vorgegebene Zahl eine Primzahl ist oder nicht. Allerdings ist eine Umkehrung des Satzes nicht möglich. Für jede Primzahl p gilt zwar, dass $a^{p-1} \equiv 1$ mod p ist, allerdings gibt es auch zusammengesetzte Zahlen n, für die ebenso $a^{n-1} \equiv 1$ mod n für mindestens eine zu n teilerfremde Basis a gilt. Aus dem Satz geht nämlich nicht hervor,

dass eine Zahl n eine Primzahl ist, wenn $a^{n-1} \equiv 1 \bmod n$ gilt, sondern lediglich, dass die Aussage für Primzahlen immer erfüllt ist.

Es ist also möglich ein falsch „positives“ Ergebnis (n ist prim obwohl n zusammengesetzt) zu erhalten. Solche zusammengesetzte Zahlen, für die der Test für mindestens eine Basis a die falsch positive Antwort prim gibt, werden auch **(Fermat-)Pseudoprimzahlen** genannt.
Wir könnten nun vorschlagen, den Test für alle möglichen Basen a durchzuführen, um solche Pseudoprimzahlen aufzudecken. Allerdings gibt es zusammengesetzte Zahlen, die sogenannten **Carmichaelzahlen**, bei denen der Test für jede Basis a die falsche Antwort prim liefert. Die kleinste dieser Zahlen, ist die Zahl 561. Bei dieser Zahl ist das fasche Ergebnis noch leicht aufzudecken, denn wer die Teilbarkeitsregel für die Zahl 3 kennt, erkennt schnell, dass diese Zahl durch 3 teilbar, also zusammengesetzt ist. Für größere Zahlen ist dies aber nicht so einfach möglich und daher stellen solche Carmichaelzahlen ein Problem dar.

Mit Hilfe dieses Tests lässt sich also nicht entscheiden, ob eine vorgegebene Zahl n eine Primzahl ist. Somit ist für unsere ursprüngliche Fragestellung, ob eine vorgegebene Zahl eine Primzahl ist, unbrauchbar. Ein negatives Ergebnis des Primzahltests, also das Ergebnis n ist keine Primzahl, kann jedoch verwendet werden und viele Zahlen können mit Hilfe dieses Test schnell ausgeschlossen werden.

4.2. Lucas-Lehmer Primzahltest

Eine weitaus effizientere Methode, um insbesondere sehr große Primzahlen zu finden bietet der Lucas-Lehmer Primzahltest für Mersenne Zahlen, zu finden in Ribenboim (2006). Die größte bisher gefundene Primzahl $2^{82.589.933} - 1$ ist eine solche Mersenne-Zahl.

Eine natürliche Zahl der Form $M_n = 2^n - 1$ nennt man Mersenne-Zahl. Eine Besonderheit der Mersenne Zahlen ist, dass sie im Binärsystem lediglich aus lauter Einsen bestehen. Betrachten wir die ersten Zahlen

$$\begin{array}{lllll} M_2 = 3 & M_3 = 7 & M_4 = 15 & M_5 = 31 & M_6 = 63 \\ M_7 = 127 & M_8 = 255 & M_9 = 511 & M_{10} = 1023 & M_{11} = 2047, \end{array}$$

so können wir erkennen, dass nicht alle Zahlen Primzahlen sind. $M_4, M_6, M_8, M_9, M_{10}$ und M_{11} gehören nicht dazu. Insbesondere können wir alle Zahlen, bei denen der Exponent n nicht prim ist, sofort ausschließen. Allerdings sind nicht alle Mersenne-Zahlen mit einer Primzahl als Exponent auch prim. M_{11} und M_{23} sind beispielsweise keine Primzahlen.

Mit Hilfe des Lucas-Lehmer Primzahltests kann die Primalität einer Mersenne-Zahl

überprüft werden. Dieser beruht auf einer von Lucas und Lehmer entwickelten rekursiven Folge:

Sei $M_n = 2^n - 1$ mit $n \in \mathbb{N}$. Wir definieren die Folge $(S_k)_{k\in\mathbb{N}}$ mit

$$S_1 = 4, \qquad S_{k+1} = S_k^2 - 2.$$

$M_n = 2^n - 1$ ist genau dann prim, wenn S_{n-2} von M_n geteilt wird.

Beispiel. *Für $n = 3$ ist $M_3 = 2^3 - 1 = 7$ und $S_2 = 4^2 - 2 = 14$. Da 14 von 7 geteilt wird, muss $M_3 = 7$ prim sein.*

Eine weitere Darstellung von S_{k+1}, welche eine Berechnung des n-ten Folgengliedes zulässt, ohne die vorhergehenden zu berechnen, ist die folgende:

$$S_{k+1} = (2 + \sqrt{3})^{2^k} + (2 - \sqrt{3})^{2^k}$$

Beispiel.

$$\begin{aligned} &n = 7 \qquad M_7 = 2^7 - 1 = 127 \\ &S_6 = (2 + \sqrt{3})^{2^5} + (2 - \sqrt{3})^{2^5} = 2.005.956.546.822.746.144 \\ &S_6 \equiv 0 \ (mod\ 127) \end{aligned}$$

Das Prinzip des Primzahltest für Mersenne-Zahlen ist sehr einfach. Die Beschränkung bildet jedoch die dazu nötige Rechenleistung. Wie im Beispiel bereits ersichtlich, werden die Folgenglieder bereits für kleines n sehr groß. Man kann nur erahnen wie lange die Berechnung für die größte bisher bekannte Primzahl mit $n = 82.589.933$ dauerte. Deshalb hat George Woltmann 1996 das Project „The GIMP“ ins Leben gerufen und sich zur Aufgabe gestellt, mit mittlerweile tausenden Freiwilligen und hochleistungsfähigen Computern solche Riesen-Mersenne-Primzahlen zu entdecken. Jeder, der die dafür notwendige Rechenleistung aufbringen kann, kann eine Software von ihrer Webseite www.mersenne.org herunterladen und sich auf die Suche begeben. Bisher wurden jedoch erst 51 Mersenne-Primzahlen gefunden.

5. Kryptographie

Die Kryptographie beschäftigt sich mit der Verschlüsselung von Nachrichten. Dabei entwickelt sie Systeme, um Nachrichten auf möglichst einfache Art und Weise zu verschlüsseln. Die Inhalte dieses Abschnittes sind vergleichsweise im Kapitel Primzahlen und Kryptographie von Rempe & Waldecker (2009) zu finden.

Schon früh war es notwendig Botschaften in verschlüsselter und somit sicherer Form zu überbringen, so dass nur derjenige, für den die Nachricht gedacht ist, sie auch lesen kann. Im Gegenzug dazu steht die Kryptoanalyse. Deren Ziel ist es, die verschlüsselten Nachrichten ohne Kenntnis des Schlüssels zu dechiffrieren. Der Wettstreit der sich schon über Jahrtausende streckt, führte dazu, dass beide Wissenschaften immer raffiniertere Methoden entwickelten.

Bereits in der Antike wurden einfachste Methoden benutz um Botschaften zu verschlüsseln. Ein einfaches Mittel, um Botschaften geheim zu halten, war das Vertauschen von Buchstaben des Alphabets. Eine der bekanntesten ist die **Cäsar-Chiffre**. Es ist überliefert, dass Cäsar das Alphabet einfach um drei Buchstaben verschoben hat, um seine Nachrichten zu verschlüsseln. Wie man sich vielleicht schon denken kann, wurde diese Vorgehensweise schon bald erkannt und die Nachrichten entziffert.

Solche sogenannte monoalphabetische Verschlüsselungen können mit Hilfe der Häufigkeitsanalyse systematisch aufgedeckt werden. Häufige Buchstaben (z.B. Vokale) und Buchstabenkombinationen, wie „st“, „sch“ und „ei“, oder im englischen der Artikel „the“ können im Verschlüsselten Text wiedergefunden werden und so nach und nach der Verschlüsselungsalgorithmus aufgedeckt werden. Somit reicht bei einer Verschlüsselung wie der Cäsar-Chiffre es aus, einen Buchstaben richtig zu erkennen und man hat den Schlüssel gefunden. Insbesondere wenn spezielle Anrede-Floskeln wie z.B. „ave cäsar“ benutzt werden.

Da schon bald klar wurde, dass solche Verschlüsselungsmethoden sehr schnell und einfach dechiffriert werden können, hat man um 1.500 n.Chr. sogenannte polyalphabetische Verschlüsselungen entwickelt. Dabei wechselt man zwischen verschiedenen Schlüsselalphabeten und eine einfache Häufigkeitsanalyse ist nicht mehr möglich. Da aber zum Entschlüsseln ein Codewort nötig ist, welches anzeigt in welcher Reihenfolge gewechselt wurde, wurden auch für diese Chiffrierung Verfahren entwickelt (z.B. der Kasiski-Test), um diese Nachrichten aufzudecken.

Bekannt ist die im 2. Weltkrieg von der Wehrmacht verwendete Verschlüsselungsmaschine **ENIGMA**, die eine sehr komplexe Form der polyalphabetischen Verschlüsselung darstellt. Diese wechselt automatisch zwischen über 100.000 verschiedenen Alphabeten. Dem englischen Mathematiker Alan Turing gelang es um 1940 die Maschine zu knacken. Die Geschichte rund um diesen Entschlüsselungserfolg von Seiten der Alliierten wurde in den beiden Filmen „Enigma - Das Geheimnis“ (2001) und „The Imitation Game - Ein streng geheimes Leben“ (2014) verfilmt. Derartige Verschlüsselungsmethoden haben die Problematik, dass das Wissen über ihren Aufbau auch gleichzeitig Lösung für die Entschlüsselung ist. Insbesondere liegt eine große Schwierigkeit darin, den Schlüssel für die Dechiffrierung sicher jenen zu übermitteln, die die Nachrichten wieder entschlüsseln müssen.

Ein großer Meilenstein der Kryptographie gelang 1975 mit der **Public-Key-Verschlüsselung**. Bei dieser Methode gibt es zwei Schlüssel, die beide vom Empfänger erstellt werden. Der öffentliche Schlüssel (public key) wird, wie der Name schon sagt, öffentlich bekannt gegeben. Dieser wird zum Verschlüsseln der Nachricht genutzt. Die geheime Nachricht kann dann nur mit dem passenden privaten Schlüssel (private key) wieder entschlüsselt werden. Durch dieses Prinzip ist keine Übertragung des Schlüssels vom Sender zum Empfänger mehr notwendig. Eine derartige Verschlüsselung nutzt das von Ronald Rivest, Adi Shamir und Leonard Adleman entwickelte RSA-Verfahren.

5.1. RSA-Verfahren

Das RSA-Verfahren ist ein Verschlüsselungsverfahren, bei dem nicht nur Sender und Empfänger einer Nachricht den Schlüssel kennen, sondern der Schlüssel wird öffentlich bekanntgegeben (public-key). Trotzdem ist nur der Empfänger in der Lage die Nachricht zu entschlüsseln, da nur er eine entscheidende Zusatzinformation (private key) besitzt. Der Trick dahinter ist eine sogenannte „one-way“-Funktion (Einwegfunktion), mit der die Nachricht leicht verschlüsselt aber nicht mehr bzw. nur mit enorm hohem Zeitaufwand entschlüsselt werden kann. Die ursprüngliche Nachricht nur mit der Kenntnis des öffentlichen Schlüssels zu berechnen, ist sogar mit der heutigen Computerleistung nicht in vernünftiger Zeit lösbar. Beim RSA-Verfahren ist diese Funktion die Bildung des Produkts von zwei Primzahlen und deren Umkehrfunktion die Primfaktorzerlegung.

Der erste Schritt ist die Erstellung der beiden Schlüssel vom Empfänger. Der Empfänger wählt zwei sehr große Primzahlen p und q und berechnet

$$n := p \cdot q \text{ und } s := (p-1)(q-1).$$

Er wählt $e \in \{1, ..., s-1\}$ so, dass $ggT(s, e) = 1$. Der Empfänger gibt n und e öffentlich bekannt. Mit diesem öffentlichen Schlüssel kann der Sender seine Nachricht verschlüsseln. Zum Entschlüsseln der Nachricht berechnet der Empfänger ganze Zahlen c und d so, dass $s \cdot c + e \cdot d = 1$. Da s und e teilerfremd sind, können diese immer mit Hilfe des erweitertem Euklidischen Algorithmus (Lemma von Bézout) berechnet werden.
d und n bilden den privaten Schlüssel, mit dem die Nachricht dechiffriert werden kann.

Im nächsten Schritt verschlüsselt der Sender seine Nachricht mit Hilfe des öffentlichen Schlüssels. Die Nachricht m, eine natürliche Zahl, die kleiner als n und zu n teilerfremd ist, wird vom Sender verschlüsselt. Er berechnet dazu den Rest b von m^e durch n. Die verschlüsselte Nachricht b wird dem Empfänger übermittelt.

Im letzten Schritt dechiffriert der Empfänger die verschlüsselte Nachricht. Der Empfänger erhält die ursprüngliche Nachricht, indem er den Rest von b^d nach Division durch n berechnet.

