

MATHEMATISCHE GRUNDLAGEN DER KRYPTOLOGIE

UNTERRICHTSVERLAUF UND HINTERGRUND

Dieses Werk ist unter einem **Creative Commons 3.0 Deutschland Lizenzvertrag** lizenziert:

- Namensnennung
- Keine kommerzielle Nutzung
- Weitergabe unter gleichen Bedingungen

Um die Lizenz anzusehen, gehen Sie bitte zu <http://creativecommons.org/licenses/by-nc-sa/3.0/de>.

Dr. Thilo Höfer – E-Mail: thilo.hoefler@rps-schule.de – April 2018

Inhaltsverzeichnis

Einleitung	3
Stellenwertsysteme (Stunde 1 – 4)	3
Grundlegender Aufbau (Stunden 1 – 2).....	3
Schriftliche Rechenverfahren (Stunde 3).....	4
Das Hexadezimalsystem (Stunde 4).....	4
Primzahlen, Teiler und Vielfache (Stunde 5 – 13)	5
Das Sieb des Eratosthenes (Stunde 5).....	5
Teilbarkeitsregeln (Stunden 6 – 8).....	6
Teilmengen und Primfaktorzerlegungen (Stunden 9 – 10).....	7
Das kgV, der ggT und der Euklidische Algorithmus (Stunden 11 – 13).....	8
Ergänzungen (Stunde 13 + x).....	9
Literatur.....	11

Einleitung

Die mathematischen Grundlagen der Kryptologie sind ein Themenstrang, der während der drei Jahre IMP kontinuierlich vertieft wird. Um diese Vertiefung auf ein festes Fundament zu setzen, beginnt die Einheit nicht mit ausschließlich „neuen“ Inhalten. Vielmehr werden einige bereits bekannte, für die Kryptologie grundlegende Inhalte wiederholt und das Wissen darüber ausgeweitet. So haben sich die Schülerinnen und Schüler sowohl im Mathematikunterricht, als auch im Aufbaukurs Informatik einiges Wissen über Primzahlen, Teilbarkeiten und Stellenwertsysteme angeeignet. Stand bisher allerdings eher das „Tun“ im Vordergrund – beispielsweise im Sinne von Regeln aufstellen und anwenden –, so soll nun auch dem Aspekt des Begründens eine immer größere Rolle zugeteilt werden. Dadurch wird erreicht, dass die Schülerinnen und Schüler die zahlentheoretischen Grundlagen verstehen, die in den kommenden Jahren als Fundament für die Kryptologie benötigt werden (zum Beispiel innerhalb der Kongruenzrechnung).

Zeichenerklärung: Für alle Arbeitsblätter innerhalb der Einheit „mathematische Grundlagen der Kryptologie“ gilt das Symbol * als Zeichen der Binnendifferenzierung nach oben – d.h. insbesondere anspruchsvollere Aufgaben, die nicht zum Pflichtbereich gehören, werden hiermit gekennzeichnet. Aufgaben, die mehrere * tragen, sind dabei vom Niveau her höher anzusiedeln als Aufgaben mit nur einem *.

Erklärung zur Formatierung im folgenden Text: Die Überschriften der Arbeitsblätter (im weiteren Text mit AB abgekürzt), auf die in den folgenden Abschnitten verwiesen wird, sind stets durch *kursive, unterstrichene Schreibweise* kenntlich gemacht. Dahinter wird in Klammern und *kursiver Schreibweise* stets der Name der Datei genannt, unter dem sich das Arbeitsblatt im Ordner „2_kopiervorlagen“, bzw. dessen Lösung im Ordner „4_loesungen“ befindet.

Stellenwertsysteme (Stunde 1 – 4)

Bereits in Klasse 5/6 lernen die Schülerinnen und Schüler im Mathematikunterricht neben dem Dezimalsystem ein weiteres Zahlensystem kennen. Spätestens im Rahmen des Aufbaukurses Informatik in Klasse 7 erfahren sie das Prinzip des Binärsystems und können natürliche Zahlen zwischen 0 und mindestens 255 in Bitfolgen darstellen und umgekehrt. Diese Kenntnisse werden nun wiederholt, weitergeführt und vertieft. Dazu vergleichen die Schülerinnen und Schüler zunächst das Binärsystem mit dem dezimalen Stellenwertsystem und überführen die beiden Darstellungen wechselseitig. Anhand der Addition und einer weiteren Grundrechenart – hier bietet die Wahl zwischen Subtraktion, Division und Multiplikation eine Gelegenheit zur Binnendifferenzierung – erweitern sie ihre Kenntnisse über die Strukturen der gängigen Rechenverfahren und deren Übertragbarkeit auf andere Stellenwertsysteme. Der abschließende Wechsel zwischen dem Binärsystem und dem Hexadezimalsystem eignet sich gut, um weitere Verknüpfungen zum Bereich der informationstechnischen Grundlagen herzustellen (z.B. Bits und Bytes, ASCII, diskrete Farbmischungen).

