Lieber Wolfgang,

die herzlichsten Glückwünsche zu Deinem „Sechziger“!

Nicht zuletzt in unserem eigenen Interesse wünschen wir Dir für die nächsten 5 Berufsjahre und auch weit darüber hinaus eine produktive Zeit als Fachdidaktiker.

Außerdem wünschen wir Dir viel Freude und Vergnügen an all den beruflichen und privaten Dingen, die Du – am liebsten mit Deiner Frau Beate – so gerne machst: Reisen (insbesondere Fernreisen und Tauchen), Sammeln (Briefmarken, alte – vor allem englische – Gläser, Urangläser, Bücher etc.) Flohmärkte besuchen, Heimwerken, Besuche von Haubenrestaurants, gemütliche Runden bei Rotwein und Zigarren.

Ad multos annos!

Modellierungsaufgaben im Mathematikunterricht – Herausforderung für Schüler und Lehrer

Werner Blum, Kassel

Zusammenfassung: In diesem Beitrag soll anhand von Beispielen aus einer laufenden Studie gezeigt werden, wie Schüler und Lehrer mit Modellierungsaufgaben umgehen, welche Probleme sich dabei zeigen und welche Möglichkeiten es gibt, diese Probleme anzugehen. Nach dem einleitenden Abschnitt 1 gebe ich in Abschnitt 2 eine Arbeitsdefinition des Begriffs „Modellieren“ und erinnere daran, warum Realitätsbezüge im Mathematikunterricht so wichtig sind. In Abschnitt 3 richte ich den Blick auf die Bearbeitungsprozesse von Schülern, während in Abschnitt 4 das unterrichtliche Handeln von Lehrern im Blickpunkt steht. Schließlich deute ich in Abschnitt 5 an, welche Erkenntnisse aus jener Studie abgeleitet werden können.

1. Einleitung

Dass Schüler *mathematisches Modellieren* lernen sollen, ist eine seit langem erhobene Forderung. Schon W. Lietzmann hat postuliert:

> *„Erst das Hin und Wider zwischen Wissenschaft und Wirklichkeit in beiderlei Richtung erschöpft die Aufgabe, die im materialen Zweck der Mathematik liegt. Ebenso wichtig wie die Anwendung einer mathematischen Tatsache auf die Wirklichkeit, aber ungleich schwerer ist die Aufgabe, in der Wirklichkeit das mathematische Problem zu sehen.“ (Lietzmann 1919, S. 66)*

Auch H.-W. Henn hat sich schon früh für einen „beziehungshaltigen“ Mathematikunterricht eingesetzt (Henn 1980).

Neu erhoben wurde diese Forderung im Zusammenhang mit der PISA-Studie (Baumert et al. 2001; Prenzel et al. 2004). Deutschen Fünfzehnjährigen werden hier beträchtliche Defizite in Bezug auf „*Mathematical Literacy*“ bescheinigt, das ist i. W. die Fähigkeit, Mathematik in Realsituationen verständig verwenden zu können. Übersetzen zwischen Realität und Mathematik, also mathematisches Modellieren, bildet das Herz von Mathematical Literacy (siehe Blum et al. 2004).

Besonders aktuell ist Modellieren dann im Kontext der länderübergreifenden *Bildungsstandards* geworden, die in Deutschland als unmittelbare Konsequenz aus den PISA-Ergebnissen etabliert worden sind (vgl. Klieme et al. 2003). Hier ist nicht der Ort, Chancen und Risiken von Bildungsstandards zu diskutieren. Es soll nur betont werden, dass mathematisches Modellieren nun nicht mehr nur als Dekoration in den Präambeln stofforientierter (und zum Teil auch stoff-

überfrachteter) Lehrpläne steht, sondern eine von sechs allgemeinen mathematischen Kompetenzen ist, die Schüler im Mathematikunterricht erwerben sollen.

Ziel dieses Beitrags ist es aufzuzeigen, welche Probleme Schüler und Lehrer mit Modellierungsaufgaben haben und welche Folgerungen hieraus für eine unterrichtliche Behandlung solcher Aufgaben gezogen werden können. Insbesondere soll gezeigt werden, dass es sich lohnt, sich diesen Herausforderungen zu stellen und Modellierungsaufgaben in selbstverständlicher Weise in den Mathematikunterricht einzubeziehen.

2. Was ist und wozu dient mathematisches Modellieren?

Es gibt ganz unterschiedliche Auffassungen vom Begriff des mathematischen Modellierens (für eine Übersicht siehe Part 1 in Blum/Galbraith/Henn/Niss 2006). Sie reichen vom Mathematisieren im engeren Sinn, d. h. vom Aufstellen eines mathematischen Modells als geeignetes Abbild eines Ausschnitts der Welt, bis zum angewandten Problemlösen im umfassendsten Sinn. Ich lege hier ein Prozessschema des Bearbeitens von realitätsbezogenen Aufgaben entsprechend Blum/Leiß (2005a) zugrunde (Abb. 1):

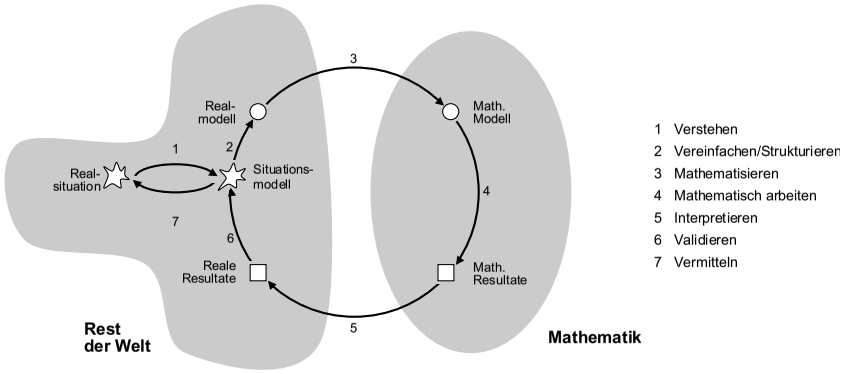

Abb. 1. Prozessschema für Modellierungsaufgaben

Nehmen wir das Aufgabenbeispiel „Leuchtturm“, das eine auch aus Schulbüchern bekannte Problemstellung beinhaltet:

Leuchtturm

In der Bremer Bucht wurde 1884 direkt bei der Küste der 30,7 m hohe Leuchtturm „Roter Sand“ gebaut. Er sollte Schiffe durch sein Leuchtfeuer davor warnen, dass sie sich der Küste nähern.

Wie weit war ein Schiff ungefähr noch vom Leuchtturm entfernt, wenn es ihn zum ersten Mal sah?

Runde geeignet. Beschreibe deinen Lösungsweg.

Der erste Schritt eines idealtypischen Lösungsprozesses ist die Konstruktion einer eigenen mentalen Vorstellung von der gegebenen Problemsituation mit dem Ziel, Situation und Fragestellung zu verstehen. Das resultierende *Situationsmodell* muss dann strukturiert und vereinfacht werden, wobei naheliegende Annahmen hier sind: Die Erde ist eine Kugel, das Schiff ist punktförmig, die Sicht ist frei, das Leuchtfeuer befindet sich an der Turmspitze und der Lichtstrahl verläuft wie eine Gerade. Das liefert ein *Realmodell* der Situation. Nun werden die Objekte und Annahmen mathematisiert. Das entsprechende *mathematische Modell* ist (mit sinnvollen Ergänzungen) ein Dreieck wie in Abb. 2 zu sehen, wobei der Erdradius $R \approx 6370$ km ist, $h = 30,8$ m bekannt und s gesucht ist.

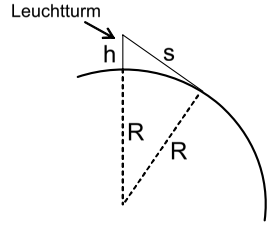

Abb. 2

Nun wird mathematisches Wissen eingesetzt: Kreistangenten stehen senkrecht auf dem zugehörigen Radius, das Modell-Dreieck ist also rechtwinklig. Pythagoras liefert dann das *mathematische Resultat*: $s \approx \sqrt{2Rh} \approx 19.8$ km. Rück-Interpretation in die Realsituation bringt das *reale Resultat*: Die Sichtweite beträgt (bei den gegebenen Bedingungen) etwa 20 km. Nun muss dieses Ergebnis kritisch geprüft werden: Waren die Annahmen vernünftig? Waren die mathematischen Überlegungen und Rechnungen korrekt? Ist die Ergebnis-Genauigkeit angemessen? Zum Beispiel kann man zusätzlich nun die Höhe des Schiffs berücksichtigen. Dann revidiert man das Modell und wiederholt den Durchlauf. Ist das Schiff z. B. 10 m hoch, resultiert eine Sichtweite von etwa 31 km. Ein Bestandteil solcher Validierungsaktivitäten könnten auch verallgemeinernde funktionale Reflexionen sein:

Wie hängt die Sichtweite von der Turmhöhe ab? Man sieht (s ungefähr proportional $\sqrt{h}$!), dass man die Turmhöhe vervierfachen muss, um die doppelte Sichtweite zu erhalten.

Wenn im Folgenden vom *mathematischen Modellieren* die Rede ist, sind die Schritte 2, 3, 5 und 6 dieses Kreislaufs gemeint. Von *Modellierungsaufgaben* spreche ich, wenn substanzielle Anforderungen in Bezug auf diesen Teil des Bearbeitens involviert sind, so wie das z. B. bei „Leuchtturm" der Fall ist.

Diese Form des Prozessschemas (man nennt dies meist prägnant den „Modellierungskreislauf") hat ihre Wurzeln zum einen in der pragmatisch orientierten Diskussion zum Modellieren als Lösen realer Problemstellungen und zum andern in der psychologisch orientierten Diskussion zu Textaufgaben. Aus letzterer kommt die Betonung des ersten Bearbeitungsschritts, des sinnentnehmenden Lesens gegebener Texte und dadurch Verstehens der gegebenen Problemsituation. Dies ist ein individuell zu vollziehender Konstruktionsakt, der oft schon eine hohe kognitive Hürde darstellt (siehe Abschnitt 3). Überhaupt stellt dieses Kreislaufschema eine wirksame Hilfe zum Beurteilen tatsächlicher individueller Bearbeitungsprozesse dar, auch wenn diese i. a. nicht so linear verlaufen, wie es das Schema suggeriert (zu „individuellen Modellierungsverläufen" vgl. Borromeo-Ferri 2006). Insbesondere sind alle Stationen dieses Kreislaufs potenzielle kognitive Hürden.