Die Berechnung von $b := m^e \bmod n$ ist ohne Probleme möglich. Umgekehrt ist, wie bereits angesprochen, die Berechnung von m aus der Potenz b ohne zusätzliche Informationen nicht effizient möglich. Kennen wir jedoch die Zahl $s := (p-1)(q-1)$, ist die Berechnung einfach.

Mit dem Satz von Fermat und dem Chinesischen Restsatz können wir zeigen, dass

$$m^s \equiv 1 \pmod{n}$$

Nach dem Chinesischen Restsatz ist $m^s \equiv 1 \pmod{n}$, wenn $m^s \equiv 1 \pmod{p}$ und $m^s \equiv 1 \pmod{q}$. Dies ist erfüllt, da nach Fermat $m^s = m^{(p-1)(q-1)} = (m^{(p-1)})^{(q-1)} \equiv 1^{(q-1)} = 1 \pmod{p}$, sowie $m^s = m^{(p-1)(q-1)} = (m^{(q-1)})^{(p-1)} \equiv 1^{(p-1)} = 1 \pmod{q}$ gilt.

Damit lässt sich zeigen, dass

$$b^d \equiv (m^e)^d = m^{e \cdot d} = m^{1-c \cdot s} = (m^s)^{-c} \cdot m \equiv 1 \cdot m = m \pmod{n}$$

und wir dadurch wieder die ursprüngliche Nachricht m erhalten.

Teil II.

Primzahlen und Kryptographie im Schulunterricht

Aufgrund der besseren Lesbarkeit wird auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) verzichtet. Alle Personenbezeichnungen und personenbezogene Wörter gelten für alle Geschlechter.

Waren vorher die Primzahlen Werkzeug zur Berechnung vom größten gemeinsamen Teiler (ggT) und dem kleinsten gemeinsamen Vielfachen (kgV), so ist auch die Berechnung jener nicht mehr auf konkrete Weise im Lehrplan zu finden.
In dem vom Bundesministerium veröffentlichtem Lehrplan für Mathematik der AHS Unterstufe (RIS, 2021) finden sich folgende Formulierungen:

1. Klasse
1.1 Arbeiten mit Zahlen und Maßen

- *anhand von Teilern und Vielfachen Einblicke in Zusammenhänge zwischen natürlichen Zahlen gewinnen*

sowie
2. Klasse
1.1 Arbeiten mit Zahlen und Maßen

- *wichtige Teilbarkeitsregeln kennen und anwenden können*

Die Primzahlen selbst werden erst in der Oberstufe genannt:
5. Klasse (1. und 2. Semester)
Mengen, Zahlen und Rechengesetze

- *Mit Primzahlen und Teilern arbeiten können; Teilbarkeitsfragen untersuchen können*

Wir wollen mit Hilfe der Schulbuchreihe *Das ist Mathematik* einen Blick auf die aktuelle Einbindung der Thematik im Mathematikunterricht der Unterstufe werfen. Da jede Schule andere Schulbücher verwendet, sowie jede Lehrperson selbst entscheidet, in wie weit sie das Schulbuch im Unterricht einsetzt, ist dies aber nur begrenzt möglich.

Die Schulbuchreihe *Das ist Mathematik* ist nach dem neuen Lehrplan konzipiert. Das bedeutet das Thema Teilbarkeit wird in der sechsten Schulstufe in *Das ist Mathematik 2* (Humenberger, 2017) als erstes großes Thema eingeführt.

Der Einstieg in das Thema Teilbarkeit ist für die Schüler über zwei Seiten mit mehreren Informationsboxen, Bildern und kleinen Rätseln sehr ansprechend gestaltet. Die Inhalte beziehen sich auf die Eigenschaften und Anwendungen der Primzahlen. Die Primzahlen

werden dabei mit den Elementen bzw. Bausteinen der Alchemie und der Chemie verglichen. Primzahlen können wie die „Urelemente“ nicht weiter zerlegt werden und alle weiteren Zahlen können durch Multiplikation der Primzahlen erreicht werden. Der Vergleich ist zum einen sehr anschaulich und unterstreicht die besondere Stellung der Primzahlen innerhalb der natürlichen Zahlen. Zum anderen ist er möglicherweise etwas zu stark, da die natürlichen Zahlen nicht aus den Primzahlen entstanden sind, wie der Vergleich nahelegt.

In diesem Abschnitt wird auch kurz auf die Problematik der Primfaktorzerlegung von sehr großen Zahlen eingegangen und der dadurch resultierende heutige Einsatz in der Datensicherheit im Internet erwähnt.

Auch wird ein kurzes Beispiel zur Kryptographie angeführt, in dem das Alphabet durch 1 und die Primzahlen bis 100 ersetzt wird und so eine geheime Botschaft vermittelt wird. Die Hinzunahme der 1 ermöglicht, dass jeder Buchstabe ersetzt wird. Das kann aber auch dazu führen, dass manche Schüler fälschlicherweise annehmen, dass 1 eine Primzahl ist. Darauf sollte in diesem Beispiel geachtet werden.

Das Thema Teilbarkeit fehlt in den beiden Einstiegsseiten. Dieses wird auf der nächsten Seite mit einem Beispiel eingeführt: Ein Mädchen Pflückt 24 Äpfel, die es anschließend schön geordnet auf einem Tisch auflegen möchte. Es gibt verschiedene Möglichkeiten.

Die aus dem Beispiel resultierenden Zahlen für die Anzahl der Reihen sowie der Äpfel pro Reihe werden als Teiler bezeichnet und in einem Mengendiagramm sowie in der Mengenschreibweise dargestellt. Im Anschluss folgt die Definition für Teiler sowie dessen Eigenschaften in einem farbig unterlegten Kasten, wodurch diese für den Schüler auf einen Blick zu erkennen sind.

Auch der Hinweis, dass durch Null nicht dividiert werden darf ist gegeben. Aus diesem Grund wird die Null in diesem Abschnitt nicht zu den natürlichen Zahlen gezählt. Es wird auch Wert auf eine mathematisch korrekte Aussprache gelegt und die mathematische Symbolik $|$ für „teilt“ und $\nmid$ für „teilt nicht“ eingeführt.

Obwohl das Einführungsbeispiel sehr anschaulich ist, wirkt die Aufgabenstellung etwas gestellt, da wohl nicht vielen Schülern einfallen würde, Äpfel in mehreren Reihen auf den Tisch auszulegen. Hier würde sich ein Aufteilen der Äpfel auf mehrere Personen wie Eltern, Großeltern, Geschwister und weitere Verwandte oder Freunde auch anbieten. Dies würde eher einer alltäglichen Handlung entsprechen. Dadurch würde jedoch ein Teil der Anschaulichkeit verloren gehen, weshalb das Beispiel durchaus seine Berechtigung hat.

Das typische Aufteilen findet sich in den anschließenden Übungen. Die Aufgaben sind nicht nur auf kleine Zahlen beschränkt, sondern es wird Beispielsweise auch die Teilbarkeit von 258.258 und 715.715 durch 7, 11 und 13 untersucht. Durch die Vorgabe der Teiler, wird jedoch nicht auf die Schwierigkeit des Auffindens von Teilern bei sehr großen Zahlen eingegangen. Hier wird der Schwerpunkt auf die Eigenschaften von besonderen Zahlen gelegt. Auch befreundete und vollkommene Zahlen werden im Anschluss noch angesprochen.

Diese Übungen können zum Differenzieren genutzt werden. Schüler, die ohne Probleme die vorherigen Übungen geschafft haben, können hier besondere Zahlen kennenlernen. Die Übung ist auch als schwierige, herausfordernde Aufgabe durch ein Plus markiert. Der Hinweis im Informationsfeld, dass wir noch nicht wissen ob es unendlich viele solcher Zahlen gibt zeigt auf, dass die Mathematik keine abgeschlossene Wissenschaft ist, sondern immer noch Potential für weitere Forschungen besteht. Hiermit kann das Interesse für ein Studium im Bereich der Mathematik geweckt werden. Da für die besonderen Eigenschaften dieser Zahlen keine weiteren Verwendungen im Buch angeführt werden, können sie aber auch übersprungen werden. Eine allgemeine Aufgabe zum Berechnen von Teilern von sehr großen Zahlen fehlt. Die Auftretenden Schwierigkeiten bei solchen Aufgaben könnten eine Verbindung zum späteren Kapitel der Teilbarkeitsregeln schaffen.

Als nächstes wird der größte gemeinsame Teiler (ggT) besprochen. Eingeführt wird er mit einem graphischen Beispiel, in dem eine vorgegebene rechteckige Fläche eines karierten Blattes in einem quadratischen Muster ausgemalt werden soll. Dabei erkennt der Handelnde, dass es sich um gemeinsame Teiler der Rechteckseiten handelt. Diese Übung lässt sich gut für den Unterricht übernehmen. Jeder Schüler kann diese oder eine etwas abgeänderte Aufgabe im eigenen Heft lösen. Die Lösung im Schulbuch kann entweder als Hilfestellung genutzt werden, im Anschluss zur gemeinsamen Besprechung oder zu einer eigenständigen Verbesserung bzw. Kontrolle genutzt werden.

Im nächsten Schritt werden die gemeinsamen Teiler zweier Zahlen als größte Zahl der Schnittmenge der beiden Teilermengen angegeben und im Mengendiagramm Dargestellt. Der ggT wird als größter dieser gemeinsamen Teiler definiert.

Die Aufgaben im ersten Teil dieses Abschnittes beschränken sich auf die von der Definition naheliegende Berechnung. Es sollen zunächst alle gemeinsamen Teiler gefunden werden. Der größte dieser Teiler ist der ggT. Die Beispiele sind auf Zahlen kleiner Hundert beschränkt. Für diese ist die angegebene Rechenweise legitim, insbesondere da in einer Übung auch das Kopfrechnen verlangt wird. Andererseits können die Übungen auch kritisch betrachtet werden, da mathematisch Gesehen der ggT die besondere Eigenschaft hat, dass wir ihn berechnen können ohne die Teiler (insbesondere nicht alle Teiler) der Zahlen zu kennen.

Im zweiten Teil wird der Euklidische Algorithmus erklärt. Hier sind Beispiele und Aufgaben für Zahlen im Hunderterbereich zu finden. Der gesamte Abschnitt ist mit dem Symbol für schwierige, herausfordernde Aufgaben markiert. Der Algorithmus wird in der verkürzten Variante mit der Division eingeführt. Die Schwierigkeit wird dadurch unnötigerweise erhöht, zumal der ggT auch einfach mit mehrfacher Subtraktion berechnet werden kann. Hier könnte die Lehrperson eine Differenzierung durchführen und beide Varianten einführen, sodass die Schüler selbst den Schwierigkeitsgrad wählen können. Die Kategorisierung als schwierige Aufgabe kann insbesondere bei leistungsschwachen

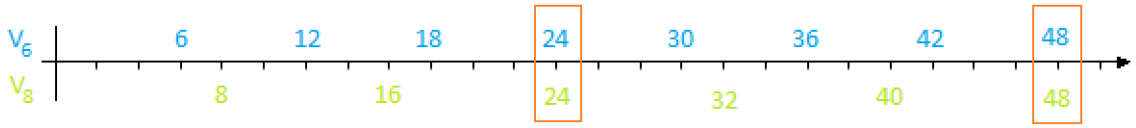


Abbildung 3: Beispielübung zum Zahlenstrahl

Schülern negativen Einfluss auf die nötige Motivation zum Erlernen der neuen Rechenmethode haben. Der Algorithmus sollte für die Schüler leicht verständlich sein, da die notwendigen mathematischen Fertigkeiten ihnen alle bereits bekannt sind.

Der Algorithmus wird im Buch auch grafisch erläutert. Dadurch wird ein weiteres Lernelement hinzugenommen, mit dessen Hilfe den Schülern erklärt werden kann, warum wir mit dem Algorithmus den ggT berechnen können.

Im nächsten Kapitel folgt das kleinste gemeinsame Vielfache. Es wird, wie im Falle des ggT, zunächst die Menge aller Vielfachen (Vielfachenmenge) erläutert. Da die Menge unendlich viele Elemente enthält, wird sie mit Hilfe einer Aufzählung der ersten Elemente dargestellt. Auf die eindeutige beschreibende Darstellung wird verzichtet. Es wird $V_3 = \{3, 6, 9, 12, 15, \dots\}$ anstelle von $V_3 = \{a \in \mathbb{N} \mid 3|a\}$ verwendet.

Da die aufzählende Darstellung bei unendlichen Mengen nicht eindeutig ist, sollten die Schüler von der Lehrperson darauf aufmerksam gemacht werden und kurz über Vor- und Nachteile dieser Schreibweise diskutiert werden. Für interessierte Schüler kann die abstraktere beschreibende Darstellung individuell eingeführt werden.

Die Null wurde zu Beginn des Kapitels der Teilbarkeit ausgeschlossen, so wird sie auch hier korrekterweise nicht in der Vielfachenmenge angegeben.