Grundlegender Aufbau (Stunden 1 – 2)

Im Bildungsplan zum Aufbaukurs Informatik wird das Prinzip des Binärsystems und die wechselseitige Umwandlung von Binärzahlen und natürlichen Zahlen zwischen 0 und 255 bereits thematisiert. Demzufolge werden die Schülerinnen und Schüler mit gewissen Vorkenntnissen aus diesem Bereich vertraut sein. Um dieses Wissen zu aktivieren, beginnt das erste AB Binärzahlen – Grundlagen (zu finden in der Datei 01_mgk_binär-Einstieg) mit einer

offenen Fragestellung und darauf abgestuften Hilfekärtchen, auf die dann wiederholende Übungen folgen (Aufgabe 1 - 3). Nach dieser Wiederholung widmet sich Aufgabe 4 dem vergleichenden Verständnis von Stellenwertsystemen. Dadurch wird das Wissen über das Prinzip des Binärsystems mit dem dezimalen Stellenwertsystem verknüpft, sodass nicht nur der grundsätzliche Aufbau von Stellenwertsystemen im Allgemeinen, sondern insbesondere auch die Gemeinsamkeiten und Unterschiede zwischen den einzelnen Stellenwertsystemen entdeckt und verbalisiert werden. Mithilfe des AB *Binärzahlen – Übungen (01_mgk_binär-Einstieg)* werden diese alten und neuen Erkenntnisse auf verschiedenen Niveaustufen eingeübt.

Das dritte und letzte AB , *Binärzahlen – Knobelspaß (01_mgk_binär-Einstieg)*, ist ein optional einsetzbares AB. Hier wird nochmals die Gelegenheit gegeben, binnendifferenzierend auf allen Niveaustufen zu üben. Es bietet jedoch mit Sicherheit ein hohes Maß an Motivation, sodass der Einsatz in der gesamten Klasse angedacht werden kann – dies muss der Fachlehrer unter Abwägen des Zeitbedarfs individuell entscheiden. Für den Fall, dass der Zeitbedarf gegen einen Einsatz in der Klasse spricht, kann es auch zur Binnendifferenzierung für einzelne leistungsstarke Schülerinnen und Schüler dienen, die im „Pflichtbereich“ eventuell deutlich schneller als ihre Mitschülerinnen und Mitschüler sind.

Schriftliche Rechenverfahren (Stunde 3)

Auch wenn keine explizite Erwähnung des mathematischen Bereichs der Numerik im Bildungsplan IMP zu finden ist, bietet er dennoch immer wieder die Möglichkeit, Einblicke in die Grundlagen der Numerik zu erfahren. Die Stunde zu den schriftlichen Rechenverfahren kann ebenso motiviert werden. Die Schülerinnen und Schüler haben nun das Binärsystem als Speichermöglichkeit für Computer kennengelernt. Ob und wie die weitere Verarbeitung bei Berechnungen funktioniert, ist jedoch noch unbekannt. Die Vorgabe des Bildungsplans, dass die Schülerinnen und Schüler neben der Addition noch eine weitere Grundrechenart schriftlich durchführen können, ist als Aufforderung zur Binnendifferenzierung zu sehen, da nicht alle Schülerinnen und Schüler dasselbe Rechenverfahren lernen müssen. Dieser Vorgabe kommt das AB *Binärzahlen – Rechenverfahren unter der Lupe (02_mgk_binär-Rechenverfahren)* nach. Zunächst widmen sich alle Schülerinnen und Schüler innerhalb der Aufgabe 1 der Addition von Binärzahlen. Da danach jede Schülerin und jeder Schüler noch ein weiteres Verfahren können muss, ist Aufgabe 2 an sich als verpflichtend zu sehen. Die Setzung des Symbols * dient hier lediglich zur Bezeichnung der Niveau-Abstufungen. Da die Schülerinnen und Schüler sich zunächst nur ein weiteres Verfahren auswählen müssen, ist die Division, die indirekt die Subtraktion einführt als ebenso schwierig anzusehen, wie die Multiplikation, bei der ein aus dem Zehnersystem unbekanntes Übertragen über mehrere Stellen erforderlich sein kann.