Wozu sollen überhaupt Realitätsbezüge in den Mathematikunterricht integriert werden? Es gibt mehrere *Gründe* dafür (vgl. Winter 2003, Blum 1996):

- Nur mit Realitätsbezügen kann der Mathematikunterricht zum Umweltverstehen, zur Alltagsbewältigung und zur Berufsvorbereitung beitragen („pragmatische" Gründe).
- Realitätsbezüge sind ein Vehikel zur Kompetenzentwicklung und sind insbesondere für die Förderung der Kompetenz Modellieren unentbehrlich („formale" Gründe).
- Realitätsbezüge helfen Schülern beim Mathematiklernen, sie dienen zum besseren Verstehen und Behalten von mathematischen Inhalten und können diese motivieren („lernpsychologische" Gründe).
- Nur mit Realitätsbezügen lässt sich ein adäquates Mathematikbild bei Schülern aufbauen („kulturbezogene" Gründe).

Mit diesen Gründen sind gleichzeitig hohe Ansprüche formuliert. Nötig ist hierzu die Behandlung eines breiten Spektrums von realitätsbezogenen Beispielen und Aufgaben, von eingekleideten Textaufgaben bis hin zu authentischen Modellierungsaufgaben. Quellen gibt es genug, so die ISTRON-Reihe bei Franzbecker (siehe Henn/Maaß 2003 und die Übersicht hierin) oder Bücher wie Herget/Scholz (1998), Herget/Jahnke/Kroll (2001) oder Büchter/Leuders (2005).

Im *Alltagsunterricht* kommen Modellierungsaufgaben und -aktivitäten eher wenig vor. Ein wesentlicher Grund dafür ist, dass der Unterricht im Vergleich

zum bewährten kalkülorientierten Unterricht anspruchsvoller wird, für Schüler und für Lehrer. *Veränderungen* der herkömmlichen Unterrichtspraxis in der Sekundarstufe I sind vor allem durch das BLK-Modellversuchsprogramm SINUS initiiert worden, das 1998 als Reaktion auf die unbefriedigenden Ergebnisse der TIMS-Studie ins Leben gerufen worden ist (Baumert et al. 1997, Henn 1999; Prenzel/Baptist 2001; Blum et al. 2000; Bendrien/Biermann/Leiß 2005). Empirische Untersuchungen haben jedoch selbst im Unterricht engagierter SINUS-Lehrer *Defizite* aufgezeigt, die offensichtlich nicht den einzelnen Lehrern anzulasten sind, sondern auf Erkenntnisdefizite zurückzuführen sind, insbesondere:

- Was genau ist das kognitive Potenzial anspruchsvoller Modellierungsaufgaben, was ist ihr jeweiliger „Aufgabenraum" („Task Space")?
- Wie bearbeiten Schüler solche Aufgaben, was sind dabei „Schlüsselstellen" und kognitive Hürden?
- Was sind hierbei schüler- und aufgabenadäquate Diagnose- und Interventionsmöglichkeiten für Lehrer?
- Welche (kurz-, mittel- und langfristigen) Wirkungen hat das Lehrerhandeln in solch aufgabenbasierten Lernumgebungen auf Leistungen und Einstellungen der Schüler?

3. Wie gehen Schüler mit Modellierungsaufgaben um?

Die Fragen am Ende von Abschnitt 2 waren Ausgangspunkt und Leitlinie für DISUM, ein interdisziplinäres Projekt zwischen Mathematik-Didaktik (Werner Blum), Pädagogik (Rudolf Messner, Universität Kassel) und pädagogischer Psychologie (Reinhard Pekrun, Universität München). DISUM bedeutet „Didaktische Interventionsformen für einen selbständigkeitsorientierten aufgabengesteuerten Unterricht am Beispiel Mathematik". Das Projekt begann im Jahr 2002, seit 2005 ist es DFG-gefördert (siehe z. B. Blum/Leiß 2003, Leiß/Blum/Messner 2006). Untersuchungsschwerpunkt sind Modellierungsaufgaben in den Klassen 8 – 10 aller Schulformen. Die Untersuchungen finden sowohl im Labor (Schülerpaare mit und ohne Lehrer lösen Aufgaben) als auch im Unterricht statt. Insbesondere gab es 2004/05 eine umfangreiche „Best-Practice-Studie", bei der besonders erfahrene und großenteils auch in der Fortbildung tätige SINUS-Lehrer aus Hauptschulen und Gymnasien diverse Modellierungsaufgaben im regulären Unterricht behandelt haben.

Ein konkretes Beispiel: Die Aufgabe „Riesenschuhe":

Riesenschuhe

Florentino poliert in einem Sportzentrum auf den Philippinen das laut Guinness-Buch der Rekorde weltgrößte Paar Schuhe. Ein Schuh ist 2,37 m breit und 5,29 m lang.

Wie groß wäre der Riesenmensch ungefähr, dem dieses Paar Schuhe passen würde?

Beschreibe deinen Lösungsweg.

Die wesentlichen kognitiven Hürden bei dieser Aufgabe liegen am Anfang der Bearbeitung, beim Verstehen der Sachsituation und Treffen geeigneter Annahmen (z. B.: proportionaler Zusammenhang Fußlänge – Menschengröße und eigener Körper als Referenz). Hier hatten viele Schüler (und übrigens auch manche Lehramtsstudenten bei parallelen Untersuchungen) große Probleme. Der folgende Auszug aus dem Lösungsprozess zweier Hauptschüler (ohne Lehrer) verdeutlicht dies:

> *Also aus den beiden Zahlen die Höhe, also die Größe des Menschen berechnen – Wenn 2,37 m die Breite des Schuhs ist und 5,29 m lang, müsste, ich glaube, 2,37 m mal 5,29 m – Dann hast' doch die Höhe von dem Menschen, glaube ich. (Auszug 1: Hauptschüler zu „Riesenschuhe")*

Die Schüler berechnen dann unmittelbar 2,37 x 5,29 m = 12,54 m als Größe des Riesenmenschen. Hier ist eine weit verbreitete Schülerstrategie sichtbar: Wenn du nicht genau weißt, was zu tun ist, dann benutze einfach ein unmittelbar verfügbares Schema, das auf die gegebenen Zahlen/Größen passt.

Ich fasse einige Beobachtungen aus Labor und Unterricht zusammen:

- Alle Schritte des Modellierungskreislaufs sind potenzielle kognitive Hürden für Schüler, variierend je nach Aufgabe und Individuum.

Folgerung: Es müssen die Teil-Kompetenzen des Modellierens (entsprechend den einzelnen Schritten des Kreislaufs) mithilfe geeigneter Aufgaben gezielt gefördert werden.

- Schüler benutzen i. a. keine bewussten Lösungsstrategien und sind bei auftretenden Schwierigkeiten oft hilflos.

Folgerung: Schülern müssen adäquate Strategien zum Lösen von Modellierungsaufgaben an die Hand gegeben werden; siehe dazu Abschnitt 4.

- Es gibt einen fundamentalen Unterschied zwischen dem „Alleine-Arbeiten" von Schülern und selbständigem Arbeiten mit Lehrerunterstützung; im ersten Fall sind Schüler oft überfordert und geben auf.

Folgerung: Die in der zeitgenössischen Pädagogik gelegentlich propagierte Abstinenz des Lehrers von Eingriffen in Lösungsprozesse ist so pauschal sicher falsch. Es geht um die subtile Balance zwischen Schüler-Selbständigkeit und Anleitung durch den Lehrer, um minimale, diagnosebasierte Interventionen bei auftretenden Schülerschwierigkeiten („Hilf mir, es selbst zu tun"). Hierzu bedarf es einer gezielten Schulung von Lehrern in Diagnose- und Interventionsmöglichkeiten bei Modellierungsaufgaben.

Der letzte Punkt leitet bereits über zu Abschnitt 4.

4. Wie gehen Lehrer mit Modellierungsaufgaben um?

Wir haben die Unterrichtsstunden der erwähnten „Best-Practice-Studie" nach unseren *Qualitätskriterien* beurteilt, bei denen wir „Fachlich gehaltvolle Unterrichtsgestaltung", „Kognitive Aktivierung der Lernenden" und „Effektive und schülerorientierte Unterrichtsführung" unterscheiden (genauer siehe bei Blum/Leiß 2005b).

In den beobachteten Stunden waren viele dieser Kriterien erfüllt. So haben sehr viele der Lehrer eine Stundenstruktur gewählt, die selbständige Modellierungsaktivitäten der Schüler begünstigt (vgl. auch Bendrien /Biermann/Leiß 2005):

1. Vorstellung der Aufgabe im Plenum
2. Einzelarbeit
3. Gruppenarbeit
4. Individuelles Aufschreiben von Lösungen
5. Präsentation von Lösungen im Plenum
6. Vergleich der Lösungen und reflektierender Rückblick

Diese Stundenstruktur erinnert an Unterrichtsskripts, wie sie im Anschluss an TIMSS aus japanischen Stunden bekannt geworden sind (Baumert/Lehmann et al. 1997). Eine Weiterentwicklung dieses Skripts erfolgte hier u. a. dadurch, dass jeder Schüler seine eigene Lösung aufschreiben musste. In den Fällen, wo Phase 4 durch eine Gruppenlösung ersetzt wurde, bestand Phase 5 oft aus einer Lösungspräsentation in neu zusammengesetzten Gruppen („Expertenmethode"/ „Gruppenpuzzle"/„Museumsrundgang"). Hier ist ein Beispiel für die Qualität so entstandener Schülerlösungen. Es geht um die bekannte Aufgabe „Tanken" (Blum/Leiß 2005a):

Tanken

Herr Stein wohnt in Trier, 20 km von der Grenze zu Luxemburg entfernt. Er fährt mit seinem VW Golf zum Tanken nach Luxemburg, wo sich direkt hinter der Grenze eine Tankstelle befindet. Dort kostet der Liter Benzin nur 0,85 Euro, im Gegensatz zu 1,1 Euro in Trier.
Lohnt sich diese Fahrt für Herrn Stein? Begründe deine Antwort.

