Melanie PLATZ, Landau, Engelbert NIEHAUS, Landau

Kooperatives Problemlösen von SchülerInnen mit besonderen mathematischen Begabungen und Lehramtsstudierenden

Ziel dieser Voruntersuchung ist es, Unterschiede im Bereich des Problemlösens von Schülerinnen und Schülern (SuS) mit besonderen mathematischen Begabungen im Vergleich zu Lehramtsstudierenden aufzuzeigen. Die Universität Koblenz-Landau, Campus Landau, bietet SuS mit besonderen mathematischen Begabungen die Gelegenheit eines betreuten Frühstudiums in konventionellen universitären Lehrveranstaltungen. Zielgruppen sind dabei SuS der Gymnasialen Oberstufe, sowie der Sekundarstufe I, die gemeinsam mit Lehramtsstudierenden an mathematischen Problemen arbeiten. Im Wintersemester 2009/2010 besuchten die SuS mit besonderer mathematischer Begabung die Vorlesung Kryptologie. Im Rahmen dieser Lehrveranstaltung wurden Frühstudierende und Studenten verglichen, besonders in Bezug auf Problemlösestrategien. Beschreibung des Vorgehens bei der Bearbeitung von Übungen zur Vorlesung durch die SuS bzw. StudentInnen, sowie die schriftlichen Lösungswege dieser wurden dazu gegenübergestellt. In diesem Zusammenhang sollen erste Hypothesen aufgestellt werden, welche mathematischen Vorkenntnisse für den erfolgreichen Abschluss der Veranstaltung notwendig sind, zum anderen wird beabsichtigt erste Folgerungen für die weitere Konzeption der Lehrveranstaltung Kryptologie zu ziehen.

1. Vorlesung zur Kryptologie im Wintersemester 2009/2010

In diesem Semester nahmen sechs Schüler und drei Schülerinnen mit besonderer mathematischer Begabung und drei Studenten und drei Studentinnen an der Vorlesung zur Kryptologie teil. Die Kryptologie gliedert sich in Kryptographie und Kryptoanalyse. Die Kryptographie ist die Wissenschaft, die sich damit befasst, Methoden zur Verheimlichung von Nachrichten zu entwickeln. Die Kryptoanalyse hingegen versucht chiffrierte Botschaften ohne bekannten Schlüssel zu dechiffrieren. In dieser Veranstaltung wurden zunächst symmetrische Algorithmen behandelt. Sender und Empfänger haben dabei den gleichen Schlüssel. Es wurden sowohl Transpositionschiffren (z.B. Gartenzaunchiffre) als auch Substitutionsalgorithmen (z.B. Cäsar-Verschlüsselung) besprochen. Diese Verschlüsselungsalgorithmen sind allerdings problemlos durch eine Häufigkeitsanalyse mit Hilfe des jeweiligen Sprachprofils durch einen Angreifer zu entschlüsseln. Um dem entgegenzuwirken, wurden Polyalphabetische Verschlüsselungsverfahren entwickelt, die ebenfalls in der Veranstaltung besprochen wurden (z.B. Verschlüsselung mit Zufallsexperimenten, Homophone Chiffrierung). Auch

die Verschlüsselung beliebiger digitaler Daten wurde thematisiert. Darüber hinaus wurden noch asymmetrische Algorithmen untersucht. Dabei haben Sender und Empfänger unterschiedliche Schlüssel. Besonderes Interesse galt dabei dem RSA-Algorithmus, ein Public-Key-Verfahren, das auf dem Problem aufbaut, dass die Faktorisierung einer großen Zahl sehr aufwändig ist.