Das Hexadezimalsystem (Stunde 4)

Die Zahldarstellungen im Binärsystem erreichen sehr schnell eine recht unübersichtliche Länge. Deshalb hat sich der Einsatz des Hexadezimalsystems (16er-System) in einigen Bereichen der Datenverarbeitung durchgesetzt. So basieren der ASCII und die Mischung von Farben am Monitor auf natürlichen Zahlen im Bereich von 0 bis 255 – das sind Zahlen, die hexadezimal zweistellig darstellbar sind. Die Stellen im Hexadezimalsystem bestehen von rechts nach links aus Vielfachen von der Zahlen $16^0 = 1$, $16^1 = 16$, $16^2 = 256$, $16^3 = 4096$, usw. Als jeweiligen Vielfachen einer Stelle werden zunächst weiterhin die Ziffern 0 bis 9 verwendet. Um beispielsweise 10, 11, 12, 13, 14 oder 15 Einer anzeigen zu können, benötigt man jedoch noch sechs weitere Ziffern. Diese werden der numerisch aufsteigenden Reihenfolge nach A, B, C, D, E und F benannt. Die Zahl $B9_{16}$ bedeutet somit (von rechts nach links) 9 Einer + 11 Sechzehner, also 185.

Die Motivation für dieses weitere Stellenwertsystem kann im Unterricht optional über das AB

Hexadezimalzahlen-Hintergrundwissen (03_mgk_binär-Hexadez) eingeführt werden, oder der Lehrer stellt dies in einem eigenständigen Lehrvortrag vor. Insbesondere Farbmischprogramme eignen sich als Präsentationsbasis, zahlreiche davon sind als Freeware im Internet verfügbar, darunter einige, die direkt aus dem Browser heraus bedienbar sind. Ein Beispiel dafür wird direkt auf dem AB angegeben. Alternativ dazu und sehr empfehlenswert ist die App Farbcode im Ordner 8_Apps (erklärende Datei: 02_alg_farbcode_mit_hex_ai) von Monika Eisenmann. Hier können die Schülerinnen und Schüler ihre Farbcodeentschlüsselung einstellen und gleich selbst anhand der App überprüfen.

Die tatsächliche Einführung des Hexadezimalsystems ist dann auf dem AB Hexadezimalzahlen – ein „neues“ Stellenwertsystem zu finden (03_mgk_binär-Hexadez). Dieses AB gliedert sich in einen erklärenden Text und die zugehörigen Anwendungsaufgaben. Da der Bildungsplan sich auf die wechselseitige Umwandlung zwischen Binär- und Hexadezimalzahlen beschränkt, widmen sich die Aufgaben 1 – 3 auch nur genau dieser. Erst in den optionalen „*-Aufgaben 4 und 5 ist an die Erklärung des Prinzips bzw. eine weitere Umformung in das Dezimalsystem gedacht.

Anmerkung: Auf dem AB wird das Hexadezimalsystem auch über die Speichergrößen motiviert. Die Größenangaben hierfür werden in der Literatur uneinheitlich verwendet. Beispielsweise wird 1 kB (1 Kilobyte) teilweise als 1000 Byte, aber auch als 1024 ($=2^{10}$) genannt – letzteres trägt aber auch den Namen KiB (1 Kibibyte). Mehr darüber findet man beispielsweise in Wikipedia unter dem Stichwort „Byte“.

Hinweis: In der Einheit „Informationsgesellschaft und Datensicherheit“ des Fachbereiches Informatik befindet sich im Bildungsplan die folgende Kompetenz: „Die Schülerinnen und Schüler können erläutern, dass moderne Verschlüsselungsverfahren auf elementaren Verschlüsselungsverfahren basieren [...]“. In den zugehörigen Materialien von Frau Miriam Klein wird dabei das AES-Verfahren erklärt und mit CryTool1 veranschaulicht. Da in der CryTool1-Visualisierung Hexadezimalzahlen verwendet werden, ist es von Vorteil, wenn in IMP-Mathematik bereits die Hexadezimalzahlen behandelt wurden (3.1.2.1 Mathematische Grundlagen der Kryptologie), bevor die Informatik dieses Thema behandelt.

Primzahlen, Teiler und Vielfache (Stunde 5 – 13)

Dieser zweite, größere Teil der Einheit Mathematische Grundlagen der Kryptologie widmet sich der Vertiefung des Wissens über Bereiche der elementaren Zahlentheorie, zum Beispiel zu Primzahlen, Teilbarkeiten, Teilern, Teilmengen und Vielfachen. Über die Kenntnisse aus dem Mathematikunterricht der Klassen 5 bis 7 hinaus lernen die Schülerinnen und Schüler weitere grundlegende Zusammenhänge, Algorithmen und Regeln kennen, die sowohl einen in sich schlüssigen Bereich der Zahlentheorie abgrenzen und darüber hinaus in den folgenden Jahren im Zuge der Kongruenzrechnung noch bedeutsam sein werden. Wie schon im ersten Teil dieser Einheit liegt zunächst die Schwierigkeit darin, das Wissen der Schülerinnen und Schüler aus den Vorjahren so zu aktivieren, dass die benötigte Ausgangsbasis bei allen (wieder) vorhanden ist und sich die Schülerinnen und Schüler, bei denen das Wissen nicht in Vergessenheit geraten ist, nicht „langweilen“. Vom ersten AB an spielt deshalb die Möglichkeit zur Binnendifferenzierung wieder eine große Rolle im vorliegenden Unterrichtsgang.

