

Skripte zur Mathematik

Algorithmen & Kryptologie

von

Christian Wyss

Skripte zur Mathematik

Algorithmen & Kryptologie

von

Christian Wyss



mathema



© 2023 Dr. Christian Wyss

Verlagslabel: mathema (www.mathema.ch)

ISBN Paperback: 978-3-384-12965-9

Hardcover: 978-3-384-12966-6

Auflage 2.0

Druck und Distribution im Auftrag des Autors:

tredition GmbH, Heinz-Beusen-Stieg 5, 22926 Ahrensburg, Germany

Das Werk, einschliesslich seiner Teile, ist urheberrechtlich geschützt. Für die Inhalte ist der Autor verantwortlich. Jede Verwertung ist ohne seine Zustimmung unzulässig. Die automatisierte Analyse des Werkes, um daraus Informationen, insbesondere über Muster, Trends und Korrelationen gemäss §44b UrhG („Text und Data Mining“) zu gewinnen, ist untersagt. Die Quellen der Bilder und deren Lizenzen sind im Anhang aufgeführt. Die Publikation und Verbreitung erfolgen im Auftrag des Autors, zu erreichen unter:

Dr. Christian Wyss, Chemin du Clos 60, 2502 Biel-Bienne, Schweiz.

Die Philosophie steht in diesem grossen Buch geschrieben, das unserem Blick ständig offen liegt – ich meine das Universum –; aber das Buch ist nicht zu verstehen, wenn man nicht zuvor die Sprache erlernt und sich mit den Buchstaben vertraut gemacht hat, in denen es geschrieben ist. Es ist in der Sprache der Mathematik geschrieben, und deren Buchstaben sind Kreise, Dreiecke und andere geometrische Figuren, ohne die es dem Menschen unmöglich ist, ein einziges Bild davon zu verstehen; ohne diese irrt man in einem dunklen Labyrinth herum.

Galileo Galilei: „*Il Saggiatore*“ (1623)

Inhaltsverzeichnis

Einleitende Worte

- I. Der Divisionsalgorithmus
- II. Der Algorithmus von Euklid
- III. Diophantische Gleichungen
- IV. Restklassen
- V. Vermischte Übungen
- VI. Kryptologie
- VII. Programmierung in Python

Schlussbemerkungen

Einleitende Worte

Diese Skripte zur Mathematik sind im Rahmen des Gymnasialunterrichts entstanden. Sie können als eigenständiges Lern- und Übungsmaterial eingesetzt werden. Sie sind jedoch primär als **unterrichts-begleitendes Material** konzipiert. Eine Einführung und Anleitung durch eine Lehrperson wird daher empfohlen.

Die Skripte enthalten **Lückentexte**. Sie dienen der Festigung des erworbenen Wissens und sollten im Plenum mit der gesamten Klasse ausgefüllt werden. Diese handschriftlichen Einträge helfen, die Schlüsselbegriffe und Aussagen zu verinnerlichen und Herleitungen und Beweise besser nachzuvollziehen.

Zu den Übungen

Um den Stoff zu vertiefen und zu festigen, halte ich es für unerlässlich, dass die Schülerinnen und Schüler eine Vielzahl von Übungen lösen. Die Skripte enthalten daher viele Übungen, die nicht nur das Erlernte festigen, sondern auch inner- und aussermathematische Anwendungen aufzeigen. Einige Übungen sind bewusst anspruchsvoller gestaltet und gehen über den üblichen Lehrstoff hinaus, können jedoch bei Bedarf übersprungen werden. Ein Stern ★ markiert, dass es sich bei der Aufgabe um eine zusätzliche Übung handelt, die über den obligatorischen Lernstoff hinausgeht. Im Folgenden werden die unterschiedlichen Übungstypen kurz erläutert.

Einstiegsbeispiel

Ein Einführungsbeispiel stellt eine Aufgabe dar, die eine neu einzuführende Thematik exemplarisch vorstellt. Diese Aufgabe soll die grundlegenden Begriffe der neuen Thematik vorwegnehmen und damit einführen. Dabei darf die Aufgabe einen gewissen Anspruch haben. Ein gemeinsames Lösen dieser Aufgaben im Plenum oder eine detaillierte Besprechung empfiehlt sich, um das Verständnis zu fördern.

Grundaufgaben

Eine Grundaufgabe ist eine Übungsaufgabe, die von den Schülerinnen und Schülern routiniert und sicher gelöst werden sollte. Durch die Bearbeitung mehrerer dieser Aufgaben sollen die Lernenden die Struktur verstehen und sich mit dem Lösungsweg vertraut machen, um ihn anschliessend situationsbezogen bei weiterführenden Aufgaben anwenden zu können.

