Hannes STOPPEL, Münster & Benjamin ROTT, Köln

Codierung mit elliptischen Kurven

1. Einleitung

Funktionen sind ein zentraler Bestandteil der (Schul-)Mathematik, mit denen man Zusammenhänge und Abhängigkeiten von Größen darstellen kann. Eine Ergänzung bzw. Verallgemeinerung stellen Kurven dar. Auch sie können mit Schulmitteln erfasst und verstanden werden. Hierdurch zeigt sich zugleich eine Verbindung zwischen geometrischen Objekten der Mathematik und der Praxis der Verschlüsselungstheorie. Reduziert man die Inhalte der Verfahren an bestimmten Stellen, so lässt sich dieses Thema in der Sek. II anwenden. Auch wenn ein paar fachwissenschaftliche Abstriche gemacht werden müssen, können die wesentlichen Strukturen doch erarbeitet werden.

Auf Basis der Unterrichtserfahrung des Erstautoren werden im Folgenden mögliche Anwendungen der Kryptographie mithilfe elliptischer Kurven in der Schule geschildert (weitere Beispiele in Stoppel & Rott, 2018a, b). Mathematische Hintergründe finden sich in Stoppel & Griese (2017, Kap. 1).

2. Elliptische Kurven

Hinter den in der Kryptographie verwendeten Kurven verbergen sich Mengen von Punkten $(x|y) \in \mathbb{R}^2$ mit $\sum_{i,j}^{n} a_{ij} \cdot x^i \cdot y^j = 0$ mit $a_{ij} \in \mathbb{R}$. Sie bilden eine Klasse ebener algebraischer Kurven, die seit langer Zeit in der Mathematik erforscht werden. Beispielsweise befasste sich bereits Newton mit Kurven (Fischer, 1994). Im 19. Jahrhundert wurden *elliptische Kurven* in Verbindung mit elliptischen Integralen untersucht (Lang, 1987). Sie fanden Anwendung im Beweis von „Fermats letztem Satz“ durch A. Wiles (1995) und sie finden seit etwa 1985 Anwendung in der Kryptographie.

3. Anwendung elliptische Kurven in der Kryptographie

Elliptische Kurven sind eine Teilmenge von Kurven mit der *Weierstraß-Gleichung* $y^2 = x^3 + a \cdot x + b$ mit $a, b \in \mathbb{R}$. Die Menge dieser Kurven ist dabei so eingeschränkt, dass keine Schnittpunkte – sog. Singularitäten – von Wegen entlang einer Kurve existieren. Dies ist bei einer solchen Kurve genau dann der Fall, wenn $4\,a^3 + 27\,b^2 \neq 0$ gilt. Kurven, die der Weierstraß-Gleichung gehorchen und keine Singularitäten besitzen, heißen *elliptische Kurven*. Abb. 1 zeigt einen Graphen einer solchen Kurve.

Die Codierung soll mithilfe elliptischen Kurven und Geraden durchgeführt werden. Dies heißt nichts anderes als eine „Addition“ zu definieren. Die

Menge der Schnittpunkte von Geraden und der Kurve bilden eine *Gruppe*, somit existieren inverse Elemente zur Decodierung.

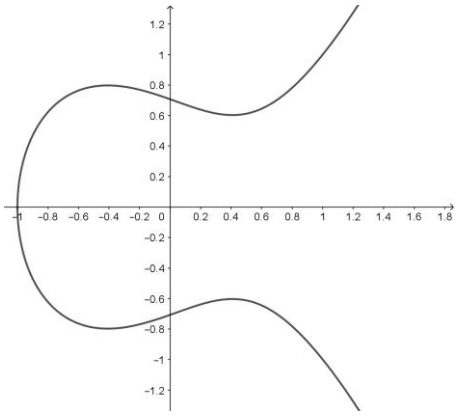

Abb. 1: Die elliptische Kurve der Weierstraß-Gleichung mit $a = -0{,}5$ und $b = 0{,}5$