Das Sieb des Eratosthenes (Stunde 5)

Auch wenn Primzahlen bereits Thema im Mathematikunterricht der Klassen 5 / 6 waren, so wird die Definition sicherlich nicht mehr im Bewusstsein aller Schülerinnen und Schüler sein. Ebenso

ist zu erwarten, dass die Antwort auf die häufig von Schülern gestellte Frage, ob die Zahl 1 als Primzahl zu werten ist oder nicht, zunächst nicht von allen gegeben werden kann. Dieser Voraussetzung folgend wird auf dem AB Primzahlen – Das Sieb des Eratosthenes (04_mgk_Primzahlen-Einstieg) eine Definition für Primzahlen vorangestellt und dann die Begründung, dass 1 keine Primzahl ist, eingefordert. „Ganz nebenbei“ ist diese Aufgabe ein gutes Beispiel dafür, dass prozessbezogene Kompetenzen wie beispielsweise das Argumentieren und das Kommunizieren von Beginn an (im Sinne von „auf relativ niedrigem Niveau“) eingefordert werden können – und dementsprechend auch sollten.

Aufgabe 2 ist vom Fachlehrer individuell zu bedenken: Es kann durchaus sein, dass die Schülerinnen und Schüler das Sieb des Eratosthenes¹ bereits kennen. Je nachdem kann es also sinnvoll sein, auf Aufgabe 2 zu verzichten und das Sieb des Eratosthenes direkt mit der zur Informatik übergreifenden Aufgabe 5 zu wiederholen (auch als Hausaufgabe denkbar).

In Aufgabe 4 können dann verschiedene Aspekte entdeckt werden. Einerseits enden alle so entstandenen Zahlen auf die Ziffer 1, was an den Faktoren 2 und 5 vor der Addition von 1 liegt. Diese Erkenntnis spielt in späteren Aufgabenstellungen eine erneute Rolle. Außerdem sind alle so erzeugten Zahlen Primzahlen. Dies kann entweder zu einem späteren Zeitpunkt zum Beweis ausgebaut werden, dass es unendlich viele Primzahlen geben muss, oder direkt an dieser Stelle als noch zu ergänzende Zusatzaufgabe für leistungsstarke Schülerinnen und Schüler eingebunden werden.

Aufgabe 3 dient einerseits dem Kennenlernen der Mersenne-Zahlen – so nennt man Zahlen, die mithilfe des Terms $2^n - 1$ erzeugt werden können –, den aktuell bedeutendsten Zahlen für die Suche nach großen Primzahlen. Gleichzeitig wird hier erneut der Bereich des Argumentierens und Beweisens eingefordert, da die Schülerinnen und Schüler durch die Aufgabe auf die Methode des Widerlegens einer Behauptung durch ein Gegenbeispiel geführt werden (ohne diese hier beim Namen zu nennen).

Teilbarkeitsregeln (Stunden 6 – 8)

Das Ziel dieser drei Unterrichtsstunden ist ein über die reine Anwendung von Teilbarkeitsregeln (wie im Bildungsplan Mathematik der Klassenstufe 6 – dort ist „nur“ das Anwenden können der Teilbarkeitsregeln 2, 3, 5, 6, 9 und 10 eingefordert) hinausgehendes Verständnis für den inneren (multiplikativen) Aufbau der natürlichen Zahlen. Auch hier steht natürlich zunächst das Wiederaufgreifen von bereits Gelerntem an erster Stelle, um dann dieses Wissen sukzessive zu erweitern und vertiefen. Beispielsweise werden einerseits noch weitere Regeln entdeckt und andererseits die vorhandenen Regeln begründet, wodurch eine Vertiefung vom reinen Anwenden zum Verständnis der „Funktionsweise“ der Regeln stattfindet.

Am Beginn der drei Stunden steht (nach der Definition von Teilbarkeit) mit Aufgabe 1 auf dem AB Teilbarkeit und Teilbarkeitsregeln: Wiederholung (05_mgk_Teilbarkeit-Wdhg) eine Think-Pair-Share-Phase zu den bereits bekannten Teilbarkeitsregeln aus Klasse 5 / 6. Da im Mathematikunterricht die kategorisierende Unterscheidung in Endstellenregeln und Quersummenregeln eventuell noch nicht durchgeführt wurde, müssen die Schülerinnen und Schüler bereits hier ein wenig die Struktur der Regeln analysieren. Aufgabe 2 dient dann dem wiederholenden Üben dieser Regeln auf verschiedenen Schwierigkeitsstufen.