Das kleinste gemeinsame Vielfache von zwei oder mehreren Zahlen wird wie der ggT über seine Eigenschaften als Vielfache jeder dieser Zahlen, sowie als das kleinste dieser gemeinsamen Vielfachen definiert. Die Berechnung erfolgt wie beim ggT über den Vergleich der Vielfachenmengen. Auch hier beschränkt sich das Schulbuch vorwiegend auf Zahlbeispiele kleiner Hundert. Die Aufgabenstellung variiert von reinen Rechenübungen mit vorgegebenen Zahlen zu Textaufgaben und auch eine anschauliche Variante der Berechnung mit Hilfe des Zahlenstrahls ist zu finden. Die Schüler sollen dabei ähnlich wie in Abbildung 3 die Elemente der beiden Vielfachenmengen auf einem Zahlenstrahl markieren, die gemeinsamen Vielfachen werden anschließend markiert.

Im Zweiten Kapitel des Themas Teilbarkeit werden die Teilbarkeitsregeln behandelt. Die Schüler lernen darin die Regeln für die Teilbarkeit durch $2, 5$ und 10, 9 und 3 sowie $100, 4$ und 25. Ein Beweis für die Teilbarkeitsregeln wird nicht angegeben, jedoch können die Schüler in zwei Aufgaben eine Begründung der Regeln für 9 und 3 selbst erarbeiten. Dadurch kann den Schülern deutlich gemacht werden, dass die Regeln bzw. Sätze in der

Mathematik nicht wie manchmal behauptet einfach „vom Himmel fallen“, sondern es immer eine Erklärung oder genauer gesagt einen Beweis dazu gibt. Das Konzept von Definition, Satz und Beweis kann hiermit den Schülern nahegebracht werden.

In weiteren Aufgaben wird auch die Teilbarkeit durch andere wie die bereits genannten Zahlen angesprochen, wobei die Schüler selbst eine Begründung angeben sollen. Dadurch wird der Fokus nicht nur auf das Einüben der wenigen Teilbarkeitsregeln gelegt. Die Aufgaben sind darauf ausgelegt, dass die Schüler die Teilbarkeitsregeln mit den zuvor gelernten Inhalten verknüpfen und sie dadurch auch verstehen. Ebenso wird dadurch verhindert, dass Schüler sich auf die Überprüfung der Teilbarkeit durch diese wenigen Zahlen beschränken. Dies kann später beispielsweise in der Bruchrechnung von Vorteil sein.

Im Anschluss werden die Summen- und Produktregel definiert. Diese sind wichtige Sätze in Bezug auf die Teilbarkeit. Im Alltag der Schüler sind sie aber wohl nicht sehr häufig zu finden. Trotzdem können sie im Bereich der Bruchrechnung vorteilhaft sein. Insbesondere bei der Problematik vom Kürzen über Summen hinweg, kann die Summenregel nochmals ins Gedächtnis gerufen werden.

In diesem Abschnitt wird auch ein weiterer Schritt in Richtung mathematisch korrekter Beweisführung gemacht. Das Wiederlegen einer Aussage ist leicht möglich, es genügt ein einziges Gegenbeispiel. Ein einzelnes Beispiel zum Belegen einer Aussage reicht aber nicht aus. Hier wird ein Beispiel in Bezug auf die Teilbarkeit geführt. „Wenn eine Zahl t die Zahl a teilt, teilt dann jedes Vielfache von t auch a?“ (Humenberger, 2017, S.30). Die allgemeine Formulierung kann für einige Schüler schwierig zu verstehen sein, deshalb ist dieses Beispiel zu Recht mit einem Plus markiert. Das Grundprinzip von Belegen und Wiederlegen sollte aber für jeden Schüler leicht verständlich sein. Behauptungen und Aussagen auch außerhalb des Bereichs Mathematik gut zu belegen bzw. zu wiederlegen ist auch eine fächerübergreifende Kompetenz, die der Mathematikunterricht vermitteln kann. Mit etwas einfacheren Beispielen kann das Konzept auch schon früher mit den Schülern besprochen werden.

Das dritte Kapitel im Themenbereich Teilbarkeit sind die Primzahlen. Auch wenn sie im Lehrplan nicht mehr zu finden sind, werden sie in diesem Schulbuch angeführt. Die Primzahlen werden definiert als „natürliche Zahlen, die nur 1 und sich selbst als Teiler (unechte Teiler) haben“ (Humenberger, 2017, S.32), insbesondere wird 1 nicht zu den Primzahlen gezählt.

Die Definition ist einfach und verständlich in zwei Sätzen formuliert. Die ersten Primzahlen werden in einer Übung mit Hilfe des Siebes von Eratosthenes berechnet. Wie auch schon bei vorherigen Übungen, wird nicht nur die Ausführung von den Schülern verlangt, sondern sie sollen zudem hinterfragen, warum es reicht die Vielfachen der Zahlen bis 7 zu streichen. Den Schülern kann damit vermittelt werden, dass es von Vorteil sein kann sich über einen vorgegebenen Ablauf Gedanken zu machen, um möglichst effizient und

zeitsparend zu Arbeiten.

Wie bei den Teilern werden auch hier spezielle Primzahlen (Primzahlzwilling und MIRP-Zahlen) vorgestellt. Auch hier sind keine Verwendungsmöglichkeiten angegeben, weshalb sie auch nicht notwendigerweise im Unterricht behandelt werden müssen.

Obwohl in den beiden Einführungsseiten von der Problematik der Primfaktorzerlegung gesprochen wurde, wird sie nun eingeführt. Im Gegensatz zum Euklidischen Algorithmus ist sie nicht mit einem Plus markiert. Dadurch erscheint sie als bevorzugte Variante zur Berechnung des ggT. Vom mathematischen Standpunkt aus, wäre es umgekehrt sinnvoller.

Die wenigen großen Zahlen, die in den Aufgaben in Primfaktoren zerlegt werden, haben gehäuft die Primzahl 2 und weitere sehr kleine Primzahlen als Faktor, wie z.B. $6720 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5 \cdot 7$. Dadurch wird die eigentlich problematische Primfaktorzerlegung noch zusätzlich verharmlost dargestellt. Die in der Einführung genannten Beispiele der Kryptographie werden nicht weiter angesprochen.

Eine in dem Bezug vertretbare Aufgabe lässt sich jedoch finden: „Von einer Zahl ist die Primfaktorzerlegung bekannt. Gib mindestens vier echte Teiler dieser Zahl an, ohne den Wert des Produkts zu berechnen!“ (Humenberger, 2017, S.33). Sind die Primfaktoren einer Zahl gegeben, können weitere Teiler der Zahl schnell berechnet werden.

Anschließend wird die Berechnung von ggT und kgV mittels Primfaktorzerlegung erläutert. Diese ist, wie die Aussage im Schulbuch zu Beginn des Abschnittes vermuten lässt, für die Schüler ganz intuitiv zu verstehen. Ist die Zerlegung bekannt, ist eine Berechnung des ggT durch die Primfaktorzerlegung möglich, in den Beispielen sollen die Primfaktoren aber erst gefunden werden. Die Aufgaben beschränken sich allerdings auf zahlen kleiner Hundert.

Das Schulbuch zeigt in diesem Kapitel auch den Zusammenhang und die Anwendungsgebiete von ggT und kgV auf. Es wird erklärt, dass $a \cdot b = ggT(a,b) \cdot kgV(a,b)$ gilt. Ausgelassen wird dabei die Möglichkeit der Berechnung des kgV mittels ggT. Da die Schüler in dieser Schulstufe noch nicht gelernt haben Formeln umzustellen ist ihnen der Zusammenhang zu $kgV(a,b) = \frac{a \cdot b}{ggT(a,b)}$ nicht klar. Dadurch kann das kgV auch durch den Euklidischen Algorithmus berechnet werden.

Als Anwendungsgebiete des ggT werden die Aufteilung in gleich große Pakete, sowie im geometrischen Bereich, das Aufteilen einer rechteckigen Fläche in gleich große Quadrate genannt. In der Bruchrechnung wird er zum Kürzen von Brüchen verwendet. Nicht vermerkt wird hier, dass weiteres Kürzen nicht mehr möglich ist und die Bruchzahl somit optimal gekürzt wurde. Da die Schüler das Kürzen von Brüchen bereits in der 1. Klasse gelernt haben, kann die Anwendung ohne den Vermerk zum optimalen Kürzen für Schüler unnötig wirken, da sie bereits eine andere Methode zum Kürzen kennen.
Zum Kürzen von Zahlen im Hunderterbereich wird im Schulbuch der zweiten Klasse zunächst die Zerlegung in Primfaktoren von Zähler und Nenner vorgeschlagen und an-

schließend durch die Primfaktoren gekürzt. Alle anderen Aufgaben sind durch Kopfrechnen lösbar, da sie sich im Bereich des kleinen Einmaleins befinden.

Das kgV hat laut Schulbuch Anwendungen bei Aufgaben, in der sich die Ausgangssituation wiederholt. Ohne das vermerkte Beispiel ist nicht ganz klar, was damit gemeint ist. Als Beispiel wird angegeben, dass die Schüler herausfinden sollen, nach wie vielen Umdrehungen die beiden unterschiedlich großen Zahnräder eines Fahrrads wieder in derselben Position stehen wie zu Beginn.

Beim Bruchrechnen gibt der kgV den kleinsten gemeinsamen Nenner an. Erreicht man das Kapitel später im Schuljahr, wird darauf zurückgewiesen.

Die Bruchrechnung ist das nächste Thema im Schulbuch. Die Brüche werden bereits in der ersten Klasse behandelt. Ohne das Wissen über Teiler und Vielfache wird das Kürzen und Erweitern von Brüchen in *Das ist Mathematik 1* (Humenberger, 2016) lediglich als Division bzw. Multiplikation von Zähler und Nenner mit einer Zahl eingeführt. Es wird nicht erklärt, wie der Schüler die Zahl finden kann, durch die er dividieren soll. Ohne das Wissen über gemeinsame Teiler kann die Aufgabe nur durch ausprobieren gelöst werden. Für die Schüler kann das zu großen Schwierigkeiten beim Rechnen mit Brüchen führen. Auch ohne das Wissen über gemeinsame Vielfache ist das Erweitern auf einen gemeinsamen Nenner durch alleiniges multiplizieren mit einer zufällig gewählten Zahl nicht ausreichend zielführend. Daher wäre es eine Überlegung wert, zumindest die Addition von Brüchen in die zweite Klasse zu verschieben.

Da die Schulbuchreihe *Das ist Mathematik* nur für die erste und zweite Klasse gibt ist dort ein Blick in die fünfte Klasse nicht möglich. Vergleichsweise werden im Schulbuch *Mathematik verstehen 5* (Malle 2017, S.26-27) die bisher gelernten Inhalte zur Teilbarkeit und zu den Primzahlen auf zwei Seiten nochmals zusammengefasst. Die beiden Seiten stehen nicht mit den restlichen Kapiteln im Zusammenhang. Der Fokus wird dabei auf die Primfaktorzerlegung gelegt. Es wird der Fundamentalsatz der Zahlentheorie formuliert, sowie eine in Sätzen formulierte Beweisskizze zur Existenz geführt. Ebenso wird die Unendlichkeit der Primzahlen mit Hilfe einer verkürzten Version des Beweises nach Euklid bewiesen. Auch hier wird die Schwierigkeit der Primfaktorzerlegung nicht angesprochen. Die wenigen Beispiele lassen sich einfach berechnen, da der Primfaktor 2 auch hier gehäuft vorkommt.

Das Schulbuch *Das ist Mathematik 2* legt viel Wert auf die korrekte mathematische Bezeichnung und Formulierung. Dies ist wichtig, für eine klare Vermittlung der Inhalte. Damit die Inhalte für die Schüler nicht zu abstrakt wirken, sollte die Lehrperson Beispiele und Verbindungen zu alltäglichen Handlungen bringen.

Die Definitionen sind klar und mit dem minimalst notwendigen mathematischen Sym-

bolen formuliert. Es werden möglichst einfache Sätze verwendet.

Es gibt eine große Variation in den Aufgaben. Sie bestehen nicht nur aus dem Einüben von Rechenregeln oder ähnlichem, sondern es werden auch Formulierungen von Definitionen und Sätzen verlangt, sowie deren Begründungen oder Beweise.

Das Schulbuch spricht die Schwierigkeit der Primfaktorzerlegung und ihre Anwendungsbereiche zwar zu Beginn an, lässt sie dann aber außen vor und vermittelt durch die gewählten Beispiele genau das Gegenteil.

Es gibt eine große Problematik bei der Berechnung von ggT und kgV mit Hilfe von Primzahlen. Wie wir gesehen haben sind die meisten Beispiele, die in der Schule verwendet werden, so aufgebaut, dass die gesuchten Primfaktoren sehr klein sind (meist kleiner 100, und sogar sehr oft keiner 50). Dadurch wird ein eigentlich sehr schwieriger und komplexer Prozess verharmlost.