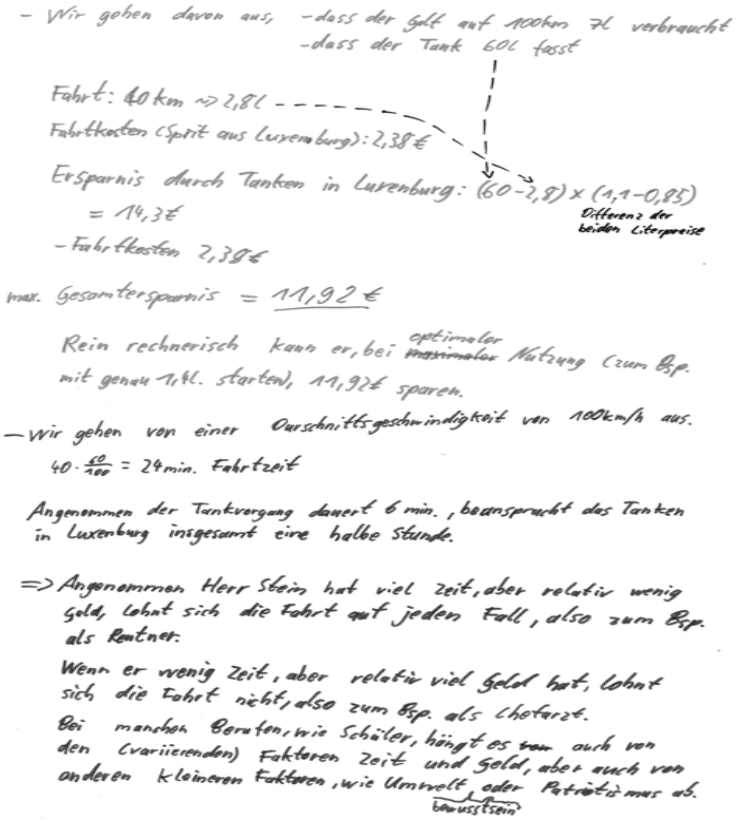

Abb. 3. Schülerlösung zu „Tanken“

Eine gymnasiale Schülergruppe produzierte die in Abb. 3 abgedruckte Lösung. Bei den Validierungsüberlegungen werden hier sogar Umweltgesichtspunkte und „Patriotismus“ (Tanken in Trier als Unterstützung der deutschen Wirtschaft) ins Spiel gebracht.

In einigen der beobachteten Stunden zu „Tanken“ fanden auch (wie schon in Abschnitt 2 bei „Leuchtturm“ angesprochen) funktionale Reflexionen statt: Wie hängt die Antwort auf die Frage, ob sich die Fahrt nach Luxemburg „lohnt“, von den getroffenen Annahmen ab? In einer der Klassen war eine Schülerfrage der willkommene Anlass hierfür:

> *Das ist doch jetzt komisch, wenn wir das jetzt sagen, angenommen, 8 Liter, und dann jetzt eine andere Gruppe sagt, keine Ahnung, 6 oder 7 Liter, dann hat ja jeder ein anderes Ergebnis später – müssen wir da nicht alle irgendwie dasselbe haben, dass wir ... (Auszug 2: Gymnasiast zu „Tanken“)*

Ein besonders schönes Beispiel zum konstruktiven Umgehen mit Schülerfehlern war in einer gymnasialen Unterrichtsstunde zu „Leuchtturm“ zu beobachten. Eine Schülergruppe hatte die Lösung „Sichtweite ≈ 20 km“ für ein punktförmiges Schiff produziert (siehe Abschnitt 2) und in einem zweiten Schritt mit der Schiffshöhe 10 m gearbeitet. Hier ist die zugehörige Lösung (Abb. 4):

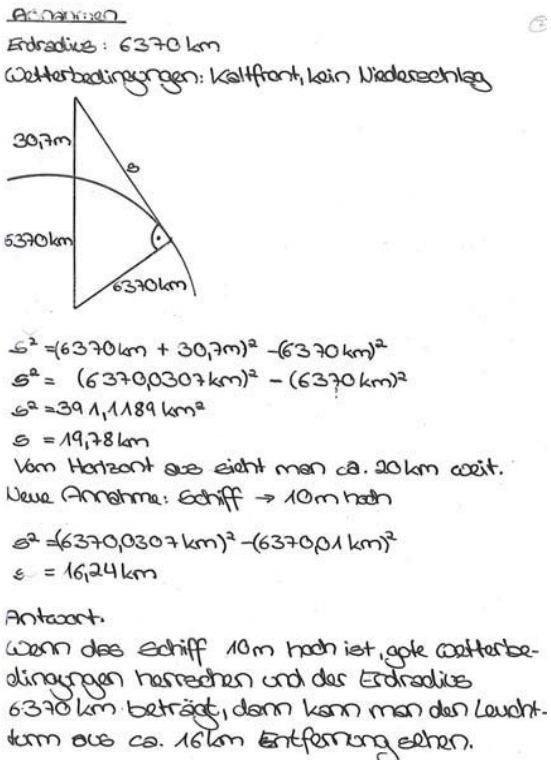

Abb. 4. Schülerlösung zu „Leuchtturm“

Die Lösung ist offensichtlich falsch (geringere Sichtweite bei höherem Schiff). Wo liegt der Fehler? Man darf die 10 m natürlich nicht einfach in die Pythagoras-Gleichung einbauen (was berechnet man dann eigentlich?), vielmehr muss man das Modell wie in Abb. 5 modifizieren, mit Ergebnis

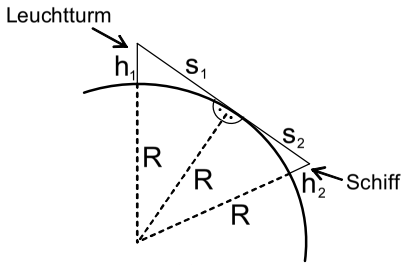

Abb. 5

$$s = s_1 + s_2 \approx \sqrt{Rh_1} + \sqrt{2Rh_2}$$

$$(= \sqrt{2R}(\sqrt{h_1} + \sqrt{h_2})).$$

Der Lehrer hatte diesen Fehler sofort registriert, aber nicht interveniert. Stattdessen berechnete er parallel zu den Schülern weitere Konsequenzen aus diesem falschen Modell (also einige Werte der Zuordnung $h_2 \to s \approx \sqrt{2R(h_1 - h_2)}$). Er ließ die Gruppe dann dieses falsche Ergebnis präsentieren, und in die beginnende Unruhe hinein thematisierte er in ganz distanzierter Form diesen kognitiven Konflikt:

Wenn ich die Frage, welchen Einfluss hat eigentlich die Höhe des Punktes auf dem Schiff, von dem aus man den Leuchtturm beobachtet. […] Ich hab das nun eben gerade mal gerechnet, mit meinem schlauen Rechner, ich möchte Euch die Ergebnisse mal kurz zeigen. […] (L. projiziert seine Rechnung mit TC an die Wand.)

[…] So, das c_1 in dieser Tabelle ist einfach die angenommene Höhe des Schiffs. c_1=0 bedeutet also die Lösung […] von Gruppe 1, die auf diese Frage gar nicht eingegangen ist. c_1=5 bedeutet 5 Meter Höhe, 10 Meter Höhe, 15 Meter Höhe. […] Es ist also tatsächlich so: Wenn man das so rechnet, wie Ihr es getan habt, dann gilt: Je höher der Punkt des Schiffes ist, desto später sieht man den Leuchtturm.

Wir haben jetzt noch etwa 5 Minuten Zeit. Ich möchte Euch bitten, dass Ihr in den 5 Minuten, und zwar jeder Tisch für sich, in den Stammgruppen also, Euch diesen Zusammenhang zwischen der Höhe des Schiffes und der Lösung dieser Aufgabe, dass Ihr Euch bitte diesen Zusammenhang anhand einer Skizze noch mal versucht klar zu machen. Ist es denn wirklich richtig so, wie es da gerechnet wurde? Ich habe es schlicht und ergreifend genau-

so gerechnet, wie der Max es vorgetragen hat. (Auszug 3: Gymnasiallehrer zu „Leuchtturm“)

Der Lehrer spielte das Problem also geschickt an die Klasse zurück, und tatsächlich gelang es den meisten Schülern, insbesondere auch der verantwortlichen Gruppe, selbständig den Fehler zu entdecken und zu korrigieren.

In dieser (von hoher fachlicher, fachdidaktischer und pädagogischer Professionalität des Lehrers geprägten) Unterrichtssituation ist die am Ende von Abschnitt 3 angesprochene Balance zwischen Lehrer-Anleitung und Schüler-Selbständigkeit wirklich gelungen. Das war aber doch eher selten der Fall. Auch in den Best-Practice-Klassen waren die Lehrerinterventionen oft nicht minimal, z. B. wurden oft direkte inhaltliche Hilfen gegeben, statt bloß strategisch einzugreifen (strategisch wäre z.B.: „Was willst du denn rauskriegen?“; „Was ist denn gegeben und was brauchst du noch?“; „Denk an die Aufgabe gestern“; „Was musst du jetzt noch machen?“).

Folgerung: Lehrer brauchen gezielte Schulung in Möglichkeiten der Intervention. Hilfreich ist hier die aus DISUM hervorgegangene Typisierung von Lehrerinterventionen (Leiß/Wiegand 2004): affektive/ organisatorische/ inhaltliche/ strategische Interventionen.

Weitere Beobachtungen:

- Lehrer setzen oft ihre eigene spezielle Variante der Aufgabenlösung unbewusst bei den Schülern durch, weil ihre Interventionen massiv von dieser Lösungsvariante geprägt sind (Beispiele siehe bei Blum/Leiß 2005b). Das führte in unserer Studie dazu, dass man Schülerlösungen aus verschiedenen Klassen zu derselben Aufgabe oft alleine schon aufgrund der Lösungsvariante einer bestimmten Klasse zuordnen konnte, entgegen der Intention aller Lehrer, multiple Lösungen zuzulassen und sogar herauszufordern. Wesentlicher Grund für dieses Lehrerverhalten ist eine unzureichende Kenntnis der Weite der Aufgabenräume, womöglich auch ein noch zu enges Mathematik-Bild.

Folgerung: Lehrer benötigten intime Kenntnis des „Task Space“ von Modellierungsaufgaben und Schulung in Bezug auf flexible, selbständigkeitserhaltende Interventionen vor diesem Hintergrund.

- Lehrer stimulieren kaum Lösungsstrategien bei Schülern, obwohl gerade für Modellierungsaufgaben mit dem Kreislaufschema (siehe Abschnitt 2), genauer: mit schülergemäßen vereinfachten Varianten dieses Schemas (siehe Abschnitt 5) ein wirksames strategisches Instrument zur Verfügung steht. Das heißt nicht nur auf Schüler-, sondern auch auf Lehrerseite ist Strategieeinsatz die Ausnahme statt die Regel.

Folgerung: Lehrer brauchen den Modellierungskreislauf als Basis für adäquate

strategische Hilfen, und sie müssen schülergemäße Konkretisierungen des Modellierungskreislaufs kennen.

Diese Defizite selbst im Best-Practice-Unterricht (der sich ansonsten, wie zu Beginn dieses Abschnitts sichtbar geworden ist, deutlich vom Alltagsunterricht abhob) unterstreichen die Notwendigkeit, die Unterrichtsqualität ins Zentrum der Lehreraus- und -fortbildung zu rücken. Die kollegiumsbezogene Fortbildung muss dabei – wie beim SINUS-Projekt – mit der Unterrichtsentwicklung vor Ort verbunden werden. Das geeignete Vehikel dafür sind kompetenzorientierte Aufgaben, mit Modellierungsaufgaben als Kern.