¹ Das Sieb des Eratosthenes ist ein Verfahren, um alle Primzahlen zwischen 2 und einer natürlichen Zahl n zu bestimmen. Dazu werden diese Zahlen zunächst notiert und dann von der Primzahl 2 beginnend zunächst alle Vielfachen der 2 gestrichen. Die nächstgrößere, nichtgestrichene Zahl wird sodann als Primzahl identifiziert (die 3) und auch deren Vielfache gestrichen. So verfährt man fort, bis alle Zahlen entweder als Primzahl identifiziert, oder gestrichen sind.

Viele Teilbarkeitsregeln begründen sich durch die beiden in Aufgabe 3 aufgezeigten Sätze. Deshalb ist es grundlegend, dass diese beiden Sätze von den Schülerinnen und Schülern beherrscht werden. Aufgrund dieser Bedeutung wird eine Besprechung dieser Aufgabe im Plenum dringend empfohlen. Im Anschluss an die Besprechung bietet es sich an, zumindest einige Teilaufgaben aus Aufgabe 4 ebenfalls im Plenum schrittweise durchzuführen. Durch diese Aufgabe schärft sich rückwirkend auch nochmals das Verständnis für die Aussagekraft und Grenzen der Sätze, insbesondere im Hinblick auf die (Nicht-)Gültigkeit der Umkehrsätze².

In Folge dieser bereits vertiefenden Wiederholung der bekannten Teilbarkeitsregeln werden dann weitere End- und Quersummenregeln durch die Schülerinnen und Schüler entdeckt und begründet. Insbesondere beim Erarbeiten des strukturellen Aufbaus der Quersummenregeln ist es sicherlich hilfreich, wenn man die Schritte im Team durchspricht. Daher ist der zweite Auftrag des AB Teilbarkeit und Teilbarkeitsregeln: Weitere Endstellen- und Quersummenregeln (05_mgk_Teilbarkeit-Wdhg) bereits als Partnerarbeit beschrieben. Ob die vorangestellten Aufträge zu den Endstellenregeln zunächst noch in Stillarbeit, oder bereits in Partnerarbeit stattfinden sollen, kann sicherlich am besten mit Blick auf die individuelle Lerngruppe entschieden werden. Die Stillarbeit bietet den Vorteil, dass sich jeder Einzelne inhaltlich intensiv hineindenken muss, ein „mentales Abtauchen“ also erschwert wird. Für den sofortigen Beginn in Partnerteams spricht, dass sich das Finden und Organisieren aller Teams auf die Anfangsphase konzentriert und nicht laufend geschieht (wie es der Fall ist, wenn sich die Teams erst nach und nach zusammensetzen, also immer dann, wenn zugehörige Partner mit den ersten Aufträgen in Stillarbeit fertig sind).

Die abschließenden Aufgaben auf dem AB Teilbarkeit und Teilbarkeitsregeln: Summen und Produkte (05_mgk_Teilbarkeit-Wdhg) widmen sich schließlich noch der Kombination mehrerer Teilbarkeitsregeln, wie es die Schülerinnen und Schüler bereits durch die Teilbarkeitsregel zum Teiler 6 kennen. Dabei sollen den Schülerinnen und Schülern die Möglichkeiten und Grenzen dieser Regelverknüpfungen bewusst werden. Das AB schließt dann mit einigen Anwendungen dieser Regeln ab, wie sie auch in einschlägigen Wettbewerben zur Mathematik immer wieder vorkommen.

Teilmengen und Primfaktorzerlegungen (Stunden 9 – 10)

Die Arbeitsblätter Teilmengen und Primfaktorzerlegungen (06_mgk_Teilmengen) der nächsten beiden Stunden sind so angelegt, dass die Schülerinnen und Schüler zunächst in Zweierteams entweder die beiden Seiten von Team Mü oder die beiden Seiten von Team Nü bearbeiten. Im Anschluss daran treffen sich je ein Team Mü und ein Team Nü, bilden somit eine Vierergruppe und bearbeiten dann die zugehörige dritte Seite mit den gemeinsamen Aufträgen für beide Teams. Mit den fachlichen Inhalten „Teilmengen“ und „Primfaktorzerlegungen“ liegt hier ein Niveau vor, das für Schülerinnen und Schüler der Klassenstufe 8 eigentlich problemlos zu bewältigen sein müsste. Dies bietet die Möglichkeit, das systematische und reflektierte (Er-)Arbeiten und die sinnvoll strukturierte Kommunikation in den Vordergrund zu stellen. So werden die Schülerinnen und Schüler durch die Aufgaben dazu angehalten, nicht nur Teilmengen und Primfaktorzerlegungen zu bestimmen, sondern das Vorgehen so zu überdenken, dass es „geschickt“ ist und dieses dann schriftlich festzuhalten. Die Partnerphase dient dabei der Kommunikation zum eigenen Vorgehen, gefolgt von der Gruppenphase, in der die Zweierteams gegenseitig als Kontrollinstanz des Formulierten eingesetzt werden (Aufgabe 1 und 2 der gemeinsamen Aufträge). Die Aufgaben 3 bis 6 dienen einem mehrschichtigen Abschluss: So wird hier das Aufstellen von Teilmengen und Primfaktorzerlegungen nicht nur nochmals geübt, sondern auch noch auf verschiedene Eigenschaften hin untersucht, sowie mit

