Die Kryptologie im Mathematikunterricht als Ideengeber für Facharbeitsthemen

von

Martin Epkenhans, Paderborn

Zusammenfassung: Durch die Behandlung der Kryptologie in einem Leistungskurs der gymnasialen Oberstufe werden in natürlicher Weise Facharbeitsthemen erschlossen. Das Herausarbeiten des mathematischen Gehaltes der Kryptologie lässt ein Plädoyer für eine stärkere Beachtung der Zahlentheorie in der Oberstufe entstehen.

Summary: We show how to use cryptography in school to find subjects for papers written by pupils. By emphasizing the mathematical impact in cryptography we vote for dealing with number theory in high school.

1 Einführung

1.1 Einleitung

Um den heutigen Ansprüchen an einen wissenschaftspropädeutischen Unterricht in der gymnasialen Oberstufe gerecht zu werden, ist in die aktuellen Richtlinien in Nordrhein-Westfalen (NRW) das verpflichtende Verfassen einer Facharbeit für alle Schülerinnen aufgenommen worden, s. [26][S. 44]. Eine „Facharbeit in Mathematik ist eine Dokumentation der eigenständigen Bearbeitung einer mathematischen Projektaufgabe durch eine Schülerin/einen Schüler oder eine Schülergruppe“, s. [27][S. 67]. Das Finden geeigneter Facharbeitsthemen stellt eine neue Herausforderung für MathematiklehrerInnen dar, der u.a. durch eine geeignete Stoffauswahl im Rahmen der Lehrpläne begegnet werden kann.

„Bildung ist zu einem öffentlichen Thema geworden. Der mathematisch-naturwissenschaftliche Unterricht ist dabei ins Gerede gekommen“, schreibt das Ministerium für Schule und Weiterbildung, Wissenschaft und Forschung des Landes NRW (MSWWF), s. [24][S. 7]. Mit vielen Initiativen bemüht sich derzeit die Bildungspolitik um eine Stärkung des mathematisch-naturwissenschaftlich-technischen Unterrichts. Dazu soll der Fachunterricht in „seiner Qualität abgesichert und wo notwendig verbessert werden“, s. [24][S. 9]. Grundlagenkompetenzen sollen gestärkt werden, die Lehr- und Lernprozesse Ansprüche von Schüler- und Wissenschaftsorientierung gleichermaßen berücksichtigen, verschiedene Lernformen wie selbstständiges und angeleitetes, individuelles und gemeinsames, fachliches und überfachliches Arbeiten variabel verbunden werden, theoretisches Lernen durch Praxisorientierung abgesichert werden und fachübergreifende Einsichten vermittelt

werden, moderne Technologien, insbesondere der Computer, sinnvoll genutzt werden, s. [24][S. 9].

Diese Leitgedanken können insbesondere bei der unterrichtlichen Vorbereitung und Begleitung von Facharbeiten im Mathematikunterricht umgesetzt werden. Dazu bedarf es geeigneter mathematischer Inhalte, deren Gehalt die Mathematik als eine lebendige Wissenschaft präsentiert.

Dieser Aufsatz soll deutlich machen, dass das aktuelle Thema Kryptologie insbesondere aus mathematischer Sicht hervorragend geeignet ist einen Unterricht zu gestalten, der nicht nur die obigen Kriterien berücksichtigt und das Erschließen von Facharbeitsthemen begünstigt, sondern auch den Bedürfnissen von SchülerInnen in dem Kurs gerecht wird, die ihre Facharbeit nicht in Mathematik schreiben.

Das in diesem Aufsatz vorgestellte Konzept stellt einen Leitplan für die unterrichtliche Umsetzung der Kryptologie im Mathematikunterricht in der Schule dar. Gleichzeitig soll es ein Plädoyer für die Behandlung zahlentheoretischer Fragestellungen in der Oberstufe sein. Die hierdurch entstehende Vernetzung mit Lerninhalten der Sekundarstufe I kann insbesondere das abstrakte mathematische Denken und Strukturieren fördern. Die zahlentheoretischen Inhalte der Sekundarstufe I können entsprechend der lernpsychologischen Weiterentwicklung der SchülerInnen neu beleuchtet und verständlich gemacht werden.

In diesem Aufsatz wird keine Unterrichtsreihe für eine fiktive Lerngruppe vorgestellt, vielmehr werden in diesem Leitkonzept von einem übergeordneten Standpunkt aus die Kryptologie als Unterrichtsgegenstand gerechtfertigt, eine Leitschnur durch dieses spannende Gebiet gespannt und die mannigfaltigen Möglichkeiten beleuchtet, die die Kryptologie speziell bei der Erschließung von Facharbeitsthemen bietet.

1.2 Die Herausforderung durch Facharbeiten für den Mathematikunterricht

Das Stellen und Betreuen von Facharbeiten stellt eine besondere Herausforderung für die Lehrkräfte dar, da das Verfassen längerer freier mathematischer Texte durch SchülerInnen nur selten geübt wird.

Die Literaturgrundlage im Mathematikunterricht besteht gewöhnlich nur aus einem Lehrbuch, das „als gemeinsame Aufgabensammlung“ dient, s. [26]. Die einführenden Erklärungen neuer mathematischer Inhalte erschöpfen sich zu oft im Behandeln konkreter Beispiele. Die Eigenproduktion mathematischer Texte der SchülerInnen findet vornehmlich beim Lösen von Aufgaben statt, von wo es noch ein weiter Weg zum Verfassen einer Facharbeit ist. Da die SchülerInnen nur in einem Fach nach freier Wahl eine Facharbeit schreiben, müssen ihnen klare Vorstellungen über die Art und Weise einer Facharbeit in Mathematik an die Hand gegeben werden. Durch die geschickte Wahl der Unterrichtsthemen können die SchülerInnen an mathematische Texte herangeführt werden, die den von den Richtlinien in-

tendierten „Umgang mit mathematischen Texten“ ebenso einüben, wie sie das Schreiben von Facharbeiten vorbereiten können, s. [26][S. 42]. Ein solches Thema ist zweifelsfrei die Kryptologie.

1.2.1 Umgang mit mathematischen Texten

„Mathematische Texte begegnen Schülerinnen und Schülern vorwiegend im Lehrbuch“, s. [26][S. 41]. Die Richtlinien beklagen, dass Lehrbücher im Mathematikunterricht häufig nur als Aufgabensammlung genutzt werden. Hingegen erhält der Erwerb von Orientierungswissen gegenüber Verfügungswissen in der Informationsgesellschaft eine höhere Bedeutung und verlangt somit nach einer Neuakzentuierung des Unterrichts, s. [34]. Der Lehrer ist nicht mehr der wissende Instruktor, der nur mit einem Lehrbuch ausgestattet, einen Großteil des Wissens schülergerecht darreicht, vielmehr wird er zum Moderator und Mittler, der Schülerinnen befähigt, sich selbstständig Wissen zu erschließen.

Mathematische Texte bewegen sich durch die „Verwendung der Fachsprache einschließlich des Variablengebrauchs und der entsprechenden Notation“ nicht selten „weit entfernt von der Alltagssprache“, s. [26][S. 41]. Teilweise folgen mathematische Texte einem stringenten logischen Aufbau und weisen durch die Benutzung der Formelsprache eine hohe Informationsdichte auf, s. [26][S. 41]. Zu selten finden sich umgangssprachliche Erläuterungen.

Gute mathematische Texte zeichnen sich durch eine übersichtliche Gliederung aus, umfangreiche Beweise werden durch Lemmata vorbereitet, der Beweis selbst wird in größere Abschnitte zerlegt, an deren Anfang das jeweilige Ziel formuliert wird. So kann man die Struktur erkennen und herausarbeiten, ohne jede einzelne Zeile des Beweises verfolgt und begriffen zu haben.