Der euklidische Algorithmus ist eine sehr einfache Methode um den ggT von beliebig großen Zahlen zu berechnen und findet immer mehr Einzug in den heutigen Unterricht. Die früher zum Großteil angewandte Methode der Primfaktorzerlegung ist für kleine Zahlen noch leicht möglich, für größere Zahlen (insbesondere wenn die Primfaktoren sehr groß sind) schwierig und für sehr große Zahlen beinahe unmöglich. Der Vorteil der Primfaktorzerlegung gegenüber dem euklidischen Algorithmus ist, dass die Eigenschaft der Teilbarkeit sehr deutlich wird. Durch die Primfaktorzerlegung berechnet der Schüler die Teiler einer Zahl und übt in diesem Zusammenhang auch die Teilbarkeitsregeln. Beim euklidischen Algorithmus ist der Zusammenhang mit der Teilbarkeit nicht mehr so klar. Deshalb kann es sein, dass für Schüler die Berechnung mittels Euklidischem Algorithmus nicht so intuitiv ist, wie die Primfaktorzerlegung.

Der eigentliche Vorteil des ggT zweier Zahlen liegt im optimalen Kürzen eines Bruches. Das kürzen von Brüchen wird aber immer noch vorwiegend mittels gemeinsamer Teiler und durch Anwendung von Einmaleins und Teilbarkeitsregeln gelöst. Dadurch verliert die Berechnung des ggT und auch des kgV an Bedeutung. Deshalb wäre es wichtig, dass die Schüler diese gelernten Fähigkeiten auch beim Rechnen mit Brüchen einsetzen.

Eine Einführung der Primzahlen erst in der 5. Klasse macht wenig Sinn, da sie dort nicht in Verbindung mit den restlichen Inhalten stehen. Da die Primzahlen direkt mit der Teilbarkeit zusammenhängen und ihre Definition auch für Schüler der 2. Klasse leicht verständlich ist, ist die Einführung gemeinsam mit der Teilbarkeit von natürlichen Zahlen sinnvoller.

Auch wenn die Primzahlen aus dem Lehrplan der Unterstufe gestrichen worden sind,

sind sie in den meisten Schulbüchern noch zu finden. Es hängt also von der Lehrperson selbst ab, in wieweit sie die Primzahlen im Unterricht behandeln möchte. Wichtig ist aber, dass ein Bezug zu ihren Anwendungsmöglichkeiten auch außerhalb des Mathematikunterrichts aufgezeigt wird und die Problematik der Primfaktorzerlegung mit den Schülern besprochen wird.

6. Einführung in die Teilbarkeit, ggT und kgV

Die Teilbarkeit ist eine wichtige Eigenschaft der ganzen Zahlen, die in der Schule besonders beim Rechnen mit Brüchen und später beim Faktorisieren von Summen eine wichtige Rolle spielt. In dieser Arbeit habe ich versucht einen Einstieg in die Teilbarkeitsrechnung zu planen, der einen problemorientierten Zugang bietet und mit wenig bis gar keinem Vorwissen möglich ist. Die Schüler sollten die Teilbarkeit als eine Eigenschaft erkennen, die auch im Alltag häufig vorkommt. Oft wenden wir sie ganz unbewusst an, ohne den theoretischen Hintergrund zu kennen. Deshalb ist es naheliegend, die Teilbarkeit nicht nur mit reinen Zahlbeispielen zu erläutern und einzuüben, sondern sie in Alltagsbeispielen einfügen.

Das Ziel der Arbeitsblätter ist nicht die Theorie den Schülern zu vermitteln, sondern ein erstes Interesse bei den Schülern zu wecken. Sie werden mit dem Problem der Teilbarkeit in Kontakt gebracht und können es mit ihrem bisherigen Wissen und einigen Hinweisen lösen. Die Theorie kann im Anschluss gemeinsam mit den Schülern erarbeitet werden. Die Schüler erkennen die Theorie als eine Verallgemeinerung ihrer ursprünglichen Aufgabe. Sie kann als Hilfsmittel zur schnellen Lösung von weiteren Problemstellungen genutzt werden. So steht die Theorie nicht als bloßes Konstrukt im Raum, welche mit einfachen Zahlbeispielen eingeübt wird. Die vollständigen Arbeitsblätter sind im Anhang zu finden.

Die Problemstellung

Ein Fliesenleger soll eine rechteckige Fläche fliesen. Er besitzt Fliesen in verschiedenen Größen. Das Ziel ist es, den Boden komplett mit einer Fliesenart auszulegen, ohne dass eine Lücke entsteht oder eine Fliese zerschnitten werden muss.

Das Beispiel des Fliesenlegers eignet sich in diesem Zusammenhang gut, da es sich neben der Teilbarkeit auch auf gemeinsame Teiler und den größten gemeinsamen Teiler (ggT) sowie auf gemeinsame Vielfache und das kleinste gemeinsame Vielfache (kgV) ausweiten lässt.

Der Aufbau der einzelnen Arbeitsblätter ist immer derselbe, mit Ausnahme des dritten Arbeitsblattes, dort fehlt der zweite Teil. Es beginnt mit einer Gruppenarbeit, in der die Schüler gemeinsam versuchen die Aufgabe zu lösen. Die Herangehensweise steht ihnen dabei völlig frei. In der zweiten Aufgabe soll jeder Schüler selbst eine ähnliche Aufgabe lösen und dabei die Erkenntnisse aus der ersten Aufgabe nutzen. Die Ergebnisse werden anschließend in der Gruppe vorgestellt und Lösungen ausgetauscht.

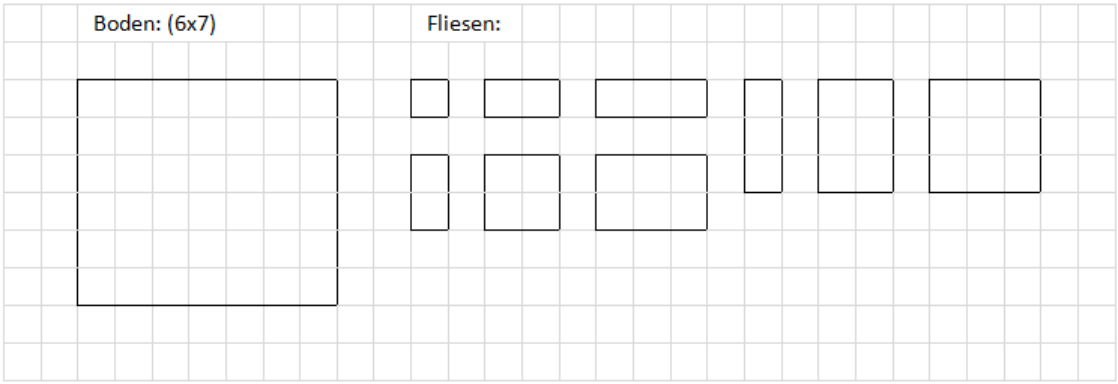
In der letzten Aufgabe sollen die Schüler selbst zu einer allgemeinen Formulierung, der im Arbeitsblatt behandelten Eigenschaft von natürlichen Zahlen gelangen. Eine vorgelegte Diskussionsfrage gibt dabei den Denkanstoß. Ihre Erkenntnisse halten die Schüler in wenigen Zeilen fest.

Arbeitsblatt Teilbarkeit 1

Im ersten Arbeitsblatt geht es um einen ersten Einstieg in die Teilbarkeit von Zahlen. Dabei wird auch auf die Primzahlen hingewiesen, die eine besondere Stellung in Bezug auf die Teilbarkeit innerhalb der natürlichen Zahlen einnehmen.

AUFGABE 1 (Gruppenarbeit)

Mit welchen Fliesen lässt sich der 6 Einheiten breite und 7 Einheiten lange Boden komplett ausfüllen? Malt die entsprechenden Fliesen aus.



Um diese Aufgabe zu lösen, ist kein Vorwissen notwendig. Das Ziel ist es, anhand des konkreten Beispiels, die Teiler der beiden Zahlen 6 und 7 herauszufinden. Diese sind als Länge und Breite einer Bodenfläche abgebildet. In diesem Beispiel werden nur die Zahlen 1, 2 und 3 als Teiler von 6 und 7 getestet. Diese sind in Fliesenform neben der Fläche abgebildet, um wird die Aufgabenstellung für die Schüler besser verständlich zu machen.

Mit dieser Aufgabe wird den Schülern nicht der Begriff des Teilers erklärt, sondern lediglich das Konzept des Teilers vermittelt. Die Schüler sollen erkennen, dass in der Breite 6 sowohl Fliesen mit der Breite 1, 2 als auch 3 passen. In der Länge 7 hingegen, lassen

sich nur Fliesen der Länge 1 einsetzen.

Ein Problempunkt an dieser Aufgabe kann sein, dass gleichzeitig zwei Teiler gesucht sind. Dies kann für manche Schüler zu Schwierigkeiten führen. Die Schüler können aber auf verschiedenen Wegen unterstützt werden. Es können beispielsweise ausgeschnittene Fliesen bereitgelegt werden, mit denen die Schüler die Flächen auslegen können. Das ermöglicht, dass die Schüler mit möglichst vielen Sinnen an das Problem herangehen können. Zusätzlich kann auch noch ein optischer Impuls gegeben werden, indem man die Fliesen unterschiedlich einfärbt. So können die Arbeitsblätter recht einfach individuell verändert werden um eine Differenzierung im Lernprozess zu ermöglichen.

AUFGABE 2 (Einzelarbeit)

Der Fliesenleger soll nach demselben Prinzip noch weitere Räume fliesen.

Bodenflächen:	12x18	15x23	5x11	9x17

a. Entscheide dich für eine der vorgegebenen Flächen. Zeichne die Fläche auf ein kariertes Blatt und versuche herauszufinden welche Fliesen möglich sind. Versuche auch noch größere Fliesen zu finden, als jene in Aufgabe 1.

b. Stelle dein Ergebnis der Gruppe vor und notiere dir die Ergebnisse deiner Mitschüler.

Im Zweiten Teil löst jeder Schüler selbstständig eine ähnliche Aufgabe, es sind lediglich die Maße des Bodens geändert worden. In diesem Falle sind die Größen der Fliesen nicht mehr begrenzt. Sobald alle Lösungen gefunden wurden, werden sie in der Gruppe ausgetauscht. Die Schüler erhalten die Ergebnisse mehrerer Beispiele und können somit erkennen, ob ein Zusammenhang zwischen der Länge und Breite des Bodens und der Länge und Breite der Fliesen existiert.

Um diesen Zusammenhang deutlich zu machen, wird in der dritten Aufgabe eine Diskussionsfrage diesbezüglich gestellt. Die Schüler werden mit Hilfe dieser Frage zur Eigenschaft der Teilbarkeit von ganzen Zahlen hingeführt.

AUFGABE 3 (Gruppenarbeit)

Diskutiert in der Gruppe und notiert euch die wichtigsten Aussagen.

Diskussionsfrage: Warum lassen sich nicht alle Fliesen benutzen?

In welchen Fällen kann nur eine Fliese mit der Länge oder Breite 1 benutzt werden oder Fliesen die über die gesamte Bodenlänge verlaufen?

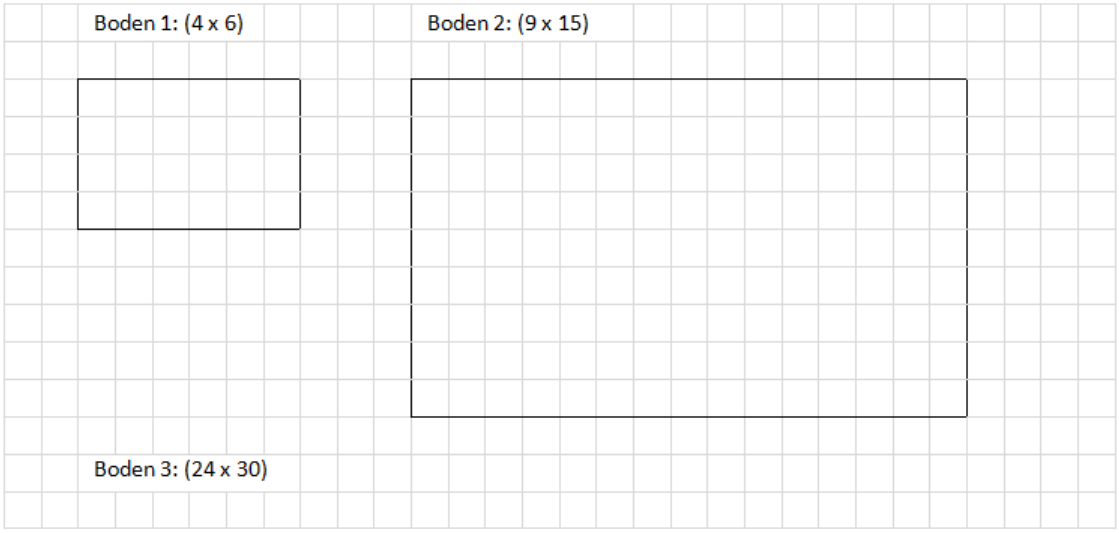
Die letzte Frage versucht einen Hinweis auf die Primzahlen zu geben. Nachdem die Schüler einige Ergebnisse gesammelt haben, sollten sie erkennen, dass Böden mit bestimmten Längen sich nicht gut fliesen lassen. Es gibt also Zahlen, die sich nur durch eins oder sich selbst teilen lassen.