² Dies ist eigentlich im Geometrie-Teil 3.1.2.3 (5) im Bildungsplan verortet. Es bietet sich aber insbesondere auch zur internen Verknüpfung an dieser Stelle an.

den Hasse-Diagrammen (und somit den Bereichen der Graphentheorie und auch der Geometrie) vernetzt. Die Besprechung dieser Aufgaben 3 bis 6 kann im Plenum derart stattfinden, dass verschiedene Gruppen jeweils eine Aufgabenlösung vorstellen und diese dann gemeinsam diskutiert werden.

Als letzte Seite befindet sich auf dem AB noch der Teil Zum Schmökern: Mersenne-Primzahlen und vollkommene Zahlen (06_mgk_Teilmengen). Dieser ist nur als „allgemeinbildende Zusatzinformation“ gedacht. Er kann „die Wartezeit“ einzelner, schon fertiger Gruppen auf die Mitschülerinnen und Mitschüler verkürzen, oder auch als Anregung für ein Referat / einen GFS-Vortrag dienen. Hierin wird der (verblüffende) Zusammenhang zwischen Mersenne-Primzahlen und vollkommenen Zahlen dargestellt.

Hinweis: In der Einheit „Informationsgesellschaft und Datensicherheit“ des Fachbereiches Informatik wird die Vigenère-Verschlüsselung thematisiert. Bei der Kasiski-Methode, die eine erfolgreiche Angriffsstrategie auf diese Verschlüsselung darstellt, benötigt man grundlegende Kenntnisse über Primfaktorzerlegungen. Deshalb ist es hier von Vorteil, wenn in IMP-Mathematik bereits die Primfaktorzerlegung behandelt wurde.

Das kgV, der ggT und der Euklidische Algorithmus (Stunden 11 – 13)

Sowohl zum kleinsten gemeinsamen Vielfachen (kgV), als auch zum größten gemeinsamen Teiler (ggT) kann man zahlreiche Anwendungsbeispiele konstruieren. Zwei davon wurden als Einstiegsimpulse (07_mgk_ggT-kgV) gewählt, um die prinzipielle Idee / Problemstellung dieser Begriffe zu motivieren. Die Einstiegsimpulse sind dafür gedacht, in Zweier- bis Vierergruppen bearbeitet zu werden, bevor die Ergebnisse im Plenum vorgestellt werden. Es ist aber auch eine Think-Pair-Share-Phase durchaus denkbar. In der Plenumsphase werden dann die Begriffe des kgV und des ggT herausgearbeitet und festgehalten. Als zeitsparende Option dienen die folgenden Seiten der Datei 07_mgk_ggT-kgV, die beiden Arbeitsblätter Das kleinste gemeinsame Vielfache – kgV und Der größte gemeinsame Teiler – ggT. Der Eingangstext kann bei entsprechender Behandlung im Unterricht (z.B. an der Tafel) weggelassen werden. Die Aufträge auf diesen beiden AB-Seiten dienen sowohl der jeweiligen Übung und Festigung dieser beiden Begriffe, als auch bereits der Verknüpfung mit der Primfaktorzerlegung (wie es im Bildungsplan eingefordert wird). Sie sind für die Bearbeitung in Stillarbeit gedacht, können aber sicherlich, wenn vom Fachlehrer gewünscht, auch in den eingangs zusammengestellten Gruppen bearbeitet werden.

Vom Bildungsplan her nicht eingefordert ist die mathematisch sicherlich reizvolle Verknüpfung beider Begriffe zur Addition von Bruchzahlen. Sie kann optional, beispielsweise als binnendifferenzierende Maßnahme, durch die jeweilige Aufgabe 4 geschaffen werden.