Der stringente Aufbau mathematischer Texte überrascht die Leser vielfach mit neuen Aussagen, überzeugt sie von deren Richtigkeit und hinterlässt die Frage: Und wie kommt man nun darauf? Eine genetisch orientierte Präsentation von mathematischen Sachverhalten erlaubt einen Blick in die Denk- und Arbeitsweise mathematischer Forschung, setzt sich jedoch der Gefahr aus, nicht als ausgereifter Beweis zu gelten. Beide Arten der textlichen Darstellung haben ihre Berechtigung und gerade der Wechsel der schriftlichen Darstellungsformen mathematischer Sachverhalte führt zu einem tieferen Verständnis von Mathematik.

SchülerInnen müssen ermutigt werden, ihre eigenen mathematischen Denkleistungen zu protokollieren und in der Retrospektive in einem hierarchischen Aufbau neu zu ordnen. Umgangssprachliche Beschreibungen von Mathematik sollen in eine formale mathematische Sprache übersetzt werden, formale Texte umgangssprachlich und informell erläutert werden.

1.2.2 Präsentation mathematischer Inhalte

Gewöhnlich findet die Diskussion über Mathematik nur im Klassenverband statt. Konventionen und Notationen lassen den Unterricht von außen wie in einer Geheimsprache geführt erscheinen. Tafel und Heft haben mehr die Funktion eines Notizzettels zur Unterstützung der eigenen Denkaktivität und der Verständigung mit Eingeweihten. Stereotype Zitationen von notwendigen Bedingungen oder die Benutzung schematischer Antwortsätze leisten keinen großen Beitrag zur mathematischen Aufsatzerziehung, die jedoch Gegenstand des Mathematikunterrichts der Oberstufe sein soll, s. [26][S. 41]. Eine große Chance, das Verfassen mathematischer Texte zu erlernen und „auch außerhalb des Unterrichts selbstständig mathematische Probleme an[zu]gehen“, bietet nun die Facharbeit, s. [26][S. 41]. Die in den Richtlinien vorgeschlagene Vorbereitung von Facharbeiten durch das Fach Deutsch kann zusätzliche Anstrengungen im Fach Mathematik nicht ersetzen, s. [26][S. 44]. Nur selten kommen SchülerInnen mit Abhandlungen zur Mathematik in Berührung, die in Umfang und Gehalt einer Facharbeit gleichzusetzen sind. Eigenproduktionen von Mathematik erreichen selten einen größeren Umfang.

2 Fachsystematische Analyse der Kryptologie – Ein Schnelldurchgang von Caesar bis zu RSA

Der hier vorgestellte Kurzdurchgang durch die Kryptologie stellt keine Unterrichtssequenz im eigentlichen Sinne dar, vielmehr werden die wichtigen kryptologischen Inhalte an einen roten Faden gehängt, der als Leitschnur zur eigenen Planung dienen kann. Die Auswahl und die Darstellung wurden bewusst so getroffen, dass der mathematische Gehalt der Kryptologie deutlich hervortritt.

Eine genaue Konzipierung von Unterricht muss die anthropogenen und soziokulturellen Bedingungen berücksichtigen, s. [42][S. 35]. So haben insbesondere die örtlichen Gegebenheiten und die Interessenlage der SchülerInnen einen maßgeblichen Einfluss auf eine eventuell fächerübergreifend oder fächerverbindend angelegte Unterrichtssequenz. Ebenso führen vorherige Gespräche mit den SchülerInnen über die Schwerpunktsetzung bei Facharbeitsthemen zu unterschiedlichen Akzentuierungen.

Kryptologie bietet die große Chance, einen komplexen und aktuellen Gegenstand der Mathematik verständlich zu behandeln, ohne an jeder Stelle in die Tiefe zu gehen. Das Gebiet zeichnet sich durch eine hohe Flexibilität in der unterrichtlichen Umsetzung aus. Zunächst sollen die fachlichen Inhalte erläutert werden.

2.1 Das Verfahren von Caesar

Caesar soll nach Aussagen des römischen Schriftstellers Sueton [40] geheime Nachrichten nach folgendem Verfahren verschlüsselt haben:

Unter das Klartextalphabet schreibt man das Geheimalphabet, jedoch um eine zuvor gewählte Anzahl von Stellen nach rechts verschoben. Diese Tabelle wird als Wertetabelle einer offensichtlich bijektiven Funktion interpretiert.

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Der Geheimtext entsteht durch das Ersetzen eines jeden Buchstabens des Klartextes durch das Bild unter dieser Funktion. Verschlüsseln wir beispielsweise das Wort *FACHARBEIT* nach dem obigen Schema, so lautet der Geheimtext *IDFKDUEHLW*. Die Entschlüsselung geschieht entsprechend.

Eine Mathematisierung dieser Verschiebechiffrierung lautet: Identifiziere jeden Buchstaben des Alphabetes mit seiner Stelle im Alphabet, beginne dabei die Zählung mit 0. Wähle ein $a \in \{0, \ldots, 25\}$ als Geheimschlüssel und setze

$$f : \{0, \ldots, 25\} \to \{0, \ldots, 25\}, \quad f(x) \equiv (x + a) \bmod 26$$

Die Dechiffrierung ist durch $x \mapsto (x - a) \bmod 26$ gegeben.

Da Caesar und seine Partner vorher den Algorithmus ausgetauscht haben, muss neben dem Geheimtext nur noch der Geheimschlüssel ausgetauscht werden. Caesar benutzte gewöhnlich $a = 3$ als Geheimschlüssel. An dieser Stelle bereits werden exemplarisch die Anforderungen an ein symmetrisches Kryptosystem deutlich:

- Der Klartext muss schnell verschlüsselt werden können.
- Eine schnelle Entschlüsselung unter Kenntnis des Algorithmus und des Schlüssels muss möglich sein.
- Ohne Kenntnis des Schlüssels soll eine Dechiffrierung gar nicht oder nur unter einem nicht vertretbaren zeitlichen Aufwand möglich sein.
- Der Schlüssel muss auf einem sicheren Weg zwischen den Partnern ausgetauscht werden können (Besonderheit eines symmetrischen Verfahrens).

Ein Algorithmus kann de facto nicht geheim gehalten werden, s. [4][S. 15]. Für die Sicherheit des Kryptosystems ist daher eine sichere Übermittlung des Schlüssels und die relative Unmöglichkeit der Dechiffrierung ohne Kenntnis des Schlüssels entscheidend.

Dieses Kryptosystem, das unter dem Namen CAESAR in die kryptologische Literatur eingegangen ist, hat in der hier präsentierten einfachen Version 25 Schlüssel (die Identität eignet sich nicht als Schlüssel). Ein einfaches Ausprobieren aller möglichen Schlüssel führt in der Mehrzahl der Geheimtexte zu nur einem vernünftigen Klartext. Ein Angreifer kann die Dechiffrierung sogar noch beschleunigen, wenn er die charakteristische Häufigkeit eines Buchstabens in einer Sprache ausnützt. In der deutschen Sprache ist E mit 17,4 % der häufigste Buchstabe, gefolgt von N mit 9,78 %, s. [4][S. 10]. Der Schlüssel von CAESAR ist eindeutig durch einen einzigen Klartextbuchstaben und sein Bild bestimmt. In einem ersten Schritt

bei einem Angriff bestimmt man den häufigsten Buchstaben im Geheimtext, nimmt an, er sei E, und dechiffriert entsprechend den Text.

Eine zu geringe Anzahl an Schlüsseln erhöht bei einem bekannten Verfahren die Angreifbarkeit. Die erfolgte Mathematisierung von CAESAR legt die folgende Verbesserung nahe: Ersetze die Vorschrift $x \mapsto (x+a) \bmod 26$ durch eine bijektive lineare Funktion $f(x) \equiv (bx+a) \bmod 26$. Aus der Problemstellung heraus ergeben sich folgende Fragen:

- Für welche *a*, *b* ist *f* bijektiv?
- Wie viele Funktionswerte muss man kennen, um diese Funktion zu bestimmen?