2. Übungsaufgaben, Beiträge zur Vorlesung und Prüfung

Begleitend zur Vorlesung wurden den SuS und StudentInnen Übungsaufgaben zur Verfügung gestellt. Obwohl die Bearbeitung dieser freiwillig war, wurden sie von fast allen TeilnehmerInnen regelmäßig gelöst. Die Bearbeitungszeit betrug, außer beim ersten Übungsblatt, eine Woche. Die Aufgaben wurden meist in Einzel- oder Partnerarbeit gelöst, obwohl auch eine Bearbeitung in Gruppen erlaubt war. Studierende und SuS kooperierten nur selten bei der Erledigung der Aufgaben. Das erste Übungsblatt wurde innerhalb der Vorlesung bearbeitet, d.h. die TeilnehmerInnen hatten 90 Minuten Zeit, um eine Kryptoanalyse an einem chiffrierten Text durchzuführen. Der Verschlüsselung lag dabei kein Algorithmus zugrunde, jeder Buchstabe des deutschen Alphabets wurde zufällig einem anderen zugeordnet und beim Verschlüsseln durch diesen ersetzt. Zur Lösung dieser Aufgabe wurde den TeilnehmerInnen das Sprachprofil der deutschen Sprache an die Hand gegeben. Nur zwei Schülern gelang es, die Aufgabe innerhalb der Vorlesung zu lösen. Die restlichen SuS baten darum, diese noch nicht aufzulösen, um weiter daran arbeiten zu können. In der folgenden Veranstaltung hatten fast alle SuS die korrekte Lösung erarbeitet. Aus dem zweiten Übungsblatt werden im Folgenden drei Aufgaben herausgegriffen. Die erste Aufgabe, zur Vererbung der Bijektivität einer Abbildung, war Gegenstand der Lehrveranstaltung, da die umkehrbar eindeutige Verschlüsselung eindeutige Dechiffrierbarkeit für den Empfänger garantiert. Diese Aufgabe hat nur eine Schülerin gelöst, obwohl sie den StudentInnen bekannt war. Dabei war auffällig, dass die Formelsprache der Schülerin sogar fast korrekt war, denn auch diese ist für die SuS neu. Des Weiteren wurde eine Aufgabe zu Beweistechniken gestellt, bei der durch Wahrheitstafeln die Äquivalenz von drei Aussagen verifiziert werden sollte. Diese war ebenfalls neu für die SuS und bekannt für die StudentInnen. Dennoch wurde sie von einigen StudentInnen unvollständig oder falsch gelöst. Eine Schülerin hingegen, löste sie vorbildlich und erfand, über die Fragestellung hinaus, noch ein Beispiel dazu. Außerdem wurde eine Aufgabe bearbeitet, die von p-adischen Stellenwertsystemen handelte. Dabei sollten Zahlen sowohl aus dem Dezimalsystem in andere Stellenwertsysteme (z.B. Dual-, Oktal-, Hexadezimalsystem), als auch umgekehrt umgerechnet werden. Diese Aufga-

be war für alle TeilnehmerInnen der Veranstaltung neu. Auffällig war, dass alle SuS sehr motiviert gegenüber dieser Aufgabe eingestellt waren und sie korrekt lösten. Nur ein Teil der StudentInnen hat selbige überhaupt versucht zu bearbeiten. Innerhalb der Vorlesung wurde die Verschlüsselung digitaler Daten behandelt, u.A. von Bildern, d.h. digitalen Fotografien. Um ein Foto zu chiffrieren war die Idee der SuS, ein zweites Foto über das zu verschlüsselnde zu legen. Diese Idee stellt sich als unvorteilhaft heraus, da beide Fotos erkennbar bleiben. Dennoch haben die SuS ein Verfahren selbst entdeckt, mit dem Bilder überlagert werden können bzw. in Videos Überblendungen realisiert werden können. Die Wertschätzung solcher Vorschläge bietet zahlreiche Möglichkeiten Mathematik und Informatik zu verbinden. Aus dem letzten Übungsblatt wird eine Aufgabe zur Kryptoanalyse des RSA-Algorithmus herausgegriffen. Bekannt waren die verschlüsselte Botschaft und der öffentliche Schlüssel. Diese Aufgabe war sowohl für die SuS als auch für die StudentInnen eine Transferaufgabe. Zur Lösung musste u.A. in der Modulorechnung effizient hohe Potenzrechnung beherrscht werden. Korrekt gelöst wurde diese Aufgabe wieder nur durch eine Schülerin. Am Ende der Veranstaltung fand eine 20-minütige mündliche Prüfung statt. Daran nahmen vier Schüler und eine Schülerin, sowie ein Student und eine Studentin teil. Bestanden haben alle SuS und ein Student. Den Studierenden aus den Altstudiengängen fehlte noch ein fachwissenschaftlicher Leistungsnachweis, den sie bisher in anderen konventionellen Lehrveranstaltungen noch nicht erwerben konnten. Dies relativiert das Bild für das Abschneiden der Lehramtsstudierenden. Die SuS erreichten in dieser Prüfung mittelmäßige Noten, da sie sich innerhalb der Lehrveranstaltung die Formelsprache und auch Beweistechniken erst aneignen mussten.