Arbeitsblatt Teilbarkeit 2

Im zweiten Arbeitsblatt lernen die Schüler gemeinsame Teiler von Zahlen und im Besonderen den größten gemeinsamen Teiler zweier Zahlen kennen. Das Arbeitsblatt hat dieselbe Problemstellung wie das erste Arbeitsblatt. In diesem Falle soll der Boden mit quadratischen Fliesen ausgelegt werden.

AUFGABE 1 (Gruppenarbeit)

Mit welchen quadratischen Fliesen (1x1, 2x2, 3x3, 4x4, ...) können diese drei Böden jeweils gefliest werden? Was ist die größte quadratische Fliese die Platz hat?



Hinweis: Überlegt euch die Antwort für Boden 3 im Kopf, oder zeichnet ihn auf ein kariertes Blatt.

Der mathematische Hintergrund ist der folgende: Es ist eine Zahl bzw. Länge gesucht, die die beiden vorgegebenen Zahlen (Länge und Breite des Bodens) teilt. Gesucht sind also gemeinsame Teiler zweier Zahlen und im speziellen der größte gemeinsame Teiler.

Die Schüler können mit Hilfe dieser Aufgabenstellung auch ohne Vorwissen den ggT zweier Zahlen herausfinden. Das kann zunächst durch einfaches ausprobieren („try and error“) passieren.

Im weiteren Schritt (Aufgabe 2) kann durch das erlangte Wissen der Aufgabe 1 und dem Vorwissen über das kleine Einmaleins, die Aufgabe schneller gelöst werden. Das Ausprobieren aller Möglichkeiten dauert sehr lange, ist aber möglich. Die Schüler können in diesem Schritt auf ihr bisheriges wissen zurückgreifen und Zusammenhänge (beispielsweise mit dem kleinen Einmaleins) finden die schneller zur Lösung führen.

AUFGABE 2 (Einzelarbeit)

Der Fliesenleger soll noch weitere Räume mit möglichst großen quadratischen Fliesen auslegen.

Bodenflächen:	7 x 12	6 x 13	7 x 14	9 x 11
	32 x 56	14 x 42	12 x 36	15 x 35

Wähle jeweils einen kleinen und einen großen Raum aus und präsentiere dein Ergebnis der Gruppe.

AUFGABE 3 (Gruppenarbeit)

Diskutiert gemeinsam: Eine 17 x 31 Bodenfläche kann nur mit einer einzigen quadratischen Fliese (mit der 1 x 1 Fliese) ausgefüllt werden. Warum?

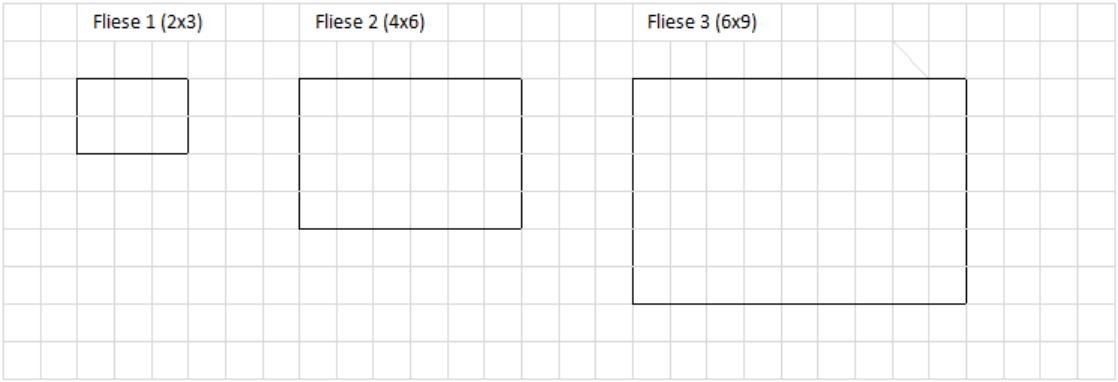
In der dritten Aufgabe ist eine Eigenschaft der Primzahlen gefordert, nämlich dass der ggT zweier Primzahlen eins ist. Ziel des Diskussionsverlaufs ist, dass die Schüler im Anschluss (wenn der Algorithmus zur Berechnung des ggT erklärt wird) nicht nur stur dieser Ausgeführt wird, sondern bereits durch Hinsehen mögliche Teiler erkannt bzw. ausgeschlossen werden. Bei großen Zahlen ist das natürlich etwas schwieriger.

Arbeitsblatt Teilbarkeit 3

Anhand der bereits bekannten Problemstellung wird im dritten Übungsblatt das kleinste gemeinsame Vielfache (kgV) eingeführt. Gesucht ist in diesem Falle nicht eine Fliese sondern eine quadratische Bodenfläche, die mit einer vorgegebenen Fliese ausgefüllt werden soll. Mathematisch gesehen suchen wir eine Zahl, die ein Vielfaches der beiden vorgegebenen Zahlen ist.

AUFGABE 1 (Gruppenarbeit)

Welche quadratischen Flächen lassen sich mit diesen Fliesen auslegen? Nennt mindestens drei! Was ist die kleinstmögliche quadratische Fläche die ihr daraus bilden könnt?



Da es unendlich viele solcher Bodenflächen gibt, sollen die Schüler (mindestens) drei nennen. Zudem wird in diesem Übungsblatt auf die Wiederholungsübungen verzichtet. Bereits in der ersten Aufgabe sollen die Schüler gemeinsam drei Beispiele lösen. Die Frage nach der kleinsten dieser Flächen zielt auf das kgV ab.

Als Unterstützung und Differenzierung für diese Aufgabe können Blätter mit verschiedenen quadratischen Flächen bereitgestellt werden, sowie die Fliesen in ausgeschnittener Form. So können die Schüler mit möglichst vielen Sinnen an diese Aufgabe herangehen.

Die zweite Aufgabe beinhaltet bereits die Diskussionsfrage. Sie geht der Frage nach, wie gemeinsame Vielfache berechnet werden können. Als Anstoß soll zunächst das Produkt der beiden Seiten der Fliese berechnet werden und im Anschluss mit den Lösungen aus der ersten Aufgabe verglichen werden. Die Schüler sollten in der Lage sein zu erkennen, dass alle Flächen aus Aufgabe 1 jeweils Vielfache der gesuchten Produkte sind. Ein Vielfaches zweier Zahlen ist also das Produkt der beiden Zahlen.

AUFGABE 2 (Gruppenarbeit)

Berechnet:

$2 \cdot 3 =$_____ $4 \cdot 6 =$_____ $6 \cdot 9 =$_____

Vergleicht die Ergebnisse mit den Lösungen aus Aufgabe 1. Welche Zusammenhänge könnt ihr erkennen?

_____

_____

Analyse

Wie Schratz und Weiser (2004) es im Zuge des problem- und anwendungsorientierten Lernens formulieren, möchte ich einen Induktiven Lernprozess erreichen, indem die Schüler von einem Beispiel auf allgemeine Gesetzmäßigkeiten schließen. Im Vordergrund bei diesen Übungen steht die aktive Tätigkeit der Schüler. Das Wissen wird ihnen nicht von der Lehrperson vorgelegt, sondern die Schüler erarbeiten es selbst. Die Aufgaben sind so zusammengesetzt, dass sie die Schüler in die richtige Richtung lenken, dabei aber gleichzeitig ein möglichst großer Spielraum zur individuellen Erkenntnisfindung geben ist.

In der Einstiegsaufgabe der Arbeitsblätter wenden die Schüler ihr bisheriges Wissen und ihre Fähigkeiten zur Problemlösung an. Auch die soziale Dimension wird durch das Arbeiten in der Gruppe gefördert, die Schüler gehen miteinander in den Dialog, um zu einer gemeinsamen Lösung des Problems zu kommen. Der gefundene Lösungsweg wird in der zweiten Aufgabe von jedem einzelnen nochmals gefordert. Jeder hat also das Interesse die Lösungsstrategie zu verstehen. Dies verhindert, dass sich in der ersten Aufgabe nur einzelne an der Problemlösung beteiligen. Alle gesammelten Erkenntnisse werden in der dritten Aufgabe diskutiert. Ziel ist es, eine allgemeine Lösungsstrategie zu finden.

Wird im Anschluss die mathematische Theorie zu den Übungen von der Lehrperson vorgestellt, sollten die von den Schülern gesammelten Lösungsstrategien nochmals aufgegriffen und diskutiert werden. Gemeinsamkeiten sollten hervorgehoben und Verbindungen zwischen Theorie und Beispiel deutlich gemacht werden. Dadurch, dass die Schüler selbst in den Erkenntnisprozess mit einbezogen wurden, ist es für sie einfacher den mathematischen Hintergrund zu verstehen. Die Schüler haben zudem das Gefühl, dass ihre Arbeit auch wertgeschätzt wird und haben ein Erfolgserlebnis, wenn die von ihnen ausgearbeitete Lösungsstrategie mit der Theorie übereinstimmt. Das kann wiederum Motivation für weitere Arbeiten liefern.

Die Arbeitsblätter können in einer Einheit gemeinsam bearbeitet werden, oder in die einzelnen Themenabschnitte aufgeteilt werden und in verschiedenen Einheiten verwendet werden. So z.B. kann das Arbeitsblatt ggT, nach den Unterrichtseinheiten zur Teilbarkeit (Theorie und Beispiele), als neuerlicher Einstieg zum Thema gemeinsame Teiler und ggT genutzt werden.

Möglichkeiten zur Differenzierung

Die Gruppenaufteilung ist auf verschiedene Arten möglich. So können gemischte Gruppen, mit leistungsstarken sowie leistungsschwachen Schülern die Möglichkeit bieten, dass

die Gruppenmitglieder sich untereinander unterstützen und so auch die leistungsschwachen Schüler die Problemstellung lösen können. Dabei ist aber zu beachten, dass nicht nur einzelne Schüler die Aufgaben lösen und die anderen einfach die Lösung abschreiben und sich nicht am Lösungsprozess beteiligen.

Eine andere Möglichkeit ist die Unterteilung der Gruppen in Leistungsstufen. Dabei ist es wichtig, dass Hilfsmittel oder erweiterte Fragenstellungen für die unterschiedlichen Gruppen bereitgestellt werden, damit jede Gruppe in etwa dem gleichen Maße gefördert und gefordert wird.

Im Zuge der Übungen habe ich bereits einige Vorschläge zur Erweiterung der Übungen vorgestellt. Als Alternative zu den ausgeschnittenen Formen können auch Klemmbausteine verwendet werden. Die größeren Formen können dabei aus mehreren Steinen zusammengeklebt werden.

Für leistungsstarke Gruppen/Schüler gibt es die Möglichkeit Zusatzaufgaben zu stellen, sowie Erweiterungsaufgaben, die nach der gemeinsamen Besprechung der Inhalte die Übungsblätter nochmals aufgreifen.

Zu Arbeitsblatt 1: Erweiterung hin zur Flächenberechnung

- Wie viele Fließen werden jeweils benötigt um die Flächen zu füllen?
- Wie groß ist die Bodenfläche, wenn ein Kästchen 1 m (10 cm, 1 dm) darstellt?

Zu Arbeitsblatt 2: ggT grafisch Berechnen

Die Berechnung des ggT mit Hilfe des euklidischen Algorithmus lässt sich grafisch anhand derselben Problemstellung berechnen (Abbildung 4).

Schritt 1: Ziehe von der größeren der beiden Längen die kleinere ab und teile die Fläche entlang dieser Linie.

Schritt 2: Fahre mit dem aus Schritt 1 erhaltenen Rechteck auf dieselbe Weise fort und wiederhohle die beiden Schritte so lange, bis du ein Quadrat anstelle eines Rechtecks erhältst. Die Seitenlänge des Quadrates ist der ggT der beiden Seiten des ursprünglichen Rechtecks.

