Zahlentheoretische Grundlagen

Daniel Langer

Inhaltsverzeichnis

1 Vorwort

Die Kryptographie ist die Wissenschaft des Ver- und Entschlüsselns von Daten bzw. Informationen. Die Grundlage dieser Wissenschaft ist die diskrete Mathematik, insbesondere die Zahlentheorie mit modularer Arithmetik. Egal mit welchem Teilgebiet der Kryptographie man sich beschäftigt, ein solides Grundwissen in diskreter Mathematik ist dazu unerlässlich. Diese Seminararbeit hat das Ziel, dieses Grundwissen zu vermitteln. Ziel ist, dass die Leser einen souveränen Umgang mit modularen Ausdrücken erlernen, insbesondere die Rechenregeln der modularen Arithmetik und wie modulare Ausdrücke sinnvoll umgewandelt bzw. vereinfacht werden können. Außerdem werden wichtige Formeln vorgestellt, die die mathematische Grundlage diverser kryptographischer Verfahren bilden. Den beiden wichtigen Aufgaben, dem Bestimmen des modularen Inversen von ganzen Zahlen und dem Lösen von modularen Gleichungen wird mit den Kapiteln 3 und 4 jeweils ein eigener Abschnitt gewidmet.
Diese Seminararbeit orientiert sich stark an dem Buch "Kryptographie - Grundlagen, Algorithmen, Protokolle"von Dietmar Wätjen. Die Gliederung, die vorgestellen Algorithmen sowie die Beweisansätze vieler der im Folgenden bewiesenen Sätze enstammen sinngemäß diesem Werk.

2 Modulare Arithmetik

In diesem Abschnitt wird zunächst der Ring $(\mathbb{Z}_n, +_n, \cdot_n, 0, 1)$ der Divisionsreste eingeführt, sowie seine Beziehung zum Ring der ganzen Zahlen. Anschließend werden die Rechengesetze vorgestellt, die sich u. A. aus dieser Beziehung ableiten lassen. Vor allem Letzteres ist nicht nur für die nachfolgenden Kapitel dieser Seminararbeit sinnvoll, sondern vor allem im Hinblick auf die praktischen Themengebiete der Kryptographie essentiell. Zum Abschluss wird eine Methode vorgestellt, wie man im Ring $\mathbb{Z}_n$ mathematische Ausdrücke mit Potenzen effizient ausrechnen kann.
Anmerkungen: Es wird im Folgenden davon ausgegangen, dass die Leser aus der Vorlesung "Diskrete Strukturen" mit den Begriffen (kommutative) Gruppe, (kommutativer) Ring, Körper sowie Homo- und Isomorphismus vertraut sind.

2.1 Der kommutative Ring $(\mathbb{Z}_n, +_n, \cdot_n, 0, 1)$

Für das gesamte Kapitel wird vereinbart, dass $n \in \mathbb{N}$ eine natürliche Zahl größer als Eins ist.

Definition 2.1 *Wir definieren die Mengen $\mathbb{Z}_n \subset \mathbb{N}_0$ und $\mathbb{Z}_n^* \subset \mathbb{N}$ wie folgt:*

- $\mathbb{Z}_n := \{0, \ldots, n-1\}$
- $\mathbb{Z}_n^* := \{x \in \mathbb{Z}_n \setminus \{0\} \mid ggT(x, n) = 1\}$

Wir betrachten den kommutativen Ring der ganzen Zahlen $(\mathbb{Z}, +, \cdot, 0, 1)$. Auf diesem definieren wir die folgende Relation:

Definition 2.2 *Zwei ganze Zahlen $a, b \in \mathbb{Z}$ heißen kongruent modulo n (geschrieben $a \equiv_n b$), wenn für ein $k \in \mathbb{Z}$ gilt:*

$$a - b = k \cdot n$$

Satz 2.1 *Bei der Relation $\equiv_n$ über $\mathbb{Z}$ handelt es sich um eine Kongruenzrelation, es gilt also für $a, b, c, a', b' \in \mathbb{Z}$:*

1. $a \equiv_n a$
2. $a \equiv_n b \quad \Rightarrow \quad b \equiv_n a$
3. $a \equiv_n b$ und $b \equiv_n c \quad \Rightarrow \quad a \equiv_n c$
4. $a \equiv_n a'$ und $b \equiv_n b' \quad \Rightarrow \quad (a + b) \equiv_n (a' + b')$ und $(a \cdot b) \equiv_n (a' \cdot b')$

Die ersten drei Punkte machen $\equiv_n$ außerdem zu einer **Äquivalenzrelation**.

Beweis:

1. $(a - a) = 0 = 0 \cdot n$

2. Aus $a - b = k \cdot n$ für ein $k \in \mathbb{Z}$ folgt $b - a = (-k) \cdot n$, also $b \equiv_n a$.

3. Aus $a - b = k_1 \cdot n$ mit $k_1 \in \mathbb{Z}$ folgt $b = a - k_1 \cdot n$. Einsetzen in $b - c = k_2 \cdot n$ ($k_2 \in \mathbb{Z}$) ergibt $a - k_1 \cdot n - c = k_2 \cdot n$, also $a - c = (k_1 + k_2) \cdot n$ und damit $a \equiv_n c$.

4. Für $k_1, k_2 \in \mathbb{Z}$ ist $(a - a') = k_1 \cdot n$ und $(b - b') = k_2 \cdot n$, also $a = a' + k_1 \cdot n$ und $b = b' + k_2 \cdot n$. Damit ist $(a+b) - (a'+b') = (a' + k_1 \cdot n + b' + k_2 \cdot n) - (a'+b') = (k_1+k_2) \cdot n$. Damit ist $(a+b) \equiv_n (a'+b')$. Außerdem ist $a \cdot b - a' \cdot b' = (a' + k_1 \cdot n) \cdot (b' + k_2 \cdot n) - a' \cdot b' = (a' \cdot k_2 + b' \cdot k_1 + k_1 \cdot k_2 \cdot n) \cdot n$. Damit ist $a \cdot b \equiv_n a' \cdot b'$. □

Die Tatsache, dass $\equiv_n$ eine Äquivalenzrelation ist, hat zur Folge, dass sie die Menge der ganzen Zahlen in paarweise disjunkte Teilmengen, die sogenannten Restklassen partitioniert.

Definition 2.3 *Sei $a \in \mathbb{Z}$. Dann nennen wir $[a]_n = \{x \in \mathbb{Z} \mid a \equiv_n x\} \subset \mathbb{Z}$ die* ***Restklasse*** *von a modulo n.*

Wir können also zu jeder ganzen Zahl a die dazugehörige Restklasse $[a]_n$ bilden. Diese besteht nach Definition 2.2 aus der Menge aller ganzen Zahlen, die sich von a um ein Vielfaches von n unterscheidet, also z.B $[3]_4 = \{\ldots, -5, -1, \mathbf{3}, 7, 11, 15, 19, 23, \ldots\}$. Das bedeutet aber, dass die Restklassen von allen ganzen Zahlen, die in einer Restklasse enthalten sind, zu dieser Restklasse identisch sind, im obigen Beispiel also beispielsweise $[-5]_4 = [-1]_4 = [3]_4 = [7]_4 = [11]_4 = [15]_4 = [19]_4 \ldots$. Dies hat wichtige Konsequenzen, die wir später noch benötigen werden:

- Es gibt insgesamt nur n verschiedene Restklassen, die Menge dieser n Restklassen bezeichnet man als Faktormenge $\mathbb{Z}/(n)$.
- In jeder Restklasse existiert genau ein Element aus der Menge $\mathbb{Z}_n$.
- Die Faktormenge ist darstellbar als: $\mathbb{Z}/(n) = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$.

Kommen wir nochmal zurück zu Satz 2.1 Punkt 4. Er bedeutet anschaulich, wenn man je eine beliebige ganze Zahl aus den zwei Restklassen $[a]_n$ und $[b]_n$ entnimmt und addiert bzw. multipliziert, dann befinden sich alle möglichen Summen bzw. Produkte jeweils in der gleichen Restklasse. Da die Zahlen $(a + b)$ bzw. $(a \cdot b)$ trivialerweise in den Restklassen $[a + b]_n$ bzw. $[a \cdot b]_n$ sind, folgt daraus, dass es sich dabei um genau diese beiden Restklassen handeln muss. Wir wollen dies an einem Beispiel veranschaulichen: Wir betrachten die beiden Restklassen $[3]_7 = \{\ldots, -11, -4, 3, 10, 17, 24, 31, 38, \ldots\}$ und $[5]_7 = \{\ldots, -9, -2, 5, 12, 19, 26, 33, 40, \ldots\}$. Alle möglichen Summen zweier Zahlen, je eine aus einer der beiden Mengen liegen allesamt in der Restklasse $[3 + 5]_7 = [8]_7 = [1]_7 = \{\ldots, -20, -13, -6, 1, 8, 15, 22, 29, 36, 43, \ldots\}$. Dies ist Anlass, auf der Menge der Restklassen $\mathbb{Z}/(n)$ zwei Operatoren zu definieren:

Definition 2.4 *Auf der Menge der Restklassen $\mathbb{Z}/(n)$ mit $a, b \in \mathbb{Z}$ sind die zwei Operatoren $\oplus$ und $\odot$ wie folgt definiert:*

- $\oplus : [a]_n \oplus [b]_n = [a+b]_n$
- $\odot : [a]_n \odot [b]_n = [a \cdot b]_n$

Nach Satz 2.1 Punkte 4 sind diese Verknüpfungen eindeutig definiert, a bzw. b können beliebige Elemente (ganze Zahlen) aus der jeweiligen Restklasse sein. Zusammen mit diesen beiden Verknüpfungen bildet die Menge der Restklassen $\mathbb{Z}/(n)$ einen kommutativen Ring $(\mathbb{Z}/(n), \oplus, \odot, [0]_n, [1]_n)$ mit additivem Einselement $[0]_n$ und multiplikativem Einselement $[1]_n$. Auf den Beweis wird an dieser Stelle verzichtet, er ergibt sich unmittelbar aus den Ringeigenschaften von $\mathbb{Z}$.

Aus Definition 2.4 ergibt sich ebenfalls unmittelbar, dass durch die Abbildung $f_n : \mathbb{Z} \to \mathbb{Z}/(n)$ mit $f_n(x) = [x]_n$ ein Homomorphismus zwischen $\mathbb{Z}$ und $\mathbb{Z}/(n)$ gegeben ist, dass für $a, b \in \mathbb{Z}$ also gilt:

$$f_n(a+b) = f_n(a) \oplus f_n(b)$$
$$f_n(a \cdot b) = f_n(a) \odot f_n(b)$$

Weiter oben hatten wir bereits festgestellt, dass sich in jeder der n Restklassen genau ein Element aus der Menge $\mathbb{Z}_n$ befindet. Deshalb können wir eine bijektive Abbildung g_n von $\mathbb{Z}/(n)$ nach $\mathbb{Z}_n$ definieren, die jede der n Restklassen auf genau dieses Element abbildet, es gilt also beispielsweise:

$$g_n([2]_5) = 2$$
$$g_n([15]_4) = 3$$

Wir wollen jetzt untersuchen, welcher Zusammenhang zwischen einer Zahl $r \in \mathbb{Z}_n$ und der dazugehörigen Restklasse $[r]_n \in \mathbb{Z}/(n)$ mit $g_n([r]_n) = r$ besteht (zur Erinnerung: eine Restklasse ist wiederum eine Menge mit ganzen Zahlen als Elementen). Nach Definition von g_n ist $r \in [r]_n$, d.h. für alle Elemente $a \in [r]_n$ gilt $a \equiv_n r$, also $a = k \cdot n + r$ mit $k \in \mathbb{Z}$. Das heißt, r entspricht dem natürlichzahligen Divisionsrest, der bei allen Elementen der Restklasse $[r]_n$ bei Divison durch n übrigbleibt.

