2 Verschlüsselung in der Antike – der Caesar-Code

Schon um 500 v. Chr. sollen hebräische Gelehrte als Verschlüsselung ein umgekehrtes Alphabet benutzt haben. Auf das deutsche Alphabet übertragen bedeutet dies: Will man einen "geheime" Botschaft verschicken, so ersetzt man in der Botschaft den Buchstaben A immer durch Z, den Buchstaben B immer durch Y usw. Der Empfänger der Nachricht geht genauso vor und erhält wieder die ursprüngliche Nachricht.

Auf Caesar geht ein anderes Verschlüsselungsverfahren zurück, bei dem man die Buchstaben des zu versendenden Textes ersetzt durch Buchstaben, die im Alphabet um eine gewisse Anzahl von Buchstaben verschoben sind: Bei einer Verschiebung um zwei Buchstaben wird A ersetzt durch C, B durch D, C durch E usw. bis zu X durch Z. Bei den letzten – in unserem Beispiel zwei – Buchstaben, fängt man wieder von vorne an, also: Y wird ersetzt durch A und Z durch B.

Mit dem Caesar-Rad ist es leicht möglich, Texte nach dieser Methode zu verschlüsseln und wieder zu entschlüsseln (vgl. Arbeitsblatt *Caesar-Code und Restklassen*, Aufgabe 1).

2.1 Was hat der Caesar-Code mit Mathematik zu tun? – Restklassen

Mit dem Caesar-Rad ersetzt man Buchstaben durch Buchstaben. Ebenso kann man auch Buchstaben durch Zahlen ersetzen, z.B. durch die Zahlen 1 bis 26. Ähnlich wie beim Caesar-Code ist man auch hier frei in der Wahl einer Verschiebung. Man kann also A durch 3 ersetzen, B durch 4 usw. bis zu X durch 26; Y entspräche dann eigentlich der 27, wird aber wieder durch die 1 ersetzt, und Z (entspräche 28) durch die 2 (vgl. Arbeitsblatt *Caesar-Code und Restklassen*, Aufgabe 2).

Bei diesem Vorgehen wird also als Zahl jeweils der Rest genommen, den man erhält, wenn man die eigentliche Zahl durch 26 dividiert (die Buchstaben 27 und 28 existieren ja nicht). Dies entspricht der Betrachtung der Restklasse modulo 26 (vgl. Arbeitsblatt *Modulo-Rechnen*, Aufgabe 1).

Bemerkung 2.1 *Beim Ersetzen der Buchstaben durch Zahlen muss man beachten, dass die Entschlüsselung nicht eindeutig ist, wenn man unterschiedliche Anzahlen von Ziffern für unterschiedliche Buchstaben verwendet: Ersetzt man beispielsweise A durch 1, B durch 2 usw., so kann 123415 sowohl ABCDAE als auch LCDO bedeuten (12 kann als AB oder als L interpretiert werden, 15 als AE oder als O). Man sollte also immer die gleiche Anzahl von Ziffern für einen Buchstaben verwenden, also etwa 01 für A, 02 für B usw., oder die Eindeutigkeit anderweitig garantieren.*

Für das Verständnis des RSA-Algorithmus benötigen wir insbesondere den Begriff der Modulo-Funktion und die Regeln für das Modulo-Rechnen.

Definition 2.1 *Will man eine natürlichen Zahl a durch eine natürliche Zahl m teilen, so erhält man einen Rest r. Für diesen Rest gilt $0 \leq r \leq m-1$. Die Modulo-Funktion liefert zu gegebenen Zahlen a und m gerade diesen Rest r. Man schreibt auch*

$$a \bmod m = r \ .$$

Man kann diese Definition auch direkt auf ganzen Zahlen a verallgemeinern. So ist beispielsweise $-7 \bmod 3 = 2$, denn es gilt $-7 : 3 = -3$ Rest 2 wegen $-7 = -3 \cdot 3 + 2$.