Da das gesuchte Quadrat die Breite 9 lückenlos ausfüllen muss, muss es damit auch das 9×9 Quadrat ausfüllen können. Dieser Teil der Fläche kann also problemlos gefliest

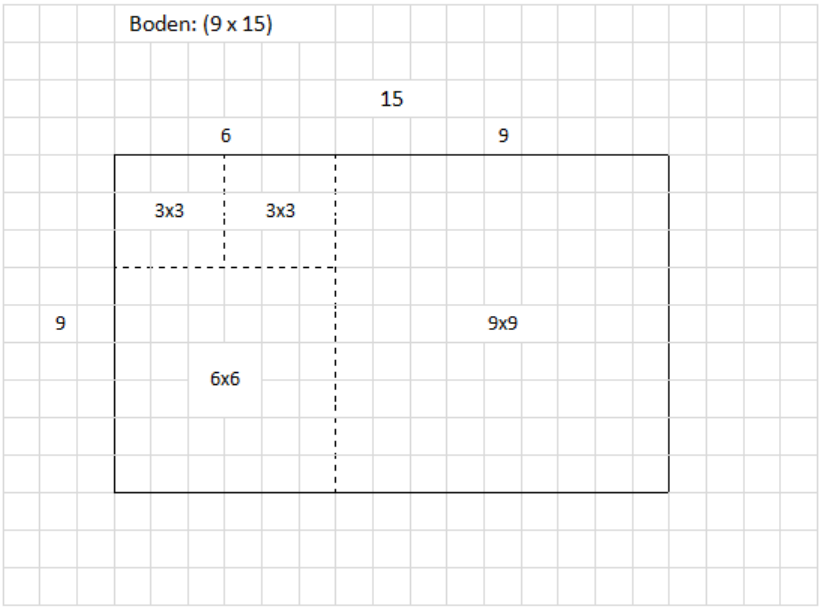


Abbildung 4: Grafische Berechnung des ggT

werden und wir können unsere Suche auf die restliche Fläche beschränken. Das gesuchte Quadrat muss also auch in das 6×9 Rechteck passen und damit auch die Länge 6 lückenlos ausfüllen. Damit kann auch ein 6×6 Quadrat mit der gesuchten Fliese gefliest werden. Mit derselben Strategie fahren wir so lange fort bis wir zum gesuchten Quadrat gelangen. Da die Fläche in jedem Schritt kleiner wird, müssen wir nach endlich vielen Schritten zum Ergebnis kommen.
Das zuletzt erhaltene Quadrat kann alle vorhergehenden Quadrate lückenlos ausfüllen.

Das zugehörige Arbeitsblatt, welches im Anhang zu finden ist, enthält zusätzlich eine genaue Beschreibung der beiden Schritte anhand des dargestellten Beispiels.

Zu Arbeitsblatt 3: Verknüpfung zur Berechnung des kgV

Diese Aufgabe kann als Einführung zur Berechnung des kleinsten gemeinsamen Vielfachen gestellt werden.

- Berechne die Fläche und den größten gemeinsamen Teiler der Seitenlänge der Fliese aus Aufgabe 1. Welcher Zusammenhang besteht zum kleinsten gemeinsamen Vielfachen?

7. Das Sieb des Eratosthenes

Da die Primzahlen aus dem Lehrplan der Unterstufe verschwunden sind und die Zeit, welche man für die einzelnen Inhalte zur Verfügung hat, generell immer knapp ist, ist eine

ausführliche Einführung in die Primzahlen meist nicht möglich. Das folgende Übungsblatt bietet einen kurzen Abstecher in die Welt der Primzahlen, welcher in einer Unterrichtsstunde gut durchführbar sein sollte. Dazu eignen sich beispielsweise auch eine Vertretungsstunde oder eine Einheit im Rahmen eines Projektes.

Das Sieb des Eratosthenes ist ein sehr einfaches Verfahren, um Primzahlen zu entdecken. Die Schüler sollten ohne Schwierigkeiten in der Lage sein, den Siebalgorithmus anzuwenden.

Die Faszination über Primzahlen war bereits bei den Griechen sehr groß. Mit den Fragen im zweiten Teil des Arbeitsblattes, möchte ich diese Faszination auch bei den Schülern wecken.

Ablauf

Die Lehrperson sollte zu Beginn den Siebalgorithmus den Schülern erklären und an der Tafel vorzeigen. Sollte etwas nicht klar sein, können die Schüler nochmals Fragen stellen. Wird das Übungsblatt als Hausaufgabe gegeben, steht eine ausführliche Erklärung des Siebalgorithmus auf dem Zusatzblatt.

Wir wissen bereits vorher, bis zu welcher Zahl wir den Algorithmus wiederholen müssen. Nachdem alle Primzahlen gefunden wurden, kann gemeinsam diskutiert werden, warum der Siebalgorithmus endet, wenn er die 15 erreicht hat. Eine mögliche Zusatzfrage wäre noch, wann der Algorithmus endet, wenn wir alle Primzahlen bis 1000 suchen. Die Antwort ist 32. Wir streichen also als letztes die Vielfachen von 31 und sind fertig.

Das Arbeitsblatt kann allein oder zu zweit bearbeitet werden. Für die Bearbeitung benötigen die Schüler Internetzugang. Die Recherche ist allerdings auch mit dem Handy möglich, sollte kein PC-Raum zur Verfügung stehen.

So viele Primzahlen

Welche Zahlen bis 200 sind Primzahlen? Du kennst sicher schon einige Primzahlen 2,3,5,7,11,13,… doch es gibt noch unendlich viele weitere Primzahlen. Wir versuchen nun die Primzahlen herauszufinden die es bis zur Zahl 200 gibt.

Das Sieb des Eratosthenes

Anstelle von Sand, sieben wir Zahlen. Wie in einen Sieb schütten wir alle Zahlen hinein und sieben die Primzahlen heraus. **Zwei ist unsere erste Primzahl.** Kreise sie ein. Wir sieben alle Zahlen heraus, die Vielfache der **zwei** sind. Die **drei** ist die kleinste Zahl, die übrig bleibt und wir kreisen sie ein. Sie ist unsere **zweite Primzahl.** Wir sieben wieder alle Zahlen heraus, die Vielfache der **drei** sind. Das machen wir so lange, bis die kleinste Zahl, die übrig bleibt, größer ist als 14. Alle Zahlen die wir nicht ausgesiebt haben sind Primzahlen.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130
131	132	133	134	135	136	137	138	139	140
141	142	143	144	145	146	147	148	149	150
151	152	153	154	155	156	157	158	159	160
161	162	163	164	165	166	167	168	169	170
171	172	173	174	175	176	177	178	179	180
181	182	183	184	185	186	187	188	189	190
191	192	193	194	195	196	197	198	199	200

Recherchiere im Internet und beantworte die Fragen:

1. Suche nach Primzahlen, die eine besondere Bedeutung haben. Zum Beispiel, wird die dreizehn oft als Unglückszahl bezeichnet. Nenne einige Beispiele.

2. Notiere wie groß der Abstand zwischen zwei aufeinanderfolgenden Primzahlen ist:

   1 *(zwischen 2 und 3)*, 2 *(zwischen 3 und 5)*, 2, 4, _____

   _____

   Erkennst du ein Muster? _____

3. Es gibt unendlich viele Primzahlen. Wie groß ist die größte Primzahl, die bis jetzt bekannt ist? Wo werden solch große Primzahlen heute verwendet?

Analyse

In diesem Arbeitsblatt steht das forschende Lernen im Fokus. Mit den Fragen soll das Interesse der Schüler geweckt werden. Einige Primzahlen sind den Schülern sicherlich bereits im Alltag begegnet. Zum Beispiel die dreizehn als Unglückszahl, oder die fünf im Pentagramm, welche mit Hexen in Verbindung gebracht werden und sicherlich noch einige mehr.

Primzahlen werden heute immer noch erforscht, weshalb die dritte Frage auch einen kleinen Einblick in das aktuelle Forschungsgeschehen der Mathematik gibt. Die Schüler werden in ihrer Recherche auf die Verwendung der Primzahlen im Bereich der Kryptographie stoßen. Dadurch wird die Mathematik ein bisschen Alltagsnäher. Zudem kann das selbst nachforschen, die Neugierde und Motivation der Schüler wecken.

8. Verschlüsselungsverfahren

Die Verschlüsselung von Nachrichten ist ein Thema, dem die Schüler sehr wahrscheinlich schon einmal begegnet sind und deshalb für sie sehr spannend und interessant sein kann. Die Kryptographie lässt sich immer wieder thematisch gut in den Unterricht eingliedern. Sie ist im Lehrplan als optionales Themengebiet gelistet.

„Neben den im Pflichtfach angegebenen Lehrinhalten, die in vertiefender Form behandelt werden können, sind im Zuge der Erweiterung folgende zusätzliche Bereiche möglich: [...]; Kryptologie und Codierung; [...]“ (RIS, 2021)

8.1. Cäsar-Chiffre

Die Kryptographie lässt sich sehr gut mit dem Geschichtsunterricht verbinden. So passt beispielsweise die Cäsar-Chiffre ideal in den Unterricht zum antiken Rom in der zweiten Klasse Unterstufe. Der Verschlüsselungsmechanismus ist für die Unterstufe leicht verständlich und einfach durchzuführen.

Materialien und Methode

Die Schüler bekommen eine Vorlage (Abbildung 5) von der Lehrperson, welche sie ausschneiden und mit einer Musterbeutelklammer verbinden können. So kann durch einfaches drehen, die Verschlüsselung verändert werden. Die Buchstaben müssen von den Schülern selbst eingetragen werden. Alternativ kann die Schablone auch von den Schülern selbst erstellt werden. Die Scheibe hat den Vorteil, dass durch einfaches drehen die Verschlüsselung

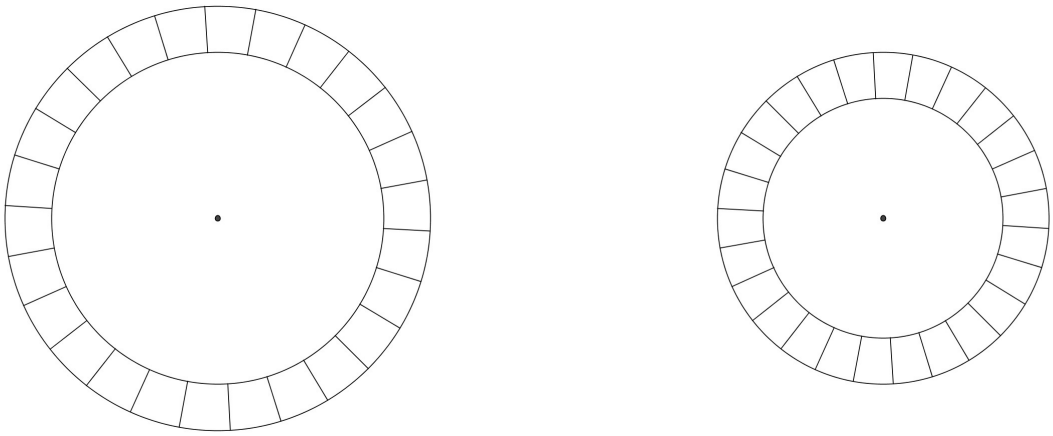


Abbildung 5: Vorlage Cäsar-Chiffre

verändert werden kann.

Als Methode eignet sich das Rollenspiel. Sie lässt ein spielerisches Lernen zu und setzt zusätzlich das Thema in einen geschichtlichen Rahmen. Der Arbeitsauftrag lautet: Spielt eine Szene nach, in der Cäsar eine verschlüsselte Nachricht von den Truppen bekommt, die in Germanien, Gallien oder Ägypten stationiert sind.

Möglicher Ablauf

Die Schüler spielen nach, wie Cäsar eine Nachricht von seinen Truppen erhält. Sie überlegen sich eine passende Nachricht, welche sie mit der soeben gefertigten Scheibe verschlüsseln. Dabei drehen sie eine der Scheiben, sodass jedem Buchstaben ein anderer zugeordnet wird. Anschließend wird die Nachricht mit den veränderten Buchstaben notiert und verschickt. Es kann auch passieren, dass die Nachricht abgefangen wird. Sobald Cäsar die Nachricht erhält, wird sie von ihm entschlüsselt. Dabei muss noch überlegt werden, wie Cäsar mittgeteilt wird, wie die Nachricht verschlüsselt wurde.

Ein weiterer spannender Aspekt in Bezug auf die Kryptographie ist auch der Versuch, den Inhalt einer verschlüsselten Nachricht herauszufinden, ohne den Schlüssel zu kennen. Diese Thematik kann im Anschluss an das Rollenspiel mit der Klasse diskutiert werden. Als Übung können die Schüler alleine oder in der Gruppe sich gegenseitig Nachrichten schicken und versuchen, diese zu entschlüsseln.

Gemeinsam mit dem Fach Deutsch, kann in einer weiteren Unterrichtsstunde die Methode der Häufigkeitsanalyse besprochen werden. Häufige Buchstaben sowie Buchstabenkombinationen in Wörtern können dafür sorgen, dass der Schlüssel recht schnell gefunden wird.

Diese Analyse kann auch gemeinsam mit den Fächern der Fremdsprachen durchgeführt werden.

Ein Hauptanliegen der Kryptographie ist es, den Verschlüsselungsmechanismus ständig zu verbessern und sicherer zu machen. So können im Anschluss in der Klasse Ideen gesammelt werden, wie man die Verschlüsselung verbessern könnte.

Die Buchstaben sind auf der Vorlage der Cäsar-Chiffre nicht eingetragen. Das bietet die Möglichkeit, dass die Schüler selbst neue Verschlüsselungstechniken entwickeln und ausprobieren können, die schwieriger zu knacken sind.