Wir definieren jetzt auf der Menge $\mathbb{Z}_n$ zwei Operatoren.

Definition 2.5 *Für $+_n$ und $\cdot_n : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ gilt mit $a, b \in \mathbb{Z}_n$:*

- $a +_n b = g_n([a+b]_n)$
- $a \cdot_n b = g_n([a \cdot b]_n)$

Die Menge $\mathbb{Z}_n$ bildet mit diesen beiden Verknüpfungen ebenfalls einen kommutativen Ring $(\mathbb{Z}_n, +_n, \cdot_n, 0, 1)$ mit additivem Einselement 0 und multiplikativem Einselement 1. Auf den Beweis wird auch hier verzichtet, er kann durch einfaches Nachrechnen geführt werden. Da sich aus Definition 2.5 mit Hilfe von Definition 2.4 unmittelbar $g_n([a]_n) +_n g_n([b]_n) = a +_n b = g_n([a]_n \oplus [b]_n)$ und $g_n([a]_n) \cdot_n g_n([b]_n) = a \cdot_n b = g_n([a]_n \odot [b]_n)$ ableiten lässt folgt, dass durch die bijektive Abbildung g_n ein Isomorphismus zwischen $\mathbb{Z}/(n)$ und $\mathbb{Z}_n$ gegeben ist. Insgesamt besteht also mit der Abbildung

f_n ein Homomorphismus zwischen $\mathbb{Z}$ und $\mathbb{Z}/(n)$ und mit der Abbildung g_n ein Isomorphismus zwischen $\mathbb{Z}/(n)$ und $\mathbb{Z}_n$. Dies bedeutet, dass mit der Abbildung $(g_n \circ f_n)$ ein Homomorphismus zwischen $\mathbb{Z}$ und $\mathbb{Z}_n$ gegeben ist. Wir definieren für die Abbildung $(g_n \circ f_n) : \mathbb{Z} \to \mathbb{Z}_n$ die Bezeichnung **mod n**. Die Abbildung $\bmod n$ bildet demzufolge jede ganze Zahl a auf ihren natürlichzahligen Divisionsrest bei Division durch n ab.
Zusammenfassend kann man also die drei wichtigen Punkte festhalten:

- Bei $(\mathbb{Z}_n, +_n, \cdot_n, 0, 1)$ handelt es sich um einen kommutativen Ring. Für die beiden Verknüpfungen $+_n$ und $\cdot_n : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ gilt:

$$a +_n b = (a + b) \bmod n$$
$$a \cdot_n b = (a \cdot b) \bmod n$$

- Zwischen diesem Ring und dem Ring der ganzen Zahlen besteht ein Homomorphismus, der durch die Abbildung $\bmod n : \mathbb{Z} \to \mathbb{Z}_n$ gegeben ist.
- Für zwei ganze Zahlen $a, b \in \mathbb{Z}$ gilt: $a \bmod n = b \bmod n \quad \Leftrightarrow \quad a \equiv_n b$

2.2 Rechengesetze

Aus der Homomorphismusbeziehung zwischen $\mathbb{Z}$ und $\mathbb{Z}_n$ ergeben sich nützliche Rechengesetze.

Satz 2.2 *Seien $n \in \mathbb{N}$ und $a, b \in \mathbb{Z}$. Dann gilt:*

$$(a + b) \bmod n = ((a \bmod n) + (b \bmod n)) \bmod n$$
$$(a \cdot b) \bmod n = ((a \bmod n) \cdot (b \bmod n)) \bmod n$$

Beweis:
Aufgrund der Homomorphismusbeziehung gilt:

$$(a + b) \bmod n = (a \bmod n) +_n (b \bmod n) = ((a \bmod n) + (b \bmod n)) \bmod n$$
$$(a \cdot b) \bmod n = (a \bmod n) \cdot_n (b \bmod n) = ((a \bmod n) \cdot (b \bmod n)) \bmod n \qquad \square$$

Satz 2.3 *Für $n \in \mathbb{N}$ und $a \in \mathbb{Z}$ gilt:*

$$(a \bmod n) \bmod n = a \bmod n$$

Beweis:
Falls $n = 1$, ist $a \bmod n = 0$ und $(a \bmod n) \bmod n = 0 \bmod n = 0$. Also ist die Gleichung für $n = 1$ erfüllt. Für $n > 1$ ist nach Satz 2.2 $a \bmod n = (a \cdot 1) \bmod n = ((a \bmod n) \cdot (1 \bmod n)) \bmod n = ((a \bmod n) \cdot 1) \bmod n = (a \bmod n) \bmod n \quad \square$

Mit Hilfe von Satz 2.3 ist eine Verallgemeinerung von Satz 2.2 möglich:

Satz 2.4 *Seien $n, k, j \in \mathbb{N}, k > j$, $a, b \in \mathbb{Z}$. Dann gilt:*

$$\begin{aligned}(a+b) \bmod n &= ((a \bmod n) + b) \bmod n = (a + (b \bmod n)) \bmod n \\ (a \cdot b) \bmod n &= ((a \bmod n) \cdot b) \bmod n = (a \cdot (b \bmod n)) \bmod n \\ (a^k) \bmod n &= ((a^{k-j} \bmod n) \cdot a^j) \bmod n \\ (a^k) \bmod n &= ((a \bmod n)^k) \bmod n\end{aligned}$$

Beweis:
Für die erste Gleichung ist mit Satz 2.2 und 2.3 $(a+b) \bmod n = ((a \bmod n) + (b \bmod n)) \bmod n = ((a \bmod n) \bmod n + (b \bmod n)) \bmod n = (a \bmod n + b) \bmod n$. Der umgekehrte Fall für b sowie für die Multiplikation (zweite Gleichung) folgt analog. Für die letzten beiden Gleichungen ist $(a^k) \bmod n = (a \cdot a^{k-1}) \bmod n = ((a \bmod n) \cdot a^{k-1}) \bmod n = (((a \bmod n) \cdot a^{k-2}) \cdot a) \bmod n = ((a \bmod n) \cdot (a \bmod n) \cdot a^{k-2}) \bmod n$. Durch rekursives Fortsetzen kommt man zu den beiden Gleichungen. □

Satz 2.5 *Seien $n, m \in \mathbb{N}$ mit $n \mid m$, $a \in \mathbb{Z}$. Dann gilt:*

$$(a \bmod m) \bmod n = a \bmod n$$

Beweis:
Nach Kapitel 2.1 ist $a \bmod m$ darstellbar als $a + k \cdot m$ für ein $k \in \mathbb{Z}$. Daraus folgt $(a + k \cdot m) \bmod n = (a + (k \cdot m) \bmod n) \bmod n = (a + 0) \bmod n = a \bmod n$. □

Eine wichtige Folgerung dieser Sätze ist, dass man bei einem Ausdruck der Form $(\ldots) \bmod n$ mit $n \in \mathbb{N}$ die mod$n$ Operation wahlweise auf beliebige Summanden bzw. Faktoren in der Klammer anwenden kann, bzw. allgemein jeden Summand/Faktor durch eine andere ganze Zahl aus der gleichen Restklasse ersetzen kann, ohne das Ergebnis zu verändern.

Beispiele

- $(364 \cdot 489 \cdot 88) \bmod 5 = ((364 \bmod 5) \cdot (489 \bmod 5) \cdot (88 \bmod 5)) \bmod 5 = (4 \cdot 4 \cdot 3) \bmod 5 = 3$
- $(10 + 4 \cdot 52 + 67^5) \bmod 13 = (10 + 4 \cdot (52 \bmod 13) + (67 \bmod 13)^5) \bmod 13 = (10 + 0 + 2^5) \bmod 13 = 42 \bmod 13 = 3$
- $(6 \cdot (5 + 58 \cdot 2)^{30}) \bmod 8 = (6 \cdot (5 + (58 \bmod 8) \cdot 2)^{30}) \bmod 8 = (6 \cdot (5 + 2 \cdot 2)^{30}) \bmod 8 = (6 \cdot 9^{30}) \bmod 8 = (6 \cdot (9 \bmod 8)^{30}) \bmod 8 = (6 \cdot 1^{30}) \bmod 8 = 6$
- $(47 \bmod 12) \bmod 3 = 47 \bmod 3 = 2$ (da $3 \mid 12$)
- $(31 \cdot 23) \bmod 32 = ((-1) \cdot (-9)) \bmod 32 = 9 \bmod 32 = 9$ (da $(-1) \equiv_{32} 31$ und $(-9) \equiv_{32} 23$)

Diese Rechengesetze werden in den weiteren Kapiteln sehr häufig (oft ohne explizit erwähnt zu werden) verwendet. Da sie, wie in den Beispielen gesehen, zum Teil drastische Vereinfachungen ermöglichen ist es für einen sinnvollen Umgang mit modularer Arithmetik empfehlenswert, sie möglichst zu verinnerlichen.

2.3 Effizientes modulares Potenzieren

In der modularen Arithmetik ist es möglich, Ausdrücke der Form $(a^m) \bmod n$, mit $a \in \mathbb{Z}$ und $m, n \in \mathbb{N}$, effizient zu berechnen, insbesondere ohne den Wert von a^m auszurechnen. Die allgemeine Vorgehensweise soll exemplarisch an einem konkreten Beispiel verdeutlicht werden: Gesucht ist das Ergebnis des Ausdrucks $(19^{100}) \bmod 13$. Würde man anfangen und als Erstes versuchen 19^{100} auszurechnen, wäre man eine Weile beschäftigt (ein Schultaschenrechner ist hier bereits nutzlos). Zum Glück ist dies nicht notwendig. Als Erstes kann man den Ausdruck mit den kennengelernten Rechengesetzen vereinfachen zu $(19^{100}) \bmod 13 = ((19 \bmod 13)^{100}) \bmod 13 = (6^{100}) \bmod 13$. Nun halbieren wir wie folgt iterativ den Exponenten:

$$
\begin{aligned}
(6^{100}) \bmod 13 &= (36^{50}) \bmod 13 = ((36 \bmod 13)^{50}) \bmod 13 = (10^{50}) \bmod 13 \\
&= (100^{25}) \bmod 13 = ((100 \bmod 13)^{25}) \bmod 13 = (9^{25}) \bmod 13 \\
&= (9 \cdot 81^{12}) \bmod 13 = (9 \cdot (81 \bmod 13)^{12}) \bmod 13 = (9 \cdot 3^{12}) \bmod 13 \\
&= (9 \cdot 9^{6}) \bmod 13 \\
&= (9 \cdot 81^{3}) \bmod 13 = (9 \cdot (81 \bmod 13)^{3}) \bmod 13 = (9 \cdot 3^{3}) \bmod 13 \\
&= (9 \cdot 3 \cdot 3^{2}) \bmod 13 = (27 \cdot 3^{2}) \bmod 13 = ((27 \bmod 13) \cdot 3^{2}) \bmod 13 \\
&= (1 \cdot 3^{2}) \bmod 13 = \mathbf{9}
\end{aligned}
$$

Bemerkenswert ist, dass wir auf diese Weise die Berechnung von $(a^m) \bmod n$ in eine Reihe von Operationen vom Typ $x \bmod n$ zerlegen können, bei denen x unabhängig von Basis a und Exponent m sicher immer kleiner n^2 ist, was im Falle unseres Beispiels sogar eine Berechnung von Hand und ohne Taschenrechner ermöglicht.