Die Schritte in der Addition sind damit gegeben durch:

1. Lege eine Gerade durch zwei Punkte P, Q der Kurve (Abb. 2, links)
2. Markiere den dritten Schnittpunkt S der Gerade mit der Kurve (Abb. 2, Mitte)
3. Spiegele diesen Punkt S an der x-Achse; dieser Punkt wird Summe der Punkte P und S genannt, notiert als $R = P \oplus Q$ (Abb. 2, rechts)

Die soeben definierte Addition von Punkten erfüllt genau die Bedingungen, sie zur Ver- und Entschlüsselung von Nachrichten nutzen zu können, denn es gilt der folgende Satz:

Satz: Es sei $y^2 = x^3 + a \cdot x + b$ eine elliptische Kurve. Dann bildet

$$\{(x;\, y) \in \mathbb{R}^2 \text{ mit } y^2 = x^3 + a \cdot x + b\} \cup \{\mathcal{O}\}$$

mit der oben definierten Addition eine abelsche Gruppe mit dem neutralen Element $\mathcal{O}$ (im Unendlichen).

Daher lässt sich dieses Verfahren in der Kryptographie anwenden.

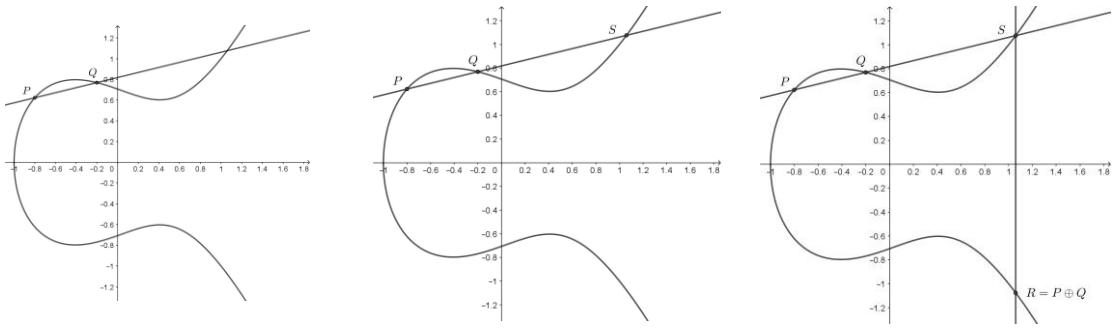

Abb. 2: Graphische Darstellung der Addition von Punkten einer elliptischen Kurve

Aus mehreren Gründen ist es sinnvoll, bei der Anwendung elliptischer Kurven in der Kryptographie mit *Restklassen* zu rechnen. Das *Modulo-Rechnen* ist Lernenden prinzipiell seit der Primarstufe als Division mit Rest bekannt. Mithilfe dieser Rechnung lässt sich auch eine Brücke zu weiteren Themen der Kryptographie bilden.

4. Didaktik und Fachwissenschaft

Fachwissenschaftliches

Die Kryptographie in Verbindung mit elliptischen Kurven lässt sich in der Schule auf unterschiedliche Art anwenden. Da sich Vieles mithilfe digitaler Medien graphisch darstellen lässt, lassen sich ggf. an bestimmten Stellen Zusammenhänge graphisch zeigen oder zumindest nachvollziehen oder auch Berechnungen mit bestimmten Formeln durchführen (siehe Stoppel & Rott, 2018). Hiermit lässt sich einerseits die Komplexität des Unterrichts senken, andererseits lässt sich der Aufwand elementarer Rechnung und Zeichnung reduzieren und damit tiefer in thematische Hintergründe eindringen. Es zeigen sich nicht zuletzt Möglichkeiten der Binnendifferenzierung.

Notwendige mathematische Voraussetzungen zur Behandlung des Themas beschränken sich auf ganzrationale Funktionen und die Wurzelfunktion. Daher ist eine thematische Behandlung bereits zu Beginn der Sekundarstufe II oder auch schon am Ende der Sekundarstufe I möglich.