5. Wie kann man Modellierungsaufgaben behandeln?

Eine Erkenntnis aus vielen empirischen Studien ist: Es gibt wohl nicht den Königsweg zum Lernerfolg (vgl. Baumert et al. 2004). Vielmehr können unterschiedliche Unterrichtsformen zu ähnlichen Effekten führen. Freilich müssen hinreichend viele der zu Beginn von Abschnitt 4 erwähnten Qualitätskriterien erfüllt sein, um überhaupt Effekte erwarten zu können. So weiß man, dass Kompetenzen wie Modellieren nur dann gefördert werden, wenn Schüler tatsächlich in Modellierungsaktivitäten involviert sind; ein Transfer von ganz andersartigen Tätigkeiten (etwa: Algorithmen abarbeiten) ist nicht erwartbar. Und man weiß, dass Lernen prinzipiell ein konstruktiver, vom Lernenden selbst durchzuführender Akt ist, der nicht durch noch so gut konzipierte „Belehrung" ersetzt werden kann. Andererseits weiß man auch, dass ein qualitätvoller Unterricht auch tatsächlich Effekte hat. So zeigt z. B. die Studie von Maaß (2004), dass es möglich ist, mit einem geeignet konzipierten Unterricht die Modellierungskompetenz von Schülern (hier: Gymnasiasten von 7./8. Klassen) substanziell zu verbessern.

In den Abschnitten 3 und 4 sind bereits mehrere spezifische, die allgemeinen Qualitätskriterien konkretisierende Gesichtspunkte genannt worden, wie man Modellierungsaufgaben im Unterricht behandeln sollte, allgemeiner gesagt: wie man Mathematikunterricht so gestalten kann, dass man eine Förderung der Modellierungskompetenz der Schüler erwarten kann. Diese Gesichtspunkte sind kurz zusammengefasst:

- Es soll ein breites Spektrum von Aufgaben behandelt werden, die gezielt auch die Teil-Kompetenzen des Modellierens ansprechen.
- Günstig zur Herausforderung von Modellierungsaktivitäten ist ein Wechsel zwischen Plenums-, Einzel- und Gruppenarbeit.
- Ziel der Lehrersteuerung ist die möglichst selbständige Aufgabenbearbeitung durch die Schüler; Lehrerinterventionen sind demgemäß diagnosebasiert, individuell-adaptiv und minimal.
- Das Spektrum von Lehrerinterventionen umfasst affektive, organisatorische, inhaltliche und strategische Interventionen; Grundlage aller inhaltlichen und strategischen Interventionen des Lehrers ist dessen detaillierte Kenntnis des Lösungsraums aller behandelten Aufgaben, speziell des Modellierungskreislaufs zu jeder Aufgabe (entsprechend Abb. 1, mit den Stationen als potenziellen kognitiven Hürden).
- Schülern sollen Lösungsstrategien für Modellierungsaufgaben an die Hand gegeben werden.
- Lösungsprozesse werden abgerundet durch reflektierende Vergleiche der produzierten Lösungen; dazu gehören auch funktionale Variationen von Eingangs-/Ausgangsdaten.

Wie angekündigt möchte ich auf den vorletzten Punkt etwas genauer eingehen: Wie können schülergemäße Lösungsstrategien für Modellierungsaufgaben aussehen? Wir haben bei DISUM einen vierschrittigen Modellierungskreislauf entwickelt, „*Lösungsplan*" genannt, der den Bearbeitungsprozess begleitet und steuert und der für Schüler aller Schulformen handhabbar ist. Abb. 6 (nächste Seite) zeigt den Lösungsplan in allgemeiner Form, so wie wir ihn in 2006 in zwei zehnstündigen Unterrichtsreihen in Klasse 8/9 der Hauptschule eingesetzt haben.[1]

Bei Schritt 2 („Gleichung aufstellen oder Dreieck einzeichnen") kann man erkennen, welche speziellen Typen von Modellierungsaufgaben in unseren Unterrichtsreihen behandelt wurden, nämlich vorwiegend Aufgaben vom Typ „Tanken", bei denen lineare Gleichungen aufzustellen sind, und Aufgaben vom Typ „Leuchtturm", bei denen ein rechtwinkliges Dreieck zu entdecken ist (die Unterrichtsreihen waren an das Thema Pythagoras angekoppelt). Aufgaben vom Typ „Riesenschuhe", bei denen aus Zeitungsartikeln mit Fotos Informationen zu entnehmen sind (bekannt aus Herget/Scholz 1998 oder Herget/ Jahnke/ Kroll 2001), waren nur in der ersten Unterrichtsreihe enthalten, weil sich gezeigt hat, dass der Lösungsplan möglichst aufgabentypspezifisch sein muss. Neben dem abgebildeten *allgemeinen* Lösungsplan wurde für jede Aufgabe ein *spezieller* Lösungsplan erstellt (zunehmend von den Schülern selbst), der die einzelnen Schritte aufgabenspezifisch konkretisiert (z. B. bei Schritt 1 statt „Situation genau vorstellen" bei „Leuchtturm" dann „Stell dir vor, du bist auf dem Schiff ...").

---

[1] Ich danke den beiden Lehrerinnen, Frau I. Schüler und Frau R. Reiff, für ihren grandiosen Unterricht.

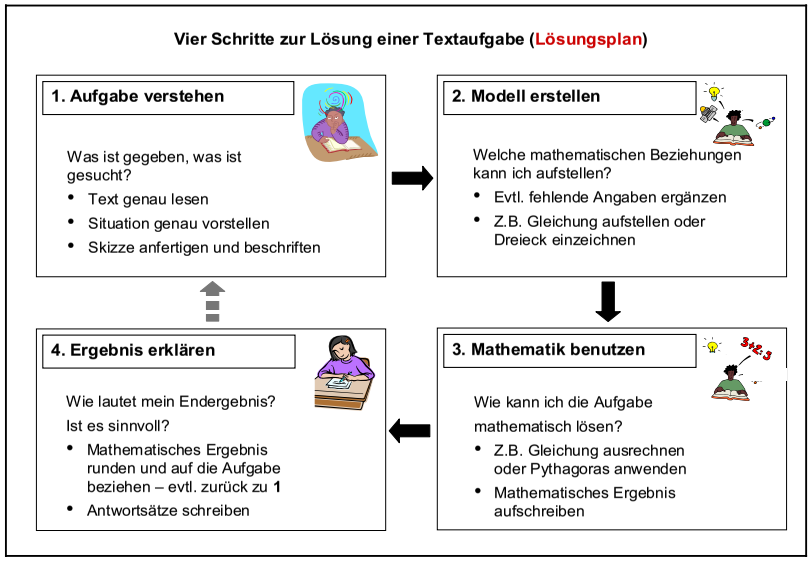

Abb. 6. „Lösungsplan“ für Modellierungsaufgaben

Unsere DISUM-Unterrichtsreihen waren noch nach weiteren Gesichtspunkten konzipiert, insbesondere nach Prinzipien der operativen Didaktik im Sinne von Aebli (vgl. dazu Aebli 1983; Messner/Reusser 2006). So waren Übungsstunden, in denen Teil-Kompetenzen des Modellierens sowie der Umgang mit dem „Lösungsplan“ gefestigt wurden, integraler Bestandteil der Reihen. Wir werden an anderer Stelle genauer über diese und weitere DISUM-Unterrichtsreihen berichten, auch über Effekte in Bezug auf Leistungen und Einstellungen der Schüler.

Global gesprochen waren die beiden durchgeführten Unterrichtsreihen (so wie auch die Studie von Maaß 2004) äußerst ermutigend: Modellieren im Mathematikunterricht ist anspruchsvoll für Schüler und Lehrer, aber Schüler sind hierbei zu hohen Leistungen fähig, wenn der Unterricht sie fordert und fördert. Das sollte unmittelbare Konsequenzen für den Unterricht wie auch für die Lehrerbildung haben.

Literatur

Aebli, H. (1983). Zwölf Grundformen des Lehrens. Eine allgemeine Didaktik auf psychologischer Grundlage. Stuttgart: Klett (12. Auflage 2002).

Baumert, J. et al. (1997). Gutachten zur Vorbereitung des Programms „Steigerung der Effizienz des mathematisch-naturwissenschaftlichen Unterrichts“. Bonn: BLK.

Baumert, J.; Lehmann, R. et al. (1997). TIMSS – Mathematisch-naturwissenschaftlicher Unterricht im internationalen Vergleich. Opladen: Leske+Budrich.

Baumert, J. et al. (Hrsg., 2001). PISA 2000. Basiskompetenzen von Schülerinnen und Schülern im internationalen Vergleich. Opladen: Leske+Budrich.

Baumert, J. et al. (2004). Mathematikunterricht aus Sicht der PISA-Schülerinnen und Schüler und ihrer Lehrkräfte. In: Prenzel, M. et al. (Hrsg., 2004). A. a. O., S. 314-354.

Bendrien, M.; Biermann, M.; Leiß, D. (2005). SINUS – Wissenschaft und Praxis treffen sich. In: Mathematikunterricht im Spannungsfeld von Evolution und Evaluation (Hrsg.: Henn, H.-W.; Kaiser, G.). Hildesheim: Franzbecker, S. 225-240.

Blum, W. et al. (2000). Gute Unterrichtspraxis – Zwei Jahre hessische Modellversuche im BLK-Programm zur Steigerung der Effizienz des mathematisch-naturwissenschaftlichen Unterrichts. Frankfurt: Hessisches Landesinstitut für Pädagogik.

Blum, W. et al. (2004). Mathematische Kompetenz. In: Prenzel, M. et al. (Hrsg., 2004). A. a. O., S. 47-92.

Blum, W. (1996). Anwendungsbezüge im Mathematikunterricht – Trends und Perspektiven. In: Kadunz, G. et al. (Hrsg.). Trends und Perspektiven. Beiträge zum 7. Internationalen Symposium zur Didaktik der Mathematik. Wien: Hölder, S. 15-38.

Blum, W.; Galbraith, P.; Henn, H.-W.; Niss, M. (Eds., 2006). Applications and Modelling in Mathematics Education. New York: Springer.

Blum, W.; Leiß, D. (2003). Diagnose- und Interventionsformen für einen selbstständigkeitsorientierten Unterricht am Beispiel Mathematik – Vorstellung des Projekts DISUM. In: Beiträge zum Mathematikunterricht 2003. Hildesheim: Franzbecker, S. 129-132.

Blum, W.; Leiß, D. (2005a). Modellieren im Unterricht mit der „Tanken”-Aufgabe. In: mathematik lehren 128, S. 18-21.