Erarbeitungsaufgaben

Erarbeitungsaufgaben sind konzipiert, um den Lernstoff zu entwickeln und die Schülerinnen und Schüler konstruktivistisch an die neue Theorie heranzuführen.

Anwendungsaufgaben

Das erworbene theoretische Wissen hat in der Regel sowohl inner- als auch aussermathematische Anwendungen. Anwendungsaufgaben sollen die Fähigkeit zur Mathematisierung fördern und die Anwendbarkeit des Gelernten verdeutlichen.

Beweisaufgaben

In Beweisaufgaben lernen die Schülerinnen und Schüler, selbstständig einfache Beweise zu führen.

Zu den Titelbildern

Die Titelblätter bieten die Möglichkeit, verschiedene Aspekte der Mathematik mit den Schülerinnen und Schülern zu thematisieren. Dies umfasst insbesondere folgende Bereiche:

Mathematik und Ästhetik

Mathematik und Kunst stehen auf vielfältige Weise in Beziehung. Ihre Verbindung zeigt sich in Musik, Malerei, Architektur, Skulptur und Textilgestaltung etc. Die Titelblätter zielen darauf ab, die Schönheit der Mathematik anhand der bildenden Kunst aufzuzeigen.

Rechenhilfsmittel

„Es ist unwürdig, die Zeit von hervorragenden Leuten mit knechtischen Rechenarbeiten zu verschwenden, weil bei Einsatz einer Maschine auch der Einfältigste die Ergebnisse sicher hinschreiben kann.“ G. W. Leibniz (1673).

Der Mensch hat bereits in der Frühzeit Rechenhilfsmittel entwickelt, angefangen vom Kerbholz über mechanische Rechenmaschinen bis hin zu analogen und digitalen Computern. Die Titelblätter illustrieren diese Entwicklung.

Geschichte der Mathematik

Die Geschichte der Mathematik reicht zurück bis ins Altertum und den Anfängen des Zählens in der Jungsteinzeit. Mathematik wurde und wird in allen Kulturkreisen praktiziert. Die Titelblätter thematisieren bedeutende Werke der Mathematik sowie herausragende Mathematikerinnen und Mathematiker, die die Entwicklung dieser Disziplin massgeblich beeinflusst haben.

Zu den Inhalten

Allgemeines

In den vorliegenden Skripten wird der Divisionsalgorithmus und die Algorithmen von Euklid (verbesserter und erweiterter) eingeführt. Dies führt zu den diophantischen Gleichungen und dem Rechnen mit Restklassen. Das erworbene Wissen wird genutzt, um das RSA-Verfahren im Detail zu studieren. Die Schülerinnen und Schüler erhalten einen vertieften Einblick in die Operationen mit ganzen Zahlen (Nullteiler, multiplikatives Inverses).

Die Aufteilung des Stoffes in mehrere Skripte dient der Flexibilität bei der Gestaltung des Unterrichts. Da Mathematik eine stark hierarchische Struktur aufweist, kann der Stoff nicht in beliebiger Reihenfolge bearbeitet werden. Die Skripte sind in einer möglichen Bearbeitungsreihenfolge angeordnet. Im Folgenden wird kurz angegeben, welches Vorwissen für jede Einheit notwendig ist.

Der Divisionsalgorithmus

Behandelter Stoff

Der Begriff des Algorithmus wird eingeführt und anschliessend Beispiel des Divisionsalgorithmus an Zahlen wie auch an Polynomen vertieft. Dabei wird der Divisionsalgorithmus zum Kürzen von Brüchen und zum Lösen von Gleichungen (Polynomdivision) angewandt.

Notwendiges Vorwissen

Die Schülerinnen und Schüler müssen bereits mit linearen und quadratischen Gleichungen und mit Bruchtermen umgehen können. Der Divisionsalgorithmus für Zahlen wird vorausgesetzt. Er kann jedoch auch mit wenig Aufwand eingeführt werden.

Algorithmus von Euklid

Behandelter Stoff

Der grösste gemeinsame Teiler (ggT) wird mit Hilfe des Fundamentalsatzes der Algebra sowie mit dem Algorithmus von Euklid und dem verbesserten Algorithmus von Euklid berechnet.

Notwendiges Vorwissen

Soll der Algorithmus auch auf Polynome angewandt werden, so muss die Polynomdivision bereits bekannt sein.