Beispiel 2.1

$$\textit{Es ist } 19 : 4 = 4 \textit{ Rest } 3 \ , \ \textit{also gilt } 19 \bmod 4 = 3 \ .$$

Analog gilt:

$$\begin{aligned} 5 \bmod 3 &= 2 \quad && \textit{denn } 5 : 3 = 1 \textit{ Rest 2,} \\ 7 \bmod 4 &= 3 \quad && \textit{denn } 7 : 4 = 1 \textit{ Rest 3,} \\ 17 \bmod 6 &= 5 \quad && \textit{denn } 17 : 6 = 2 \textit{ Rest 5.} \end{aligned}$$

Man kann leicht zeigen, dass folgende Rechenregeln gelten:

$$\begin{aligned} (a \pm b) \bmod m &= (a \bmod m \pm b \bmod m) \bmod m \\ (a \cdot b) \bmod m &= (a \bmod m) \cdot (b \bmod m) \bmod m \\ (a^b) \bmod m &= (a \bmod m)^b \bmod m \end{aligned}$$

Im täglichen Leben rechnet man recht häufig modulo 10, zum Beispiel bei der schriftlichen Addition. Eine normale Uhr mit Stundenzeiger funktioniert analog zu modulo 12; digitale Tageszeitangaben (24h) analog zu modulo 24.

Zum Einüben und Vertiefen des Verständnisses der Modulofunktion dient das Arbeitsblatt *Modulo-Rechnen.*

Definition 2.2 *Die Restklasse einer Zahl a modulo einer Zahl m ist die Menge aller ganzen Zahlen, die bei Division durch m denselben (positiven) Rest lassen wie a. Man schreibt:* $[a]_m = \{b \in \mathbb{Z} \mid \exists k \in \mathbb{Z} : b = k \cdot m + a\} = \{b \mid b \equiv a \bmod m\}$. *Jedes Element einer Restklasse bezeichnet man auch als Repräsentant der Restklasse. Die Menge aller Restklassen modulo m schreibt man häufig auch als* $\mathbb{Z}/m\mathbb{Z} = \{[0]_m, [1]_m, [2]_m, \ldots, [m-1]_m\}$.

Beispiel 2.2 (Restklassen modulo 2)
Die Restklasse von 0 modulo 2 ($[0]_2$) ist die Menge der geraden Zahlen.
Die Restklasse von 1 modulo 2 ($[1]_2$) ist die Menge der ungeraden Zahlen.

Beispiel 2.3 (Restklassen modulo 3) *Es gibt drei Restklassen modulo 3: Eine Zahl ist durch drei teilbar, oder sie hat Rest 1, oder sie hat Rest 2. Das heißt:*

$$\begin{aligned} [0]_3 &= \{\cdots, -6, -3, 0, 3, 6, \cdots\} \\ [1]_3 &= \{\cdots, -5, -2, 1, 4, 7, \cdots\} \\ [2]_3 &= \{\cdots, -4, -1, 2, 5, 8, \cdots\} \ . \end{aligned}$$

Man beachte dabei, dass ein Rest von -2 einem Rest von 1 entspricht:
$(-5) : 3 = -1$ *Rest* -2
$(-5) : 3 = (-6 + 1) : 3 = -2$ *Rest* 1 .
Also haben wir $[-5]_3 = [-2]_3 = [1]_3$

Man kann für Restklassen eine Addition einführen. So ist z.B.

$$[1]_3 + [2]_3 = [3]_3 = [0]_3 \ .$$

Denn: Dividiert man zwei Zahlen a und b durch 3 und $a \bmod 3 = 1$, $b \bmod 3 = 2$, so gibt es Zahlen $k_1, k_2 \in \mathbb{Z}$ mit $a = 3 \cdot k_1 + 1$ und $b = 3 \cdot k_2 + 2$. Damit ist

$$a + b = k_1 \cdot 3 + 1 + k_2 \cdot 3 + 2 = (k_1 + k_2) \cdot 3 + 3 = (k_1 + k_2 + 1) \cdot 3$$

und somit $(a + b) \bmod 3 = 0$.

Entsprechend gilt für die Multiplikation von Restklassen z.B.

$$[2]_3 \cdot [2]_3 = [4]_3 = [1]_3 \ .$$

Dies sieht man folgendermaßen: Seien a und b zwei ganze Zahlen mit $a \bmod 3 = 2$ und $b \bmod 3 = 2$. Dann gibt es Zahlen $k_1, k_2 \in \mathbb{Z}$ mit $a = 3 \cdot k_1 + 2$ und $b = 3 \cdot k_2 + 2$. Damit ist

$$\begin{aligned} a \cdot b &= (k_1 \cdot 3 + 2) \cdot (k_2 \cdot 3 + 2) \\ &= (k_1 \cdot k_2 \cdot 3 + 2 \cdot k_2 + 2 \cdot k_1) \cdot 3 + 2 \cdot 2 \\ &= (k_1 \cdot k_2 \cdot 3 + 2 \cdot k_2 + 2 \cdot k_1 + 1) \cdot 3 + 1 \end{aligned}$$

und $a \cdot b$ hat bei Division durch 3 den Rest 1, also $(a \cdot b) \bmod 3 = 1$.