Nun ist man schon fast mitten in der Theorie der Restklassenringe. Es wird deutlich, dass eine Gleichung $c \equiv bx + a \bmod 26$ für gewisse $b \neq 0$ nicht universell lösbar ist. Die Interpretation des Graphen einer linearen Funktion als Gerade legt die Antwort auf die zweite Frage nahe. Diese Sichtweise leistet einen großen Beitrag zur Vernetzung des Wissens und bereitet bereits auf das RSA-Verfahren vor, s. [29].

2.2 Transpositionsalgorithmen und monoalphabetische Chiffrierungen

Im Gegensatz zu Verschiebechiffrierungen bleiben die Buchstaben bei einem Transpositionsalgorithmus, was sie sind, aber nicht wo sie sind. Diese Art der Chiffrierung ist von den Skytalen aus Sparta bekannt, s. [4][S. 3].

Eine monoalphabetische Chiffrierung ist eine bijektive Abbildung des Alphabetes in sich (oder ein gleichmächtiges Alphabet), also eine Permutation, d.h. eine bijektive Abbildung. Die hohe Anzahl ($\approx 4 \cdot 10^{26}$) möglicher Schlüssel täuscht jedoch über die Sicherheit hinweg. Die bereits vorgestellte Dechiffrierung mittels Häufigkeitsanalyse kann durch Zählen der Bigramme (Buchstabenpaare) im Geheimtext noch verfeinert werden. Das häufigste Bigramm der deutschen Sprache ist EN mit einem Anteil von 3,88 %, s. [4][S. 17 ff].

2.3 Die Vigenère-Verschlüsselung

Ein historisch recht erfolgreiches Kryptosystem ist das vom französischen Diplomaten Blaise de Vigenère (1523 bis 1596) entwickelte polyalphabetische Kryptosystem, welches auch heute noch vielfach in Romanen oder Kriminalfilmen benützt wird und erst nach 300 Jahren geknackt wurde. Bei diesem Kryptosystem wird die charakteristische Häufigkeit eines Buchstabens dadurch verschleiert, dass er zu verschiedenen Buchstaben codiert wird, je nach Position im Klartext.

Der Schlüssel besteht aus einem Wort $a_1 \ldots a_n$ der Länge n ($a_1, \ldots, a_n$ sind die Buchstaben des Wortes). Steht ein Buchstabe a an der m-ten Stelle im Klartext, so bestimmt man $i \in \{1, \ldots, n\}$ mit $i \equiv m \bmod n$. Verschlüsselt wird a zu $f_{a_i}(a)$, wo-

bei f_{a_i} die durch den Buchstaben a_i definierte Verschiebechiffrierung bedeutet (z.B. Buchstabe $a_i = V$ definiert die Verschiebung $A \mapsto V, B \mapsto W$ etc.). Wir haben an dieser Stelle bewusst auf die sonst übliche Einführung der Vigenère-Verschlüsselung mit Hilfe des Vigenère-Quadrates verzichtet, um so eine dem Funktionsbegriff nähere Beschreibung zu präsentieren (siehe [3]). Ein Angriff auf die Vigenère-Chiffrierung mit dem sog. Kasiski-Test erfolgt in zwei Schritten: Zunächst ermittelt man die Länge des Schlüsselwortes. Danach bestimmt man das Schlüsselwort mittels Häufigkeitsanalyse. Eine genauere Beschreibung findet man z.B. in [3].

2.4 Das RSA-Verfahren

Entsprechend der Maxime von Auguste Kerckhoffs (1835 bis 1903) darf die Sicherheit eines Kryptosystems nur von der Geheimhaltung des Schlüssels, nicht von der Geheimhaltung des Algorithmus abhängen, s. [2][S. 207 Regel Nr. 3]. Eine elektronische Kommunikation vorher unbekannter Partner ist ohne einen öffentlichen Algorithmus undenkbar. Die bisher vorgestellten symmetrischen Chiffrierverfahren haben einen großen Nachteil: Die Teilnehmenden müssen im Besitz des gleichen Geheimschlüssels sein, der über den gleichen (ungeschützten) Weg wie der Text selbst ausgetauscht werden muss. Einen Ausweg bieten asymmetrische Verfahren, auch Public-Key-Verfahren genannt, wie sie 1976 von Diffie und Hellman publiziert wurden, s. [9].

Jeder Teilnehmer *B* erhält einen öffentlichen Schlüssel E_B (= encryption, engl.) und einen geheimen Schlüssel D_B (= decryption, engl.). Für Absender und Adressat haben sich die Namen Alice und Bob eingebürgert. Wie verschlüsselt nun Alice ihre Nachricht *m* an Bob? Alice chiffriert *m* zu $c = E_B(m)$ mit Hilfe des öffentlichen Schlüssels von Bob und sendet *c* an Bob. Dieser dechiffriert die Nachricht mit seinem geheimen Schlüssel D_B zu $D_B(c)$. Die Funktion E_B muss nun die folgenden Bedingungen erfüllen:

- Sie muss leicht zu berechnen sein.
- Ihre Umkehrfunktion muss für einen Angreifer schwer zu bestimmen sein.

Solche Funktionen heißen Trapdoor-Funktionen.

Eine geniale Realisierung dieser Idee gelang Rivest, Shamir und Adleman mit dem von ihnen 1978 publizierten, heute RSA-Verfahren genannten asymmetrischen Kryptosystem, s. [32]. Ein weiteres bekanntes Public-Key-Verfahren ist 1985 von ElGamal vorgestellt worden, s. [12]. Letzteres basiert auf der Schwierigkeit, den diskreten Logarithmus zu bestimmen.

An dieser Stelle soll das bekanntere RSA-Verfahren vorgestellt werden, welches auf der Erkenntnis beruht, dass man von einer Zahl vergleichsweise leicht ent-

scheiden kann, ob sie eine Primzahl ist, aber nur schwer die Primfaktoren bestimmen kann. Weiter wird ausgenutzt, dass algorithmisch Potenzieren leicht, Wurzelziehen jedoch schwer möglich ist.

Jeder Teilnehmer erhalt zwei verschiedene große Primzahlen p und q berechnet deren Produkt $N = pq$. Bezeichne φ die Euler'sche φ-Funktion, s. [23][S. 111]. Weiter wählt man eine zu $\varphi(N) = (p-1)(q-1)$ teilerfremde Zahl e und berechnet ein multiplikatives Inverses $d \bmod \varphi(N)$, d.h. ein d mit $ed \equiv 1 \bmod \varphi(N)$. Veröffentlicht wird nun das Schlüsselpaar (e, N), geheim gehalten werden d, p, q, $\varphi(N)$. Dabei können p, q und $\varphi(N)$ sogar vernichtet werden. Alice benutzt nun zum Verschlüsseln ihrer Nachricht m den öffentlichen Schlüssel (e, N) von Bob, berechnet

$$c \equiv m^e \bmod N \quad \text{mit} \quad c \in \{0, \ldots, N-1\}$$

und sendet c an Bob. Dieser berechnet mit seinem geheimen Schlüssel d den Wert

$$x \equiv c^d \bmod N \quad \text{mit} \quad x \in \{0, \ldots, N-1\}.$$

Nun gilt $x \equiv c^d \equiv m^{ed} \equiv m \bmod N$, so dass Bob die Nachricht entschlüsselt hat.

Dieses Verfahren wirft die folgenden Fragen auf:

- Mathematische Fragen zur Begründung von RSA:
  - Wieso gibt es zu einer zu $\varphi(N)$ teilerfremden Zahl e eine Zahl d mit $ed \equiv 1 \bmod \varphi(N)$, d.h. wieso ist $e \bmod \varphi(N)$ invertierbar?
  - Warum gilt $m^{ed} \equiv m \bmod N$?
- Mathematische Fragen zur Sicherheit von RSA:
  - Warum ist es schwer, von der Kenntnis von e und N auf d zu schließen?
  - Wie schnell kann man Zahlen faktorisieren?
- Mathematische Fragen zur Realisierung von RSA:
  - Wie findet man leicht große Primzahlen?
  - Wie kann man schnell multiplizieren?
  - Wie kann schnell modulo N potenziert werden?
  - Wie kann ein Inverses von $e \bmod \varphi(N)$ bestimmt werden (unter Kenntnis von $\varphi(N)$)?