Diophantische Gleichungen

Behandelter Stoff

Die diophantischen Gleichungen werden eingeführt. Die linearen diophantischen Gleichungen werden analysiert und systematisch gelöst. Dabei wird der erweiterte Algorithmus von Euklid eingesetzt. Nicht-lineare diophantische Gleichungen werden thematisiert, insbesondere wird der grosse Satz von Fermat diskutiert.

Notwendiges Vorwissen

Die Schülerinnen und Schüler müssen den verbesserten Algorithmus von Euklid bereits kennen.

Restklassen

Behandelter Stoff

Die Division mit Rest und die Modulo-Funktion werden im Detail diskutiert und sie werden zur Berechnung von Prüfziffern (IBAN, ISBN) und dem Osterdatum (Gauss'sche Osterformel) angewandt. Restklassen werden eingeführt und mit Hilfe von Additions- und Multiplikationstabellen untersucht. Dabei werden die Begriffe des Nullteilers und des multiplikativen Inversen erläutert.

Notwendiges Vorwissen

Die Schülerinnen und Schüler müssen den verbesserten Algorithmus von Euklid bereits kennen.

Vermischte Übungen

Behandelter Stoff

Dies ist ein Repetitionsdossier mit Übungen zu den vorangegangenen Themen.

Notwendiges Vorwissen

Der verbesserte Algorithmus von Euklid, der Divisionsalgorithmus (Polynomdivision) und das Rechnen mit der Modulo-Funktion bzw. mit Restklassen müssen vertraut sein.

Kryptologie

Behandelter Stoff

Das Konzept der symmetrischen und asymmetrischen Kryptosysteme wird erklärt und an Beispielen erläutert (Caesar-Verschlüsselung, Skytale, Enigma, RSA-Verfahren). Insbesondere das RSA-Verfahren wird detailliert studiert. Das Verfahren wird sowohl angewandt wie auch bewiesen. Dazu sind der erweiterte Algorithmus von Euklid, der kleine Satz von Fermat und der Chinesische Restsatz notwendig.

Notwendiges Vorwissen

Der kleine Satz von Fermat und der Chinesische Restsatz werden im Skript eingeführt, der erweiterte Algorithmus von Euklid wird jedoch vorausgesetzt. Auch sind Rechnungen in Restklassen – insbesondere mit grossen Potenzen – notwendig.

Programmierung in Python

Behandelter Stoff

Einfache Algorithmen werden in Python implementiert.

Notwendiges Vorwissen

Grundkenntnisse in Python werden vorausgesetzt. Zudem müssen die Algorithmen von Euklid und die Modulo-Funktion bekannt sein.

Algorithmen

Der Divisionsalgorithmus

1. Was ist ein Algorithmus?¹

Unter einem Algorithmus versteht man allgemein eine genau definierte Handlungsvorschrift zur Lösung eines Problems oder einer bestimmten Art von Problemen in endlich vielen Schritten.²

Im täglichen Leben lassen sich leicht Beispiele für Algorithmen finden: Ein Kochrezept stellt beispielsweise einen Algorithmus dar, sofern alle Angaben genau genug sind und es für alle Teilaufgaben, wie beispielsweise Braten oder Rühren, ebenfalls Algorithmen vorliegen. Auch Reparatur- und Gebrauchsanleitungen oder Hilfen zum Ausfüllen von Formularen sind in der Regel Algorithmen. Ein weiteres, etwas präziseres Beispiel sind Waschmaschinenprogramme.



Ein Algorithmus hat folgende Eigenschaften³:

- Das Verfahren muss in einem endlichen Text eindeutig beschreibbar sein.
- Jeder Schritt des Verfahrens muss tatsächlich ausführbar sein.
- Das Verfahren darf zu jedem Zeitpunkt nur endlich viel Speicherplatz benötigen.
- Das Verfahren darf nur endlich viele Schritte benötigen.

Darüber hinaus wird der Begriff Algorithmus in praktischen Bereichen oft auf die folgenden Eigenschaften eingeschränkt:

- Der Algorithmus muss bei denselben Voraussetzungen das gleiche Ergebnis liefern.
- Die nächste anzuwendende Regel im Verfahren ist zu jedem Zeitpunkt eindeutig definiert.