Addition und Multiplikation von Restklassen lässt sich einfach mit Hilfe entsprechender Tabellen darstellen. Die Additions- und die Multiplikationstabelle für das Rechnen mit Restklassen modulo 3 sehen folgendermaßen aus:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Für die Restklassen modulo 4 erhalten wir folgende Tabellen:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Zum Einüben und Vertiefen des Verständnisses von Restklassen dient das Arbeitsblatt *Restklassen.*

2.2 Nachteile des Caesar-Codes und Verallgemeinerungen

Insgesamt gibt es beim Caesar-Code nur 25 verschiedene Möglichkeiten, eine Nachricht zu verschlüsseln. (Die Einstellung des Caesar-Rads, bei jedem Buchstaben derselbe Buchstabe wieder zugeordnet wird, kann nicht als Verschlüsselung bezeichnet werden.) Wenn also jemand eine Nachricht abfängt und den Verdacht hat, sie könnte mit dem Caesar-Code verschlüsselt sein, so ist es sogar per Hand relativ leicht möglich, alle Möglichkeiten auszuprobieren und so die Nachricht zu entschlüsseln.

Arbeitsblatt: Restklassen (I)

Wenn wir alle ganzen Zahlen im Hinblick auf ihre Teilbarkeit durch z.B. die Zahl 6 untersuchen, können wir die ganzen Zahlen in 6 Teilmengen unterteilen, je nachdem, welcher (positive) Rest r bei der Division durch 6 übrig bleibt. Wir bezeichnen diese Teilmengen mit $[r]_6$ und nennen sie die Restklassen modulo 6. So ist beispielsweise

$$[0]_6 = \{\ldots, -12, -6, 0, 6, 12, \ldots\}$$

die Restklasse 0 modulo 6, die alle ganzen Zahlen enthält, die durch 6 teilbar sind, und

$$[2]_6 = \{\ldots, -10, -4, 2, 8, 14 \ldots\}$$

ist die Restklasse 2 modulo 6, die alle ganzen Zahlen enthält, die bei Division durch 6 den *positiven* Rest 2 haben. So ist etwa

$$8 : 6 = 1 \text{ Rest } 2$$

und

$$-10 : 6 = -2 \text{ Rest } 2, \text{ denn } -10 = -2 \cdot 6 + 2 \ .$$

In der folgenen Tabelle sind die Restklassen modulo 6 nochmals zusammengefasst:

$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$6 \cdot k$	$6 \cdot k + 1$	$6 \cdot k + 2$	$6 \cdot k + 3$	$6 \cdot k + 4$	$6 \cdot k + 5$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
-12	-11	-10	-9	-8	-7
-6	-5	-4	-3	-2	-1
0	1	2	3	4	5
6	7	8	9	10	11
12	13	14	15	16	17
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

Verdeutlichung der dritten Spalte dieser Tabelle:

$$\begin{aligned} -10 &= -2 \cdot 6 + 2 \\ -4 &= -1 \cdot 6 + 2 \\ 2 &= 0 \cdot 6 + 2 \\ 8 &= 1 \cdot 6 + 2 \\ 14 &= 2 \cdot 6 + 2 \end{aligned}$$

Man kann entsprechend natürlich auch andere Zahlen als die 6 nehmen und kommt dann zur allgemeinen Definition von Restklassen modulo einer natürlichen Zahl m:

Definition: Die *Restklasse* einer ganzen Zahl a modulo einer Zahl m ist die Menge all der Zahlen, die bei Division durch m denselben (*positiven*) Rest lassen wie a. Die Restklasse von a modulo m bezeichnet man als $[a]_m$, und es gilt

$$[a]_m = \{b \in \mathbb{Z} | \text{ es gibt ein } k \in \mathbb{Z} \text{ mit } b = k \cdot m + a\} \ .$$

Man kann die ganzen Zahlen also in Restklassen einteilen. Jede Zahl, die zu einer Restklasse gehört, heißt auch Repräsentant der Restklasse.