Nun ist man mitten in der Zahlentheorie. Die Existenz und Berechnung eines Inversen von $e \bmod \varphi(N)$ wird mit dem erweiterten Euklidischen Algorithmus begründet und durchgeführt. $m^{ed} \equiv m \bmod N$ folgt aus dem Satz von Fermat-Euler, s. [22][S. 123] bzw. [31][S. 167]. Die Frage nach schnellem Multiplizieren und Potenzieren führt direkt in die Theorie des Stellenwertsystems und zur Untersuchung bekannter schriftlicher Rechenverfahren.

2.5 Wie findet man große Primzahlen?

Bereits die in der Sekundarstufe I durchgeführten Primfaktorzerlegungen kommen ohne Primzahltests nicht aus (Klasse 5/6, [25][S. 39]). In den konkreten Anwendungen reicht gewöhnlich eine Tabelle aller Primzahlen $\leq B$ für eine nicht allzu große Schranke *B* aus. Das RSA-Verfahren benötigt jedoch weitaus größere Primzahlen.

Eine bekannte Art eine solche Tabelle zu erstellen, ist das Sieb des Eratosthenes, mit dem eine Liste aller Primzahlen $\leq B$ erstellt werden kann, s. [25][als Ergänzung in der Erprobungsstufe]. Für große Zahlen ist dieses Verfahren allerdings nicht praktikabel. Alternativ kann man zufällig eine große Zahl *n* wählen und überprüfen, ob *n* eine Primzahl ist. Der naive Test setzt direkt bei der Definition einer Primzahl an, sucht unter allen Zahlen $< n$ nach Teilern von *n* und kann durch die folgende leicht einzusehende Beobachtung beschleunigt werden: Hat man unter den Zahlen $\leq \sqrt{n}$ keinen Teiler $\neq 1$ gefunden, so ist *n* bereits eine Primzahl.

Heute werden üblicherweise probabilistische Primzahltests wie etwa der Solovay-Strassen-Primzahltest oder der Rabin'sche Primzahltest eingesetzt, s. [38], [30]. Der erstgenannte Test nützt Eigenschaften des Jacobisymbols aus und ist wegen der Komplexität der damit verbundenen Zahlentheorie für den Unterricht nicht geeignet. Näher liegend ist es, zunächst an den kleinen Satz von Fermat anzuknüpfen: Wenn *n* eine Primzahl ist, dann gilt für jede zu *n* teilerfremde Zahl *a*

$$a^{n-1} \equiv 1 \bmod n \,. \qquad (*)$$

Die Umkehrung ist jedoch falsch. Die Häufigkeit der zusammengesetzten Zahlen *n*, für die die Aussage (*) für alle zu *n* teilerfremden Zahlen gültig ist (die so genannten Carmichaelzahlen), ist im Vergleich zur Verteilung der Primzahlen recht gering; so gibt es z.B. genau 1770 Carmichaelzahlen $\leq 25 \cdot 10^9$, aber mehr als $4 \cdot 10^7$ Primzahlen in diesem Bereich. Die Hoffnung, dass es nur endlich viele Ausnahmen für die Umkehrung des kleinen Satzes von Fermat gibt, konnte nicht erfüllt werden, s. [1]. Der kleine Fermat-Test berechnet für eine Zahl die Reste $2^{n-1} \bmod n$, $3^{n-1} \bmod n$, $5^{n-1} \bmod n$ etc. und testet, ob das Ergebnis $\equiv 1 \bmod n$ ist. Wenn $a^{n-1} \not\equiv 1 \bmod n$ für ein *a* gilt, dann ist *n* mit Sicherheit keine Primzahl, man hat jedoch keinen nichttrivialen Primteiler gefunden. Auf diese Art kann man z.B. feststellen, dass die Fermatzahl $F_6 = 2^{64} + 1 = 18446744073709551617$ nicht prim ist, da $3^{n-1} \not\equiv 1 \bmod n$ ist.

Der Primzahltest von Rabin nutzt folgenden Sachverhalt aus: Sei *n* eine Zahl mit $n \equiv 3 \bmod 4$. Dann ist *n* genau dann eine Primzahl, wenn für alle zu *n* teilerfremden Zahlen *a* gilt

$$a^{(n-1)/2} \equiv \pm 1 \bmod n \,.$$

Ist n zusammengesetzt, so gilt für die Menge A aller zu n teilerfremden Zahlen a mit $0 < a < n$, für die $a^{(n-1)/2} \equiv \pm 1 \bmod n$ ist:

$$\mathrm{Card}(A) \leq \tfrac{1}{4}\varphi(N),$$

s. [14][S. 101]). Wiederholt man den Test häufig genug, so stellt man entweder fest, dass n zusammengesetzt ist, oder man kann mit großer Sicherheit sagen, dass n eine Primzahl ist.

Einen Einblick in die Theorie der Primzahlen und der Primzahlverteilung auf einem elementaren Niveau enthält [8][Kapitel 5].

2.6 Faktorisierungsalgorithmen

Die Sicherheit von RSA vertraut auf die Schwierigkeit, eine Zahl in ihre Primfaktoren zu zerlegen. Wie schwierig ist Faktorisieren tatsächlich? Bereits in der Orientierungsstufe werden Primfaktorzerlegungen durchgeführt. Diese Verfahren benötigen bei großen Zahlen einen nicht zu vertretenden Aufwand. Der Erfolg einer Attacke auf RSA hängt von der Güte eines Faktorisierungsalgorithmus ab. Die von den Autoren des RSA-Verfahrens angegebene 129-stellige zusammengesetzte Zahl wurde 1994 von Atkins, Graff, Lenstra und Leyland in das Produkt zweier Primzahlen (mit 64 und 65 Stellen) zerlegt. Sie schalteten dazu 1600 Computer parallel, s. [14][S. 124]. Den aktuellen Rekord beim Faktorisieren nicht-spezieller Zahlen hat Te Riele am 12.8.1999 aufgestellt, als er die beiden 78-stelligen Primteiler einer 155-stelligen Zahl in einer CPU-Zeit von 37,7 Jahren gefunden hat, s. [28][S. 10]. Es stellen sich somit die folgenden Fragen

- Wie schnell kann schnelles Faktorisieren sein?
- Wie schnell sind die existierenden Algorithmen?

Die erste Frage kann bisher nicht beantwortet werden. Die Komplexitätsuntersuchungen der bekannten Faktorisierungsalgorithmen geben eine Antwort auf die Frage, wie die Primzahlen gewählt werden sollen, so dass der Aufwand zum Faktorisieren der Zahl N für den Angreifer in keiner vernünftigen Relation zum Nutzen steht.

Neben Verfahren, die die Theorie der Kettenbrüche oder der elliptischen Kurven benutzen, sei hier besonders auf die Pollard'sche Rho-Methode hingewiesen [14][S. 107]: Sei N eine natürliche Zahl. Wähle einen zufälligen Startwert x_0, berechne mit Hilfe der Abbildung

$$f : \{0, 1, \ldots, N-1\} \to \{0, 1, \ldots, N-1\}, \quad f(x) \equiv \left(x^2 + 2\right) \bmod N$$

die iterative Folge $(x_i)_{i \geq 0}$ mit $x_i = f(x_{i-1})$ bis zu einer Stelle $i = B$. Diese Folge mündet nach einer Vorperiode in einen Zykel. Die Gestalt der Bahn erinnert so an die Form des griechischen Buchstaben ρ, was den Namen des Verfahrens erklärt.

Man bestimmt nun $d_i = \mathrm{ggT}(x_{2i} - x_i, N)$ für $i = 1, 2, \ldots, B$. Gilt $d_i \neq 1$ und $d_i \neq N$, so ist d_i ein nichttrivialer Teiler von *N*.