Auf der letzten Seite in 07_mgk_ggT-kgV befinden sich schließlich noch Weitere Übungen zu kgV und ggT. Sie stellen, neben der reinen Übungsaufgabe 1 und der für leistungsstarke Schüler einzusetzenden Aufgabe 6, in den Aufgaben 2 – 5 eine weitere Auswahl aus den eingangs erwähnten zahlreichen Anwendungsbeispielen zusammen.

Sozusagen als krönender Abschluss dieser Einheit in Klasse 8 wird der Euklidische Algorithmus behandelt. Hier bietet sich nochmals die Chance, auf vielfältigste Art Kompetenzen und Inhalte zu fordern und zu fördern. Es wurde versucht, diese Vielschichtigkeit des Euklidischen Algorithmus im Unterrichtsgang durch die Konzeption der vorliegenden Arbeitsblätter zu berücksichtigen (08_mgk_Euklid). So besteht die Eingangssequenz daraus, den Algorithmus algebraisch zu verstehen und anwenden zu können. Diese kann in Still- oder Partnerarbeit, aber auch im Plenum durchgeführt werden. Die Begründung von Aufgabe 2a, dass es sich um den ggT handeln muss, kann dabei leistungsstärkeren Schülerinnen und Schülern überlassen werden (deshalb das *-Symbol), alle anderen können die Aussage als gegeben verwenden und

somit auch ohne Beweis weiterarbeiten. Als Hausaufgabe, zur Binnendifferenzierung oder für den fächerverbindenden Einsatz kann dann Aufgabe 4 dienen.

Nachdem die Schülerinnen und Schüler mit dem Euklidischen Algorithmus vertraut sind, findet eine Gruppenarbeit statt, in der sie für das inhaltliche Verständnis des Algorithmus wertvolle Verknüpfungen zwischen Algebra und Geometrie nachvollziehen. Durch die anschließende Präsentationsphase finden auch Übungen von prozessbezogenen Kompetenzen im Bereich der Kommunikation statt. Und nicht zuletzt entstehen in dieser Phase sicherlich Poster, die die Ästhetik der Mathematik ins Klassenzimmer transportieren können.

Für sehr leistungsstarke Klassen wäre hier auch ein Unterrichtsgang in vertauschter Reihenfolge denkbar. Dabei stellt man einen der drei geometrischen Zugänge aus der Gruppenarbeit voran und lässt die Schülerinnen und Schüler diesen dann „algebraisieren“, also in Terme fassen, wodurch der Euklidische Algorithmus entsteht.

Ergänzungen (Stunde 13 + x)

Die geometrischen Veranschaulichungen des Euklidischen Algorithmus wiesen bereits auf die Eleganz der Mathematik hin. Neben der Möglichkeit, über die Spirale auf dem letzten Arbeitsblatt Gruppe 3: Rechtecke mit Quadraten auslegen eine Verbindung zum Themengebiet der Fibonacci-Zahlen zu schaffen, bietet der vorliegende Themenbereich *mathematische Grundlagen der Kryptologie* noch zahlreiche spannende oder verblüffende Zusammenhänge. Sie zu entdecken gehört zwar nicht zum Pflichtbereich, ist aber dennoch „eine Reise wert“. Die folgenden Anregungen können daher eingesetzt werden, wo immer es passt. Beispielsweise können sie als Themen für Referate oder GFSen verwendet werden. Oder es bleiben letztlich noch Stunden übrig – der vorliegende Entwurf von 13 Stunden fügt sich ja lediglich in eine 27-stündige Planung ein – dann wäre es sicher lohnenswert, den Blick noch ein wenig zu weiten.

Mögliche Themen / Inhalte zur Ergänzung:

- Im Ordner *7_Apps* finden sich einige Apps (und die zugehörigen Dokumentationsdateien), die mithilfe des App-Inventors passend zur vorliegenden Unterrichtseinheit von Monika Eisenmann entwickelt wurden. Wenn man die Teilgebiete I und M fächerverbindend unterrichten möchte, so findet man darin gute Anregungen für Themenstellungen (und Beispiele zu deren Realisierung).
- Zur Ergänzung der Zahlensysteme lässt sich gut der folgende Kartentrick als offene „Durchschat ihr den Trick“-Aufgabe stellen: 27 unterschiedliche Karten werden gemischt. Ein Zuschauer zieht verdeckt eine Karte, sieht sie sich an und schiebt sie wieder an eine beliebige Stelle in den Stapel. Der „Zauberer“ legt nun den Stapel mit Bildseite nach unten vor sich hin und verteilt die Karten nacheinander abwechselnd auf drei Ablagen – Bild nach oben. Der Zuschauer sieht dabei zu und markiert nachdem alle Karten auf die drei Ablagen verteilt wurden, in welcher Ablage sich die gezogene Karte befindet. Der Zauberer legt die drei Ablagestapel aufeinander, den markierten Stapel nach ganz unten (Bildseiten immer noch oben!). Nun wird der Stapel umgedreht (Bildseite nach unten) und erneut auf die drei Ablagen verteilt und markiert. Danach noch einmal - auf dem letztlich zusammengestellten Stapel befindet sich dann die gezogene Karte ganz unten. Dieser Trick lässt sich natürlich auch auf 64 Karten erweitern ...
- Beweis des Satzes „Es gibt unendlich viele Primzahlen“. Dieser wurde auf dem AB Primzahlen – Das Sieb des Eratosthenes (04_mgk_Primzahlen-Einstieg) in Aufgabe 4 vorbereitet. Eine mögliche Erweiterung führt zuvor noch auf den

