Vertiefungskurs Mathematik

Rechnen mit Restklassen – Didaktische Hinweise

Das Thema Rechnen mit Restklassen ist im vorläufigen Bildungsplan des Vertiefungskurses ein Wahlthema. Es empfiehlt sich, dieses einige Stunden zu behandeln. Erfahrungsgemäß macht der Umgang mit Zahlen den Schülerinnen und Schülern großen Spaß und es werden einige wichtige Grundlagen gelegt, wie beispielsweise die Begründung der Teilbarkeitsregeln. Das RSA-Verfahren trifft ebenfalls in der Regel auf großes Interesse. Vom kognitiven Anspruch her sind die Inhalte gut zu verstehen und auch schon zu Beginn der Jahrgangsstufe 1 möglich. Besonderer Vorkenntnisse sind keine notwendig.

Der vorliegende Unterrichtsgang umfasst vier Doppelstunden. Er startet mit der Definition einer Restklasse modulo n als Menge der ganzen Zahlen, die beim Teilen durch n denselben Rest lassen. Diese Definition ist für alle $n \in \mathbb{N}$ mit $n \geq 2$ sinnvoll. Für die Grundvorstellung einer Restklasse kann man bei geraden bzw. ungeraden Zahlen oder bei der Uhrzeit anknüpfen. Sobald die Klassenbildung verstanden ist, geht man zu den kanonischen Repräsentanten 0; 1; …; n-1 über. Dass man beim Rechnen mit Restklassen vor der Ausführung der Addition, Multiplikation oder der Potenzierung schon zu einer kongruenten Zahl übergehen kann, ist für die Schülerinnen und Schüler überraschend und erfreulich, da sich dadurch der Rechenaufwand teilweise erheblich reduzieren lässt. Eine interessante Anwendung stellt die Kalenderrechnung dar. Behandelt wird die Fragestellung, welcher Wochentag an einem bestimmten Datum sein wird bzw. war.

Einen kleinen Einblick in algebraische Strukturen bekommen die Schülerinnen und Schüler bei der Thematisierung von Additions- und Multiplikationstafeln modulo n. Dies kann anhand von in den Tabellen auftretenden Symmetrien besprochen werden. An dieser Stelle könnte man deutlich vertiefen und beispielsweise die Frage der Existenz eines multiplikativen Inversen sowie von möglichen Nullteilern ansprechen.

Die aus der Unterstufe bekannten und noch viele weiteren Teilbarkeitsregeln natürlicher Zahlen lassen sich sehr einfach mithilfe des Rechnens mit Restklassen beweisen. Im zugehörigen Arbeitsblatt ist eine Auswahl dazu aufgeführt. Man kann auch hier vertiefen und zum Beispiel eine Teilbarkeitsregel für die Zahl 37 beweisen. (Die 3-er Quersumme muss durch 37 teilbar sein.)

Zumindest eine kurze Thematisierung des RSA-Verfahrens lohnt sich. Dieses ist als Beispiel für ein asymmetrisches Verschlüsselungsverfahren sehr lehrreich und immer noch aktuell. Das vorliegende Arbeitsblatt liefert einen Einblick in das dem RSA-Verfahren zugrunde liegende Prozedere. Die Bestimmung des privaten Schlüssels aus dem öffentlichen Schlüssel mithilfe des Euklidischen Algorithmus wird nicht erklärt. Auch der Kleine Satz von Fermat wird nicht bewiesen. Hier besteht eine Fülle von Vertiefungsmöglichkeiten. Vor der Beschäftigung mit dem RSA-Verfahren ist eine Einführung in die Kryptographie sinnvoll, insbesondere die Unterscheidung zwischen symmetrischen und asymmetrischen Verschlüsselungsverfahren und der Bedeutung letzterer im Zeitalter der Online-Käufe. Auch historische Aspekte, wie das Cäsar-Verfahren oder die Verschlüsselungsmaschine Enigma, sind lohnend. Im Internet findeen sich eine Fülle gut aufbereiteter Information sowie Simulationen der Verfahren.