Eine Analyse der Rho-Methode muss klären, wie groß die Wahrscheinlichkeit ist, dass für einen nichttrivialen Primteiler p von N zwei zufällig gewählte Zahlen $x_i \neq x_j$ kongruent modulo p sind, d.h. $x_i \equiv x_j \bmod p$ gilt. Hiermit sind wir beim Geburtstagsparadoxon der Stochastik angelangt. Sowohl die probabilistischen Primzahltests wie die Faktorisierungsalgorithmen benutzen Zufallszahlen, ein weiteres wichtiges Gebiet der Stochastik.

3 Einbettung der Kryptologie in den Unterricht

3.1 Hinweise zur unterrichtlichen Umsetzung

3.1.1 Obligatorische Unterrichtsziele

Am Ende der Sequenz sollen die SchülerInnen sich in die wichtigsten Grundlagen der Kryptologie eingearbeitet haben und die Herausforderung für die Mathematik durch die Kryptologie und den Beitrag der Mathematik zur Kryptologie exemplarisch erfahren haben. Dies impliziert, dass sie

- die Notwendigkeit eines Public-Key-Kryptosystems erkannt haben,
- eine mögliche Realisierung eines asymmetrischen Verfahrens kennen gelernt haben (RSA oder ElGamal),
- die wesentlichen mathematischen Begründungen für die Korrektheit des Verfahrens kennen gelernt haben (Satz von Fermat-Euler, Euklidischer Algorithmus – zum Verständnis der Verfahren besteht nicht die Notwendigkeit, diese Sätze im Klassenverband zu beweisen; je nach Akzentuierung im Unterricht kann hierauf zu Gunsten eines Facharbeitsthemas verzichtet werden),
- exemplarisch die Komplexität (asymptotische Laufzeit) von Primzahltests und Faktorisierungsalgorithmen erfahren haben,
- exemplarisch erfahren haben, welchen Beitrag die Mathematik zur Entwicklung effizienter Algorithmen leistet.

Die Behandlung eines Public-Key-Verfahrens nimmt die zentrale Rolle in diesem Konzept ein, da hiermit die eingangs gestellten Fragen nach einem nach heutigem Wissen sicheren System beantwortet werden und in kanonischer Weise ein Katalog noch zu behandelnder mathematischer Themen erstellt wird.

3.1.2 Zur Einführung in die Kryptologie

Die zu Beginn des letzten Kapitels gemachten Ausführungen zu den Anfängen der Kryptographie sind bei einer Schwerpunktsetzung auf moderne Verfahren nicht unbedingt erforderlich, sie eignen sich jedoch gut als Motivation eines fächerübergreifenden Unterrichts und für eine erste Mathematisierung der kryptologischen

Probleme. Ein Vorteil, auf den insbesondere in einem dem genetischen Prinzip folgenden Mathematikunterricht nicht verzichtet werden soll. Auch Puhlmann [29] hat sehr schön dargestellt, wie der Weg von CAESAR zu RSA dem Aufbau der Rechenoperationen Addition – Multiplikation – Potenzierung folgen kann.

3.1.3 Das RSA-Verfahren

Will man die Behandlung des Euklidischen Algorithmus zu Gunsten anderer Inhalte umgehen, so ist eine Beschränkung auf Primzahlen $p, q \equiv 2 \bmod 3$ und die Wahl von $e = 3$ möglich. Dann gilt $\varphi(N) \equiv 1 \bmod 3$, d.h. es gibt ein a mit $\varphi(N) = 3a + 1$. Wähle dann $d \equiv -a \bmod \varphi(N)$ und es folgt sofort $3d \equiv 1 \bmod \varphi(N)$. Diese Vereinfachung bringt einen Verlust an Sicherheit mit sich, der durchaus zum Thema einer Facharbeit gemacht werden kann, für den Fortgang des Unterrichts aber keine Relevanz hat, s. [6][S. 21].

Ein Beweis des Satzes von Fermat-Euler im Klassenverband ist zum Gesamtverständnis von RSA entbehrlich. Das stichprobenhafte Berechnen von $a^{N-1} \bmod N$ für Primzahlen N kann als Ausgangspunkt für eine Vermutung dienen, die etwa durch ein Literaturstudium bestätigt werden kann. Eine schülergerechte Anleitung hierzu findet sich etwa in [33].

3.1.4 Lernvoraussetzungen

Die moderne Kryptologie benutzt die Sprache der Zahlentheorie, deren Grundelemente in der Sekundarstufe I bereitgestellt werden. Die Division mit Rest wird vielfach schon im Bereich der Grundschule gelehrt, teilweise kennen die SchülerInnen die Schreibweise der modularen Arithmetik aus dem Informatikunterricht. Die Begriffe ‚Primzahl' und ‚Teilerfremdheit' gehören zu den obligatorischen Inhalten im Lernbereich Algebra der Orientierungsstufe, s. [25][S. 39], wohingegen das Sieb des Eratosthenes zum Ergänzungsbereich gezählt wird.

Beim Studium der Komplexität (asymptotische Laufzeit) von Primzahltests wird eine Vernetzung zum Begriff der Asymptotik hergestellt, wie er teilweise im Zusammenhang mit der Behandlung der Potenzfunktionen mit negativen Exponenten in den Jahrgangsstufen 9/10 eingeführt wird [36][S. 35] und später beim Studium gebrochen rationaler Funktionen in der Sekundarstufe II vertieft wird. Die Thematisierung probabilistischer Primzahltests und der Kryptoanalyse klassischer Systeme knüpfen an die Stochastik und Kombinatorik aus den Themenkreisen Lottoproblem und Bernoulliexperiment an.

Eine für einen Leistungskurs angemessene vertiefte mathematische Sicht auf die Kryptologie setzt einen sicheren Gebrauch der Variablenschreibweise und eine Grundeinsicht in mathematisches Beweisen voraus.

3.1.5 Möglichkeiten des Computereinsatzes

Bereits Euklid (ca. 285 v.Chr. im Buch IX, Satz 20) hat bewiesen, dass es unendlich viele Primzahlen gibt. Auch bei Pierre de Fermat (1601 bis 1665) und Carl Friedrich Gauß (1777 bis 1855) spielten Primzahlen aus verschiedenen Gründen eine große Rolle. So vermutete Fermat, dass die heute Fermat'sche Zahlen genannten Zahlen $F_n = 2^{2^n} + 1$ für alle natürlichen Zahlen *n* Primzahlen sind, was er für $n = 1, 2, 3, 4$ auch verifiziert hat. Nun hat Leonhard Euler (1707 bis 1783) gezeigt, dass $F_5 = 641 \cdot 6700417$ gilt. Gauß fand Faktorisierungsalgorithmen, mit denen er bis zu achtstellige Zahlen in Primfaktoren zerlegen konnte, siehe seine *Disquisitiones Arithmeticae* [17].

Sicherlich würde heute keinen SchülerInnen, die mit den zur Behandlung leichter mathematischer Probleme ausreichenden Computerkenntnissen ausgestattet sind, der Fehler von Fermat unterlaufen, auch ist das Faktorisieren achtstelliger Zahlen für SchülerInnen keine Sensation. An dieser Stelle wird aber auch klar, dass durch eine kognitive Leistung der Fehler von Fermat bereits lange vor der Entwicklung des Computers erkannt worden ist. Primfaktorzerlegungen haben schon vor Jahrhunderten eine bedeutende Stelle in der Mathematik eingenommen.

Einerseits kann man durch den Einsatz von Computern diese Verfahren für weit größere Zahlen anwenden. Andererseits hat die Existenz von Computern und den damit verbundenen Kommunikationsmitteln zu einer Belebung eines alten Forschungsgebietes beigetragen. Der Computer spielt in diesem Zusammenhang eine zweifache Rolle. Er ist Motivation für die Kryptologie und er kann als Werkzeug bei der Erschließung arithmetischer Zusammenhänge genutzt werden. In einem Mathematikkurs, in dem die SchülerInnen im Umgang mit einem Computeralgebrasystem vertraut sind, bieten sich genügend Einsatzmöglichkeiten des Computers an, womit eine weitere Forderung der neuen Richtlinien sinnvoll in die Tat umgesetzt wird, s. [26][S. 47]. Dieser Aspekt soll an dieser Stelle nicht vertieft werden, da er nicht unmittelbar mit der zentralen Fragestellung dieses Aufsatzes verbunden ist. Erwähnt sei hier nur die dem Buch *Einführung in die Zahlentheorie* von Friedrich Schwarz beiliegende interaktive CD, die unter anderem eine Bibliothek mit Primzahlen enthält, s. [35].