„Satz: Wenn $a : t = m \text{ Rest } x$ und $b : t = n \text{ Rest } y$, dann ist $a + b$ durch t teilbar, wenn $x + y$ durch t teilbar ist.“

bevor der Beweis dann durchgeführt wird. Für sehr leistungsstarke Schülerinnen und Schüler bietet sich eventuell sogar eine entsprechende Binnendifferenzierung direkt im Unterricht an. Material dazu findet sich z.B. im MA-THEMA Material (Juni 2016) [Mall].

- Rund um die Primzahlen gibt es viel zu entdecken. Bereits innerhalb des Unterrichtsganges sind einige Eigenschaften genannt, die vertieft und erweitert werden können. Beispielsweise Primzahlzwillinge, Mirp-Zahlen oder vollkommene Zahlen – um nur drei davon zu nennen. Man findet hierzu bereits viel mithilfe von Suchmaschinen im Internet. Eine umfangreiche Zusammenstellung gibt es auch in [Boru].
- Im Umfeld der Begriffe kgV / ggT gibt es eine schöne Methode, die Primfaktorzerlegung von Zahlen mit Lochkarten darzustellen und durch Übereinanderlegen den ggT / das kgV zu bestimmen. Dazu werden die Primfaktoren auf Karteikärtchen zeilenweise nach Häufigkeit gelocht. Ein Unterrichtskonzept dazu findet sich in [Heit].
- Zu den Teilbarkeitsregeln gibt es natürlich noch die verschiedensten Regeln zu finden. Ganz schön herausfordernd sind beispielsweise die 7er oder 13er-Regel (Alle Teilbarkeitsregeln sind schnell im Internet auffindbar).
- Der Kasiski-Test bietet eine Möglichkeit, mithilfe von Primfaktorzerlegungen und Teilmengen das Schlüsselwort eines Geheimtextes, der mit dem Vigenère-Verfahren verschlüsselt wurde, zu knacken. Da im Informatik-Teil eine grundlegende Angriffsstrategie auf dieses Verfahren zu behandeln ist, bietet sich dazu ein zwischen Mathematik und Informatik abgestimmtes Vorgehen an.
- Eine weitere anschauliche Interpretation des Euklidischen Algorithmus ist das Wiegen mit lediglich zwei unterschiedlich schweren Wägestücken (entsprechend den Zahlen, deren ggT gesucht ist). Beispielsweise findet man dies unter [Posa] auf S.188 (Unterrichtseinheit 79). Diese kann man verknüpfen mit dem Wiegen in anderen Zahlensystemen, z.B. bei [Stri] – Wiegen im 3er-System.
- Oben bereits erwähnt, in dieser Auflistung nur nochmals für die Vollständigkeit: Fibonacci-Zahlen als Erweiterung nach der zugehörigen Spirale in der quadratischen Auslegung eines Rechtecks (Euklidischer Algorithmus).

Literatur

- [Boru] Borucki, Hans: Mathematik zum Schmökern. Aulis, Köln (2006)
- [Heit] Heitzer, Johanna: Lochkarten zur Primfaktorzerlegung. In: mathematik lehren 176, S. 14-17. Friedrich in Velber, Seelze (2013)
- [Mall] Mallas, Helmut; et al.: MA-THEMA Aufgaben.
Diese sind im Internet frei zugänglich auf <http://www.mathema.math.uni-kiel.de/>.
Lehrkräfte können über <http://www.mathema.math.uni-kiel.de/lehrer/> auf die Lösungen zugreifen. Dazu genügt eine formlose Anmeldung per E-Mail bei HelmutMallas@t-online.de, und man erhält ein Passwort. (Zuletzt abgerufen am 20.04.2018)
- [Posa] Posamentier, Alfred: 119 Unterrichtseinheiten. Klett-Verlag, Stuttgart (1994)
- [Stri] Strick, Heinz-Klaus: Mathematik ist schön – Wiegen im 3er-System.
www.Mathematik-ist-schoen.de – April-Aufgabe aus Kalender "Mathematik ist schön"³
(Zuletzt abgerufen am 20.04.2018)