Blum, W.; Leiß, D. (2005b). Filling Up – The Problem of Independence-Preserving Teacher Interventions in Lessons with Demanding Modelling Tasks. In: CERME-4 – Proceedings of the Fourth Conference of the European Society for Research in Mathematics Education. Guixol.

Borromeo-Ferri, R. (2006). Individual Modelling Routes of Pupils – Analysis of Modelling Problems in Mathematics Lessons from a Cognitive Perspective. In: Haines, C. et al. (Eds.). ICTMA-12: Model Transitions in the Real World. Chichester: Horwood.

Büchter, A.; Leuders, T. (2005). Mathematikaufgaben selbst entwickeln. Berlin: Cornelsen Scriptor

Henn, H.-W. (1980). Die Theorie des Regenbogens als Beispiel für beziehungshaltige Analysis. In: Journal für Mathematik-Didaktik 1, S. 62-85.

Henn, H.-W. (1999). Das BLK-Projekt – Herausforderung und Chance. In: Henn, H.-W. (Hrsg.). Mathematikunterricht im Aufbruch. Hannover: Schroedel, S. 7-13.

Henn, H.-W.; Maaß, K. (Hrsg., 2003). Materialien für einen realitätsbezogenen Mathematikunterricht. ISTRON-Schriftenreihe Band 8. Hildesheim: Franzbecker.

Herget, W.; Jahnke, T.; Kroll, W. (2001). Produktive Aufgaben für den Mathematikunterricht in der Sekundarstufe I. Berlin: Cornelsen.

Herget, W.; Scholz, D. (1998): Die etwas andere Aufgabe – aus der Zeitung. Seelze: Kallmeyer.

Klieme, E. et al. (2003). Zur Entwicklung nationaler Bildungsstandards. Eine Expertise. Bonn: BMBF.

Leiß, D.; Blum, W.; Messner, R. (2006). Die Förderung selbständigen Lernens im Mathematikunterricht – Problemfelder bei ko-konstruktiven Lösungsprozessen. In: Journal für Mathematik-Didaktik 27.

Leiß, D.; Wiegand, B. (2004). A Classification of Teacher Interventions in Mathematics Teaching. In: Zentralblatt für Didaktik der Mathematik 37(3), S. 240-245.

Lietzmann, W. (1919). Methodik des mathematischen Unterrichts, I. Teil. Leipzig: Quelle&Meyer.

Maaß, K. (2004). Mathematisches Modellieren im Unterricht. Hildesheim: Franzbecker.

Messner, R. u. Reusser, K. (2006). Aeblis Didaktik auf psychologischer Grundlage im Kontext der zeitgenössischen Didaktik. In: Baer, M. et al. (Hrsg.). Didaktik auf psychologischer Grundlage. Bern: hep-Verlag.

Prenzel, M. et al. (Hrsg., 2004). PISA 2003: Der Bildungsstand der Jugendlichen in Deutschland – Ergebnisse des zweiten internationalen Vergleiches. Münster: Waxmann.

Prenzel, M.; Baptist, P. (2001). Das BLK-Modellversuchsprogramm Steigerung der Effizienz des mathematisch-naturwissenschaftlichen Unterrichts. In: BMBF (Hrsg.) TIMSS – Impulse für Schule und Unterricht. Bonn: BMBF Publik, S. 59-73.

Winter, H. (2003). Mathematikunterricht und Allgemeinbildung. In: Henn, H.-W.; Maaß, K. (Hrsg.). Materialien für einen Realitätsbezogenen Mathematikunterricht. Hildesheim: Franzbecker, S. 6-15.

Mit Mathematik unterschreiben: Ein Vorschlag für den Schulunterricht

Bruno Ebner und Martin Folkers

Zusammenfassung. Vorgeschlagen wird ein Schulprojekt für die Klassenstufen 10 oder 11 des Gymnasiums, welches im Rahmen eines fächerübergreifenden allgemeinbildenden Unterrichts mit möglichst geringen mathematischen Hilfsmitteln das Thema „digitale Unterschriften“ behandelt. Die Schulfächer Mathematik, Informatik, Geschichte und Rechtskunde werden dabei als gleichwertig betrachtet. Für die Realisierung wird das klassische RSA-Verfahren verwendet und eine mögliche Simulationen mit einem CAS (Maple) und mit einer professionelleren Simulationssoftware (CrypTool) auf dem Computer vorgestellt.

Im Rahmen von Lehrerfortbildungen und Vorlesungen für Schüler und Schülerinnen haben wir schon mehrfach das Thema „Digitale Unterschriften“ behandelt. Inhaltlich gehört dieses Thema zur Kryptologie, also der Wissenschaft der Verschlüsselung und Entschlüsselung von Informationen. Kryptologie ist sicher ein beliebtes und auch attraktives Thema für den Schulunterricht, auf das viele Schüler und Schülerinnen anspringen, hat es doch mit Geheimnissen und Verrat zu tun. Schnell werden Assoziationen geweckt zu Abenteuern, Spannung, Geheimdiensten, Kriminalfällen etc. Behandelt werden dann z. B. folgende Fragen

- Wie hat Caesar in römischer Zeit seine militärischen Anordnungen vor Angriffen des Feindes geschützt? Wie hat es Napoleon gemacht?
- Wie wird es heute im Computerzeitalter gemacht, wenn Geheimnisse sicher ausgetauscht werden sollen?

Dieser Zugang zum Thema Kryptologie ist im Rahmen des Schulunterrichts kritisch zu sehen, wenn man als Ziel einen fächerübergreifenden und allgemeinbildenden Unterricht vor Augen hat. Wie interessant ist die Frage, wie Caesar oder Napoleon militärische Geheimnisse verborgen haben? Wenn man solche Fragen im Mathematikunterricht stellt, wird die Mathematik sehr schnell aus dem Alltag herausgenommen und in die „Rätselecke“ geschoben. Andererseits ist das Thema Verschlüsselung und Datensicherheit für die Schule von enormer Bedeutung, denkt man an das Internet, welches auf Kinder und Jugendliche eine magische Anziehungskraft ausübt. Um dem Anspruch gerecht zu werden, die Grundprinzipien der Verschlüsselungstechnologie im Mathematikunterricht realitätsnah zu unterrichten, wird der Vorschlag gemacht, sich der Kryptologie nicht über die Verschlüsselung, sondern über die „digitale Unterschrift“ zu nähern. Dieser Ansatz hat den Vorteil, dass er mathematische Grundprinzipien der Arithmetik auf ideale Weise mit den Grundprinzipien des

Bürgerlichen Rechts verbindet. Das Internet ist kein rechtsfreier Raum und war es auch zu keinem Zeitpunkt. Dies wollen vor allem junge Internetnutzer oft nicht zur Kenntnis nehmen. Alle Bewegungen im Internet wie z.B. das beliebte Kopieren und Verbreiten von Spielen oder Musiktiteln kann gravierende rechtliche Folgen haben, deren sich Jugendliche wegen mangelnder Rechtskenntnisse nicht bewusst sind. Wenn der Mathematikunterricht fächerübergreifend mit einem Rechtskundeunterricht dazu beitragen kann, die Rechtskenntnisse von Jugendlichen zu verbessern, so sollte diese Chance genutzt werden.

Der Ursprung der uns heute bekannten und verbreiteten Unterschrift lässt sich fünftausend Jahre zurückverfolgen. Neben der Unterschrift wird im sprachlichen Gebrauch auch das Wort Signatur verwendet, welches aus der lateinischen Sprache stammt und das Wort Signum, das Zeichen, beinhaltet. Es geht also darum, ein Zeichen zu setzen, welches als Zeugnis der Herkunft dient. Solche Zeichen treten in verschiedenen Kulturkreisen zuerst in Form von Siegeln auf, da in früherer Zeit die Schriftform sehr wenigen Personen vorbehalten war. In China gilt der Abdruck des Siegels als die traditionelle Namensunterschrift, heute oft ergänzt durch den handschriftlichen Namenszug. Durch vermehrten Handel und damit verbundenen Handelsgesetzen wurde im Laufe der Zeit die Authentifizierung der Herkunft von Gegenständen und Dokumenten immer wichtiger. Hierzu dienten neben dem Daumenabdruck auch die berühmten drei Kreuze, welche ihre Eindeutigkeit durch die Beglaubigung eines Notars erhielten (Entstehung des Notariatswesens). Durch die zunehmende Verbreitung der Schrift im Bürgertum wurde das Siegel in Europa von der von Hand geschriebenen Unterschrift zunächst ergänzt und schließlich verdrängt. So wurde die verbindliche Unterschrift im 17. Jahrhundert ins englische Rechtssystem eingeführt. Mit dem Inkrafttreten des Bürgerlichen Gesetzbuches (BGB) im Jahr 1900 wurde das Unterschriftenwesen auch in Deutschland eindeutig gesetzlich geregelt. Durch die Etablierung im Recht legt die Unterschrift Folgendes formal fest: Herkunft, Authentizität, Exklusivität und Verbindlichkeit. Für weitere Informationen zur Geschichte der Unterschrift siehe Gehring (1998a, b). Eine lesenswerte Einführung in die Historie der Verschlüsselungstechniken findet man bei Schmeh (2004). Parallel zum Mathematikunterricht könnte man im Geschichtsunterricht die Alphabetisierung im beginnenden Industriezeitalter bis zur modernen Informationsgesellschaft thematisieren. Ein guter Einstieg sind die Internetseiten des Max-Planck-Instituts für Geschichte, Göttingen.

Mit der Einführung der digitalen Kommunikationsplattform Internet und dem so entstandenen neuen Raum für Handel und Recht wird die Notwendigkeit einer neuen Form der Signatur deutlich. Da das physikalische eigenhändige Unterschreiben nicht mehr durchführbar ist, aber trotzdem Verträge abgeschlossen und verbindliche Abmachungen getroffen werden, wurden neue Konzepte ent-

wickelt und umgesetzt. Das Konzept der digitalen Signatur als Authentifizierungsmittel überträgt die Rolle des historischen Siegels in das digitale Zeitalter.

Ziel ist es, mit möglichst einfachen mathematischen Hilfsmitteln ein digitales Äquivalent zur menschlichen Unterschrift zu konstruieren. Dieses Äquivalent soll es erlauben, ohne körperliche Anwesenheit durch geeignete Modifizierung des zu signierenden (digitalen) Dokuments eine „rechtsgültige“ Unterschrift unter dieses Dokument zu leisten. Um mit mathematische Methoden ein digitales Äquivalent für die traditionelle Unterschrift auf Papier zu konstruieren, muss man sich zunächst klar werden über einige wesentliche Funktionen, die eine handschriftliche Unterschrift hat und die eine digitale Signatur ebenfalls leisten muss Bitzer/Brisch (1999). Diese Funktionen sind

- **Echtheitsfunktion**: Gewähr, dass die Erklärung einzig vom Unterzeichner stammt.
- **Identitätsfunktion**: Die Unterschrift macht gleichzeitig die Identität des Ausstellers des Dokumentes deutlich.
- **Warnfunktion**: Im Gegensatz zur mündlichen Erklärung wird die Relevanz der Vertragsvereinbarung durch die Unterschrift herausgestellt.
- **Abschlussfunktion**: Ein Entwurf enthält im Allgemeinen keine Unterschrift. Eine Unterschrift verdeutlicht den Willen zur Vollendung.
- **Beweisfunktion**: Die Rechtsprechung geht bei unterschriebenen Dokumenten von der Vermutung der Richtigkeit und Vollständigkeit aus.

