

Cäsar und die modulare Arithmetik

Welcher Zusammenhang besteht zwischen dem Cäsar-Verfahren und der Modulo-Rechnung? Bearbeite dazu folgende Aufgaben.

1. Ergänze die Cäsar-Tabelle. Verschiebe dabei das Alphabet um 9 Stellen nach LINKS!

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

2. Verschlüssele nun: G U T. : _____

3. Statt mit Buchstaben arbeiten wir nun mit Zahlen. Ordne dazu jedem Buchstaben zunächst eine Zahl zu, beginnend bei 0.

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

0 1

Die Verschiebung in 1. entspricht dem Schlüssel $e = 9$. Die Verschlüsselung soll durch eine Rechenoperation ausgedrückt werden. Beschreibe, wie die Zahl des Klarbuchstabens mit dem Schlüssel verrechnet werden muss:

4. Verschlüssele nun mit dem folgenden Verfahren:

Schreibe den Buchstaben als Zahl \rightarrow addiere den Schlüssel \rightarrow schreibe als Buchstaben

G \rightarrow \rightarrow \rightarrow

U \rightarrow \rightarrow \rightarrow

T \rightarrow \rightarrow \rightarrow

5. Beschreibe, welches Problem bei R auftritt. _____

6. Beschreibe, wie man das Problem mit Hilfe der modulo-Rechnung lösen kann. _____

7. Stelle einen einzigen Term auf, mit dem sich die Nummer des Geheim-Buchstabens aus der Nummer des Klar-Buchstabens (auch für die Problemfälle) berechnen lässt.

8. Stelle ebenso einen Term für das Entschlüsseln auf: _____
Überprüfe deine Formel für das obige Beispiel.

9. Schreibe die Entschlüsselung auch als ADDITION (wenn du sie in 8. schon als Addition geschrieben hast: Wie lautet die gleichwertige Subtraktion dazu?):

10. Verschlüssele SUPER mit dem Schlüssel 15 im Cäsar-Verfahren herkömmlich und mit Hilfe der Modulo-Rechnung.