3 Modulare Inverse

Bei vielen kryptographischen Verfahren steht man früher oder später vor folgender Problemstellung:
Zu gegebenen Zahlen $a \in \mathbb{Z}$ und $n \in \mathbb{N}$ ist eine Zahl $x \in \mathbb{Z}$ gesucht, für die gilt:

$$(a \cdot x) \bmod n = 1 \tag{1}$$

Ziel dieses Abschnitts ist es, zu untersuchen unter welchen Bedingungen Lösungen dieser Gleichung existieren und wie diese berechnet werden können. Es ist leicht ersichtlich, dass gilt:

Satz 3.1 *Seien $a \in \mathbb{Z}$, $n \in \mathbb{N}$, $x \in \mathbb{Z}_n$ und $x' \in [x]_n$. Dann gilt:*

$$(a \cdot x) \bmod n = 1 \Leftrightarrow (a \cdot x') \bmod n = 1$$

Beweis:
Mit Hilfe von Satz 2.4 folgt:

$$\begin{aligned} \Rightarrow: &\quad (a \cdot x') \bmod n = (a \cdot (x' \bmod n)) \bmod n = (a \cdot x) \bmod n = 1 \\ \Leftarrow: &\quad (a \cdot x) \bmod n = (a \cdot (x' \bmod n)) \bmod n = (a \cdot x') \bmod n = 1 \end{aligned}$$ □

Der Satz soll anhand zweier Beispiele verdeutlicht werden:

- Aus der Lösung $x = 2 \in \mathbb{Z}_5$ der Gleichung $(3 \cdot x) \bmod 5 = 1$ folgt, dass auch die Zahlen 7, 12, 17, 22 ... $\in \mathbb{Z}$ Lösungen sind.
- Aus der Lösung $x = 24 \in \mathbb{Z}$ der Gleichung $(4 \cdot x) \bmod 5 = 1$ folgt, dass auch $24 \bmod 5 = 4 \in \mathbb{Z}_5$ eine Lösung ist.

Aus der Existenz einer Lösung $x \in \mathbb{Z}$ von Gleichung (1) folgt also sofort die Existenz unendlich vieler weiterer Lösungen in $\mathbb{Z}$. Das Entscheidende ist aber, dass man die Suche nach Lösungen in $\mathbb{Z}$ auf die Suche nach Lösungen in $\mathbb{Z}_n$ reduzieren kann. Aus diesem Grund behandelt der Rest des Kapitels nur noch die Frage nach einer Lösung $x \in \mathbb{Z}_n$ von Gleichung (1), welche als das **modulare Inverse von a modulo n** (auch geschrieben als $a^{-1} \bmod n$) bezeichnet wird.

3.1 Die Existenz eines modularen Inversen

Ob, und wenn ja, wie viele Lösungen $x \in \mathbb{Z}_n$ Gleichung (1) besitzt, klärt Satz 3.3. Davor muss allerdings noch ein weiterer Satz eingeführt werden.

Satz 3.2 *Seien $a \in \mathbb{Z}$, $n \in \mathbb{N}$ und ggT(a,n) = 1. Dann gilt für $i, j \in \mathbb{Z}_n$ mit $i \neq j$:*

$$(a \cdot i) \bmod n \neq (a \cdot j) \bmod n$$

Beweis:
Der Beweis erfolgt durch Widerspruch. Aus der Annahme $(a \cdot i) \bmod n = (a \cdot j) \bmod n$ folgt $a \cdot i - a \cdot j = a \cdot (i-j) = k \cdot n$ für ein $k \in \mathbb{Z}$. Da $ggT(a,n) = 1$, muss gelten: $n \mid (i-j)$ Dies ist für $i \neq j$ jedoch ein Widerspruch, da für $i, j \in \mathbb{Z}_n$ immer gilt: $-n < (i-j) < n$ □

Als Beispiel betrachten wir $(14 \cdot x) \bmod 5$ und setzen für x alle Zahlen aus $\mathbb{Z}_5$ ein:
$(14 \cdot 0) \bmod 5 = 0$
$(14 \cdot 1) \bmod 5 = 4$
$(14 \cdot 2) \bmod 5 = 3$
$(14 \cdot 3) \bmod 5 = 2$
$(14 \cdot 4) \bmod 5 = 1$
Man erkennt, dass die Ergebnisse alle paarweise verschieden sind.
An diesem Beispiel wird bereits eine für die nachfolgenden Betrachtungen essentielle Eigenschaft deutlich, die sich unmittelbar aus Satz 3.2 ergibt:

Korollar 3.1 *Für $a \in \mathbb{Z}$, $n \in \mathbb{N}$ mit ggT(a,n) = 1 ist die Abbildung $f : \mathbb{Z}_n \to \mathbb{Z}_n$ mit $f(x) = (a \cdot x) \bmod n$ eine Permutation, d.h zu jedem Element $x_1 \in \mathbb{Z}_n$ existiert **genau** ein $x_2 \in \mathbb{Z}_n$, das durch f auf x_1 abgebildet wird.*

Beweis:
Nach Satz 3.2 ist die Abbildung injektiv. Da Urbild- und Bildemenge identisch sind und somit gleiche (und endliche) Kardinalität haben ist sie damit zwangsweise auch surjektiv, was sie insgesamt zu einer Permutation macht. □

Damit kann nun die Frage nach den Bedingungen für die Lösbarkeit von Gleichung (1) beantwortet werden.

Satz 3.3 *Seien $a \in \mathbb{Z}, n \in \mathbb{N}$, $n \geq 2$ und $g = ggT(a, n) \in \mathbb{N}$. Dann gilt für die Gleichung $(a \cdot x) \bmod n = 1$ **in Abhängigkeit von g**:*

- ***g ≠ 1***
  *Die Gleichung $(a \cdot x) \bmod n = 1$ besitzt **keine** Lösung $x \in \mathbb{Z}_n$ und ist damit insgesamt in $\mathbb{Z}$ unlösbar*
- ***g = 1***
  *Die Gleichung $(a \cdot x) \bmod n = 1$ besitzt **genau eine Lösung** $x \in \mathbb{Z}_n$ und es gilt: $ggT(x,n) = 1$*

Beweis:
Zuerst wird der Fall $g \neq 1$ betrachtet. Angenommen es existiert eine Lösung $x \in \mathbb{Z}_n$ der Gleichung, dann folgt daraus $(a \cdot x - k \cdot n) = 1$ für ein $k \in \mathbb{Z}$. Dies ergibt $g \cdot (\frac{a}{g} \cdot x - k \cdot \frac{n}{g}) = 1$, also $g \mid 1$, was für $g \neq 1$ einen Widerspruch bedeutet.
Als nächstes der Fall $g = 1$. Da $1 \in \mathbb{Z}_n$, exsitiert nach Korollar 3.1 genau ein $x \in \mathbb{Z}_n$, für das $(a \cdot x) \bmod = 1$ erfüllt ist. Dass für dieses x $ggT(n,x) = 1$ gelten muss, wird durch Widerspruch gezeigt. Sei $h = ggT(n,x) \in \mathbb{N}$. Weiterhin ist x eine Lösung von

$(a \cdot x) \text{mod} = 1$. Analog zum Fall $g = 1$ bedeutet dies nun, dass gilt: $a \cdot x - k \cdot n = 1$ für ein $k \in \mathbb{Z}$. Das bedeutet $h \cdot (a \cdot \frac{x}{h} - k \cdot \frac{n}{h}) = 1$, also $h \mid 1$, was für $h \neq 1$ wieder einen Widerspruch bedeutet, also $h = ggT(x, n) = 1$ impliziert. $\square$

Wir können nun also sagen, unter welchen Bedingungen das modulare Inverse zu einer gegebenen ganzen Zahl a existiert. Außerdem gewinnen wir aus Satz 3.3 zwei weitere wichtige Erkenntnisse:

- Zu einer ganzen Zahl a mit $ggT(a, n) = 1$ kommen nur die Elemente aus $\mathbb{Z}_n$ als modulare Inverse modulo n in Frage, die teilerfremd zu n sind, also nur die Elemente aus $\mathbb{Z}_n^*$
- Im Umkehrschluss bedeutet dies, dass nicht alle Elemente aus $\mathbb{Z}_n$ modulare Inverse modulo n besitzen, sondern nur die Elemente aus $\mathbb{Z}_n^*$.

Diese Erkenntnisse sollen an zwei Beispielen demonstriert werden:
Beispiel 1
Wir suchen das Inverse von 25 modulo 18 (auch geschrieben als $25^{-1} \text{ mod } 18$), also ein $x \in \mathbb{Z}_{18}$, das die Gleichung $(25 \cdot x) \text{ mod } 18 = 1$ erfüllt. Da 25 und 18 teilerfremd sind, wissen wir, dass ein Inverses in $\mathbb{Z}_{18}$ existiert. Außerdem wissen wir, dass dieses Inverse in der Menge $\mathbb{Z}_{18}^* = \{1, 5, 7, 11, 13, 17\}$ enthalten sein muss. Statt die Zahlen von 0 bis 18 durchzuprobieren genügt es also, in der Menge $\{1, 5, 7, 11, 13, 17\}$ zu suchen, wo wir $25^{-1} \text{ mod } 18 = 13$ finden.
Beispiel 2
Wir suchen die Inversen von 4 und 5 modulo 6 ($4^{-1} \text{ mod } 6$ bzw. $5^{-1} \text{ mod } 6$). Da $ggT(4, 6) = 2$, die Zahlen 4 und 6 somit nicht teilerfremd sind, wissen wir dass $4^{-1} \text{ mod } 6$ nicht existiert. Zur Demonstration probieren wir trotzdem exemplarisch die Zahlen von 0 bis 5 durch.
$(4 \cdot 0) \text{ mod } 6 = 0$
$(4 \cdot 1) \text{ mod } 6 = 4$
$(4 \cdot 2) \text{ mod } 6 = 2$
$(4 \cdot 3) \text{ mod } 6 = 0$
$(4 \cdot 4) \text{ mod } 6 = 4$
$(4 \cdot 5) \text{ mod } 6 = 2$
Für $5^{-1} \text{ mod } 6$ hingegen ist $ggT(5, 6) = 1$ und $5^{-1} \text{ mod } 6 = 5 \in \mathbb{Z}_6^* = \{1, 5\}$.

