Zahlentheorie und Kryptographie

zum Selbstlernen

Vorwort

Dies ist ein Skript zum Selbststudium. Du kannst hier etwas Zahlentheorie und ein klassisches und drei aktuelle Verschlüsselungsverfahren kennenlernen. Das, was Du hier über Zahlentheorie lernst, reicht aus, um zu verstehen, wie verschlüsselt wird und warum die Verschlüsselungsverfahren funktionieren.

Der Text ist im Wesentlichen der Mitschrieb aus einem Online-Kurs *Zahlentheorie und Kryptographie* im Schülerseminar für Klasse 8-10. Du findest diesen und andere Kurse auf der Seite

`https://pnp.mathematik.uni-stuttgart.de/iadm/Zirkel/material-Schuelerseminar/`

Falls Du beim Studium des vorliegenden Textes Fragen hast, kannst Du beim Online-Kurs im entsprechenden Video nachsehen, dort gibt es ausführlichere Erklärungen. Um die Verbindung zu finden, ist hier am Rand des Textes markiert, wann die einzelnen Einheiten des Online-Kurses beginnen.

Die Aufgaben sind auch die selben wie im Online-Kurs. Im Lerntext sind keine Lösungen dabei, damit Du sie selber lösen kannst. Bei den Aufgaben ist oft Platz, um Deine Lösungen aufzuschreiben. Manchmal musst Du aber auch ein extra Blatt für die Berechnungen dazunehmen. Falls Du Deine Lösungen überprüfen willst, stehen alle Aufgaben mit Lösungen im letzten Kapitel dieses Skripts.

Ich wünsche Dir viel Spaß beim Durcharbeiten des Skripts und bei den Aufgaben!

August 2024 Peter Lesky

Inhalt

1 Diophantische Gleichungen

Beginn Online-Einheit 1

Gegeben:	$a, b, c \in \mathbb{N} = \{0, 1, 2, 3, 4, \ldots\}$
Gesucht:	$x, y \in \mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$
so dass	$ax + by = c$
Vereinbarung:	Schreibe die Lösungen als Zahlenpaare $(x \mid y)$

Anmerkungen: 1) Mengen werden mit Hilfe von Mengenklammern $\{\ldots\}$ angegeben. Zwischen den Mengenklammern wird beschrieben, welche Elemente die Menge besitzt.

2) Betrachtet man alle rationalen Lösungen $(x \mid y)$ einer Gleichung $ax + by = c$, so liegen diese auf einer Geraden, falls nicht $a = b = 0$ gilt. Das besondere an diophantischen Gleichungen ist, dass man nur Lösungen $(x \mid y)$ mit ganzzahligen x, y betrachtet.

Aufgabe 1

Versuche, jeweils ganzzahlige Lösungen $(x \mid y)$ der angegebenen Gleichung zu finden.
Falls du vermutest, dass es keine Lösung gibt, begründe deine Vermutung.

a) $x + 3y = 10$:

b) $3x + 7y = 1$:

c) $18x + 12y = 3$:

d) $5x + 5y = 1$:

e) $5x + 15y = 50$:

f) $18x + 12y = 66$:

Anmerkung: Wir sehen, dass es nur Lösungen gibt, wenn jede Zahl, die Teiler von a und von b ist, auch c teilt. Diese Tatsache schreiben wir im Folgenden in mathematischer Sprache auf.

Definition: 1) Seien $a \in \mathbb{Z}$, $k \in \mathbb{N}_+ = \{1, 2, 3, \ldots\}$. Dann heißt k Teiler von a, geschrieben $k \mid a$, falls es ein $a' \in \mathbb{Z}$ gibt, so dass $a = a' \cdot k$.

Beispiele: $a = 35$ hat die Teiler $1, 5, 7, 35$, denn
$a = 35 \cdot 1 \quad (a' = 35)$
$a = 7 \cdot 5 \quad (a' = 7)$
$a = 5 \cdot 7 \quad (a' = 5)$
$a = 1 \cdot 35 \quad (a' = 1)$

$a = -35$ hat die selben Teiler.

$a = 0$ hat alle positiven natürlichen Zahlen als Teiler: $\underbrace{0}_{a} = \underbrace{0}_{a'} \cdot k$.

2) Seien $a, b \in \mathbb{Z}$, nicht beide 0. Dann ist der größte gemeinsame Teiler von a, b definiert durch

$$\mathrm{ggT}(a, b) := \max \underbrace{\{k \in \mathbb{N}_+ : k \mid a \text{ und } k \mid b\}}_{\text{Menge der gemeinsamen Teiler von } a \text{ and } b}.$$

Anmerkungen: 1) Hier wird die Menge durch eine Bedingung beschrieben, die die Elemente erfüllen müssen. Man liest den Doppelpunkt als *für die gilt* oder *die die folgende Eigenschaft besitzen*. Nach dem $\max$ steht die Menge aller Elemente k von $\mathbb{N}_+$, für die gilt, dass k Teiler von a und k Teiler von b ist. Mit $\max$ wird das größte Element dieser Menge bezeichnet.