Im Verlauf der Anwendung elliptischer Kurven in der Kryptographie stellt sich mithilfe von Graphen und von Formeln zur Ver- und Entschlüsselung von Texten heraus, dass die Operation der Verschlüsselung eines Buchstabens eine gewisse Struktur besitzt. Es regt zur Untersuchung der Rechenoperation auf Gesetzmäßigkeiten an. Bei dieser Untersuchung stoßen SchülerInnen auf Gesetzmäßigkeiten, die u.U. zum Begriff der Gruppe führen können.

Didaktisches

Wie sich an Obigem und in Stoppel & Rott (2018) zeigt, lassen sich fachwissenschaftliche Bereiche der Kryptographie mit elliptischen Kurven der Hochschule hinreichend zur Anwendung thematischer Grundlagen in der Schule reduzieren, ohne dass die Grundideen der Ver- und Entschlüsselung mithilfe elliptischer Kurven verlorengehen. Untersucht man entsprechende Unterrichtsreihen auf enthaltene Leitideen und mathematische Kompetenzen, so zeigt sich, dass quasi alle von ihnen in der Unterrichtsreihe enthalten sind. Enthaltene Leitideen sind gegeben bzgl. *Algorithmus und Zahl* (L1), *Raum und Form* (L3) und *funktionalem Zusammenhang* (L4). Geförderte mathematische Kompetenzen liegen bei *mathematischer Organisation* (K1)

und *Lösung* (K2) von Problemen, der *Anwendung mathematischer Darstellung* (K4), dem *Umgang mit symbolischen, formalen und technischen Elementen der Mathematik* (K5) und *mathematischer Kommunikation* (K6).

6. Fazit

Seit Jahren dreht sich Vieles um den Übergang von der Schule zur Hochschule. Häufige Kritikpunkte liegen im Bereich mangelnder Voraussetzungen in Verbindung mit Vertrautheit mit Strukturen (Vogt, 2017). Wirft man insgesamt einen Blick in Richtung der fachwissenschaftlichen Inhalte der Unterrichtssequenz, so zeigen sich zahlreiche Komponenten, die zu einer Brücke zwischen Schule und Hochschule beitragen können. Einerseits treten von Seiten der Hochschulen gewünschte Fähigkeiten auf, andererseits bewegt man sich hier auch in Bezug zu den Grunderfahrungen nach Winter (1995), denn erforscht werden Erscheinungen der Welt, mathematische Gegenstände und Sachverhalte. Außerdem erwerben SchülerInnen durch den thematischen Bezug zur Welt über die Mathematik hinausgehende Problemlösefähigkeiten und besitzen die Gelegenheit, über die Sinnhaftigkeit der Unterrichtsinhalte nachzudenken. Damit bildet sich eine Brücke zwischen Schule und Hochschule.

Literatur

Fischer, G. (1994). *Ebene algebraische Kurven*. Braunschweig: Vieweg.

Lang, S. (1987). *Elliptic functions* (2nd ed.). *Graduate texts in mathematics: Vol. 112*. New York: Springer-Verlag.

Stoppel, H., & Griese, B. (2017). *Übungsbuch zur Linearen Algebra: Aufgaben und Lösungen* (9., erw. Aufl.). *Grundkurs Mathematik*. Wiesbaden: Springer Fachmedien.

Stoppel, H., & Rott, B. (2018, in Rez.). Worte in der Sprache von Kurven. In H.-G. Weigand & N. Oleksik (Eds.), *Mathematische Erkundungen*. Norderstedt: Casio.

Vogt, T. (2017). Hausaufgaben für alle? *Mitteilungen der Deutschen Mathematiker-Vereinigung*, *25*(2), 90–105.

Wiles, A. (1995). Modular elliptic curves and Fermat's Last Theorem. *Annals of Mathematics*, *142*(3), 443–551.

Winter, H. (1995). Mathematikunterricht und Allgemeinbildung. *Mitteilungen der Gesellschaft für Didaktik der Mathematik*, (61), 37–46.