3.1.1 Die Berechnung des ggT mit Hilfe des euklidschen Algorithmus

Da die Frage nach der Existenz eines modularen Inversen an die Frage nach der Teilerfremdheit zweier Zahlen geknüpft ist, ist es sinnvoll, an dieser Stelle einen Algorithmus vorzustellen, mit dem der größte gemeinsame Teiler zweier Zahlen berechnet werden kann. Es handelt sich dabei um den **euklidschen Algorithmus**[1]. In Pseudocode lautet

[1] benannt nach dem antiken griechischen Mathematiker Euklid (ca. 300 v.Chr.), und damit einer der ältesten bekannten Algorithmen überhaupt

der euklidsche Algorithmus wie folgt:

Algorithmus 3.1
Eingabe: $n, a \in \mathbb{N}$
Ausgabe: $d = ggT(n, a) \in \mathbb{N}$
begin
$g_0 := n$;
$g_1 := a$;
$i := 1$;
while $g_i \neq 0$ **do**
$g_{i+1} := g_{i-1} \bmod g_i$;
$i := i + 1$;
end;
$d := g_{i-1}$;
end;

Beweis der Korrektheit:
Zuerst wird gezeigt, dass der Algorithmus terminiert. Da g_2 das Ergebnis einer $\bmod g_1$ Operation ist, muss $g_2 \in \{0, \ldots, g_1 - 1\}$, also echt kleiner als $g_1 = a$ sein. Für alle anderen g_{i+1} gilt ebenfalls, dass sie das Ergebnis einer $\bmod g_i$ Operation sind. Also gilt für alle $i \in \mathbb{N}$: $0 \leq g_{i+1} < g_i$. Also muss die Abbruchbedingung zwangsweise irgendwann erreicht werden und der Algorithmus somit terminieren.
Jetzt muss noch bewiesen werden, dass das Ergebnis des Algorithmus tatsächlich der ggT von a und n ist. Dazu benötigen wir den folgenden

Satz 3.4 *Sei $a, b \in \mathbb{N}$, $b < a$. Dann gilt:*

- $b \mid a \Rightarrow ggT(a,b) = b$
- $b \nmid a \Rightarrow ggT(a,b) = ggT(a \bmod b,\ b)$

Beweis:
Im ersten Fall is b ein Teiler von a. Trivialerweise ist b auch Teiler von sich selbst. Also ist b gemeinsamer Teiler von a und b. Da ein Teiler von b niemals größer sein kann als b, ist b zugleich $ggT(a, b)$.
Um den zweiten Fall zu beweisen muss man zeigen, dass jeder gemeinsame Teiler von a und b auch ein gemeinsamer Teiler von $(a \bmod b)$ und b ist und umgekehrt (Beweisidee nach [3], Lemma 3.15). Sei nun $d \in \mathbb{N}$ ein beliebiger Teiler von a und b, $r \in \mathbb{N}$ mit $r = a \bmod b$. Dann ist $r = a - k \cdot b$ für ein $k \in \mathbb{N}$. Also ist $r = d \cdot (\frac{a}{d} - k \cdot \frac{b}{d})$, also $d \mid r$. Ist nun umgekehrt d ein gemeinsamer Teiler von r und b (weiterhin ist $r = a \bmod b$), dann ist $a = k \cdot b + r$ für ein $k \in \mathbb{N}$. Daraus folgt $a = d \cdot (k \cdot \frac{b}{d} + \frac{r}{d})$, also $d \mid a$. $\square$

Mit Hilfe von Satz 3.4 können wir den Korrektheitsbeweis fortführen. Zu Beginn des Algorithmus wird g_0 mit n, und g_1 mit a initialisiert. Wenn $a = n$ terminiert der Algorithmus nach einem Schleifendurchlauf und liefert korrekterweise a als Ergebnis zurück. Falls

$a < n$, so gilt nach Satz 3.4 Punkt 2, solange sich der Algorithmus in der Schleife befindet: $\text{ggT}(g_{i+1}, g_i) = \text{ggT}(g_i, g_{i-1})$, also rekursiv für alle $i \in \mathbb{N}$ $ggT(g_{i+1}, g_i) = ggT(a, n)$. Falls $a > n$ muss beachtet werden, dass als erstes ein zusätzlicher Schleifendurchlauf nötig ist, der $g_2 = n$ setzt (also die Reihenfolge von a und n vertauscht und die Kleinere von beiden nach vorne setzt). In diesem Fall gilt aber ebenfalls $ggT(g_0, g_1) = ggT(g_1, g_2)$, die Korrektheit des Algorithmus bis zum Schleifenabbruch bleibt davon also unbeeinflusst. Angenommen die Schleife wird nun bei einem bestimmten Index $j \in \mathbb{N}$ verlassen. Dies bedeutet $g_j = 0$, also $g_{j-2} \bmod g_{j-1} = 0$, mit $g_{j-2} > g_{j-1}$. Mit Satz 3.4 Punkt 1 ergibt sich $ggT(g_{j-2}, g_{j-1}) = g_{j-1}$, und über die rekursive Beziehung folgt daraus: $ggT(a, n) = g_{j-1}$. Damit ist die Korrektheit des euklidschen Algorithmus bewiesen. □

Beispieldurchlauf:
gesucht: ggT(18,30)
$g_0 = 18$
$g_1 = 30$
$g_2 = 18 \bmod 30 = 18$
$g_3 = 30 \bmod 18 = 12$
$g_4 = 18 \bmod 12 = \mathbf{6}$
$g_5 = 12 \bmod 6 = 0$
Beim Index 5 wird die Schleife verlassen und der Algorithmus liefert $g_4 = 6$ als ggT der Zahlen 18 und 30.

3.2 Die Berechnung des modularen Inversen

Nach dem vorherigen Abschnitt wissen wir jetzt also, unter welchen Bedingungen zu einer ganzen Zahl a das modulare Inverse bezüglich einer natürlichen Zahl n existiert. Wir haben auch eine triviale Möglichkeit kennengelernt, wie man das modulare Inverse im Falle der Existenz finden kann. Diese bestand darin, einfach alle in Frage kommenden Zahlen, also alle Elemente aus $\mathbb{Z}_n^*$ durchzuprobieren. Im Fall des Beispiels des vorherigen Abschnitts, als das Inverse von 35 modulo 18 gesucht war, war dieses Vorgehen noch mit vertretbarem Aufwand verbunden. Für praktische Zwecke ist dies jedoch nicht geeignet, da zum Einen in der Praxis die Zahl n in einer anderen Größenordnung als 18 liegt. Außerdem muss die Zahl n sehr häufig als Primzahl gewählt werden, so dass dann theoretisch alle Zahlen von 1 bis $n-1$ als modulare Inverse in Frage kommen. Glücklicherweise gibt es Möglichkeiten, die Bestimmung des modularen Inversen effizienter durchzuführen. Deren mathematische Grundlage sowie deren Anwendung sind Thema dieses Abschnitts.

3.2.1 Berechnung des modularen Inversen mit dem Satz von Euler

Definition 3.1 *Sei $n \in \mathbb{N}$. Dann wird mit $\varphi(n)$ die euler'sche φ-Funktion bezeichnet. Der Wert $\varphi(n)$ entspricht der Anzahl der Zahlen in $\mathbb{Z}_n$, die teilerfremd zu n sind. Also ist $\varphi(n) = \mid \mathbb{Z}_n^* \mid$.*

Satz 3.5 (Satz von Euler) *Sei $a \in \mathbb{Z}, n \in \mathbb{N}$ und ggT(a,n) = 1. Dann gilt:*

$$a^{\varphi(n)} \bmod n = 1$$

Beweis:

$$(a^{\varphi(n)} \cdot \prod_{x \in \mathbb{Z}_n^*} x) \bmod n \tag{2}$$

$$= (\prod_{x \in \mathbb{Z}_n^*} (a \cdot x)) \bmod n \tag{3}$$

$$= (\prod_{x \in \mathbb{Z}_n^*} ((a \cdot x) \bmod n)) \bmod n \tag{4}$$

$$= (\prod_{x \in \mathbb{Z}_n^*} x \bmod n) \bmod n \tag{5}$$

$$= (\prod_{x \in \mathbb{Z}_n^*} x) \bmod n \tag{6}$$

Begründung der einzelnen Schritte:
Die Äquivalenz von (3) und (4), (5) und (6) folgt aus Satz 2.2. Der Schritt von (2) nach (3) ist damit begründet, dass $a^{\varphi(n)}$ und $\prod_{x \in \mathbb{Z}_n^*} x$ beide aus $\varphi(n)$ Faktoren bestehen, und somit immer ein a mit einem x zu einem Faktor zusammengefasst werden kann. Die Äquivalenz von (4) und (5) resultiert aus zwei Gründen. Da a und x teilerfremd zu n sind, ist auch $(a \cdot x)$ teilerfremd zu n und damit nach Satz 3.4 (Punkt 2) auch $(a \cdot x) \bmod n$. Also ist $(a \cdot x) \bmod n \in \mathbb{Z}_n^*$. Daraus leitet sich mit Satz 3.2 ab, dass $(a \cdot x) \bmod n$ für $x \in \mathbb{Z}_n^*$ eine Permutation auf $\mathbb{Z}_n^*$ ist, dass also gilt:

$$\prod_{x \in \mathbb{Z}_n^*} ((a \cdot x) \bmod n) = \prod_{x \in \mathbb{Z}_n^*} x$$

Somit ergibt sich aus der Gleichheit von (2) und (6) insgesamt

$$(a^{\varphi(n)} \cdot \prod_{x \in \mathbb{Z}_n^*} x) \bmod n = (\prod_{x \in \mathbb{Z}_n^*} x) \bmod n$$

Dies bedeutet für ein $k_1 \in \mathbb{Z}$

$$(a^{\varphi(n)} \cdot \prod_{x \in \mathbb{Z}_n^*} x) - \prod_{x \in \mathbb{Z}_n^*} x = k_1 \cdot n$$

also

$$(a^{\varphi(n)} - 1) \cdot \prod_{x \in \mathbb{Z}_n^*} x = k_1 \cdot n$$

Da alle $x \in \mathbb{Z}_n^*$ teilerfremd zu n sind, ist auch $\prod_{x \in \mathbb{Z}_n *} x$ teilerfremd zu n, woraus für ein $k_2 \in \mathbb{Z}$ folgt

$$a^{\varphi(n)} - 1 = k_2 \cdot n$$

also

$$a^{\varphi(n)} = k_2 \cdot n + 1$$

Dies ist gleichbedeutend mit

$$a^{\varphi(n)} \bmod n = 1 \qquad \square$$

Falls n eine Primzahl ist folgt aus dem Satz von Euler unmittelbar der

Satz 3.6 (Satz von Fermat) *Sei $a \in \mathbb{Z}$, $p \in \mathbb{N}$ eine Primzahl und ggT(a,p) = 1. Dann gilt:*

$$a^{p-1} \bmod p = 1$$

Beweis:
Falls p eine Primzahl ist, sind alle Elemente aus $\{1, \ldots, p-1\}$ teilerfremd zu p, also $\mathbb{Z}_p^* = \{1, \ldots, p-1\}$, und damit $\varphi(p) = \mid \mathbb{Z}_p^* \mid = p - 1$. Mit dem Satz von Euler ergibt sich damit $a^{p-1} = 1$. $\square$

Der Beweis des Satz von Euler ist zugegebenermaßen etwas langatmig, aber durch seine Bedeutung gerechtfertigt. Dank ihm steht uns nun eine Formel zur Verfügung mit der wir das modulare Inverse einer ganzen Zahl sofort berechnen können.