Hier einige Beispiele:

- Das Alphabet auf einer Scheibe umdrehen
- Die Nachricht zusätzlich rückwärts schreiben
- Durchmischung der Buchstaben (nicht nach dem Alphabet, sondern durcheinander auf die Scheibe schreiben)
- Nach jedem Wort den Schlüssel wechseln (die Scheibe nach jedem Wort um x Buchstaben weiterdrehen)

Analyse

Diese Unterrichteinheit beinhaltet vorwiegend anwendungsorientiertes Lernen sowie das dialogisch, kooperative Lernen. Das Rollenspiel ist eine Methode die auch von Schratz und Weiser (2003) im Zuge des anwendungsorientierten Lernens genannt wird. Die Schüler sind dabei selbst aktiv tätig und erlernen die Verschlüsselungstechnik durch praktische Anwendung. Gleichzeitig setzen sie sich aber auch mit den Problemen auseinander, die diese Art der Verschlüsselung aufweist. Die Schüler erfahren diese am eigenen Leib und so wird ein reflexives Denken gefördert, welches nicht direkt von der Lehrperson eingefordert werden muss.

Durch den geschichtlichen Bezug ist der Inhalt des Rollenspiels nicht sehr alltagsnah für die Schüler. Dafür bietet das Rollenspiel die Gelegenheit, sich in die damalige Welt hineinzuversetzen und die Geschichte hautnah zu erleben. Alternativ kann das Rollenspiel auch ohne Geschichtsbezug gestaltet werden, indem die Schüler beispielsweise eine geheime Nachricht an einen Freund oder eine Freundin schreiben, die von niemand anderem gelesen werden soll.

Mit der Häufigkeitsanalyse werden die Schüler in ihrer Problemlösekompetenz gefordert. Hier ist es wichtig, dass die Schüler und nicht die Lehrperson Lösungsvorschläge vorbringen. Die Schüler werden dabei aufgefordert ihre Sprache näher zu analysieren,

oder falls die Übung in einer Fremdsprache durchgeführt wird sich vielleicht auf eine neue Art und Weise sich mit der Sprache zu beschäftigen.

8.2. RSA-Verfahren

Das RSA-Verfahren ist eine wichtige Verschlüsselungstechnik des 21. Jahrhunderts. Es wird beispielsweise genutzt, um Kartenzahlungen und Homebanking sicher zu machen, oder auch, um einen Datenaustausch im Internet vor Angriffen zu schützen.

Die mathemaischen Fähigkeiten, um das RSA-Verfahren anwenden zu können, sollten die Schüler bereits in der Unterstufe erlangt haben. Die in den folgenden Seiten vorgestellten Arbeitsblätter sind jedoch für die Oberstufe konzipiert. Es gibt mehrere Gründe, warum das Thema eher in der Oberstufe, als in der Unterstufe behandelt werden sollte. Zum einen haben die Schüler in der Unterstufe noch wenig Erfahrung mit Kartenzahlungen und Homebanking gemacht, da die meisten ihre Ersparnisse nicht selbst verwalten. Das Thema wird erst dann interessant, wenn sie selbst Geld verdienen und es sicher verwalten möchten.

Ein weiterer Aspekt der hinzukommt ist, dass zwar die Anwendung selbst nicht kompliziert, der Mechanismus dahinter jedoch nicht ganz trivial ist. Eine reflexive Auseinandersetzung darüber, ob das Verfahren sicher ist, sollte auf jeden Fall stattfinden.

Damit das Verfahren auch so alltagsnah wie möglich ist, wurden etwas größere Zahlen gewählt, die von den Schülern der Unterstufe nur sehr schwer und mit großem Rechenaufwand zu bewerkstelligen wären.

Vorwissen

Die Schüler kennen Primzahlen und den größten gemeinsamen Teiler. Sie können potenzieren und mit Rest dividieren. Da die Zahlen recht groß werden, ist in diesem Zusammenhang der Einsatz der Modularrechnung von Vorteil. Technologieunterstützt kann so der Rest von großen Zahlen schnell berechnet werden. Des Weiteren sollte das Konzept von Gleichungen mit zwei Unbekannten und ganzzahligen Lösungen verständlich sein. Auch hier wird die Lösung, wegen der großen Zahlen mit einem Computeralgebrasystem oder einer Onlineanwendung berechnet.

Material und Ablauf

Als Einstieg in die Stunde, erklärt die Lehrperson den Schülern das Grundprinzip des RSA-Verfahrens und dessen Einsatz in der Verschlüsselung von Bankcodes. Um einen Blick in diese Verschlüsselungstechnik zu werfen, sollen die Schüler selbst Nachrichten mit Hilfe des RSA-Verfahrens verschlüsseln und wieder entschlüsseln.

Das Material ist für Dreiergruppen konzipiert. Die Gruppe besteht aus Sender, Empfänger und Hacker. Jedes Gruppenmitglied erhält einen eigenen Arbeitsauftrag. Am Ende sollte eine Nachricht erfolgreich verschlüsselt und wieder entschlüsselt werden. Der Auftrag des Hackers ist nur bedingt erfüllbar. Die Problematik der Primfaktorzerlegung kann im Vorfeld angesprochen werden, oder bei der anschließenden Feedbackrunde aufgegriffen werden.

Sollte genügend Zeit übrig sein, können die Rollen in den Gruppen getauscht werden, oder noch weitere Nachrichten verschickt werden. Am Ende sollte noch Zeit für eine kurze Feedback-Runde eingeplant werden, in der die Schüler ihre Eindrücke und Erkenntnisse, aber auch Schwierigkeiten und eventuelle Unklarheiten äußern können. Falls die Thematik der Sicherheit des Verfahrens nicht von den Schülern angesprochen wird, sollte diese noch von der Lehrperson angesprochen werden. Das Konzept, dass die Primfaktorzerlegung nicht so einfach durchführbar ist, kann den Schülern verständlich erklärt werden. Für interessierte Schüler gibt es die Möglichkeit, Artikel oder Internetseiten vorzuschlagen, die das RSA-Verfahren möglichst einfach erklären. Die Besprechung mit der gesamten Klasse ist nicht sinnvoll, da die Inhalte nicht im Lehrplan zu finden sind und so die benötigte Zeit nicht zu rechtfertigen ist.

Für die Bearbeitung der Arbeitsblätter benötigen die Schüler einen Internetzugang oder Zugang zu einem Computeralgebrasystem (CAS). Da die Zahlen sich im Millionenbereich bewegen, würde die Berechnung zu viel Zeit in Anspruch nehmen. Es ist wichtig, dass der Rechenweg für die Schüler trotzdem nachvollziehbar und verständlich ist.

Des Weiteren kann die Lehrperson eine Liste mit Primzahlen austeilen. Eine solche sollte aber auch leicht im Internet zu finden sein.

SENDER: KUNDE/BANKOMAT

Auftrag: Überlege dir eine vierstellige Zahl, die du versenden möchtest (Sie entspricht dem Code der Bankomatkarte). Warte bis du vom Empfänger den öffentlichen Schlüssel bekommst, der aus zwei Zahlen n und e besteht. Mit diesen Zahlen kannst du deine Nachricht verschlüsseln.

Du möchtest der Bank eine vierstellige Zahl übermitteln. Deine Zahl muss kleiner sein als die Zahl n des öffentlichen Schlüssels sein.

Beispiel: 4628 *ich notiere die Zahl* $\boldsymbol{m = 4.628}$

$\boldsymbol{m =}$

Nachricht

Von der Bank bekommst du die Zahlen des **öffentlichen Schlüssels:**

$\boldsymbol{n =}$ $\boldsymbol{e =}$

a. Berechne mit Hilfe eines Rechenprogramms den Rest von m^e nach Division durch n.
Beispiel: $4.628^7 \, mod \, 4.063.531 = \boldsymbol{1.081.910 = b}$

$\boldsymbol{b =}$

Verschlüsselte Nachricht

Teile dem Empfänger und dem Hacker (wir nehmen an der Hacker hat irgendwie Zugriff zur Nachricht bekommen) die verschlüsselte Nachricht b mit.

EMPFÄNGER: BANK

Auftrag: Erstelle einen Schlüssel, mit dem der Sender seine Nachricht verschlüsseln kann. Erstelle zusätzlich einen zweiten Schlüssel, mit dem du die Nachricht wieder entschlüsseln kannst.

Suche dir zwei Primzahlen aus (mindestens vierstellig). Zeige sie keinem! *Beispiel:* $1231 und\ 3301$

Primzahl 1 | Primzahl 2

a. multipliziere die beiden Primzahlen. *Beispiel:* $1.231 \cdot 3.301 = \mathbf{4.063.531}$

$\boldsymbol{n} =$
öffentlicher Schlüssel

b. ziehe von beiden Primzahlen 1 ab und multipliziere sie dann miteinander.
Beispiel: $1.231 - 1 = 1.230;\quad 3.301 - 1 = 3.300;\quad 1.230 \cdot 3.300 = \mathbf{4.059.000}$

$\boldsymbol{s} =$

c. Wähle eine kleine Primzahl e. Überprüfe ob der größte gemeinsame Teiler dieser Zahl und s eins ist. Wenn nicht, wähle eine andere Primzahl, bis du eine findest mit $ggT(e, s) = 1$.
Beispiel: $ggT(7, 4.059.000) = 1?$ *stimmt, also wähle ich* $\boldsymbol{e = 7}$

$\boldsymbol{e} =$
öffentlicher Schlüssel

Halte die Zahl s geheim! Sage allen die Zahlen n und e (grüne Kästchen). Das ist der **öffentliche Schlüssel.** Nun kann der Sender seine Nachricht verschlüsseln. Berechne in der Zwischenzeit den **privaten Schlüssel d**:

d. Berechne mit Hilfe des erweiterten euklidischem Algorithmus (EEA) c und d so, dass $s \cdot c + e \cdot d = 1$ (nutze dafür eine online Anwendung –Achtung: sollte der Wert für d negativ sein, ist $d + s$ dein privater Schlüssel). c wird nicht mehr benötigt.
Beispiel: $4.059.000 \cdot c + 7 \cdot d = 1 \quad für\ c = -6\ und\ \boldsymbol{d = 3.479.143}$

$\boldsymbol{d} =$
privater Schlüssel

Entschlüssle die Nachricht b, die du vom Sender erhalten hast

Berechne den Rest von b^d nach Division durch und du erhältst die ursprüngliche Nachricht.
Beispiel: $b = 1.081.910 \qquad 1.081.910^{3.479.143} mod\ 4.063.531 = 4.628$

$\boldsymbol{b} =$
Verschlüsselte Nachricht

$\boldsymbol{m} =$
Nachricht

HACKER

Auftrag: Knacke den privaten Schlüssel der Bank

Du bekommst den öffentlichen Schlüssel von der Bank:

$n =$ $e =$

Die Zahl n ist das Produkt von zwei vierstelligen Primzahlen ($n = p_1 \cdot p_2$). Findest du diese Primzahlen heraus, besitzt du dieselben Informationen wie die Bank und du kannst jede Nachricht entschlüsseln.

a. Wie viele vierstellige Primzahlen gibt es?
b. Aus welchen Primzahlen besteht die Zahl n?

Du warst in der Lage die verschlüsselte Nachricht b abzufangen:

$b =$

Verschlüsselte Nachricht

c. Der Sender erhält b, indem er die ursprüngliche Nachricht m mit e potenziert und anschließend den Rest nach Division durch n berechnet. Kannst du diesen Rechenweg umkehren um zur ursprünglichen Nachricht zu gelangen? Was ist der Nachteil dieser Methode?

Analyse

Die Arbeitsblätter sind danach ausgelegt, dass Schüler ihr bisheriges Wissen dazu nutzen, um dieses in einem neuen Problemfeld anzuwenden. Die Qualitätsdimensionen nach Schratz und Weiser (2004), die hier im Mittelpunkt stehen, sind also vorwiegend die Wissens- und Anwendungsdimension. Die Arbeitsblätter geben einen strickten Ablauf vor. Die Schüler sind dadurch in ihrem Lernen etwas eingeschränkt. Dies ist aber notwendig, um das komplexe Verfahren für jeden Schüler durchführbar zu machen. Mit Hilfe der Arbeitsblätter schafft es so jeder Schüler diese moderne Verschlüsselungstechnik zu nutzen, um einen Code oder eine Nachricht geheim zu übermitteln.

Das Arbeitsblatt des Hackers gibt allerdings auch die Möglichkeit das forschende Lernen in dieser Unterrichtseinheit zu fördern. Die Schüler sollen als Hacker selbst eine Möglichkeit finden, um hinter die verschlüsselte Nachricht zu kommen. Das Ziel ist dabei nicht die Lösung des Problems, sondern viel mehr die eigenen Fähigkeiten auszuschöpfen. Diese sollen dazu genutzt werden, um hinter das mathematische Verfahren zu blicken und selbst auf die Probleme zu stoßen, die eine Dechiffrierung fast unmöglich machen.

Die Gruppenbildung und die anschließende Feedbackrunde mit der gesamten Klasse fördert auch das dialogisch, kooperative Lernen. Während der Bearbeitung der Arbeitsblätter sind die Schüler durch die Aufgabenstellung auf sich allein gestellt, deshalb ist der anschließende Dialog umso wichtiger. Um diesen Aspekt noch stärker zu fördern, können die Arbeitsblätter auch jeweils zu zweit bearbeitet werden, damit sich die Schüler gegenseitig unterstützen und austauschen können. Insbesondere in der Rolle des Hackers könnten so neue Ideen entstehen.