Folgende Aspekte sind für die Rolle der (digitalen) Unterschrift bei der Authentifizierung von Dokumenten wichtig.

- Die Unterschrift ist **unterzeichnerabhängig**, sie kann nur von **einer** Person erzeugt werden.
- Der Empfänger überzeugt sich durch die Unterschrift, dass der Unterzeichner das Dokument gelesen und **bewusst unterschrieben** hat. Die Unterschrift wurde also **willentlich** unter das Dokument gesetzt.
- Die Unterschrift kann **nicht gefälscht werden**.
- Die Unterschrift ist **nicht wiederverwendbar**, sie kann nicht auf ein anderes Dokument übertragen oder an ein anderes Dokument angehängt werden.
- Das unterzeichnete Dokument ist **nicht veränderbar**, nachträgliche Änderungen des Dokuments sind ohne Änderung der Unterschrift nicht möglich.
- Die Unterschrift kann später nicht geleugnet werden.

Die angegebenen Eigenschaften sind notwendige Voraussetzungen für die Anerkennung einer digitalen Signatur. Sie sind zu sehen als funktionale Parallelen

zu den Eigenschaften der eigenhändigen Unterschrift.

Die digitale Kommunikation stellt derzeit noch keine schriftliche Kommunikation dar. Nach der gesetzlichen Regelung im Bürgerlichen Gesetzbuch (BGB) gilt die Schriftform nur dann als gegeben, wenn ein Dokument eigenhändig mit dem Namenszug versehen wurde. Das Gesetz sieht für eine Anzahl von Verträgen oder Rechtshandlungen vor, dass sie schriftlich abgeschlossen werden müssen. Dies ist beispielsweise beim Bürgschaftsvertrag, beim Grundstücks oder Häuserkauf, bei der Verfassung des Testaments oder dem Ehevertrag der Fall. Dies bedeutet, dass überall dort, wo ein Schriftformzwang besteht, diese Verträge (nach deutschem Recht) im Internet nicht abgeschlossen werden können. Prinzipiell können alle Formen elektronischer Dokumente im Rahmen eines Prozesses zu Beweiszwecken eingebracht werden. Sie unterliegen damit der rechtlichen Beurteilung durch den gesetzlichen Richter (Prinzip der freien Beweiswürdigung im deutschen Recht). Es gilt dabei der Grundsatz, dass jede Partei die für sie günstigen Tatsachen darlegen und beweisen muss.

In der Bundesrepublik Deutschland wurden erstmalig 1997 mit dem Signaturgesetz (SigG) und der dazugehörigen Signaturverordnung (SigV) rechtliche Rahmenbedingungen für digitale Signaturen geschaffen. Dieser rechtliche Rahmen wurde im Jahr 2001 (aktuelle Fassung 2005) ersetzt durch die Verkündung des „Gesetzes über Rahmenbedingungen für elektronische Signaturen“ (SigG) und der „Verordnung zur elektronischen Signatur“ (SigV), welche den im Jahr 1999 beschlossenen EU-Richtlinien entsprechen. Hierin ist u. a. festgelegt, dass beim Verfahren der digitalen Signatur nur als geeignet eingestufte Kryptoalgorithmen und Hashfunktionen verwendet werden dürfen, deren Eignung vom Bundesamt für Sicherheit in der Informationstechnik (BSI) festgestellt wurde. Einzelheiten und genauere Informationen findet man auf den Internetseiten der Bundesnetzagentur: http://www.bundesnetzagentur.de. Darstellungen der rechtlichen Seite findet man in Bitzer/Brisch (1999) und Bertsch (2002).

Die meisten heute auf dem Markt befindlichen Signaturverfahren arbeiten nach dem Prinzip der asymmetrischen Verschlüsselung. Bei einem derartigen Verfahren wird jedem Teilnehmer T des Systems eine Signaturfunktion s_T und eine Verifikationsfunktion v_T zugeordnet. Dabei ist s_T geheim (geheimer Schlüssel), also nur T bekannt, wahrend v_T eine öffentlich zugängliche Funktion ist, z. B. abgelegt in einem Teilnehmerverzeichnis (öffentlicher Schlüssel). Es ist praktisch nicht möglich, aus der öffentlichen Funktion v_T auf die geheime Funktion s_T zu schließen. Ein Teilnehmer T unterschreibt eine Nachricht m, indem er seine Signaturfunktion auf die Nachricht m anwendet; er erhält daraus die elektronische Signatur

$$sig = s_T(m).$$

Er sendet sowohl m als auch sig an einen beliebigen Empfänger. Dieser ist in der Lage, aus m und sig mit Hilfe der öffentlichen Verifikationsfunktion v_T die Korrektheit der Signatur zu überprüfen. Dies ist bei vielen Verfahren so realisiert, dass gilt

$$v_T(sig) = m,$$

mit anderen Worten: bei einer Verifikation wird überprüft, ob die Anwendung von v_T auf sig die Ausgangsnachricht wieder rekonstruiert.

Zur Konstruktion von Signaturfunktionen werden so genannte Einwegfunktionen verwendet. Eine Funktion, die einfach zu berechnen ist, deren Umkehrung jedoch nur mit großem Aufwand berechnet werden kann, nennt man Einwegfunktion. Kann man die Umkehrung mit Hilfe von Zusatzinformationen einfach bestimmen, so nennt man diese Zusatzinformation Falltür und die Funktion selber eine Falltürfunktion (vgl. Beutelspacher (2001), Schmeh (2001), eine genauere mathematische Definition findet man in Bauer (1997)).

Eine Einweg-Funktion ohne Falltür ist (nach heutigem Wissen) die Multiplikation von Primzahlen. Es sei $X := \{(p, q) \in \mathbb{N}^2 \mid p, q \text{ Primzahlen}, K \leq p < q\}$, dabei sei $K \in \mathbb{R}$ hinreichend groß. Die injektive Funktion

$$f : X \to \mathbb{N}, (p, q) \to f(p, q) := p \cdot q$$

ist ein Kandidat für eine Einweg-Funktion, es sind bis heute keine Falltüren bekannt. Weiter ist bis heute kein effizientes Verfahren (öffentlich) bekannt, eine 200-stellige Dezimalzahl (oder größer) in ihre Primfaktoren zu zerlegen (von Sonderfällen abgesehen).

Erster Schritt beim Aufbau eines Signaturverfahrens

Da es unser Ziel ist, ein digitales Dokument zu signieren, können wir voraussetzen, dass unser Dokument in Form einer natürlichen Zahl $m \in \mathbb{N}$ vorliegt. Um diese natürliche Zahl m weiterzubearbeiten, tritt aber das Problem auf, dass diese Zahl in der Regel erheblich zu groß ist. Daher wird bei den heute gängigen Signaturverfahren zunächst in einem ersten Schritt von dem Dokument m eine Art Abriss (Komprimat, Quersumme oder Fingerabdruck, Hashwert) ermittelt. Für die Erzeugung eines Hashwertes eines Dokumentes werden so genannte Einweg-Hashfunktionen verwendet. Das Hashverfahren ist für alle Teilnehmer des Systems dasselbe und jedem Teilnehmer frei zugänglich, es dient nur der Komprimierung des Dokumentes, nicht aber der Verschlüsselung oder Chiffrierung. Die digitale Signatur zum Dokument m wird dann im zweiten

Schritt erzeugt, indem die Signaturfunktion s_T auf den Hashwert des Dokumentes m angewendet wird (vgl. Bauer (1997) und Schmeh (2001)).

Das heute verbreitetste Hashverfahren ist der „Secure Hash Algorithmus“ (SHA), welcher 1992 vom National Institute for Standards and Technology“ (NIST) und der „National Security Agency“ (NSA) entwickelt wurde. Die Länge eines Hashwertes bei diesem Verfahren beträgt 160 Bit. Auf Hashalgorithmen werden wir nicht eingehen, weitere Informationen findet man bei Schmeh (2001) und im Hinblick auf den Schulunterricht bei Baumann (1999b).

Zweiter Schritt beim Aufbau eines Signaturverfahrens

Die eigentliche Erzeugung einer digitalen Signatur besteht in der Verwendung einer Einwegfunktion mit Falltür, welche mit Hilfe zahlentheoretischer Hilfsmittel konstruiert wird. Jedem Teilnehmer T des Systems werden dabei zwei Zahlen $e = e_T$ und $d = d_T$ zugeordnet. Die Zahl e_T ist der geheime Schlüssel von Teilnehmer T und nur diesem bekannt. Sie entspricht der Signaturfunktion s_T von T. Die Zahl d_T ist der öffentliche Schlüssel von T und entspricht der Verifikationsfunktion v_T. Sie ist im Teilnehmerverzeichnis des Systems öffentlich zugänglich. Die zugehörige Einwegfunktion mit Falltür hat die Gestalt

$$f\colon\ e_T \to d_T \text{ für alle Teilnehmer T des Systems.}$$

Mit Hilfe eines offen gelegten Verfahrens wird dann vom Teilnehmer T aus dem Hashwert $h(m)$ eines Dokumentes m unter Verwendung seines geheimen Schlüssels e_T eine Signatur zu m erstellt. Diese Signaturdatei wird an das Dokument angehängt und zusammen mit dem Dokument m an den Empfänger geschickt. Das Verfahren besteht aus einer Signaturfunktion

$$sig:\ (h(m), e_T) \to sig_T\ (h(m)) = \text{digitale Signatur zu } m,$$

welche unter Verwendung von e_T auf $h(m)$ angewandt die Signatur von T unter das Dokument m liefert und einer Verifikationsfunktion v, für die gilt

$$v:\ (sig_T(h(m)), d_T) \to v_T(sig_T(h(m)) = h(m).$$

Prüfung (Verifikation) der Unterschrift durch den Empfänger

Nach Vorliegen der beiden Dateien m und der angehängten Signaturdatei führt der Empfänger zwei Schritte durch:

- Er bestimmt mit dem vorgegebenen Hashverfahren den Hashwert des Dokumentes m.
- Er wendet die öffentlich bekannte Verifikationsfunktion $v = v_T$ des Absenders T auf die Signaturdatei an.