Satz 3.7 *Sei $a \in \mathbb{Z}$, $n \in \mathbb{N}$ mit ggT(a,n) = 1. Dann gilt für das modulare Inverse $a^{-1} \bmod n$ von a:*

$$a^{-1} \bmod n = a^{\varphi(n)-1} \bmod n$$

Beweis:
Nach dem Satz von Euler gilt: $(a \cdot a^{\varphi(n)-1}) \bmod n = a^{\varphi(n)} \bmod n = 1 \qquad \square$

Dank Satz 3.7 haben wir nun die Möglichkeit, das modulare Inverse explizit mit Hilfe einer geschlossenen Formel zu berechnen.

Beispiele:

- Wir wollen erneut das Inverse von 25 modulo 18 berechnen, diesmal unter Zuhilfenahme von Satz 3.7. $\mathbb{Z}_{18}^* = \{1, 5, 7, 11, 13, 17\}$, also $\varphi(18) = 6$. Damit erhalten wir $25^{-1} \bmod 18 = 25^{6-1} \bmod 18 = 25^5 \bmod 18 = 13$.
- Noch praktischer ist Satz 3.7 bei der Berechnung des Inversen von 23 modulo 71. Da 71 eine Primzahl ist sind alle Zahlen von 1 bis 70 mögliche Inverse. Mit Satz 3.7 erhalten wir mit $\varphi(71) = 71 - 1 = 70$ für $23^{-1} \bmod 71$:
  $23^{-1} \bmod 71 = 23^{70-1} \bmod 71 = 23^{69} \bmod 71 = 34$.

3.2.2 Berechnung des modularen Inversen mit dem erweiterten euklidschen Algorithmus

Die Berechnung des modularen Inversen $a^{-1} \bmod n$ mit Hilfe von Satz 3.7 hat den Nachteil, dass der Wert von $\varphi(n)$ bekannt sein muss. Wenn n keine Primzahl ist (falls n prim ist, ist $\varphi(n) = n - 1$), ist die Berechnung von $\varphi(n)$ unter Umständen relativ aufwändig. Es gibt allerdings eine alternative Möglichkeit, die eine modifizierte Form des euklidschen Algorithmus benutzt (erweiterter euklidscher Algorithmus). Die Erweiterung besteht darin, dass man, nachdem man sich im Algorithmus iterativ von den Startwerten zum ggT heruntergearbeitet hat, nicht abbricht, sondern sich rekursiv zu den Startwerten zurückarbeitet und damit eine Darstellung erhält, die allgemein in Satz 3.8 beschrieben wird.

Satz 3.8 *Seien n, $a \in \mathbb{N}$, mit $n > a$. Dann liefert der erweiterte euklidsche Algorithmus in allgemeiner Form die drei Werte $g \in \mathbb{N}$ und $u, v \in \mathbb{Z}$ als Resultat zurück, so dass gilt:*

$$g = ggT(n, a)$$
$$g = u \cdot n + v \cdot a$$

Im Fall, dass $ggT(a, n) = 1$ ist, erhält man also die Gleichung $u \cdot n + v \cdot a = 1$. Daraus leitet sich ab:

$$(u \cdot n + v \cdot a) \bmod n = 1 \bmod n = 1$$
$$((u \cdot n) \bmod n + (v \cdot a) \bmod n) \bmod n = 1$$
$$((v \cdot a) \bmod n) \bmod n = 1$$
$$(v \cdot a) \bmod n = 1$$

Der Rückgabewert $v \in \mathbb{Z}$ ist somit ein modulares Inverses von a modulo n. Der Wert $v \bmod n$ liefert also das modulare Inverse $a^{-1} \bmod n \in \mathbb{Z}_n$.
Eine modifizierte Version des erweiterten euklidschen Algorithmus, die statt g, u, und v nur das modulare Inverse als Resultat zurückliefert lautet in Pseudocodeschreibweise:

Algorithmus 3.2
Eingabe: $n, a \in \mathbb{N}$, $n > a$ und $ggT(a, n) = 1$
Ausgabe: $x = a^{-1} \bmod n \in \mathbb{Z}_n$
begin
$g_0 := n$; $g_1 := a$;
$u_0 := 1$; $v_0 := 0$;
$u_1 := 0$; $v_1 := 1$;
$i := 1$;
while $g_i \neq 0$ **do**
$y := g_{i-1}$ div g_i;
$g_{i+1} := g_{i-1} - y \cdot g_i$; (oder anders: $g_{i+1} := g_{i-1} \bmod g_i$)
$u_{i+1} := u_{i-1} - y \cdot u_i$;
$v_{i+1} := v_{i-1} - y \cdot v_i$;

$i := i + 1$;
end
$x := v_{i-1} \bmod n$;
end

Beweis von Satz 3.8 und der Korrektheit von Algorithmus 3.2:
Dass der Algorithmus terminiert ergibt sich mit der gleichen Begründung wie bei Algorithmus 3.1. Für die Korrektheit des Algorithmus wird über Induktion gezeigt, dass nach jedem Schleifendurchlauf die folgende Invariante gilt: $g_i = u_i \cdot n + v_i \cdot a$
Für die Startwerte $i = 0$ und $i = 1$ ist diese erfüllt:

$$g_0 = n = 1 \cdot n + 0 \cdot a$$
$$g_1 = a = 0 \cdot n + 1 \cdot a$$

Induktionsschritt für i+1:
Es gilt die Induktionsannahme:

$$g_{i-1} = u_{i-1} \cdot n + v_{i-1} \cdot a$$
$$g_i = u_i \cdot n + v_i \cdot a$$

Da $g_{i+1} = g_{i-1} \bmod g_i$ gesetzt wird und $y = g_{i-1} \operatorname{div} g_i$, gilt:

$$\begin{aligned} g_{i+1} &= g_{i-1} - y \cdot g_i \\ &= u_{i-1} \cdot n + v_{i-1} \cdot a - y \cdot (u_i \cdot n + v_i \cdot a) \\ &= (u_{i-1} - y \cdot u_i) \cdot n + (v_{i-1} - y \cdot v_i) \cdot a \end{aligned}$$

Damit die Invariante erfüllt ist, muss also gelten:

$$u_{i+1} = u_{i-1} - y \cdot u_i$$
$$v_{i+1} = v_{i-1} - y \cdot v_i$$

Genau mit diesen Werten werden die Variablen u_{i+1} und v_{i+1} aber in der Schleife belegt, was die Gültigkeit der Invariante zeigt. Da nach Beendigung der Schleife g_{i-1} analog zum einfachen euklidschen Algorithmus den ggT von a und n enthält gilt also:

$$ggT(a, n) = 1 = u_{i-1} \cdot n + v_{i-1} \cdot a$$

Algorithmus 3.2 hat also mit g_{i-1}, u_{i-1} und v_{i-1} die drei Zahlen berechnet, die die beiden Gleichungen aus Satz 3.8 erfüllen. Da diese Version aber nur das modulare Inverse berechnen soll, wird lediglich der Wert $v_{i-1} \bmod n \in \mathbb{Z}_n$ als Ergebnis zurückgegeben, womit Satz 3.8 und die Korrektheit von Algorithmus 3.2 bewiesen ist. □

Algorithmus 3.2 unterliegt der Einschränkung, dass a kleiner als n sein muss, also $a \in \mathbb{Z}_n$. Man kann ihn aber trotzdem ohne Probleme nutzen um das modualre Inverse zu jeder Zahl $a \in \mathbb{Z}$ zu berechnen, indem man statt direkt mit a, mit $a \bmod n$ in den Algorithmus

geht. Die Äquivalenz von $a^{-1} \bmod n$ und $(a \bmod n)^{-1} \bmod n$ folgt aus Satz 3.1.

Beispiel
Wir wollen den erweiterten euklidschen Algorithmus an einem Beispiel ausprobieren: Gesucht ist erneut das Inverse von 23 modulo 71. Die folgende Tabelle zeigt die Variablenbelegung der Schleifendurchläufe, die entscheidenden Werte sind fett markiert.

i	y	g_i	u_i	v_i
0	-	71	1	0
1	3	23	0	1
2	11	2	1	-3
3	2	**1**	**-11**	**34**
4	-	0	23	-71

Die fettgedruckten Werte liefern die Gleichung: $-11 \cdot 71 + 34 \cdot 23 = 1$, aus der wir unmittelbar $23^{-1} \bmod 71 = 34$ ablesen können.

3.3 Weitere für die Praxis relevante Formeln

Es müssen an dieser Stelle noch zwei Formeln vorgestellt werden, die in der Praxis in nahezu allen Gebieten der Kryptographie eine wichtige Rolle spielen. Inhaltlich gehört dieser Unterabschnitt eigentlich in Kapitel 2, die Beweise der Sätze setzen aber die Bekanntheit der Sätze dieses Kapitels voraus, so dass dies deswegen hier erfolgt.

Satz 3.9 *Sei $n \in \mathbb{N}$, $a \in \mathbb{Z}$ mit ggT(a,n) = 1. Außerdem seien r_1, $r_2 \in \mathbb{N}_0$ mit $r_1 \bmod \varphi(n) = r_2 \bmod \varphi(n)$. Dann gilt:*

$$a^{r_1} \bmod n = a^{r_2} \bmod n$$

Beweis:
Wir nehmen an, dass $r_1 > r_2$, der Fall $r_1 < r_2$ folgt umgekehrt analog (für $r_1 = r_2$ ist der Satz trivialerweise erfüllt). Das bedeutet, es gibt ein $k \in \mathbb{N}$ so dass $r_1 = r_2 + k \cdot \varphi(n)$. Daraus folgt $a^{r_1} \bmod n = a^{r_2 + k \cdot \varphi(n)} \bmod n = (a^{r_2} \cdot (a^{\varphi(n)})^k) \bmod n =$
$(a^{r_2} \cdot (a^{\varphi(n)} \bmod n)^k) \bmod n$. Nach Satz 3.5 ist der letzte Ausruck äquivalent zu
$(a^{r_2} \cdot 1^k) \bmod n$, womit sich insgesamt $a^{r_1} \bmod n = a^{r_2} \bmod n$ ergibt. □

Beispiel
Wir wollen den Ausdruck $(4^{200}) \bmod 9$ berechnen. Da $ggT(4, 9) = 1$ folgt mit $\varphi(9) = 6$ und Satz 3.9: $(4^{200}) \bmod 9 = (4^{200 \bmod \varphi(9)}) \bmod 9 = (4^{200 \bmod 6}) \bmod 9 = (4^2) \bmod 9 = 7$.