2) Warum darf nicht $a = b = 0$ gelten? Im Fall $a = b = 0$ besteht die Menge aller gemeinsamen Teiler aus ganz $\mathbb{N}_+$ und besitzt kein größtes Element.

Beispiel: $a = 70,\ b = 98$:

a hat die Teiler $1, 2, 5, 7, 10, 14, 35, 70$,
b hat die Teiler $1, 2, 7, 14, 49, 98$,
Menge der gemeinsamen Teiler: $\{1, 2, 7, 14\}$,
Größtes Element der Menge: $\mathrm{ggT}(70, 98) = 14$.

Satz: Aus $k \mid a$ und $k \mid b$ und $x, y \in \mathbb{Z}$ folgt $k \mid (ax + by)$.

Beweis:
$$k \mid a \;\Rightarrow\; a = a'\,k$$
$$k \mid b \;\Rightarrow\; b = b'\,k$$
$$\Rightarrow\; ax + by \;=\; a'\,kx + b'\,ky \;=\; \underbrace{(a'\,x + b'\,y)}_{\in\mathbb{Z}}\,k$$
$$\Rightarrow\; k \mid (ax + by) \qquad \square$$

Satz: Besitzt die Gleichung $ax + by = c$ eine Lösung $(x \mid y)$ mit $x, y \in \mathbb{Z}$, so folgt $\mathrm{ggT}(a, b) \mid c$.

Beweis: $\mathrm{ggT}(a, b) \mid a$ und $\mathrm{ggT}(a, b) \mid b$
$$\overset{\text{letzter Satz}}{\Rightarrow} \mathrm{ggT}(a, b) \mid \underbrace{(ax + by)}_{=c}. \qquad \square$$

Folgerung: Ist $\mathrm{ggT}(a, b)$ kein Teiler von c, so hat $ax + by = c$ keine ganzzahlige Lösung.

Aufgabe 2

Gegeben sind diophantische Gleichungen der Form $ax + by = c$. Bestimme jeweils die Menge der gemeinsamen Teiler von a und b, den $\mathrm{ggT}(a, b)$ und untersuche, ob $\mathrm{ggT}(a, b)$ Teiler von c ist. Falls es Lösungen gibt, vereinfache die Gleichung, indem Du beide Seiten durch die selbe geeignet gewählte Zahl teilst und rate eine Lösung $(x \mid y)$.

a) $18x + 12y = 24$:

Menge der gemeinsamen Teiler von 18 und 12: $\{ \qquad \}$,

$\mathrm{ggT}(12, 18) = \square$.

Die Gleichung ist

☐	nicht lösbar, denn	
☐	lösbar, denn ich habe eine Lösung gefunden:	
	Vereinfachte Gleichung:	
	Eine Lösung: $(x \mid y) =$	$(\quad \mid \quad)$

b) $45x + 30y = 5$:

Menge der gemeinsamen Teiler von 45 und 30: $\{\quad\}$,

$\mathrm{ggT}(45, 30) =$ $\square$.

Die Gleichung ist

- $\square$ nicht lösbar, denn $\square$
- $\square$ lösbar, denn ich habe eine Lösung gefunden:
  - Vereinfachte Gleichung: $\square$
  - Eine Lösung: $(x \mid y) =$ $(\quad \mid \quad)$.

Anmerkung: Bei großen Zahlen a und b ist es ziemlich umständlich, die Menge aller gemeinsamen Teiler zu bestimmen. Wir lernen im nächsten Kapitel eine Methode kennen, die die Berechnung des größten gemeinsamen Teilers vereinfacht.

2 Der euklidische Algorithmus

Teilen mit Rest:

$13 : 4 = 3$ R 1 bedeutet: $13 = 3 \cdot 4 + 1$

$223 : 25 = 8$ R 23 bedeutet: $223 = 8 \cdot 25 + 23$

Satz (Teilen mit Rest): Seien $a, b \in \mathbb{N}_+$. Dann gibt es eindeutig bestimmte Zahlen $k, r \in \mathbb{N} = \{0, 1, \ldots\}$, so dass gilt:

$$a = kb + r \quad \text{und} \quad 0 \le r \le b - 1.$$

Anmerkung: Ohne die Bedingung $0 \le r \le b - 1$ sind k, r nicht eindeutig, z.B.

$$23 = 4 \cdot 5 + 3 \quad \text{und} \quad 23 = 3 \cdot 5 + 8.$$

Aufgabe 3

Teile jeweils a durch b mit Rest und schreibe die Lösung als Gleichung $a = k \cdot b + r$ auf.

a) $a = 143,\ b = 12$:

b) $a = 14130,\ b = 58$:

c) $a = 1\,111\,111,\ b = 2\,222$:

d) $a = 123\,321,\ b = 2\,010$:

Hinweis: Teil a) geht im Kopf, aber für die anderen Aufgabenteile ist ein Taschrechner hilfreich.