3.2 Begründung für den Unterrichtsgegenstand Kryptologie

3.2.1 Allgemeine Begründung

„Chiffrierte Nachrichten, Geheimcode, Geheimdienst, Briefe abfragen, Code knacken – Assoziationen, die eine hinreichende Motivation für Schüler liefern, sich mit Kryptologie auseinanderzusetzen", schreibt Seiffert, s. [37]. „Eine didaktische Begründung ergibt sich dagegen aus dem weit verbreiteten Einsatz von Datenbanksystemen mit Verarbeitung personenbezogener Daten", so Seiffert weiter. Heibey

und Pfitzmann sehen das Thema „Kryptographie“ im „Spannungsfeld zwischen Staat und jedem einzelnen in der Gesellschaft“. Die rasante Entwicklung des Internets und des E-Commerce bedingen einen hohen Sicherheitsstandard bei der Kommunikation, elektronische Unterschriften ersetzen die persönliche Authentifizierung, s. [16].

3.2.2 Fächerübergreifende Aspekte

Die Entwicklung und Untersuchung von Geheimschriften ist heute eindeutig in den Disziplinen Mathematik und Informatik verankert. Die obige Einführung zeigt, dass der Einsatz kryptographischer Systeme einen starken gesellschaftspolitischen Aspekt hat. Die Verschlüsselungsverfahren CAESAR oder der Einsatz von Skytalen gibt dem Ganzen eine historische Note, die durch literarische Aspekte bereichert werden kann, wie Beutelspacher überzeugend in dem Mathewelt-Arbeitsheft [5] darlegt, wo er SchülerInnen mit Gedichten von Ringelnatz oder der Geschichte von Kalle Blomquist konfrontiert, um sie mit dem Phänomen der Kryptologie vertraut zu machen. Die Kryptologie öffnet so auch die sonst eher schwer zu öffnende Tür zwischen Mathematik und den Fächern Geschichte und Deutsch zur Gestaltung eines fächerübergreifenden Unterrichts.

3.2.3 Kryptologie als mathematische Disziplin

Das Interesse an der Benutzung von Geheimschriften ist primär nichtmathematischer Natur. Hingegen sind die Entwicklung und die Umsetzung kryptographischer Verfahren eindeutig im Spannungsfeld von Mathematik und Informatik angesiedelt. Zwar sehen Fumy und Rieß [15][S. 14] die Informatik „als Disziplin an der Nahtstelle zwischen Mathematik und Elektrotechnik als die ‚Heimatdisziplin‘ der Kryptologie“, der Nachweis der Sicherheit heutiger Verschlüsselungsverfahren ist jedoch eindeutig mathematischer Natur. „Kryptologie ist eine mathematische Disziplin“, so Beutelspacher, s. [4][S. vii]. Für H. Kautschitsch liefert die Kryptographie zahlreiche Beispiele für einen anwendungsbezogenen Mathematikunterricht, „wobei die Anwendung nicht wirklichkeitsfremd oder gekünstelt wirkt, vor allem ist sie altersgemäß“, s. [20].

Als mathematische Disziplin ist die moderne Kryptologie in der Zahlentheorie verankert. Die Sprache der Zahlentheorie ist elementar und den SchülerInnen aus der Sekundarstufe I bekannt. Sachverhalte und Fragestellungen der Zahlentheorie können vielfach leicht verständlich und schülergerecht formuliert werden. Wie etwa der Beweis der Vermutung von Fermat gezeigt hat, gehört die Beantwortung mancher zahlentheoretischer Fragestellungen zu den großen Herausforderungen der modernen Mathematik. „Manche Ergebnisse der ‚reinen‘ Mathematik (hier vor allem der Zahlentheorie) [finden] noch nach Jahrhunderten ‚lebenswichtige‘ Anwendungen. So erweist sich die Mathematik des 20. Jahrhunderts (dem Schüler) nicht als tote Wissenschaft, die nur aus Axiomatik und Verwaltung der alten Sätze be-

steht“, so H. Kautschitsch zur Kryptologie, s. [20]. Mathematik kann sich als eine lebendige Disziplin präsentieren.

Mathematik erscheint vielen Menschen als ein abgeschlossenes Gebilde, das keine weitere Entwicklung mehr zulässt. „Mathematische Forschung, was ist das? Habt ihr denn noch nicht alle Formeln erfunden?“, so oder ähnlich reagieren vielfach Menschen beim Zusammentreffen mit einem mathematischen Wissenschaftler. Die Zahlentheorie, eingeschlossen die Kryptologie, ist ein hervorragend geeignetes Feld, auf dem SchülerInnen in Kontakt mit offenen Fragen der Mathematik kommen können.

In Anknüpfung an die 23 mathematischen Probleme, die Hilbert im Jahr 1900 auf einem Kongress in Paris vorgestellt hat, hat das Clay Mathematics Institute CMI sieben „mathematische Kopfnüsse“ benannt, auf deren Lösung der amerikanische Multimillionär Landon T. Clay eine Million Dollar ausgesetzt hat, s. [19], [7]. Unter diesen sieben Problemen sind die der Zahlentheorie zuzurechnenden Vermutungen von Riemann einerseits und Birch und Swinnerton-Dyer andererseits. Die Riemannsche Vermutung mit ihrem Bezug zur Verteilung der Primzahlen hat Einfluss auf die Komplexitätsuntersuchungen von Faktorisierungsalgorithmen. Die Vermutung von Birch und Swinnerton-Dyer beschäftigt sich mit der Menge der rationalen Lösungen von Gleichungen der Form $y^2z = x^3 + axz^2 + bz^3$, d.h. elliptischer Kurven. Moderne Faktorierungsalgorithmen machen sich algebraische Eigenschaften elliptischer Kurven zu Nutze.

Neben diesen beiden Problemen, die einen eindeutigen Bezug zur Kryptologie aufweisen, ist ein weiterer Baustein auf dem Weg zum Nachweis der Sicherheit kryptographischer Systeme in die Liste der sieben Probleme, auf die der Milleniumspreis ausgesetzt worden ist, aufgenommen worden. Die Frage lautet „$P = NP$?“, anders ausgedrückt: Wie schwer können algorithmisch berechenbare Probleme wirklich sein?, s. [7]. Hierbei steht *NP* für Optimierungsprobleme, die berechenbar sind, und *P* für die Teilmenge von Problemen, die sogar effizient lösbar sind, d.h. für die es einen Algorithmus gibt, dessen Laufzeit polynomiell von der Größe der Ausgangsdaten abhängt. Man vermutet heute, dass $P \neq NP$ gilt. Hieraus würde folgen, dass die Faktorisierung von Zahlen ein algorithmisch schwieriges Problem ist. Das RSA-Verfahren wäre somit auf heutigen Rechnern ein sicheres Verfahren. Auch die Beschleunigung der Prozessoren würde hieran nichts ändern.

Natürlich können weder die Riemann’sche Vermutung noch die Vermutung von Birch und Swinnerton-Dyer mathematisch verständlich im Unterricht formuliert werden, diese Hinweise dienen mehr dem Hintergrundwissen der Lehrkraft. Ein Bericht über die Existenz dieses Preises, etwa als Kurzreferat, basierend auf dem Artikel in [7] und einer weiteren Internetrecherche, kann jedoch die mathematische Bedeutung der Kryptologie verdeutlichen; insbesondere unterstreicht die Auswahl dieser sieben Probleme, wie sehr die Kryptologie eine mathematische Disziplin ist.