Satz 3.10 *Seien $e, n \in \mathbb{N}$ mit $ggT(e, \varphi(n)) = 1$. Dann ist die Abbildung $f : \mathbb{Z}_n^* \to \mathbb{Z}_n^*$ mit $f(x) = x^e \bmod n$ eine Bijektion. Für die Umkehrfunktion $f^{-1} : \mathbb{Z}_n^* \to \mathbb{Z}_n^*$ gilt: $f^{-1}(x) = x^d \bmod n$ mit $d = e^{-1} \bmod \varphi(n) \in \mathbb{Z}_{\varphi(n)}$.*

Beweis:
Zunächst zeigen wir, dass f auf $\mathbb{Z}_n^*$ abgeschlossen ist. Wenn $x \in \mathbb{Z}_n^*$, dann ist auch x^e teilerfremd zu n ($ggT(x^e, n) = 1$). Falls $x^e < n$ ist $x^e = x^e \bmod n$ und damit $x^e \bmod n \in \mathbb{Z}_n^*$. Falls $x^e > n$ folgt mit Satz 3.4 (Punkt 2) $ggT(x^e \bmod n, n) = ggT(x^e, n) = 1$, also $x^e \bmod n \in \mathbb{Z}_n^*$.
Als Nächstes zeigen wir, dass die Abbildung f in $\mathbb{Z}_n^*$ injektiv und damit auch bijektiv ist. Dazu nehmen wir an, es existieren $a, b \in \mathbb{Z}_n^*$ mit $a^e \bmod n = b^e \bmod n$. Außerdem sei $d = e^{-1} \bmod \varphi(n) \in \mathbb{Z}_n^*$. Dann folgt aus $a^e \bmod n = b^e \bmod n$

$$\begin{aligned}(a^e \bmod n)^d &= (b^e \bmod n)^d \\ (a^e \bmod n)^d \bmod n &= (b^e \bmod n)^d \bmod n \\ ((a^e)^d) \bmod n &= ((b^e)^d) \bmod n \\ a^{e \cdot d} \bmod n &= b^{e \cdot d} \bmod n\end{aligned}$$

woraus sich mit Satz 3.9 und $(e \cdot d) \bmod \varphi(n) = 1 \bmod \varphi(n)$

$$\begin{aligned}a^1 \bmod n &= b^1 \bmod n \\ a \bmod n &= b \bmod n\end{aligned}$$

ergibt. Für $a, b \in \mathbb{Z}_n^*$ ist $a \neq b$ somit ein Widerspruch.
Aus der obigen Gleichungsfolge kann man zudem die Gleichung $(a^e \bmod n)^d \bmod n = a \bmod n$ ableiten. Dies bedeutet aber $f^{-1}(f(a)) = a \bmod n = a$, womit auch unmittelbar folgt, dass f^{-1} die Umkehrfunktion von f ist. $\square$

4 Modulare Gleichungen

Wir wollen die Erkenntnisse des vorangegangenen Abschnitts erweitern. In Kapitel 3 haben wir uns mit der Lösung der Gleichung $(a \cdot x) \bmod n = 1$ für gegebene $a \in \mathbb{Z}$, $n \in \mathbb{N}$ und gesuchtes $x \in \mathbb{Z}_n$ beschäftigt. Nun ersetzen wir auf der rechten Seite der Gleichung die Zahl 1 durch eine Variable und erhalten für gegebene $a, b \in \mathbb{Z}$ und $n \in \mathbb{N}$ die allgemeine modulare Gleichung

$$(a \cdot x) \bmod n = b \bmod n \tag{7}$$

Das Lösen dieser Gleichung, also das Bestimmen aller $x \in \mathbb{Z}_n$, die diese Gleichung erfüllen, ist das Thema dieses Kapitels.

4.1 Lösen modularer Gleichungen

Wie viele Lösungen Gleichung (7) besitzt, hängt stark von den Variablen a, n und b ab. Alle möglichen Fälle sind in Satz 4.1 zusammengefasst.

Satz 4.1 *Seien a, $b \in \mathbb{Z}$, $n \in \mathbb{N}$, $n \geq 2$ und $g = ggT(a, n) \in \mathbb{N}$. Dann gilt in Abhängigkeit von b und g für die Gleichung*

$$(a \cdot x) \bmod n = b \bmod n$$

1. $\boldsymbol{g = 1}$
   Die Gleichung besitzt ***genau die eine Lösung*** $x = (a^{-1} \cdot b) \bmod n \in \mathbb{Z}_n$
2. $\boldsymbol{g \neq 1}$ ***und*** $\boldsymbol{g \nmid b}$
   Es existiert ***keine*** *Lösung $x \in \mathbb{Z}_n$*
3. $\boldsymbol{g \neq 1}$ ***und*** $\boldsymbol{g \mid b}$
   Es existieren in $\mathbb{Z}_n$ g Lösungen der Form

$$x_t = x_0 + t \cdot \frac{n}{g} \qquad t = 0, 1, 2, \ldots, g-1$$

$$\text{mit } x_0 = \left(\frac{b}{g} \cdot \left(\frac{a}{g}\right)^{-1}\right) \bmod \left(\frac{n}{g}\right)$$

Beweis:
Wir betrachten zunächst den Fall $g = 1$. Es ist $b \bmod n \in \mathbb{Z}_n$. Aus Satz 3.2 wissen wir daher, dass es genau ein $x \in \mathbb{Z}_n$ gibt, das über die Abbildung $f : \mathbb{Z}_n \to \mathbb{Z}_n$ mit $f(x) = (a \cdot x) \bmod n$ auf $b \bmod n$ abgebildet wird. Dass es sich dabei um $x = (a^{-1} \cdot b) \bmod n$ handelt, zeigen wir durch Einsetzen:

$$\begin{aligned}
&(a \cdot (a^{-1} \cdot b) \bmod n) \bmod n \\
&= (a \cdot a^{-1} \cdot b) \bmod n \\
&= ((a \cdot a^{-1}) \bmod n \cdot b) \bmod n \\
&= (1 \cdot b) \bmod n \\
&= b \bmod n
\end{aligned}$$

Damit ist Punkt 1 bewiesen.

Der Fall $g \neq 1$ ist etwas komplizierter. Wir nehmen an, dass $x \in \mathbb{Z}_n$ eine Lösung der Gleichung ist, dass also gilt: $(a \cdot x) \bmod n = b \bmod n$. Dies ist gleichbedeutend mit $(a \cdot x) - b = k_1 \cdot n$ für ein $k_1 \in \mathbb{Z}$, also $b = a \cdot x + k_1 \cdot n$. Da $g \mid a$ und $g \mid n$ folgt daraus $b = g \cdot (\frac{a}{g} \cdot x + k_1 \cdot \frac{n}{g})$, also $g \mid b$. Daran sehen wir sofort, dass keine Lösung existieren kann, wenn b nicht durch g teilbar ist (Punkt 2).

Im Weiteren wird deswegen nun $g \mid b$ angenommen. Um eine Aussage über das Lösungsverhalten zu machen, brauchen wir einen weiteren Satz, den wir an dieser Stelle einschieben.

Einschub
Satz 4.2 *Seien $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$, $g = ggT(a, n) \in \mathbb{N}$ und $g \mid b$. Dann gilt für alle $x \in \mathbb{Z}$:*

$$(a \cdot x) \bmod n = b \bmod n \quad \Leftrightarrow \quad \left(\frac{a}{g} \cdot x\right) \bmod \left(\frac{n}{g}\right) = \left(\frac{b}{g}\right) \bmod \left(\frac{n}{g}\right)$$

Beweis:
$\Rightarrow$: Angenommen x ist eine Lösung von $(a \cdot x) \bmod n = b \bmod n$. Dies ist gleichbedeutend mit $(a \cdot x) - b = k_2 \cdot n$ für ein $k_2 \in \mathbb{Z}$. Daraus folgt $(\frac{a}{g} \cdot x) - \frac{b}{g} = k_2 \cdot \frac{n}{g}$. Das bedeutet aber, dass $(\frac{a}{g} \cdot x) \bmod (\frac{n}{g}) = (\frac{b}{g}) \bmod (\frac{n}{g})$.
$\Leftarrow$: Angenommen x ist eine Lösung von $(\frac{a}{g} \cdot x) \bmod (\frac{n}{g}) = (\frac{b}{g}) \bmod (\frac{n}{g})$. Dies bedeutet, dass $(\frac{a}{g} \cdot x) - \frac{b}{g} = k_2 \cdot \frac{n}{g}$ für ein $k_2 \in \mathbb{Z}$, woraus aber folgt, dass $(a \cdot x) - b = k_2 \cdot n$, also $(a \cdot x) \bmod n = b \bmod n$. $\square$

Fortsetzung des Beweises von Satz 4.1:
Satz 4.2 bedeutet anschaulich, dass z.B. die Gleichung $(4 \cdot x) \bmod 6 = 10 \bmod 6$ mit $ggT(4, 6) = 2$ in $\mathbb{Z}$ die gleiche Lösungsmenge besitzt wie die Gleichung
$(2 \cdot x) \bmod 3 = 5 \bmod 3$, d.h. jede ganze Zahl x, die eine von beiden Gleichungen löst, ist auch Lösung der Anderen.

Dank Satz 4.2 haben wir also die Möglichkeit, die Lösungen der Gleichung
$(a \cdot x) \bmod n = b \bmod n$ zu bestimmen, indem wir die Lösungen der Gleichung
$(\frac{a}{g} \cdot x) \bmod (\frac{n}{g}) = (\frac{b}{g}) \bmod (\frac{n}{g})$ bestimmen, da beide Lösungsmengen in $\mathbb{Z}$ identisch sind. Dies ist insoweit ein Vorteil, als wir das Problem damit auf eine Gleichung reduziert haben, für die $ggT(\frac{a}{g}, \frac{n}{g}) = 1$ gilt, die also in $\mathbb{Z}_{(\frac{n}{g})}$ eindeutig lösbar ist. Nach Punkt 1 ist diese Lösung

$$x_0 = \left(\frac{b}{g} \cdot \left(\frac{a}{g}\right)^{-1}\right) \bmod \left(\frac{n}{g}\right) \quad \in \mathbb{Z}_{(\frac{n}{g})}$$

Damit sind nach Satz 3.1 allgemein alle Lösungen $x_t \in \mathbb{Z}$ der Gleichung
$(\frac{a}{g} \cdot x) \bmod (\frac{n}{g}) = (\frac{b}{g}) \bmod (\frac{n}{g})$, und damit von Gleichung (7) darstellbar als

$$x_t = x_0 + t \cdot \left(\frac{n}{g}\right) \qquad t \in \mathbb{Z}$$

Da wir aber nur an den Lösungen in $\mathbb{Z}_n$ interessiert sind, beschränken wir den Parameter t auf $0, \ldots, g-1$ und erhalten die Formel aus Punkt 3, die von allen Lösungen in $\mathbb{Z}$ diejenigen g Lösungen liefert, die in $\mathbb{Z}_n$ liegen. $\square$