Stimmen die beiden erhaltenen Werte überein, geht er von einem unverfälschten und authentischen Dokument aus.

Es gibt auf dem Markt eine Reihe von mathematischen Kryptoalgorithmen, mit denen man digitale Signaturfunktionen konstruieren kann. Wegen der Durchsichtigkeit und Einfachheit der verwendeten mathematischen Hilfsmittel bietet sich für den Schulunterricht aber nur das klassische RSA-Verfahren an, zumindest dann, wenn im Rahmen eines fächerübergreifenden Unterrichts (Mathematik, Informatik, Geschichte und Rechtskunde) die Mathematik nicht alle anderen nichtmathematischen Aspekte dominieren soll. Andere mathematisch anspruchsvollere Verfahren finden sich in Beutelspacher et al. (2005).

Das RSA-Verfahren als Signaturverfahren

Das RSA-Signaturverfahren verwendet als Einwegfunktion die Multiplikation von zwei großen verschiedenen Primzahlen.

Schlüsselerzeugung: Jeder Teilnehmer T wählt zwei verschiedene große Primzahlen $p, q \in \mathbb{N}$ (beide z. B. etwa 100 Dezimalstellen) und bildet $n = p \cdot q$. Weiter wählt jeder Teilnehmer eine Zahl $e \in \mathbb{N}$ (z. B. 9 Dezimalstellen) mit

$$\text{ggT}(e, (p-1)\cdot(q-1)) = 1.$$

Der öffentliche Schlüssel des (von T) bestimmt sich aus der linearen Kongruenz

$$e \cdot d \equiv 1 (\text{mod}\ (p-1)\cdot(q-1)).$$

Öffentlicher Schlüssel: $(d, n), d = d_T, n = n_T, 2 \le d < (p-1)\cdot(q-1)$

Der öffentliche Schlüssel (von T) wird abgelegt in einem öffentlichen Teilnehmerverzeichnis.

Privater Schlüssel: $(e, n),\ e = e_T, n = n_T, 2 \le d < (p-1)\cdot(q-1)$

Der private Schlüssel (e, n) (genauer der Schlüsselteil $e = e_T$) sowie die zur Erzeugung benötigten Primzahlen p und q müssen geheim bleiben, dürfen also nur T bekannt sein und sollten (dürfen) **nicht auf der Festplatte gespeichert** sein. Das Signaturgesetz schreibt vor, dass der geheime Schlüssel auf einer Chipkarte eingebrannt und versiegelt wird. Von dieser kann er nicht ausgelesen werden. Die Chipkarte kann nur benutzt werden, wenn zusätzlich eine PIN-

Nummer die Nutzung frei schaltet. Da der geheime Schlüssel von der Chipkarte nicht ausgelesen werden kann, findet der Verschlüsselungsvorgang vollständig im Inneren der Chipkarte statt. Hierzu enthält die Chipkarte einen speziellen Prozessor, welcher für diese Aufgabe optimiert ist.

Erzeugung einer Signatur unter das Dokument m ($m \in \mathbb{N}$)

Der Absender T zerlegt die Nachricht m (diese sei o. B. d. A. in Form einer Zahl gegeben) in r (gleichlange) Blöcke $m_1, m_2, ..., m_r$ jeder Block $m_j < n$ (gegebenenfalls muss der letzte Block mit Nullen aufgefüllt werden), und sendet

- die Nachricht m und
- die angehängte Signaturdatei $m_1^e \pmod n, m_2^e \pmod n, \ldots, m_r^e \pmod n$

Unterschriftenprüfung durch den Empfänger

Der Empfänger schaut den öffentlichen Schlüssel $d_T = (d, n)$ des (vermeintlichen) Absenders im Teilnehmerverzeichnis nach und bildet

$$\begin{array}{ccccc} (m_1^e)^d \pmod n & & (m_2^e)^d \pmod n & \ldots & (m_r^e)^d \pmod n \\ \equiv & & \equiv & & \equiv \\ (m_1) \pmod n & & (m_2) \pmod n & \ldots & (m_r) \pmod n \end{array}$$

Danach fügt er die erhaltenen Blöcke $m_1^{e \cdot d} \pmod n, m_2^{e \cdot d} \pmod n, \ldots, m_2^{e \cdot d} \pmod n$ wieder zusammen. Stimmt die dann resultierende Zahl mit der Nachricht m überein, so erkennt er die Unterschrift als echt an. Bei dieser und der folgenden Maple-Realisierung einer digitalen Signatur wird aus Gründen der Übersichtlichkeit auf die Zwischenschaltung eines Hashverfahrens verzichtet.

Welche mathematischen Hilfsmittel werden benötigt?

- *erweiterter euklidischer Algorithmus (für die Erzeugung des Schlüsselpaares)*
- *elementares Rechnen mit linearen Kongruenzen*
- *kleiner Satz von Fermat (zweimal angewendet reicht aus!)*

Mit diesen Hilfsmitteln lässt sich das RSA-Verfahren beweisvollständig (Korrektheitsbeweis) behandeln. Für die Details siehe Bartholome et al. (2006), Padberg (1999) und Trappe/Washington (2002). Bei der Diskussion des RSA-Verfahrens tauchen natürlich zwei Fragen auf, die nicht verschwiegen werden dürfen.

- Die Frage nach der **Durchführbarkeit**, also die Frage, ob man schnell und problemlos große Primzahlen finden kann. Es gibt eine Reihe von effizienten Primzahltests, welche auch in Maple realisiert sind, mit denen man hinreichend große Primzahlen erzeugen kann bzw. mit denen man auch für sehr große Zahlen erkennen kann, ob es sich um eine Primzahl handelt.
- Die Frage nach der **Sicherheit**, also die Frage, ob das Problem der Primzahlzerlegung für große Zahlen möglicherweise effizient bewerkstelligt werden kann.

Für beide Fragen muss auf die sehr reichhaltige Literatur verwiesen werden, z.B. Bartholome et al. (2006), Trappe/Washington (2002) oder das Online-Skript CrypTool (2003). Auch wenn man diese Fragen im Schulunterricht nicht wirklich detailliert behandeln kann, so kann man doch mit Hilfe von Maple den Unterschied zwischen Primzahlerkennung und Primzahlzerlegung für Schüler und Schülerinnen erfahrbar machen und diskutieren.

Maple-Realisierung

In diesem Abschnitt wird eine mögliche Realisierung im CAS-System Maple vorgestellt. Zur Durchführung des Verfahrens werden einige Variablen und Prozeduren gebraucht, die im Folgenden angegeben werden. Als erstes wird der zu signierende Text (brief.txt) eingelesen. Gleichzeitig werden die nötigen Primzahlen und Schlüssel erzeugt bzw. berechnet.

```
read("C:/Brief.txt");
p := nextprime(41014208971);   #erste Primzahl
q := nextprime(21025160973);   #zweite Primzahl
e := 1003;                     #e geheimer Schlüssel
igcdex(e, (p-1)*(q-1), d, y);  #berechnet öffentl. Schlüssel d
e*d mod((p-1)*(q-1));          #als Probe muss 1 rauskommen
b := 4;                        #b gibt die Blocklänge an
```

Dann wird das Alphabet (98 Zeichen), mit dem gearbeitet wird, definiert. Es handelt sich um eine Variable des Typs „string“.

```
Alphabet := 'aäbcdefghijklmnoöpqrstuüvwxyzAÄBCDEFGHIJKLMNO
ÖPQRSTUÜVWXYZ1234567890-=~!@%^&*()_+,./<'>?;:"[]{}| ';
```

Als nächstes muss der Text in eine Zahl (Dezimalzahl) umgewandelt werden. Die Prozedur benötigt die zuvor definierte Variable Alphabet.

```
Text_Zahl := proc(st)
    local l, n, s, i;
    global Alphabet;
    l := length(st);
    if l = 0 then RETURN(0) end if;
    n := 1;
    for i to l do
        s := SearchText(substring(st, i .. i), Alphabet);
        if not type(s, numeric) or s = 0 then
            ERROR('Das Zeichen '.(substring(st, i .. i)).'
            gehört nicht zum Alphabet')
        end if;
        n := 100*n+s
    end do;
    n-10^(2*l)
end:
```

In der for-Schleife wird bei jedem Durchlauf die *i*-te Stelle des Textes in der Variable Alphabet gesucht und die Position als numerischer Wert ausgegeben. Dieser liegt bei der oben definierten Wahl des Alphabets zwischen 0 und 98. Da zweistellige Zahlen als Werte in der Schleife auftauchen, werden durch die Zeile `n := 100*n+s` an die entstehende Zahl `n` in jedem Durchlauf zwei Nullen angehängt. welche dann durch `s` ersetzt werden. Zuletzt wird die erste 1 noch gelöscht, da sie nicht zum ursprünglichen Text gehört. Mit dem Befehl

```
Zahl := Text_Zahl(Brief);
```


wird der eingelesene Brief in eine Zahl umgewandelt. Um das im vorherigen Abschnitt besprochene RSA-Verfahren zu verwenden, muss die entstandene Zahl in Blöcke aufgeteilt werden. Dies realisiert die folgende Prozedur.

```
Zahl_Blockliste := proc(z, b)
    local B, i, K, l, lZ, p, Z;
    Z := z;
    B := b;
    lZ := length(Z);
    l := ceil(1/B*lZ);
    K := [ ];
    for i to l do
        Z := 1/(10^B)*Z;
        p := 10^B*frac(Z);
        K := [p, op(K)];
        Z := trunc(Z)
    end do;
    K
end:
```

Mit `l := ceil(1/B*lZ)` wird die Anzahl der entstehenden Blöcke berechnet und `K:=[]` erzeugt eine leere Blockliste. In der for-Schleife wird bei jedem Durchlauf die Zahl um die Blocklänge hinter den Dezimalpunkt geschoben, dann werden die entstehenden Nachkommaziffern in die Blockliste geschrieben und die Zahl auf die nächste ganze Zahl abgerundet. Der Maple-Befehl op gibt die Elemente aus einer Liste aus. Mit

```
BL := Zahl_Blockliste(Zahl, b);        #BL bez. die Blockliste
```

wird aus der Zahl eine Blockliste der Länge *b* berechnet. Die Signaturdatei und die Überprüfung der Signatur werden durch die folgende Prozedur erzeugt. Der Befehl `nops` gibt die Anzahl der Elemente aus einer Liste aus. Die eigentliche Ver- bzw. Entschlüsselung wird in der Schleife realisiert.

```
RSA := proc(BL, M, s)
    local L, Ls, ss, i;
    L := BL;
    ss := s;
    Ls := [ ];
    for i to nops(L) do
        Ls := [op(Ls), (L[i] &^s) mod M]
        end do;
        Ls
end:
```