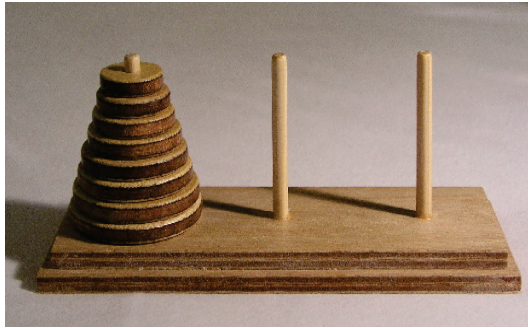
¹ Seite „Algorithmus“ in der Wikipedia – Die freie Enzyklopädie. 16. Dezember 2023

² Das Wort Algorithmus geht zurück auf das Arabische und ist eine Abwandlung oder Verballhornung des Namens von Abu Dscha'far Muhammad ibn Musa al-Chwarizmi, dessen Namensbestandteil (Nisba) al-Chwarizmi „der Choresmier“ bedeutet und auf die Herkunft des Trägers aus Choresmien verweist. Als dessen Lehrbuch „Über die indischen Ziffern“ (verfasst um 825 in Bagdad) im 12. Jahrhundert aus dem Arabischen ins Lateinische übersetzt und hierdurch in der westlichen Welt zur wichtigsten Quelle für die Ausbreitung der Kenntnis der indischen (heute meist als 'arabische' bezeichneten) Ziffern und des schriftlichen Rechnens mit diesen Ziffern wurde, wurde auch der Name des Verfassers in Anlehnung an die Anfangsworte der ältesten Fassung dieser Übersetzung (Dixit Algorismi: „Algorismi hat gesagt“) in der Form Algorismus latinisiert und in der Folgezeit mit Varianten wie alchorismus, algoarismus und mit Entlehnungen in die Volkssprachen (altfranzösisch algorisme, argorisme, mittellenglisch augrim, augrym) zu einer allgemeinen Bezeichnung für die von al-Chwarizmi gelehrt Kunst des Rechnens mit solchen Ziffern, desgleichen zu einem gebräuchlichen Werktitel für mittelalterliche und frühneuzeitliche Schriften über diese Kunst. (Wikipedia)

³ Seite „Algorithmus“ in der Wikipedia – Die freie Enzyklopädie. 16. Dezember 2023

2. Die Türme von Hanoi

Das Spiel *Die Türme von Hanoi* besteht aus drei gleich grossen Stäben A, B und C, auf die mehrere gelochte Scheiben gelegt werden, alle verschieden gross. Zu Beginn liegen alle Scheiben auf Stab A, der Grösse nach geordnet, mit der grössten Scheibe unten und der kleinsten oben. Ziel des Spiels ist es, den kompletten Scheiben-Stapel von A nach C zu versetzen.



Bei jedem Zug darf die oberste Scheibe eines beliebigen Stabes auf einen der beiden anderen Stäbe gelegt werden, vorausgesetzt, dort liegt nicht schon eine kleinere Scheibe. Folglich sind zu jedem Zeitpunkt des Spieles die Scheiben auf jedem Feld der Grösse nach geordnet.

Aufgabe 1: Löse das Problem für 3 Scheiben. Kannst Du die Aufgabe auch für 4, 5, 6 oder gar 7 Scheiben lösen? Kannst Du einen allgemeinen Algorithmus zur Lösung dieses Problems angeben? Wie viele Züge a_n braucht es bei optimaler Strategie bei n Scheiben? Gib eine rekursive und eine explizite Formel an. Gib also eine Formel an, mit der die Anzahl Züge a_n direkt aus der Anzahl Scheiben n berechnet werden kann (explizite Formel). Eine Rekursionsformel gibt an, wie Du aus der Anzahl Zügen a_n bei n Scheiben die Anzahl Züge a_{n+1} bei $n+1$ Scheiben berechnen kannst.

3. Der Divisionsalgorithmus

Das Verfahren zur schriftlichen Division zweier natürlicher Zahlen, welches Du in der Schule kennengelernt hast, ist ein Algorithmus – der Divisionsalgorithmus.

Aufgabe 2: Führe folgende Divisionen (ohne Taschenrechner) aus:

- a) $216 : 4$ b) $4'767 : 7$
- c) $3'255 : 15$ d) $51'255 : 17$
- e) Schreibe eine Handlungsanleitung (einen Algorithmus) für die Division zweier Zahlen.

Aufgabe 3: Führe folgende Divisionen mit Rest (ohne Taschenrechner) aus:

- a) $217 : 4$ b) $5'869 : 7$
- c) $9'452 : 15$ d) $1'108 : 17$
- e) Schreibe eine Handlungsanleitung (einen Algorithmus) für die Division zweier Zahlen mit Rest.