- Das Telefonbuch ordnet jedem Namen eine Telefonnummer zu. Um aus der Telefonnummer aber auf den Namen zurückschließen zu können, müsste man die Einträge einzeln durchlesen (solange man sich nicht eines elektronischen Telefonbuchs mit Suchfunktion bedient).
- Man kann leicht eine Nachricht in einen Briefkasten einwerfen. Den Briefkasten öffnen und damit die Nachricht lesen kann jedoch nur, wer den privaten Schlüssel für seinen Briefkasten besitzt.

Zum Verständnis des Begriffs dient das Arbeitsblatt *Einwegfunktionen*.

3.2 Das multiplikative Inverse modulo einer Zahl m

Um Ver- und Entschlüsselung des RSA-Verfahrens verstehen zu können, benötigen wir neben dem Begriff der Primzahl und elementarem Rechnen mit Restklassen lediglich noch den Begriff des multiplikativen Inversen modulo einer Zahl m.

Definition 3.2 *Sind a und m zwei teilerfremde positive ganze Zahlen, so ist die multiplikative Inverse von a modulo m diejenige (eindeutig bestimmte) positive Zahl $b < m$, welche die Gleichung*

$$1 \equiv a \cdot b \bmod m$$

erfüllt. Man schreibt auch $b = a^{-1} \bmod m$.

Beispiel 3.1 *Ein erstes Beispiel: Sei $a = 7$ und $m = 3$. Gesucht sei das multiplikative Inverse von 7 modulo 3, also $b = 7^{-1} \bmod 3$. Mit anderen Worten, wir suchen die ganze Zahl $b < 3$, für die*

$$1 \equiv 7 \cdot b \bmod 3$$

ist. Dies ist ganz einfach, wenn wir eine Multiplikationstabelle für die Restklassen modulo 3 haben; denn dann können wir die gesuchte Zahl b ganz einfach hieraus ablesen. Zunächst ist $7 \bmod 3 \equiv 1$. Aus der Multiplikationstabelle modulo 3 (vgl. Abschnitt 2.1) lesen wir ab: $1 \cdot 1 = 1$. Also ist hier $b = 1$.

Beispiel 3.2 *Ein zweites Beispiel: Sei $a = 7$ und $m = 4$. Gesucht sei jetzt das multiplikative Inverse von 7 modulo 4, also $b = 7^{-1} \bmod 4$. Mit anderen Worten, wir suchen die ganze Zahl $b < 4$, für die*

$$1 \equiv 7 \cdot b \bmod 4$$

ist. Es ist $7 \bmod 4 \equiv 3$. Aus der Multiplikationstabelle modulo 4 (vgl. Abschnitt 2.1) lesen wir ab: $3 \cdot 3 = 1$. Also ist hier $b = 3$.

Bemerkung 3.1 *Die multiplikative Inverse von a modulo m existiert nur, wenn a und m teilerfremd sind. Man kann dies exemplarisch aus den entsprechenden Multiplikationstabellen ablesen.*

Es gibt einfache mathematische Methoden, um das multiplikative Inverse modulo einer Zahl m zu bestimmen (vgl. Abschnitt 4.2). In der Praxis führt man die RSA-Verschlüsselung und die RSA-Entschlüsselung mit Hilfe von Computern durch, auf denen man diese Methoden einfach programmieren kann.

4.2.2 Bestimmung des multiplikativen Inversen zweier Zahlen mit dem Euklidischen Algorithmus

Sind a und m zwei teilerfremde positive ganze Zahlen, so ist die multiplikative Inverse b zu a modulo m die eindeutig bestimmte positive Zahl $b < m$, welche die Gleichung

$$(b \cdot a) \bmod m = 1$$

erfüllt. Diese Gleichung können wir auch schreiben als

$$1 = b \cdot a + k \cdot m \tag{4}$$

mit $k \in \mathbb{Z}$. Wir wollen in diesem Abschnitt beschreiben, wie man die multiplikative Inverse berechnen kann. Das Ziel unseres Vorgehens wird dabei sein, die Zahl 1 als Linearkombination der Zahlen a und m zu schreiben.