Euklidischer Algorithmus: Gesucht $\mathrm{ggT}(468, 60)$.

Teilen mit Rest:
$$\begin{aligned} 468 &= 7 \cdot 60 + 48 \\ 60 &= 1 \cdot 48 + 12 \\ 48 &= 4 \cdot 12 \end{aligned} \quad \Rightarrow \mathrm{ggT}(468, 60) = 12$$

Stimmt das immer?

Anmerkung: Wir werden nun klären, dass der euklidische Algorithmus immer den größten gemeinsamen Teiler liefert. Dazu beweisen wir zunächst einen Satz, der dafür sehr hilfreich ist.

Satz: Sei $a = k \cdot b + r$. Dann gilt $\mathrm{ggT}(a, b) = \mathrm{ggT}(b, r)$.

Beweis: 1) $\mathrm{ggT}(b, r)$ teilt b und r.

$\overset{\text{früherer Satz}}{\Rightarrow}$ $\mathrm{ggT}(b, r)$ teilt $a = k \cdot b + 1 \cdot r$

$\Rightarrow$ $\mathrm{ggT}(b, r)$ teilt a und b

$\Rightarrow$ $\mathrm{ggT}(b, r) \leq \mathrm{ggT}(a, b)$.

2) Löse die Gleichung nach r auf: $r = a - k \cdot b$.

Wie vorher folgt: $\mathrm{ggT}(a, b)$ teilt b und r

$\Rightarrow$ $\mathrm{ggT}(a, b) \leq \mathrm{ggT}(b, r)$.

1) und 2) $\Rightarrow$ $\mathrm{ggT}(b, r) = \mathrm{ggT}(a, b)$. □

Euklidischer Algorithmus für $\mathrm{ggT}(98, 126)$:

$$\begin{array}{rcl} \overbrace{126}^{a} &=& 1 \cdot \overbrace{98}^{b} + \overbrace{28}^{r} \\ 98 &=& 3 \cdot 28 + 14 \\ 28 &=& 2 \cdot 14 \end{array} \quad \begin{array}{l} \overset{\text{Satz}}{\Rightarrow} \\ \Rightarrow \\ \Rightarrow \end{array} \quad \begin{array}{rcl} \mathrm{ggT}(\overbrace{126}^{a}, \overbrace{98}^{b}) &=& \mathrm{ggT}(\overbrace{98}^{b}, \overbrace{28}^{r}) \\ \mathrm{ggT}(98, 28) &=& \mathrm{ggT}(28, 14) \\ \mathrm{ggT}(28, 14) &=& 14 \\ \hline \Rightarrow \mathrm{ggT}(126, 98) &=& 14 \end{array}$$

Anmerkung: Die letzte Rechnung zeigt, dass der euklidische Algorithmus immer den ggT liefert.

Aufgabe 4

Berechne mit dem Euklidischen Algorithmus:

a) $\mathrm{ggT}(150, 54)$,

b) $\mathrm{ggT}(300, 468)$,

c) $\mathrm{ggT}(2717, 2431)$,

d) $\mathrm{ggT}(4263, 4641)$.

3 Eine Lösung berechnen

Beginn Online-Einheit 2

Gesucht: Alle ganzzahligen Lösungen von $110x + 32y = 8$.

Anmerkung: Bisher haben wir Lösungen erraten. Wir lernen nun, wie man Lösungen systematisch berechnet. Am Schluss des Kapitels können wir alle Lösungen dieser Gleichung berechnen.

Satz: Zu beliebig gewählten natürlichen Zahlen a, b gibt es ganze Zahlen x, y, so dass

$$ax + by = \mathrm{ggT}(a, b).$$

Beispiel: Erweiterter Euklidischer Algorithmus für $110x + 32y = \mathrm{ggT}(110, 32)$.

Schritt 1:	Schritt 2:
$110 = 3 \cdot 32 + 14$	$14 = 110 - 3 \cdot 32$
$32 = 2 \cdot 14 + 4$	$4 = 32 - 2 \cdot 14$
$14 = 3 \cdot 4 + 2$	$2 = 14 - 3 \cdot 4$
$4 = 2 \cdot 2$	

$$
\begin{aligned}
\Rightarrow \mathrm{ggT}(110, 32) = 2 &= 14 - 3(\overbrace{32 - 2 \cdot 14}^{4=}) \\
&= 14 - 3 \cdot 32 + 6 \cdot 14 = 7 \cdot 14 - 3 \cdot 32 \\
&= 7(\overbrace{110 - 3 \cdot 32}^{14=}) - 3 \cdot 32 = 7 \cdot 110 - 21 \cdot 32 - 3 \cdot 32 \\
&= 7 \cdot 110 - 24 \cdot 32
\end{aligned}
$$

$\Rightarrow (x \mid y) = (7 \mid -24)$ ist eine Lösung.