Es ist höchste Zeit, Satz 4.1 an einigen Beispielen zu veranschaulichen:
Beispiel 1
Wir suchen die Lösungen $x \in \mathbb{Z}_9$ der Gleichung $(5 \cdot x) \bmod 9 = 6 \bmod 9$. Da $ggT(5,9) = 1$ wissen wir, dass genau eine Lösung existiert. Es ist $5^{-1} \bmod 9 = 2$ (siehe Kapitel 3). Damit ergibt sich mit Satz 4.1: $x = (2 \cdot 6) \bmod 9 = 3$. $3 \in \mathbb{Z}_9$ ist also die Lösung dieser modularen Gleichung.
Beispiel 2
Wir suchen die Lösungen $x \in \mathbb{Z}_{20}$ der Gleichung $(8 \cdot x) \bmod 20 = 9 \bmod 20$. Hier ist $g = ggT(8,20) = 4$, aber $4 \nmid 9$. Damit ist die Gleichung unlösbar.
Beispiel 3
Wir suchen die Lösungen $x \in \mathbb{Z}_{20}$ der Gleichung $(8 \cdot x) \bmod 20 = 12 \bmod 20$. Wieder ist $g = ggT(8,20) = 4$, diesmal ist aber $4 \mid 12$. Also existieren vier Lösungen in $\mathbb{Z}_{20}$. Nach Satz 4.2 ist diese Gleichung von der Lösungsmenge in $\mathbb{Z}$ äquivalent zur Gleichung $(2 \cdot x) \bmod 5 = 3 \bmod 5$ (alle Parameter werden durch $g = 4$ geteilt), die in $\mathbb{Z}_5$ aufgrund von $ggT(2,5) = 1$ eindeutig lösbar ist. Die Lösung lautet (Berechnung analog Beispiel 1): $x_0 = 4$. Daraus erhalten wir mit Satz 3.1, dass allgemein alle ganzen Zahlen der Form $x_k = 4 + k \cdot 5$ mit $k \in \mathbb{Z}$ Lösungen unserer modularen Gleichung sind, in diesem Fall also die Zahlen ..., -6, -1, **4**, **9**, **14**, **19**, 24, 29, 34, ...Aus dieser Menge nehmen wir uns mit den Zahlen 4, 9, 14 und 19 die vier Gesuchten heraus, die in $\mathbb{Z}_{20}$ liegen, also $x_0 = 4$, $x_1 = 9$, $x_2 = 14$ und $x_3 = 19$.
Anmerkung:
In diesem Beispiel wurde bewusst nicht einfach nur die Formel aus Satz 4.1 Punkt 3 angewendet, sondern es wurden noch einmal alle Schritte, die eine Seite zuvor zu dieser Formel geführt haben an einem konkreten Beispiel durchgegangen.
Beispiel 4
Wir suchen die Lösungen $x \in \mathbb{Z}_{10}$ der Gleichung $(4 \cdot x) \bmod 10 = 12 \bmod 10$. Da $ggT(4,10) = 2$ und $2 \mid 12$, existieren zwei Lösungen. Zuerst berechnen wir x_0. Es gilt: $x_0 = (\frac{12}{2} \cdot (\frac{4}{2})^{-1}) \bmod (\frac{10}{2}) = (6 \cdot 2^{-1}) \bmod 5$. Mit Kapitel 3 erhalten wir $2^{-1} \bmod 5 = 3$ und damit $x_0 = (6 \cdot 3) \bmod 5 = 3$. Allgemein gilt damit für die Lösungen: $x_t = x_0 + t \cdot \frac{10}{2}$ mit $t \in \{0, 1\}$, also $x_0 = 3$ und $x_1 = 8$.

4.2 Lösen modularer Gleichungen mit dem chinesischen Restsatz

Eine alternative Methode zum Lösen von Gleichung (7) besteht in der Anwendung des chinesischen Restsatzes. Dabei wird die zu lösende modulare Gleichung nach bestimm-

ten Regeln in mehrere modulare Gleichungen zerlegt. Eine gemeinsame Lösung all dieser Gleichungen ist dann zugeleich Lösung der gesuchten Gleichung (7). Damit der chinesische Restsatz hier anwendbar ist, ist es allerdings notwendig, unsere Problemstellung, das Lösen von Gleichung (7), etwas umzusgestalten.

Satz 4.3 *Seien $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$. Dann gilt für alle $x \in \mathbb{Z}$:*

$$(a \cdot x) \bmod n = b \bmod n \quad \Leftrightarrow \quad (a \cdot x - b) \bmod n = 0$$

Beweis:
Es gilt für ein $k \in \mathbb{Z}$:

$$(a \cdot x) \bmod n = b \bmod n \quad \Leftrightarrow \quad a \cdot x - b = k \cdot n \quad \Leftrightarrow \quad (a \cdot x - b) \bmod n = 0 \qquad \square$$

Das Lösen der modularen Gleichung (7) ist also gleichbedeutend mit dem Finden der modularen Nullstellen des Polynoms $f(x) = a \cdot x - b$.
Anmerkungen:

- *Von der Äquivalenz dieser beiden Gleichungen wird in den folgenden Sätzen mehrfach Gebrauch gemacht, ohne dass dies jedesmal explizit erwähnt wird.*
- *In den folgenden Sätzen wird nur der Sonderfall eines linearen Polynoms $f(x) = a \cdot x - b$ über $\mathbb{Z}$ betrachtet, da nur dies für unsere Problemstellung relevant ist. Die Sätze 4.4 und 4.5 gelten aber gleichermaßen auch für allgemeine Polynome höheren Grades über $\mathbb{Z}$.*

Damit ist der folgende Satz 4.4 anwendbar.

Satz 4.4 *Seien $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$ und $d_1, d_2, \ldots, d_t \in \mathbb{N}$, $t \in \mathbb{N}$, mit $n = d_1 \cdot d_2 \cdot \ldots \cdot d_t$ und $ggT(d_i, d_j) = 1$ für $i \neq j$. Dann gilt für $x \in \mathbb{Z}$:*

$$(a \cdot x - b) \bmod n = 0 \quad \Leftrightarrow \quad (a \cdot x - b) \bmod d_i = 0 \quad \textit{für alle } i \in \{1, \ldots, t\}$$

Beweis:
$\Rightarrow$: Beweis exemplarisch für d_1. Aus $n \mid (a \cdot x - b)$ folgt $(a \cdot x - b) = k_1 \cdot n = k_1 \cdot d_1 \cdot d_2 \cdot \ldots \cdot d_t = k_2 \cdot d_1$ für $k_1 \in \mathbb{Z}$, $k_2 = k_1 \cdot d_2 \cdot \ldots \cdot d_t \in \mathbb{Z}$. Also gilt $d_1 \mid (a \cdot x - b)$. Analog verfährt man für die anderen d_i.
$\Leftarrow$: Da $d_1 \mid (a \cdot x - b)$ ist $(a \cdot x - b) = k_1 \cdot d_1$ für ein $k_1 \in \mathbb{Z}$. Aus $d_2 \mid (a \cdot x - b) = k_1 \cdot d_1$ und $ggT(d_1, d_2) = 1$ folgt $d_2 \mid k_1$, also $k_1 = k_2 \cdot d_2$ für ein $k_2 \in \mathbb{Z}$. Dies ergibt $(a \cdot x - b) = k_2 \cdot d_1 \cdot d_2$. Dies kann man sukzessive für alle weiteren d_i durchführen, so dass man am Ende $(a \cdot x - b) = k_t \cdot d_1 \cdot d_2 \cdot \ldots \cdot d_t = k_t \cdot n$ erhält ($k_t \in \mathbb{Z}$), also $n \mid (a \cdot x - b)$. $\square$

Satz 4.4 bedeutet anschaulich, wenn eine Zahl z.B. durch 21 teilbar ist, dann ist sie auch durch 3 und durch 7 teilbar. Umgekehrt, wenn eine Zahl z.B. durch 8 und durch 9 teilbar ist, kann man sicher sagen, dass sie durch 72 teilbar ist. Man muss jedoch auf die Teilerfremdheit der einzelnen Faktoren achten. So ist eine Zahl, die durch 2 und durch 4 teilbar ist, nicht zwangsläufig durch 8 teilbar.

Um den chinesischen Restsatz anwenden zu können, ist jetzt noch ein letzter Schritt notwendig, der sich aus folgendem Satz ergibt.

Satz 4.5 *Seien* $a, b \in \mathbb{Z}$, $n, d_1, d_2, \ldots, d_t \in \mathbb{N}$, $t \in \mathbb{N}$, *mit* $ggT(d_i, d_j) = 1$ *für* $i \neq j$ *und* $n = d_1 \cdot d_2 \cdot \ldots \cdot d_t$. *Wir betrachten die Gleichung*

$$(a \cdot x - b) \bmod n = 0$$

und dazu die t *Gleichungen*

$$\begin{aligned}(a \cdot x - b) \bmod d_1 &= 0\\ (a \cdot x - b) \bmod d_2 &= 0\\ &\ldots\\ (a \cdot x - b) \bmod d_t &= 0\end{aligned}$$

Dann gilt für jedes $x \in \mathbb{Z}$*:*

$$(a \cdot x - b) \bmod n = 0 \quad \Leftrightarrow \quad x \bmod d_i = x_i \quad \textit{und} \quad (a \cdot x_i - b) \bmod d_i = 0$$

für alle $i \in \{1, \ldots, t\}$ und $x_i \in \mathbb{Z}_{d_i}$

Beweis:
$\Rightarrow$: Wir führen den Beweis für d_1. Für die anderen d_i verläuft er analog. Aus $(a \cdot x - b) \bmod n = 0$ folgt mit Satz 4.4 $(a \cdot x - b) \bmod d_1 = 0$, also $(a \cdot (x \bmod d_1) - b) \bmod d_1 = 0$. Dies bedeutet, dass mit $x_1 = x \bmod d_1$ die Gleichung $(a \cdot x_1 - b) \bmod d_1 = 0$ gilt.
$\Leftarrow$: Für alle $i \in \{1, \ldots, t\}$ gilt, dass aus der Annahme folgt: $(a \cdot x_i - b) \bmod d_i = (a \cdot (x \bmod d_i) - b) \bmod d_i = (a \cdot x - b) \bmod d_i = 0$. Mit Satz 4.4 ergibt sich damit $(a \cdot x - b) \bmod n = 0$. $\square$

Die Sätze 4.3 bis 4.5 sollen zusammengefasst auf ein konkretes Beispiel angewendet werden. Dazu greifen wir Beispiel 4 aus Kapitel 4.1 auf, gesucht sind also die Lösungen $x \in \mathbb{Z}_{10}$ der Gleichung $(4 \cdot x) \bmod 10 = 12 \bmod 10$. Zuerst zerlegen wir die Zahl 10 in die beiden teilerfremden Zahlen 2 und 5. Damit erhalten wir unter Anwendung von Satz 4.4 die beiden Gleichungen

$$\begin{aligned}(4 \cdot x) \bmod 2 &= 12 \bmod 2\\ (4 \cdot x) \bmod 5 &= 12 \bmod 5\end{aligned}$$

deren gemeinsame Lösungen wir suchen. Im Allgemeinen sind die auf diese Art entstehenden Gleichungen im Vergleich zur Ausgangsgleichung aufgrund der kleineren Module (hier 2 und 5 statt 10) einfacher zu lösen, was die Vorgehensweise rechtfertigt. Für die erste Gleichung erhalten wir in $\mathbb{Z}_2$ die Lösungsmenge $L_1 = \{0, 1\}$, für die zweite in $\mathbb{Z}_5$ die Lösungsmenge $L_2 = \{3\}$ (siehe Kapitel 4.1). Aus Satz 4.5 folgt jetzt, dass für alle

Lösungen $x \in \mathbb{Z}_{10}$ der Ausgangsgleichung entweder

$$x \bmod 2 = 0$$
$$x \bmod 5 = 3$$

oder

$$x \bmod 2 = 1$$
$$x \bmod 5 = 3$$

gelten muss. Wir erhalten also zwei modulare Gleichungssysteme. Jedes $x \in \mathbb{Z}_{10}$, das eines dieser beiden Gleichungssysteme löst, ist Lösung unserer Ausgangsgleichung. Die Anzahl der Gleichungssysteme, die man erhält hängt von der Anzahl der Lösungen der Einzelgleichungen ab, in die man die ursprüngliche Gleichung aufgespaltet hat. Für jede mögliche Kombination jeweils einer Lösung jeder Gleichung erhält man ein Gleichungssystem. In unserem Beispiel hat die erste Gleichung die beiden Lösungen 0 und 1, die Zweite die Lösung 3. Dies ergibt die beiden Gleichungssysteme mit 0 und 3 bzw. 1 und 3 auf der rechten Seite der Gleichungen.