Literatur

Bücher

Herrmann, Dietmar (2020). *Die Antike Mathematik, Die Geschichte der Mathematik in Alt-Griechenland und im Hellenismus.* Berlin: Springer Spektrum.

Rempe-Gillen, Lasse & Waldecker Rebecca (2016). *Primzahltests für Einsteiger. Zahlentheorie – Algorithmik – Kryptographie.* Wiesbaden: Springer Spektrum.

Ribenboim, Paulo (2006). *Die Welt der Primzahlen. Geheimnisse und Rekorde.* Berlin: Springer.

Stroth, Gernot & Waldecker Rebecca (2019).*Elementare Algebra und Zahlentheorie.* 2. Auflage, Cham: Birkhäuser.

Schulbücher

Humenberger (Hrsg.) u.a. (2016). *Das ist Mathematik 1. Schulbuch.* Wien: öbv.

Humenberger (Hrsg.) u.a. (2017). *Das ist Mathematik 2. Schulbuch.* Wien: öbv.

Malle u.a. (2017). *Mathematik verstehen 5. Schülerbuch.* Wien: öbv.

Artikel

Schratz, Michael & Weiser, Bernhard (2002): Dimensionen für die Entwicklung der Qualität von Unterricht. *Journal für Schulentwicklung 4/2002*, S. 36 - 47.

Webseiten

RIS (2021): Lehrpläne – allgemeinbildende höhere Schulen. Verfügbar unter: `https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10008568` , abgerufen am 30.11.2021.

Mersenne Research, Inc. (2021): Great Internet Mersenne Prime Search GIMPS. Finding World Record Primes Since 1996. Verfügbar unter: `https://www.mersenne.org/`, abgerufen am 30.11.2021.

Abbildungen

Wellcome Library, London (2014, 8. Oktober). Portrait of Euclid. https://commons.wikimedia.org/wiki/File:Portrait_of_Euclid_Wellcome_L0019815.jpg, zugeschnitten, https://creativecommons.org/licenses/by/4.0/legalcode

Anonym (2006, 17. März). Eratosthenes. https://commons.wikimedia.org/wiki/File:Eratosthenes.jpg, zugeschnitten, https://creativecommons.org/publicdomain/zero/1.0/legalcode

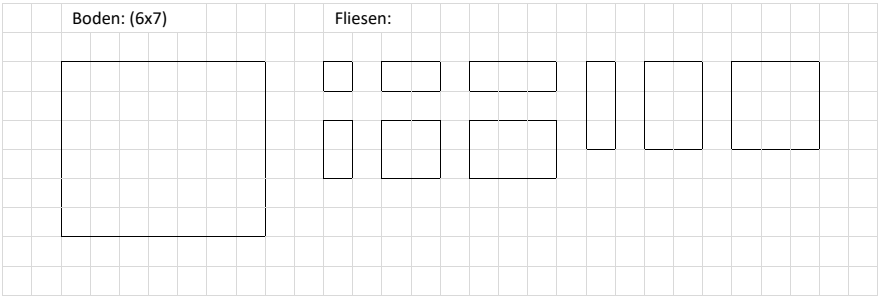
Anhänge

Arbeitsblatt Teilbarkeit 1

Ein Fliesenleger soll eine rechteckige Fläche fliesen. Er besitzt Fliesen in verschiedenen Größen. Das Ziel ist es, den Boden komplett mit einer Fliesenart auszulegen, ohne dass eine Lücke entsteht oder eine Fliese zerschnitten werden muss.

AUFGABE 1 (Gruppenarbeit)

Mit welchen Fliesen lässt sich der 6 Einheiten breite und 7 Einheiten lange Boden komplett ausfüllen? Malt die entsprechenden Fliesen aus.



AUFGABE 2 (Einzelarbeit)

Der Fliesenleger soll nach demselben Prinzip noch weitere Räume fliesen.

Bodenflächen: 12x18 15x23 5x11 9x17

a. Entscheide dich für eine der vorgegebenen Flächen. Zeichne die Fläche auf ein kariertes Blatt und versuche herauszufinden welche Fliesen möglich sind. Versuche auch noch größere Fliesen zu finden, als jene in Aufgabe 1.

b. Stelle dein Ergebnis der Gruppe vor und notiere dir die Ergebnisse deiner Mitschüler.

AUFGABE 3 (Gruppenarbeit)

Diskutiert in der Gruppe und notiert euch die wichtigsten Aussagen.

Diskussionsfrage: Warum lassen sich nicht alle Fliesen benutzen?

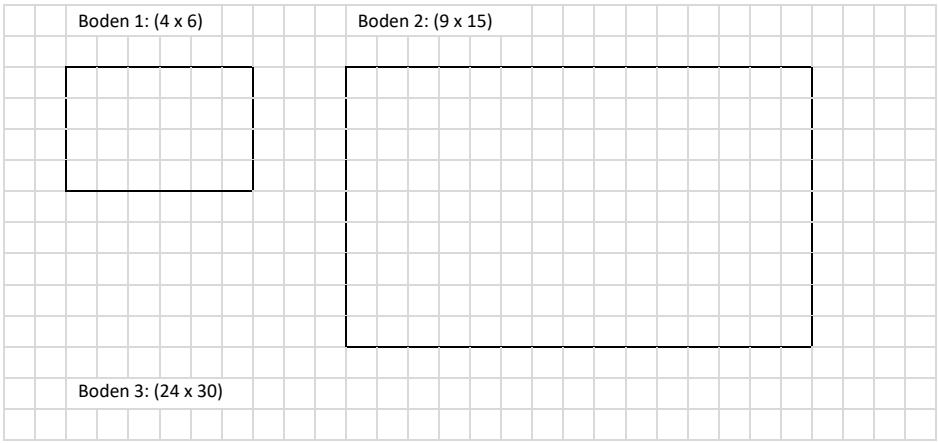
In welchen Fällen kann nur eine Fliese mit der Länge oder Breite 1 benutzt werden oder Fliesen die über die gesamte Bodenlänge verlaufen?

Arbeitsblatt Teilbarkeit 2: Der größte gemeinsame Teiler (ggT)

Ein Fliesenleger soll eine rechteckige Fläche fliesen. Er besitzt Fliesen in verschiedenen Größen. Das Ziel ist es, den Boden komplett mit einer Fliesenart auszulegen, ohne dass eine Lücke entsteht oder eine Fliese zerschnitten werden muss.

AUFGABE 1 (Gruppenarbeit)

Mit welchen quadratischen Fliesen (1x1, 2x2, 3x3, 4x4, …) können diese drei Böden jeweils gefliest werden? Was ist die größte quadratische Fliese die Platz hat?



Hinweis: Überlegt euch die Antwort für Boden 3 im Kopf, oder zeichnet ihn auf ein kariertes Blatt.

Boden 1: _____

Boden 2: _____

Boden 3: _____

AUFGABE 2 (Einzelarbeit)

Der Fliesenleger soll noch weitere Räume mit möglichst großen quadratischen Fliesen auslegen.

Bodenflächen:	7 x 12	6 x 13	7 x 14	9 x 11
	32 x 56	14 x 42	12 x 36	15 x 35

Wähle jeweils einen kleinen und einen großen Raum aus und präsentiere dein Ergebnis der Gruppe.

AUFGABE 3 (Gruppenarbeit)

Diskutiert gemeinsam: Eine 17 x 31 Bodenfläche kann nur mit einer einzigen quadratischen Fliese (mit der 1 x 1 Fliese) ausgefüllt werden. Warum?

_____

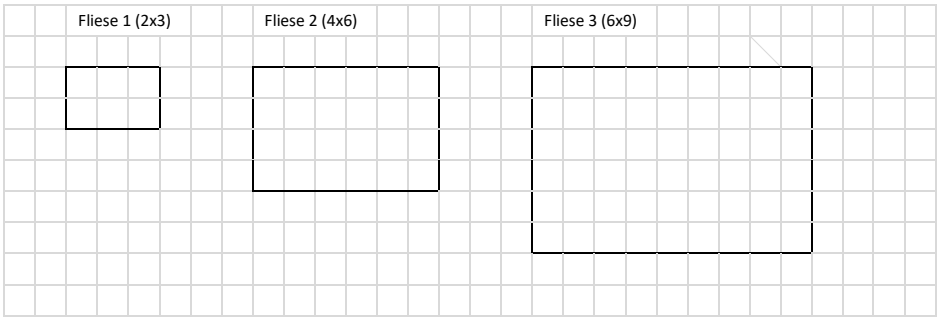
_____

Arbeitsblatt Teilbarkeit 3: Das kleinste gemeinsame Vielfache (kgV)

Ein Fliesenleger soll eine rechteckige Fläche fliesen. Er besitzt Fliesen in verschiedenen Größen. Das Ziel ist es, den Boden komplett mit einer Fliesenart auszulegen, ohne dass eine Lücke entsteht oder eine Fliese zerschnitten werden muss.

AUFGABE 1 (Gruppenarbeit)

Welche quadratischen Flächen lassen sich mit diesen Fliesen auslegen? Nennt mindestens drei! Was ist die kleinstmögliche quadratische Fläche die ihr daraus bilden könnt?



Fliese 1: _____

Fliese 2: _____

Fliese 3: _____

AUFGABE 2 (Gruppenarbeit)

Berechnet:

$2 \cdot 3 =$_____ $4 \cdot 6 =$_____ $6 \cdot 9 =$_____

Vergleicht die Ergebnisse mit den Lösungen aus Aufgabe 1. Welche Zusammenhänge könnt ihr erkennen?

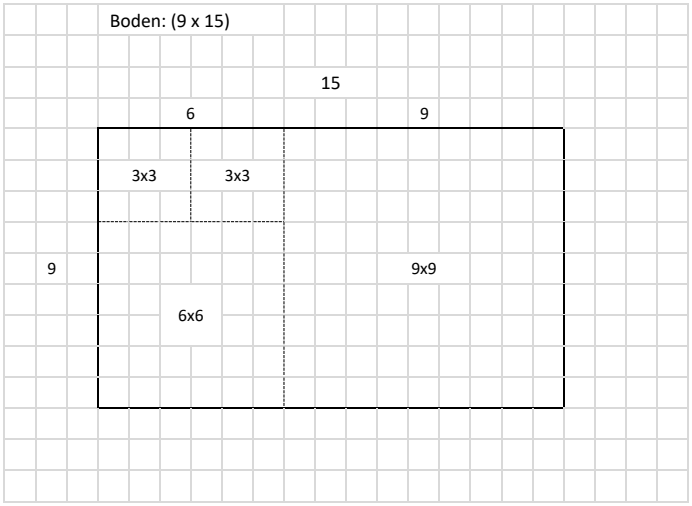
_____

_____

_____

_____

Den ggT mit dem euklidischen Algorithmus grafisch berechnen



Schritt 1: Ziehe von der größeren der beiden Längen die kleinere ab und teile die Fläche entlang dieser Linie.

In unserem Beispiel schneiden wir von der Länge 15 neun Kästchen ab. Wir teilen die Fläche senkrecht und erhalten ein 9 mal 9 Quadrat und ein 6 mal 9 Rechteck.

Schritt 2: Fahre mit dem aus Schritt 1 erhaltenen Rechteck auf dieselbe Weise fort und wiederhohle die beiden Schritte so lange, bis du ein Quadrat anstelle eines Rechtecks erhältst. Die Seitenlänge des Quadrates ist der ggT der beiden Seiten des ursprünglichen Rechtecks.

Wir teilen im zweiten Schritt das Rechteck waagrecht auf, in dem wir sechs Kästchen von der Breite 9 abziehen. Wir erhalten ein 6x6 Quadrat und ein 3x6 Rechteck.

Wir wiederholen dasselbe für das 3x6 Rechteck indem wir die Länge 6 um drei Kästchen verkleinern. Wir erhalten zwei 3x3 Quadrate und sind fertig.

Der größte gemeinsame Teiler von 9 und 15 ist 3.

Warum funktioniert das?

Da das gesuchte Quadrat die Breite 9 lückenlos ausfüllen muss, muss es damit auch das 9x9 Quadrat ausfüllen können. Dieser Teil der Fläche kann also problemlos gefliest werden und wir können unsere Suche auf die restliche Fläche beschränken. Das gesuchte Quadrat muss also auch in das 6x9 Rechteck passen und damit auch die Länge 6 lückenlos ausfüllen. Damit kann auch ein 6x6 Quadrat mit der gesuchten Fliese gefliest werden. Mit derselben Strategie fahren wir so lange fort bis wir zum gesuchten Quadrat gelangen. Da die Fläche in jedem Schritt kleiner wird, müssen wir nach endlich vielen Schritten zum Ergebnis kommen.

Kontrolle: Das zuletzt erhaltene Quadrat kann alle vorhergehenden Quadrate lückenlos ausfüllen.