Um diese multiplikative Inverse zu bestimmen, können wir den Euklidischen Algorithmus verwenden. Es sei $a = 5$ und $m = 8$. Wir führen jetzt in der linken Spalte den Euklidischen Algorithmus durch, bis der Rest 1 auftaucht, in der rechten Spalte schreiben wir dies in einer multiplikativen Form:

$$8 : 5 = 1 \text{ Rest } 3 \iff 8 = 1 \cdot 5 + 3 \tag{5}$$
$$5 : 3 = 1 \text{ Rest } 2 \iff 5 = 1 \cdot 3 + 2 \tag{6}$$
$$3 : 2 = 1 \text{ Rest } 1 \iff 3 = 1 \cdot 2 + \boxed{\mathbf{1}} \tag{7}$$

Idee des weiteren Vorgehens: Die Grundlage für das weitere Vorgehen ist, dass bei teilerfremden Zahlen im Euklidischen Algorithmus als Rest irgendwann die Zahl $\boxed{1}$ auftaucht. Die Idee ist jetzt, die letzte Gleichung in der Form $\boxed{\mathbf{1}} = 3 - 1 \cdot 2$ zu schreiben und hier die Zahlen 2 und 3, die als Reste in vorherigen Schritten des Euklidischen Algorithmus entstanden sind (vgl. die Gleichungen (5) und (6), mit Hilfe dieser Gleichungen zu eliminieren, so dass man auf der rechten Seite nur noch Vielfache der ursprünglichen Zahlen 8 und 5 erhält, also

$$1 = k_1 \cdot 5 + k_2 \cdot 8 \tag{8}$$

mit ganzen Zahlen k_1 und k_2. (Man mache sich klar, dass diese Gleichung der Gleichung (4) entspricht.) Betrachten wir Gleichung (8) modulo 8, so erhalten wir

$$1 = (k_1 \cdot 5) \bmod 8$$

und das multiplikative Inverse zu 5 modulo 8 ist die Zahl k_1 mod 8.

Durchführung dieser Idee: Wie gerade beschrieben, verwenden wir die einzelnen Schritte des Euklidischen Algorithmus (in der multiplikativen Form) in umgekehrter Reihenfolge. Die letzte Gleichung in der multiplikativen Form (7) können wir auch schreiben als

$$1 = 3 - 1 \cdot 2 \ . \tag{9}$$

Die 2 in dieser Gleichung wollen wir mit Hilfe von (6) ersetzen und lösen daher (6) nach dem Rest (d.h. nach der Zahl 2) auf

$$2 = 5 - 1 \cdot 3 \ .$$

Einsetzen in Gleichung (9) liefert

$$1 = 3 - 1 \cdot (5 - 1 \cdot 3) = 2 \cdot 3 - 1 \cdot 5 \ . \tag{10}$$

Analog ersetzen wir jetzt die Zahl 3 in dieser Gleichung mit Hilfe des ersten Schritts des Euklidischen Algorithmus. Dazu lösen wir Gleichung (5) nach dem Rest (d.h. der Zahl 3) auf

$$3 = 8 - 1 \cdot 5$$

und setzen dies in Gleichung (10) ein:

$$1 = 2 \cdot (8 - 1 \cdot 5) - 1 \cdot 5 = 2 \cdot 8 - 3 \cdot 5 \ .$$

Betrachten wir diese Gleichung jetzt modulo 8, so erhalten wir

$$1 = (-3 \cdot 5) \bmod 8 = (5 \cdot 5) \bmod 8 \qquad \text{wegen} \qquad -3 \bmod 8 = 5 \bmod 8 \ .$$

Offenbar gilt also $1 = (5 \cdot 5) \bmod 8$ und wir haben die multiplikative Inverse zu 5 modulo 8 gefunden. Es ist die Zahl 5 selber. Wir können dies leicht überprüfen:

$$(5 \cdot 5) \bmod 8 = 25 \bmod 8 = 1 \ .$$

Ein zweites Beispiel: Wir suchen die modulare Inverse zu 13 mod 160. Euklidischer Algorithmus:

$$160 : 13 = 12 \text{ Rest } 4 \implies 160 = 12 \cdot 13 + 4 \tag{11}$$

$$13 : 4 = 3 \text{ Rest } 1 \implies 13 = 3 \cdot 4 + 1 \tag{12}$$

Wir gehen wieder rückwärts vor und erhalten aus (12)

$$1 = 13 - 3 \cdot 4 \ . \tag{13}$$

Ersetzen wir hierin die Zahl 4 gemäß Gleichung (11) durch

$$4 = 160 - 12 \cdot 13 \ ,$$

so erhalten wir aus (13)

$$1 = 13 - 3 \cdot (160 - 12 \cdot 13) = 13 - 3 \cdot 160 + 3 \cdot 12 \cdot 13 = 37 \cdot 13 - 3 \cdot 160 \ .$$