4 Themen für Facharbeiten

Die Kryptologie wirft viele Fragen auf, die im Unterricht nicht ausreichend geklärt werden können; dennoch kann ein Gesamtverständnis erreicht werden. Auf diesem Wege entstehen in natürlicher Weise Ausgangspunkte für Facharbeiten. Der Unterricht kann so gestaltet werden, dass diese Fragen offensichtlich werden und die SchülerInnen so die Gelegenheit erhalten, selbstständig Themengebiete für ihre Facharbeit zu benennen.

Nachfolgend werden einige Vorschläge für Facharbeitsthemen gemacht, die eindeutig mathematisch orientiert sind. Bei der Auswahl der Themen wurde von einem überdurchschnittlichen Interesse an Mathematik bei den betreffenden SchülerInnen ausgegangen. Einige Aspekte der Kryptologie können in Facharbeiten ausgelagert werden (z. B. Thema 5, 6) oder alternativ im Unterricht behandelt werden. Im letzten Fall wären diese Themen eventuell für eine Facharbeit nicht anspruchsvoll genug.

1. Thema: *Analyse schriftlicher Rechenverfahren unter besonderer Berücksichtigung der Multiplikation und verschiedener Stellenwertsysteme*.
   Gebiet: Reine Mathematik mit einem leichten Bezug zur Informatik.
   Aufgabenstellung: Untersuchen und beschreiben Sie die konventionellen Verfahren zur schriftlichen Multiplikation zweier natürlicher Zahlen. Bestimmen Sie die Anzahl der benötigten Rechenschritte. Das folgende Multiplikationsverfahren ist u.a. unter dem Namen russische Bauernregel bekannt: Zwei Zahlen *a*, *b* werden wie folgt multipliziert: In einer Tabelle stehen *a*, *b* in einer Zeile, in der nächsten Zeile steht das Doppelte von *a* und der ganzzahlige Anteil der Hälfte von *b*; diese Prozedur wird solange wiederholt, bis man man beim *b*-Wert 1 angelangt ist. Danach markiert man die Zeilen, in denen in der rechten Spalte eine ungerade Zahl steht. Die *a*-Werte dieser Zeilen werden danach addiert und ergeben das Produkt *ab*. Beschreiben Sie die russische Bauernregel zur Multiplikation unter Benutzung der Binärdarstellung einer Zahl. Wenden Sie diese Idee anschließend zur Entwicklung eines schnellen Potenzierungsalgorithmus an. Literaturhinweis: [14]
2. Thema: *Der Restklassenring $\mathbb{Z}/N\mathbb{Z}$, eine mathematische Fundierung von RSA*.
   Gebiet: Reine Mathematik (Zahlentheorie).
   Aufgabenstellung: Erläutern Sie die Einführung des Restklassenringes $\mathbb{Z}/N\mathbb{Z}$. Gehen Sie dabei insbesondere auf die Wohldefiniertheit der Addition und Multiplikation ein. Erläutern Sie anschließend einen schnellen Weg, $a^k \bmod N$ zu berechnen und begründen Sie ihn. Literaturhinweis: [14]
3. Thema: *Das Verfahren von ElGamal.*
   Gebiet: Reine Mathematik.
   Aufgabenstellung: Erläutern und beschreiben Sie das Verfahren von ElGamal. Erklären Sie insbesondere die ihnen aus der Schule nicht bekannten Begriffe.

Schildern Sie den groben Beweisgang durch Zitation der notwendigen Sätze. Auf welche Annahmen stützt sich im Wesentlichen die Sicherheit des Verfahrens von ElGamal? Literaturhinweis: [14]

4. Thema: *Der Euklidische Algorithmus*.
   Gebiet: Zahlentheorie.
   Aufgabenstellung: Beschreiben Sie den Euklidischen Algorithmus. Erläutern Sie, warum der Euklidische Algorithmus nach endlich vielen Schritten abbricht. Schildern Sie, wie man mit dem Euklidischen Algorithmus den ggT und das kgV zweier Zahlen bestimmen kann. Illustrieren Sie an aussagekräftigen Beispielen, dass dieser Weg schneller ist als eine Faktorisierung dieser Zahlen. Literaturhinweise: [14], [31]
5. Thema: *Eine mathematische Modellierung von Verschiebechiffren*.
   Gebiet: Mathematisierung.
   Aufgabenstellung: Formulieren Sie das Chiffrierverfahren von Caesar umgangssprachlich und in der Sprache der modularen Arithmetik. Beschreiben Sie insbesondere die Chiffrierfunktion mathematisch. Verallgemeinern Sie diese spezielle Art linearer Funktionen zur Gewinnung von Chiffrierverfahren mit einer größeren Schlüsselanzahl. Literaturhinweise: [39], [4]
6. Thema: *Die Kryptoanalyse monoalphabetischer Chiffrierungen*.
   Gebiet: Stochastik und Mathematisierung.
   Aufgabenstellung: Erklären Sie das Prinzip der monoalphabetischen Chiffrierung. Zeigen Sie, wie auf diese Art verschlüsselte Texte unter Ausnutzung charakteristischer Häufigkeiten von Buchstaben und Bigrammen dechiffriert werden können. Literaturhinweis: [4]
7. Thema: *Über das Finden großer Primzahlen.*
   Gebiet: Algorithmik und Zahlentheorie.
   Aufgabenstellung: Schildern Sie das Sieb des Eratosthenes. Zeigen Sie, wie man einen naiven Primzahltest schrittweise verfeinern kann. Beschreiben Sie anschließend einen probabilistischen Primzahltest. Illustrieren Sie die Verfahren mit Beispielen und vergleichen Sie den Aufwand dieser Verfahren. Benutzen Sie dazu ein Computeralgebrasystem. Literaturhinweise: [14], [31]
8. Thema: *Über die Faktorisierung natürlicher Zahlen.*
   Gebiet: Algorithmik und Zahlentheorie.
   Aufgabenstellung: Schildern Sie ein Verfahren zur Faktorisierung einer natürlichen Zahl. Erläutern Sie den Primzahlsatz und begründen Sie, warum das naive Testen aller in Frage kommenden Primteiler kein wirklich geeigneter Zugang ist. Literaturhinweise: [14], [31]
9. Thema: *Interaktives Beweisen – Ist das Mathematik?*
   Gebiet: Logik, Stochastik, Informatik.

Aufgabenstellung: Erläutern Sie, wie man durch interaktives Beweisen einen Partner davon überzeugen kann, dass man im Besitz eines Beweises ist, ohne diesen Beweis preiszugeben.

Die vorgestellten Facharbeitsthemen berücksichtigen die unterschiedlichen Interessenlagen von SchülerInnen und fallen in verschiedene Typen der in den Richtlinien als geeignet eingestuften Aufgabenfelder, s. [26][S. 44]:

- Erarbeitung eines neuen Stoffgebietes
- Beschreibung von Methoden und Verfahren, die aus Zeitgründen im Unterricht keinen Platz haben
- Einsatz des Computers
- Historischer Überblick
- Anschauliches Stoffgebiet mit in die Tiefe gehender mathematischer Struktur

Neben den hier eindeutig in der Mathematik angesiedelten Themen fungiert die Kryptologie als Ideengeber für Facharbeiten in Informatik, Deutsch, Sozialwissenschaften, Politik, Geschichte und sogar Englisch und Latein.

Die Implementation kryptographischer Algorithmen ist eine interessante Aufgabe in der Informatik. Die sich beim Verschlüsseln von Daten ergebenden Fragen des Datenschutzes können aus Sicht der sozialwissenschaftlichen Fächer diskutiert werden. Auf die aktuellen Veränderungen im Bereich der globalen Kommunikation hat die Bundesregierung mit der Erneuerung ihrer Kryptopolitik reagiert, s. [16][S. 11]. Anreize für das Aufgreifen historischer Themen können die Verschlüsselung von Caesar, die Chiffriermaschine Enigma oder der Einsatz von Kryptosystemen bei der Überwachung von Rüstungskontrollabkommen sein, s. [13].