Aufgaben:

1. (a) Versuche die obige Tabelle in Worte zu fassen.
   (b) Fertige eine entsprechende Tabelle für $m = 5$ an.
   (c) Bestimme $[0]_3$, $[1]_3$ und $[1]_4$.
   (d) Gib drei verschiedene Repräsentanten der Restklassen $[3]_7$ und $[2]_8$ an.
   (e) Kennst Du Anwendungen von Restklassen im täglichen Leben?

Arbeitsblatt: Restklassen (II)

Definition: Die *Restklasse* einer ganzen Zahl a modulo einer Zahl m ist die Menge all der Zahlen, die bei Division durch m denselben (*positiven*) Rest lassen wie a. Die Restklasse von a modulo m bezeichnet man als $[a]_m$, und es gilt

$$[a]_m = \{b \in \mathbb{Z} | \text{ es gibt ein } k \in \mathbb{Z} \text{ mit } b = k \cdot m + a\} \quad .$$

Man kann die ganzen Zahlen also in Restklassen einteilen. Jede Zahl, die zu einer Restklasse gehört, heißt auch Repräsentant der Restklasse.

Beispiele: $[0]_6 = \{\ldots, -12, -6, 0, 6, 12, \ldots\}$ und $[2]_6 = \{\ldots, -10, -4, 2, 8, 14 \ldots\}$

Man kann für Restklassen eine natürliche Addition und eine natürliche Multiplikation definieren. Dazu nimmt man jeweils einen Repräsentanten der zu addierenden/multiplizierenden Restklassen, addiert bzw. multipliziert diese Repräsentanten und bestimmt, zu welcher Restklasse die Summe bzw. das Produkt gehören. Das Ergebnis ist tatsächlich unabhängig davon, welche Repräsentanten man ausgewählt hat.

Beispiel: Man will Produkt und Summe von $[4]_7$ und $[5]_7$ berechnen. Betrachten wir dazu einerseits die Repräsentanten 4 und 5, andererseits die Repräsentanten 11 und 12. Dann gilt

$4 + 5 = 9$, $\quad 9 \bmod 7 = 2$	$11 + 12 = 23$, $\quad 23 \bmod 7 = 2$
$4 \cdot 5 = 20$, $\quad 20 \bmod 7 = 6$	$11 \cdot 12 = 132$, $\quad 132 \bmod 7 = 6$

Auch für andere Wahlen von Repräsentanten kommen immer dieselben Ergebnisse heraus. Daher schreibt man auch

$$\begin{aligned} [4]_7 + [5]_7 &= [2]_7 \\ [4]_7 \cdot [5]_7 &= [6]_7 \end{aligned}$$

Aufgaben:

1. Zeige, dass für alle Repräsentanten $a \in [4]_7$ und $b \in [5]_7$ gilt: $a + b \in [2]_7$. Benutze dafür, dass sich a und b schreiben lassen als $a = 7 \cdot k_1 + 4$ und $b = 7 \cdot k_2 + 5$ mit ganzen Zahlen k_1 und k_2 und ermittle, welchen Rest $a + b$ bei Division durch 7 hat.

2. Zeige, dass für alle Repräsentanten $a \in [4]_7$ und $b \in [5]_7$ gilt: $a \cdot b \in [6]_7$. Benutze dafür, dass sich a und b schreiben lassen als $a = 7 \cdot k_1 + 4$ und $b = 7 \cdot k_2 + 5$ mit ganzen Zahlen k_1 und k_2 und ermittle, welchen Rest $a \cdot b$ bei Division durch 7 hat.

3. Leicht darstellen kann man Addition und Multiplikation von Restklassen mit Tabellen. Wenn aus dem Zusammenhang klar ist, welche Restklassen man betrachtet, kann man die Symbole $[\ ]_m$ auch weglassen.

   (a) Zeige, dass für die Restklassen modulo 3 folgende Additions- und Multiplikationstabelle gilt:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

   (b) Ermittle Additions- und Multiplikationstabelle für die Restklassen modulo 6.

+	0	1	2	3	4	5
0						
1						
2						
3						
4						
5						

·	0	1	2	3	4	5
0						
1						
2						
3						
4						
5						