Betrachten wir diese Gleichung modulo 160, so erhalten wir

$$1 = (37 \cdot 13) \bmod 160 \ .$$

Das multiplikative Inverse zur Zahl 13 modulo 160 ist die Zahl 37. Probe:

$$13 \cdot 37 = 481 = 3 \cdot 160 + 1$$

Leichter geht die Berechnung (sowohl von Hand als auch in Hinblick auf die Programmierung), wenn man folgende Variante des Algorithmus verwendet:

Einfachere Variante:
Wir suchen wieder eine positive Zahl $b < 160$, so dass $(13 \cdot b) \bmod 160 = 1$ gilt.

Zeile	Verfahren			Erläuterung
(I)	160	1	0	Dies steht für $\boxed{160} = \boxed{1} \cdot 160 + \boxed{0} \cdot 13$
(II)	13	0	1	Dies steht für $\boxed{13} = \boxed{0} \cdot 160 + \boxed{1} \cdot 13$
				Wie oft geht 13 in 160? 12 mal; also (III) = (I) $-12\cdot$ (II)
(III)	4	1	-12	Dies steht für $\boxed{4} = \boxed{1} \cdot 160\boxed{-12} \cdot 13$
				Wie oft geht 4 in 13? 3 mal; also (IV) = (II) $-3\cdot$ (III)
(IV)	$\boxed{1}$	-3	$\boxed{37}$	Dies steht für $\boxed{1} = \boxed{-3} \cdot 160 + \boxed{37} \cdot 13$

Das Verfahren hat jetzt in der ersten Spalte eine 1 erzeugt. Damit haben wir die multiplikative Inverse zu 13 mod 160 gefunden. Sie steht in der letzten Spalte des Verfahrens und lautet 37.

Analog können wir das alternative Verfahren auch auf unser erstes Beispiel $a = 5$ und $m = 8$ anwenden:

(I)	8	1	0	
(II)	5	0	1	Wie oft geht 5 in 8? 1 mal; also (III)=(I)$-1\cdot$(II)
(III)	3	1	-1	Wie oft geht 3 in 5? 1 mal; also (IV)=(II)$-1\cdot$(III)
(IV)	2	-1	2	Wie oft geht 2 in 3? 1 mal; also (V)=(III)$-1\cdot$(IV)
(V)	1	2	-3	In erster Spalte taucht 1 auf; multiplikative Inverse gefunden!

In diesem (und anderen Beispielen) taucht als multiplikative Inverse eine negative Zahl (hier: -3) auf. Wir sind jedoch an einer positiven Zahl b interessiert. Diese erhalten wir leicht durch $-3 \bmod 8 = 5$. Dies kann man auch sehen, wenn man Gleichung (V) ausgeschrieben betrachtet:

$$1 = 2 \cdot 8 - 3 \cdot 5 = (-3 \cdot 5) \bmod 8 = (5 \cdot 5) \bmod 8$$

und $b = 5$ ist tatsächlich die multiplikative Inverse modulo 8 zu 5.

Arbeitsblatt: Multiplikatives Inverses modulo einer Zahl m

Dieses Arbeitsblatt beschreibt, wie man die multiplikative Inverse berechnet. Arbeitet die Schritte sorgsam durch und beantwortet die Fragen.

Definition: Sind a und m zwei *teilerfremde* positive ganze Zahlen, so ist die multiplikative Inverse b zu a modulo m die eindeutig bestimmte positive Zahl $b < m$, welche die Gleichung

$$(b \cdot a) \bmod m = 1$$

erfüllt. Diese Gleichung können wir auch schreiben als

$$1 = k \cdot m + b \cdot a \qquad \text{mit } k \in \mathbb{Z}. \tag{1}$$

Suche das multiplikative Inverse durch Ausprobieren: Sei $a = 13$ und $m = 16$. Wir suchen eine Zahl b, so dass $(13 \cdot b) \bmod 16 = 1$ ist.

$$\begin{aligned} 13 \cdot 2 \bmod 16 &= 10 \\ 13 \cdot 3 \bmod 16 &= 7 \\ 13 \cdot 4 \bmod 16 &= 4 \\ 13 \cdot 5 \bmod 16 &= 1 \end{aligned}$$

Wenn a und m größer werden ...: Ausprobieren führt nur bei kleinen Zahlen zum Ziel, bei großen Zahlen kann der Rechenaufwand riesig werden.