4. Fazit

In diesem Semester wurden zum ersten Mal SuS aus der 8. Jahrgangsstufe für ein Frühstudium zugelassen, um Grenzen der Förderung zu untersuchen und erste Erfahrungen in einer Lehrveranstaltung Kryptologie zu sammeln. Es hat sich gezeigt, dass auch diese SuS eine universitäre Lehrveranstaltung bestehen können und die Vorkenntnisse zum Ver- und Bestehen in der Kryptologie ausreichen können. Allerdings sollte der ikonischen Veranschaulichung von Beweisideen aus der Algebra und Zahlentheorie ein besonderer Stellenwert eingeräumt werden, an dem sich die formale Struktur der Beweise orientiert. Ein erfolgreicher Abschluss der SuS aus der Klassenstufe 8 erlaubt allerdings keine Rückschlüsse auf den erfolgreichen Abschluss in anderen Lehrveranstaltungen (z.B. Lineare Algebra, Analysis). Unterschiede zwischen den SuS und StudentInnen in Bezug auf Problemlösestrategien waren im Hinblick auf Motivation, Ehrgeiz und Kreativität

festzustellen. Die SuS arbeiteten während der Vorlesung, im Vergleich zu den StudentInnen, sehr gut mit und trugen mit kreativen Beiträgen zur Veranstaltung bei. Ursache dafür könnte sein, dass die SuS die Mitarbeit von der Schule gewöhnt sind und in der Vorlesung keine Angst davor haben, fehlerhafte Beiträge zu liefern. Besonders Transferaufgaben standen die SuS ehrgeiziger und motivierter als die StudentInnen gegenüber. Die Übungsaufgaben wurden von den SuS vollständiger bearbeitet als von den StudentInnen, d.h. jede einzelne Frage wurde explizit beantwortet oder es wurden sogar noch selbst erfundene Aufgaben zu diesem Thema bearbeitet. Die StudentInnen setzten stellenweise bei ihren Lösungsvorschlägen einiges als „offensichtlich" oder „bekannt" voraus, beantworteten dadurch aber die Fragestellungen nicht vollständig. Die Veranschaulichung algebraischer und zahlentheoretischer Zusammenhänge, die für die SuS konstruktive Beiträge zur Lehrveranstaltung ermöglichte, waren für StudentInnen keine Hilfe, um ein Bestehen der Lehrveranstaltung zu erreichen. Für die weitere Konzeption der Lehrveranstaltung Kryptologie kann nun gefolgert werden, dass eine verstärkte Kooperation zwischen SuS und Lehramtstudierenden nur dann erreicht werden kann, wenn die Studierenden als Mindestvoraussetzung ein gutes fachliches Verständnis der Inhalte besitzen und die gleiche Motivation bei der Bearbeitung der Aufgaben vorliegt, wie bei den SuS. Spezielle betreute Übungsphasen, in denen Tandems aus SuS und StudentInnen gemeinsam die Übungsaufgaben lösen, muss Ausgangspunkt der Lehr-Lernumgebung sein, die Hilfen für SuS und didaktisch-analytische Lernumgebungen für die Lehramtsstudierenden bietet. Mit einer didaktischen Zielsetzung innerhalb einer fachlichen Lehrveranstaltung könnten die Studierenden erste Erfahrungen zu Problemlösekompetenzen von SuS mit besonderer mathematischer Begabungen sammeln und Konsequenzen für die Differenzierung des eigenen Unterrichts ableiten. Eine solche Analyse des Lernprozesses der SuS sollte schriftlich in Form eines Protokolls festgehalten werden. Außerdem wäre es möglich, die Veranstaltung, die momentan als Vorlesung gehalten wird, in Form eines Seminars stattfinden zu lassen. Die TeilnehmerInnen der Veranstaltung könnten in Gruppen eingeteilt werden, die Probleme aus dem Themengebiet der Kryptologie bearbeiten und ihre Ergebnisse am Ende der Veranstaltung präsentieren.

Literatur

Beutelspacher, A. (2005). *Kryptologie.* Wiesbaden: Friedr. Vieweg & Sohn Verlag/GWV Fachverlage GmbH.

Tücke, M. (2005): *Schulische Intelligenz und Hochbegabung für (zukünftige) Lehrer und Eltern.* Münster: LIT Verlag (Osnabrücker Schriften zur Psychologie; Bd. 9).

Vock, M.; Preckel, F.; Holling, H. (2007): *Förderung Hochbegabter in der Schule.* Göttingen: Hogrefe-Verlag.