Die modularen Gleichungssysteme können unabhängig voneinander mit dem chinesischen Restsatz gelöst werden.

Satz 4.6 (Chinesischer Restsatz) *Seien $n \in \mathbb{N}, d_1, d_2, \ldots d_t \in \mathbb{N}$, $x_1, x_2, \ldots, x_t \in \mathbb{Z}$, $t \in \mathbb{N}$ mit $n = d_1 \cdot d_2 \cdot \ldots \cdot d_t$ und $ggT(d_i, d_j) = 1$ für $i, j \in \{1, \ldots, t\}$ und $i \neq j$. Dann gilt: Das modulare Gleichungssystem*

$$x \bmod d_1 = x_1 \bmod d_1$$
$$x \bmod d_2 = x_2 \bmod d_2$$
$$\ldots$$
$$x \bmod d_t = x_t \bmod d_t$$

besitzt in $\mathbb{Z}_n$ **genau** eine Lösung. Diese berechnet sich zu

$$x = \left(\sum_{j=1}^{t} \frac{n}{d_j} \cdot y_j \cdot x_j \right) \bmod n$$

wobei

$$y_i = \left(\frac{n}{d_i} \right)^{-1} \bmod d_i$$

für alle $i \in \{1, \ldots, t\}$.

Hinweis: Um eventuellen Missverständnissen vorzubeugen sei an dieser Stelle noch einmal betont, dass in obigem modularen Gleichungssystem die Zahl x die einzige Unbekannte

ist. Alle anderen Parameter (insbesondere die x_i) sind vorgegeben. Dies wird vor allem deshalb erwähnt, um Verwechslungen mit linearen Gleichungssystemen aus der linearen Algebra zu vermeiden, bei denen meist die x_i die gesuchten Variablen sind.

Beweis:
Als Erstes betrachten wir die y_i. Bei y_i handelt es sich um das Inverse von $(\frac{n}{d_i})$ modulo d_i. Aufgrund der Teilerfremdheit der d_i untereinander ist $(\frac{n}{d_i})$ teilerfremd zu d_i, so dass nach Satz 3.3 sämtliche y_i existieren und eindeutig sind. Nehmen wir jetzt ein beliebiges $k \in \{1, \ldots, t\}$ und die dazugehörige Gleichung $x \bmod d_k = x_k \bmod d_k$. Dann gilt:

$$\begin{aligned} x \bmod d_k &= \left((\sum_{j=1}^{t} \frac{n}{d_j} \cdot y_j \cdot x_j) \bmod n \right) \bmod d_k \\ &= \left(\sum_{j=1}^{t} \frac{n}{d_j} \cdot y_j \cdot x_j \right) \bmod d_k \qquad (Satz\,2.5) \\ &= \left(\sum_{j=1}^{t} ((\frac{n}{d_j} \cdot y_j \cdot x_j) \bmod d_k) \right) \bmod d_k \end{aligned}$$

Für die einzelnen Summanden $(\frac{n}{d_j} \cdot y_j \cdot x_j) \bmod d_k$ gilt: Falls $j \neq k$ ist $\frac{n}{d_j} \bmod d_k = 0$ und damit $(\frac{n}{d_j} \cdot y_j \cdot x_j) \bmod d_k = 0$. Es bleibt in der Summe also nur der Summand $(\frac{n}{d_k} \cdot y_k \cdot x_k) \bmod d_k$ übrig. Für diesen gilt: $(\frac{n}{d_k} \cdot y_k \cdot x_k) \bmod d_k = (1 \cdot x_k) \bmod d_k = x_k \bmod d_k$. Damit erfüllt x die Gleichung $x \bmod d_k = x_k \bmod d_k$. Da k in $\{1, \ldots, t\}$ beliebig gewählt war folgt, dass x alle Gleichungen des Gleichungssystems löst.

Bleibt noch zu zeigen, dass x in $\mathbb{Z}_n$ die einzige Lösung ist. Angenommen es existiert noch eine weitere Lösung $x' \in \mathbb{Z}_n$, $x \neq x'$. Dann gilt für alle d_i mit $i \in \{1, \ldots, t\}$ $x \bmod d_i = x' \bmod d_i$, also $(x - x') = k_i \cdot d_i$ mit $k_i \in \mathbb{Z}$. Da alle d_i paarweise teilerfremd sind, folgt daraus insgesamt $(x - x') = k \cdot d_1 \cdot d_2 \cdot \ldots \cdot d_t = k \cdot n$ mit $k \in \mathbb{Z}$. Da für x und $x' \in \mathbb{Z}_n$ allerdings stets $-n < (x - x') < n$ gilt, folgt $k = 0$ und damit $x = x'$ im Widerspruch zur Annahme $x \neq x'$. $\square$

Mit Hilfe des chinesischen Restsatzes können wir unser obiges Beispiel nun zu Ende rechnen. Wir hatten die beiden modularen Gleichungssysteme

$$\begin{aligned} x \bmod 2 &= 0 \\ x \bmod 5 &= 3 \end{aligned}$$

und

$$\begin{aligned} x \bmod 2 &= 1 \\ x \bmod 5 &= 3 \end{aligned}$$

Wir erhalten $y_1 = (\frac{10}{2})^{-1} \bmod 2 = 5^{-1} \bmod 2 = 1$, $y_2 = (\frac{10}{5})^{-1} \bmod 5 = 2^{-1} \bmod 5 = 3$. Damit ergibt sich für das erste Gleichungssystem $x = ((\frac{10}{2}) \cdot 1 \cdot 0 + (\frac{10}{5}) \cdot 3 \cdot 3) \bmod 10 = 8$,

für das Zweite erhalten wir $x = ((\frac{10}{2}) \cdot 1 \cdot 1 + (\frac{10}{5} \cdot 3 \cdot 3)) \bmod 10 = 3$. Dies ergibt insgesamt die beiden Lösungen $x_0 = 3$ und $x_1 = 8$, in Einklang mit den Lösungen, die wir bereits in Kapitel 4.1 (Beispiel 4) erhalten hatten.

4.2.1 Abschließendes Beispiel zum chinesischen Restsatz

Um das Vorgehen noch einmal zu verdeutlichen wird abschließend noch ein weiteres etwas umfangreicheres Beispiel am Stück durchgerechnet:
Wir suchen die Lösungen $x \in \mathbb{Z}_{60}$ der Gleichung $(3 \cdot x) \bmod 60 = 12 \bmod 60$. Zunächst zerlegen wir die Zahl 60 in die drei teilerfremden Zahlen 3, 4 und 5. Daraus erhalten wir die drei Gleichungen

$$(3 \cdot x) \bmod 3 = 12 \bmod 3$$
$$(3 \cdot x) \bmod 4 = 12 \bmod 4$$
$$(3 \cdot x) \bmod 5 = 12 \bmod 5$$

Die erste Gleichung hat in $\mathbb{Z}_3$ die Lösungsmenge $L_1 = \{0, 1, 2\}$, die beiden Anderen sind in $\mathbb{Z}_4$ bzw. $\mathbb{Z}_5$ jeweils eindeutig lösbar mit $L_2 = \{0\}$ und $L_3 = \{4\}$. Wenn wir alle Kombinationen aus jeweils einer Lösung jeder Gleichung durchgehen, erhalten wir damit insgesamt die folgenden drei modularen Gleichungssysteme

$x \bmod 3 = 0$	$x \bmod 3 = 1$	$x \bmod 3 = 2$
$x \bmod 4 = 0$	$x \bmod 4 = 0$	$x \bmod 4 = 0$
$x \bmod 5 = 4$	$x \bmod 5 = 4$	$x \bmod 5 = 4$

Jedes dieser Gleichungssysteme liefert uns genau eine Lösung unserer Ausgangsgleichung. Zuerst berechnen wir die y_i, die für alle drei Systeme gleich sind. Wir erhalten:

$$y_1 = (\frac{60}{3})^{-1} \bmod 3 = 20^{-1} \bmod 3 = 2$$
$$y_2 = (\frac{60}{4})^{-1} \bmod 4 = 15^{-1} \bmod 4 = 3$$
$$y_3 = (\frac{60}{5})^{-1} \bmod 5 = 12^{-1} \bmod 5 = 3$$

Damit erhalten wir für das erste Gleichungssystem

$$x = (\frac{60}{3} \cdot 2 \cdot 0 + \frac{60}{4} \cdot 3 \cdot 0 + \frac{60}{5} \cdot 3 \cdot 4) \bmod 60 = 144 \bmod 60 = 24$$

für das Zweite

$$x = (\frac{60}{3} \cdot 2 \cdot 1 + \frac{60}{4} \cdot 3 \cdot 0 + \frac{60}{5} \cdot 3 \cdot 4) \bmod 60 = 184 \bmod 60 = 4$$

und für das Dritte

$$x = (\frac{60}{3} \cdot 2 \cdot 2 + \frac{60}{4} \cdot 3 \cdot 0 + \frac{60}{5} \cdot 3 \cdot 4) \bmod 60 = 224 \bmod 60 = 44$$

Durch Einsetzen kann man die Richtigkeit dieser drei Lösungen verifizieren.

5 Literaturverzeichnis

1. Wätjen, Dietmar: Kryptographie - Grundlagen, Algorithmen, Protokolle
   2. Auflage 2008

2. Struckmann, Werner und Wätjen, Dietmar: Mathematik für Informatiker - Grundlagen und Anwendungen
   1. Auflage 2007

3. Steger, Angelika: Diskrete Strukturen - Band 1
   2. Auflage 2007

4. Mayr, Ernst W.: Vorlesungsskript "Diskrete Strukturen" zum Wintersemester 2011/12 an der Technischen Universität München