Mache dir folgendes klar: Wenn es uns gelingt, die Zahl 1 als Linearkombination der Zahlen a und m zu schreiben, d.h. wenn wir eine Darstellung der Form (1) finden, ist $b \bmod m$ gerade die gesuchte multiplikative Inverse.

Um eine solche Darstellung zu finden, verwenden wir den Euklidischen Algorithmus, der folgendermaßen abläuft: Wir starten mit den beiden Gleichungen

$$\begin{aligned} &\text{(I)} && \boxed{16} &&= \boxed{1} \cdot 16 + \boxed{0} \cdot 13 \\ &\text{(II)} && \boxed{13} &&= \boxed{0} \cdot 16 + \boxed{1} \cdot 13 \end{aligned}$$

Da die 13 nur *einmal* in die 16 passt, berechnen wir Gleichung (III) als

$$\text{(III)} = \text{(I)} - 1 \cdot \text{(II)}$$

und erhalten

$$\text{(III)} \qquad \boxed{3} = \boxed{1} \cdot 16 + \boxed{-1} \cdot 13 \ .$$

Die 3 (linke Seite von Gleichung (III)) passt *viermal* in die 13 (linke Seite von Gleichung (II)). Daher berechnen wir Gleichung (IV) als

$$\text{(IV)} = \text{(II)} - 4 \cdot \text{(III)}$$

und erhalten

$$\text{(IV)} \qquad \boxed{1} = \boxed{-4} \cdot 16 + \boxed{5} \cdot 13 \ .$$

Auf der linken Seite von Gleichung (IV) ist jetzt eine $\boxed{1}$ erzeugt worden. Damit haben wir die multiplikative Inverse modulo 16 zu 13 gefunden. Es ist die Zahl, die auf der rechten Seite als Faktor bei der 13 steht, modulo 16, also $5 \bmod 16 = 5$. Dies können wir leicht überprüfen und finden in der Tat $5 \cdot 13 \bmod 16 = 65 \bmod 16 = 1$.

Ein zweites Beispiel: Als zweites Beispiel betrachten wir jetzt $a = 13$ und $m = 160$. Wir suchen also wieder eine positive Zahl $b < 160$, so dass $(13 \cdot b) \bmod 160 = 1$ gilt. Dazu gehen wir genauso vor wie im ersten Beispiel, verwenden aber ein etwas kürzeres Schema. In der Spalte Erläuterung sind die Gleichungen nochmals ausgeschrieben; die Spalte Koeffizienten enthält nur die Koeffizienten dieser Gleichungen, die aber ausreichen, wenn wir das Verfahren erst einmal gut kennen.

Gleichung	Koeffizienten			Erläuterung
(I)	160	1	0	Dies steht für $\boxed{160} = \boxed{1} \cdot 160 + \boxed{0} \cdot 13$
(II)	13	0	1	Dies steht für $\boxed{13} = \boxed{0} \cdot 160 + \boxed{1} \cdot 13$
				Wie oft geht 13 in 160? 12 mal; also (III) = (I) $- 12 \cdot$ (II)
(III)	4	1	-12	Dies steht für $\boxed{4} = \boxed{1} \cdot 160 + \boxed{\text{-12}} \cdot 13$
				Wie oft geht 4 in 13? 3 mal; also (IV) = (II) $- 3 \cdot$ (III)
(IV):	$\boxed{1}$	-3	$\boxed{37}$	Dies steht für $\boxed{1} = \boxed{\text{-3}} \cdot 160 + \boxed{37} \cdot 13$

Das Verfahren hat jetzt in der ersten Spalte eine 1 erzeugt. Damit haben wir die multiplikative Inverse zu 13 mod 160 gefunden. Sie steht in der letzten Spalte des Verfahrens und lautet 37 mod 160 = 37. Manchmal dauert es auch einige Schritte länger, bis die 1 in der ersten Spalte entsteht.

Aufgaben:

1. Mache Dir klar, wie der oben beschriebene Algorithmus funktioniert.

2. Finde
   a) die multiplikative Inverse von 15 modulo 26
   b) die multiplikative Inverse von 5 modulo 48