Der Gebrauch von Geheimschriften übt auf viele Autoren eine große Anziehungskraft aus z.B. A.C. Doyle, A. Lindgren oder E.A. Poe, s. z.B. [11], [10], den Text aus A. Lindgren: *Kalle Blomquist lebt gefährlich* in [5] oder die Ausführungen von F.L. Bauer über das Gedicht *The Gold Bug* von E.A. Poe [2][S. 301]. Das Spiel mit Worten und Buchstaben, das Überlisten der charakteristischen Häufigkeiten einzelner Buchstaben durch die Nichtbenutzung eines bestimmten Buchstabens kann als Anstoß für eine Facharbeit im Bereich Deutsch dienen. Viele weitere schöne Beispiele hierzu findet man in dem Buch von F.L. Bauer *Entzifferte Geheimnisse* [2].

Literatur

[1] W. R. Alford, A. Grandville, C. Pommerance. There are infinitely many Carmichael numbers. *Ann. Math. Ser.*, 140:703–722, 1994.

[2] F. L. Bauer. *Entzifferte Geheimnisse: Methoden und Maximen der Kryptologie*. Springer Verlag, Berlin, Heidelberg, 1997.

[3] A. Beutelspacher. Kryptographie: Eine Einführung in die Wissenschaft von der Geheimhaltung der Daten. *MU*, 33(3):4–14, 1987.

[4] A. Beutelspacher. *Kryptologie*. Vieweg Verlag, Braunschweig, 2002. 6. Auflage.

[5] A. Beutelspacher. Nqwär=?Ha+püßsdgtj, Geheimschriften. *mathematik lehren*, Heft 72, 1994.
[6] A. Beutelspacher, J. Schwenk, K.-D. Wolfenstetter. *Moderne Verfahren der Kryptographie*. Vieweg Verlag, Braunschweig, 1995.
[7] W. Blum. Mathematik für Millionen. *Die Zeit*, 22:Wissen 34, 2000.
[8] J. H. Conway, R. K. Guy. *Zahlenzauber: von natürlichen, imaginären und anderen Zahlen*. Birkhäuser Verlag, Basel, Boston, Berlin, 1997, aus dem Amerikan. von Manfred Stern.
[9] W. Dieffie, M. J. Hellman. New directions in cryptography. *IEEE Trans. Inf. Theory*, 22:644– 654, 1976.
[10] A. Conan Doyle. *The Adventure of the Dancing Men*, Band 19. Doubleday, Doran and Company, Garden City, The Crowborough edition, 1930.
[11] A. Conan Doyle. *The Valley of the Fear*, Band 15. Doubleday, Doran and Company, Garden City, The Crowborough edition, 1930.
[12] T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans. Inf. Theory*, 31:469–472, 1985.
[13] A. Engel. Datenschutz durch Chiffrieren: Mathematische und algorithmische Aspekte. *MU*, 6:30–51, 1979.
[14] O. Forster. *Algorithmische Zahlentheorie*. Vieweg Verlag, Braunschweig, Wiesbaden, 1996.
[15] W. Fumy, H. P. Rieß. *Kryptographie*. Oldenbourg, München, 1994. 2. Auflage.
[16] Innovation und Arbeitsplätze in der Informationsgesellschaft des 21. Jahrhunderts. Aktionsprogramm der Bundesregierung. Bundesministerium für Wirtschaft und Technologie/Bundesministerium für Bildung und Forschung. Referat Öffentlichkeitsarbeit, 1999.
[17] C. F. Gauß. *Disquisitiones Arithmeticae*. Chelsea Publishing Company, New York, 1965. Deutsche Übersetzung von H. Maser.
[18] H. W. Heibey, A. Pfitzmann. Kryptographie. Herausforderung für Staat und Gesellschaft. *Log In*, 16:37–43, 1996.
[19] J. M. Kantor. Hilbert's problems and their sequels. *Math. Intelligencer*, 18(1):21–30, 1996.
[20] H. Kautschitsch. Mathematik in der Kryptographie. In: *ÖMG-Lehrerfortbildungstagung Wien*, Band 10 der ÖMG Didaktik-Reihe, S. 80–95, 1983.
[21] D. E. Knuth. *The Art of Computer Programming*, Band 2. Addison Wesley, Reading Mass., 1981.
[22] L. Kronecker. *Vorlesungen über Zahlentheorie*. Springer Verlag, Berlin, Heidelberg, New York, 1978. Erster Band. reprint.
[23] F. Lorenz. *Einführung in die Algebra*. Teil I. BI-Wissenschaftsverlag, Mannheim, Wien, Zürich, 1987.
[24] Stärkung des mathematisch-naturwissenschaftlich-technischen Unterrichts. Ministerium für Schule und Weiterbildung, Wissenschaft und Forschung des Landes Nordrhein-Westfalen, 1999.
[25] Ministerium für Schule und Weiterbildung des Landes Nordrhein-Westfalen. Richtlinien und Lehrpläne für das Gymnasium – Sekundarstufe I – in Nordrhein-Westfalen. Mathematik. Ritterbach Verlag, 1981. Heft 3401.
[26] Ministerium für Schule und Weiterbildung, Wissenschaft und Forschung des Landes Nordrhein-Westfalen. Richtlinien und Lehrpläne für die Sekundarstufe II – Gymnasi-

um/Gesamtschule in Nordrhein-Westfalen. Mathematik. Ritterbach Verlag, 1999. Heft 4720.
[27] W. Moldenhauer. Die Facharbeit in Mathematik. *MNU*, 67–71, 1999.
[28] G. Nebe. Faktorisieren ganzer Zahlen. *Jahresber. Deutsch. Math.-Verein.*, 102(1):1–14, 2000.
[29] H. Puhlmann. Kryptographie verstehen. Ein schülergerechter Zugang zum RSA-Verfahren. Preprint Nr. 2000, 1998. Technische Universität Darmstadt.
[30] M. O. Rabin. Probabilistic algorithms for primality testing. *J. Number Theory*, 12:128–138, 1980.
[31] R. Remmert, P. Ullrich. *Elementare Zahlentheorie*. Birkhäuser Verlag, Basel, Boston, 1987.
[32] R. L. Rivest, A. Shamir, L. Adleman. A method for obtaining digital signatures and public key cryptosystems. *Commun. ACM*, 21:120–126, 1978.
[33] R. H. Schulz. Primzahlen in öffentlichen Chiffrierverfahren. *mathematik lehren*, 61:56–64, 1993.
[34] R. Schulz-Zander. Lernen in der Informationsgesellschaft. *Pädagogik*, 3:8–12, 1997.
[35] F. Schwarz. *Einführung in die Zahlentheorie*. Teubner, Stuttgart, Leipzig, 1998.
[36] Lambacher Schweizer. LS 10. Klett Verlag, Stuttgart, 1996.
[37] M. Seiffert. Verschlüsselungsmethoden. *Log In*, 14:25–40, 1994.
[38] R. Solovay, V. Strassen. A fast Monte Carlo test for primality. *SIAM J. Comp.*, 6:4–85, 1977. Erratum Vol. 7 (1978) 118.
[39] T. Sonar. *Angewandte Mathematik, Modellbildung und Informatik*. Vieweg, Braunschweig, 2001.
[40] C. Suetonius Tranquillus. *De Vita Caesarium Libri VIII*. Bibliotheca Scriptorum Graecorum et Romanorum Teubneriana. Teubner, Stuttgart, 1978.
[41] K.-U. Witt. *Algebraische Grundlagen der Informatik*. Vieweg-Verlag, Braunschweig, 2001.
[42] F. Zech. *Grundkurs Mathematikdidaktik. Theoretische und praktische Anleitung für das Lehren und Lernen von Mathematik*. Beltz Verlag, Weinheim, Basel, 1997.

Anschrift des Verfassers

Martin Epkenhans
Fakultät für Elektrotechnik, Informatik und Mathematik
Universität Paderborn
33095 Paderborn
E-Mail: martine@uni-paderborn.de