Der Aufruf für die Erzeugung bei Verwendung des Schlüssels *e* lautet jetzt:

```
SIG := RSA(BL, p*q, e);
```

Um aus einer Blockliste wieder eine zusammenhängende Zahl und aus der Zahl wieder einen Text zu generieren, werden die beiden folgenden Prozeduren verwendet.

```
Blockliste_Zahl := proc(BL, b)
    local B, i, n, L, Z;
    L := BL;
    B := b;
    Z := 0;
    n := nops(L);
    for i to n do
        Z := Z + L[i]*10^(B*(n -i))
    end do;
    Z
end:
```

Die Berechnung der Zahl aus der Blockliste vollzieht sich in der for-Schleife. Jedes Element *i* aus der Blockliste wird mit $10^{(b\cdot(n-i))}$ multipliziert und dann aufaddiert. Dabei bezeichnet *b* die Blocklänge und *n* die Gesamtanzahl der Blöcke.

```
Zahl_Text := proc(n)
    local s, m, l, p, i, ans;
    global Alphabet;
    m := n;
    l := floor(1/2*trunc(evalf(log10(m))))+1;
    ans := "";
    for i to l do
        m := iquo(m,100,'p');
        if length(Alphabet) < p then
          ERROR('Der Zahl entspricht kein vernünftiger Text')
        end if;
        s := substring(Alphabet,p .. p);
        ans := cat(s,ans)
    end do;
    ans
end:
```

In der letzten Prozedur berechnet l die Anzahl der entstehenden Buchstaben, der Befehl substring sucht die entsprechenden Buchstaben in der Variable Alphabet, und mit cat wird der Text zusammengefügt. Mit den eingeführten Prozeduren lässt sich das Ergebnis unter Verwendung des öffentlichen Schlüssels *d* verifizieren:

```
SIGPR := RSA(SIG, p*q, d);
Zahl2 := Blockliste_Zahl(SIGPR, b);
Zahl_Text(Zahl2);
```

Bei korrekter Signatur erscheint in der Maple Ausgabe der ursprüngliche Brief. Weiterführende Maple- und Matlab-Realisierungen findet man in Trappe/Washington (2002).

Unter der zugehörigen Webadresse http://www.prenhall.com/washington kann man Maple und Matlab-Worksheets downloaden.

Die oben beschriebene Realisierung mit Hilfe von Mapleprozeduren, befreit vom Einsatz von Hashfunktionen, sollte nur eine Zwischenlösung sein, um die Wirkungsweise einer digitalen Signatur zu klären. Es bleibt der Wunsch, eine realistischere Demonstration zur Verfügung zu haben. Hierzu bietet sich die Verwendung der CrypTool-Software an, welche kostenlos (Freeware) im Internet unter der Netzadresse http://www.cryptool.de erhältlich ist.

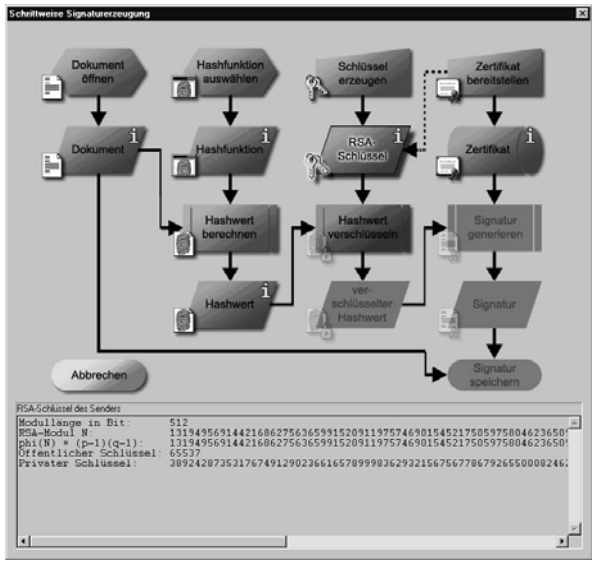

Abb. 1. Screenshot zur schrittweisen Signaturerzeugung in CrypTool

Der obige Screenshot zeigt die Simulation des Ablaufplanes für die professionelle Erzeugung und Verifizierung einer digitalen Signatur. CrypTool wurde nach eigenen Angaben gemeinsam von Wirtschaft und Hochschulen als adäquates didaktisches Medium für eine moderne Lehre entwickelt. Mit dieser Software steht eine interaktive Plattform bereit, um die Wirkungsweise einer digitalen Signatur zu demonstrieren.

Schlussbemerkung

Das hier vorgestellte Unterrichtsthema ist so angelegt, dass es als Projekt (z. B. als AG) im Rahmen des gymnasialen Unterrichts durchgeführt werden kann. Wert gelegt werden sollte dabei auf eine saubere Darstellung der arithmetischen Grundsätze. Es hat aber wenig Sinn, dieses Thema unter Negierung gesellschaftlicher Verhältnisse und ohne Verankerung in unserer Rechtsordnung zu unterrichten. Es soll nicht verschwiegen werden, dass viele Fragen nicht angesprochen werden, wie z. B. die Frage nach technischen Realisierungen, die Frage nach notwendigen administrativen Einrichtungen und die Frage nach der (augenblicklichen) Akzeptanz der elektronischen „Unterschrift“ in der Bevölkerung. Hier muss auf weiterführende Literatur verwiesen werden.

Wenn man mit unseren obigen Maple-Prozeduren unter Verwendung der Primzahlen p=419 und q=211 sowie dem geheimen Schlüssel e=1003 und der Blocklänge b=3 unter einen eingelesenen Brief die folgende digitale Signatur

erzeugt

SIG :=

[71672, 22648, 4304, 32075, 86962, 16509, 20637, 63235, 46002, 68353, 15055, 58421, 33937, 36675, 63817, 34051, 6608, 36492, 36403, 34287, 46002, 29891, 82340, 32075, 83175, 73974, 47794, 20826, 64747, 11805, 6608, 20826, 66432, 14624, 54886, 68353, 47794, 83790, 45181, 12243, 28181, 61645, 33210, 8718, 76749, 64163, 64163, 59535, 28181, 11805, 13560, 17438, 72461, 34287, 86598, 55327, 63462, 54345, 45181, 33894, 58046, 30489, 1563, 70316, 76993, 56615, 82475, 22391, 73043, 20864, 55134, 32075, 11892, 34209, 61024, 36492, 35782, 86511, 13560, 51470, 73566, 34051, 15055, 19216, 15055, 15485, 76522, 76749, 20637, 78143, 6076, 32683, 61501, 20826, 80794, 85754],

und diese Signatur mit dem zugehörigen öffentlichen Schlüssel d=72727 verifiziert, lautet die Antwort von Maple:

Wir, die Autoren, und das Institut für Stochastik der Universität Karlsruhe wünschen Dir, lieber Wolfgang, alles Gute zu Deinem 60. Geburtstag.

Literatur

Bauer, F. L. (1997). Entzifferte Geheimnisse (2nd ed.). Berlin: Springer-Verlag.

Bartholome, A. et al. (2006). Zahlentheorie für Einsteiger (5th ed.). Vieweg-Verlag.

Baumann, R. (1999a). Digitale Unterschrift. In: *LOG IN* 19, S. 46-49.

Baumann, R. (1999b). Digitale Unterschrift. In: *LOG IN* 19, S. 82-88.

Bertsch, A. (2002). Digitale Signaturen. Berlin: Springer-Verlag.

Beutelspacher, A. et al. (2001). Moderne Verfahren der Kryptographie (4th ed.). Braunschweig/Wiesbaden: Vieweg-Verlag.

Beutelspacher, A. et al. (2005). Kryptografie in Theorie und Praxis. Braunschweig/Wiesbaden: Vieweg-Verlag.

Bitzer, F., Brisch, K. M. (1999). Digitale Signatur. Berlin: Springer-Verlag.

CrypTool (2003). CrypTool-Skript. http://www.cryptool.de/downloads/CrypToolScript 1 3 04 de.pdf.

Gehring, R. (1998a). Digitale Signaturen. Diplomarbeit. Technische Universität Berlin. http://ig.cs.tu-berlin.de/ma/rg/ap/1998-04/Gehring-DigitaleSignaturen-1998-04-08.pdf.

Gehring, R. (1998b). Digitale Signaturen (I). In: Linux-Magazin 8/98.

Gehring, R. (1998c). Digitale Signaturen (II). In: Linux-Magazin 10/98.

Gehring, R. (1999). Digitale Signaturen (III). In: Linux-Magazin 3/99.

Padberg, F. (1999). Zahlentheorie und Arithmetik. Spektrum Akademischer Verlag.

Schmeh, K. (2004). Die Welt der geheimen Zeichen. w3L-Verlag Dortmund.

Schmeh, K. (2001). Kryptografie und Public-Key-Infrastrukturen im Internet (2nd ed.). Heidelberg: dpunkt.verlag.

Trappe, W.; Washington, L. C. (2005). Introduction to Cryptography with Coding Theory (2nd ed.). Prentice-Hall Upper Saddle River.

Eytelwein, Seile und Poller – Oder: Warum kann ich ein großes Schiff mit einer Hand festhalten?

Frank Förster

Zusammenfassung: Ausgehend vom alltäglichen Phänomen der Seilreibung skizziert dieser Artikel einen Weg für einen modellierenden, fächerübergreifenden und experimentellen Mathematikunterricht. Die experimentell nachgewiesene Exponentialfunktion kann dabei in der Sekundarstufe I qualitativ und in der Sekundarstufe II auch quantitativ modelliert werden.

Alltägliche Phänomene für den Mathematikunterricht nutzbar zu machen, ist Anliegen vieler Artikel von Hans-Wolfgang Henn (vgl. z. B. Henn 1993, 1995, 1997, 2002, Büchter/Henn 2004). „Besonders wichtig und interessant“ sind dabei, nach Henn (1994, S. 67), „Messungen zu exponentiellem Verhalten.“ Die experimentell nachgewiesene Exponentialfunktion kann dabei in der Sekundarstufe I qualitativ und in der Sekundarstufe II auch quantitativ modelliert werden.

Neulich im Projekt …

… , als sich an diesem Nachmittag mathematisch interessierte Grundschülerinnen und -schüler in der mathematischen Lernwerkstatt der TU Braunschweig trafen, behauptete ich, Lena und Laura seien stärker als acht Jungs – zumindest würden diese es nicht schaffen, die Mädchen im Tauziehen zu besiegen. Na, da war was los … Also runter und ausprobieren. Natürlich war es für die Jungs kein Problem, die beiden Mädchen „über den Hof zu ziehen“ – selbst meine Hilfe nützte da zunächst nichts. Aber dann nahm ich das Seil und schlang es zweimal um einen Laternenpfahl (Abb. 1).

Abb. 1. Ein merkwürdiges Tauziehen