Anmerkung: Wir sehen am Beispiel, dass diese Methode immer funktioniert. Einen allgemeinen Beweis sparen wir uns.

Aufgabe 5

Bestimme jeweils eine ganzzahlige Lösung $(x \mid y)$ der angegebenen Gleichung. Berechne dazu in den Aufgabenteilen a) und d) zunächst den ggT der Koeffizienten mit Hilfe des euklidischen Algorithmus. Erweitere dann den Algorithmus, um eine Lösung zu finden.

a) $96x + 66y = 6$,

b) $96x + 66y = 18$ (verwende hierzu die Lösung aus Teil a)),

c) Für beliebiges fest vorgegebenes $n \in \mathbb{N}$: $96x + 66y = n \cdot 6$ (auch hier erweist sich die Lösung aus Teil a) als nützlich),

d) $119x + 143y = 1$,

e) $119x + 143y = 4$.

Anmerkung: Im Aufgabenteil c) kannst Du sehen, wie man im allgemeinen Fall eine Lösung berechnet. Dies schreiben wir als Satz auf und beweisen ihn auch.

Satz: Seien $a, b, c \in \mathbb{N}$ gegeben, so dass $\mathrm{ggT}(a, b) \mid c$. Dann hat

$$ax + by = c \; (= n \cdot \mathrm{ggT}(a, b))$$

mindestens eine ganzzahlige Lösung $(x \mid y)$.

Beweis: Es gibt ein $n \in \mathbb{N}$, so dass $c = n \cdot \mathrm{ggT}(a, b)$.

Letzter Satz $\Rightarrow$ es gibt ganzzahlige x, y mit

$$
\begin{aligned}
&ax + by = \mathrm{ggT}(a, b) \qquad \mid \cdot n \\
\Leftrightarrow\ &n(ax + by) = n \cdot \mathrm{ggT}(a, b) \\
\Leftrightarrow\ &a(nx) + b(ny) = c \\
\Rightarrow\ &(nx \mid ny) \text{ ist ganzzahlige Lösung.} \qquad \square
\end{aligned}
$$

Beispiel: $110x + 32y = \mathrm{ggT}(110, 32) = 2$ hat die Lösung $(7 \mid -24)$.

$\Rightarrow$ $110x + 32y = 8 = 4 \cdot 2$ hat die Lösung $(4 \cdot 7 \mid 4 \cdot (-24)) = (28 \mid -96)$.

Anmerkung: Jetzt können wir eine Lösung berechnen. Nun kümmern wir uns darum, wie man alle Lösungen erhält.

4 Alle Lösungen berechnen

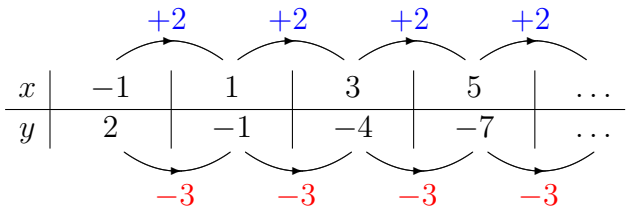
Aufgabe 6

Bestimme durch Probieren mehrere ganzzahlige Lösungen $(x \mid y)$, möglichst alle.

a) $3x + 2y = 1$:

b) $3x + 9y = 3$:

Beobachtung: Die Gleichung $3x + 2y = 1$ hat die Lösungen



D.h. x wird in 2er Schritten erhöht und y in 3er Schritten erniedrigt.

Satz: 1) Ist $(x_0 \mid y_0)$ eine Lösung von $ax + by = c$, dann sind alle Zahlenpaare

$$(x \mid y) \;=\; (x_0 + k \cdot b \mid y_0 - k \cdot a) \text{ mit } k \in \mathbb{Z} \qquad (*)$$

ebenfalls Lösungen.

2) Gilt $\mathrm{ggT}(a, b) = 1$, dann sind durch $(*)$ alle Lösungen gegeben.

Beweis: 1) Durch $(*)$ sind Lösungen gegeben, denn

$ax + by \;=\; a(x_0 + kb) + b(y_0 - ka) \;=\; ax_0 + \cancel{akb} + by_0 - \cancel{bka} \;=\; c.$

2) Sei $(x \mid y)$ irgendeine Lösung von $ax + by = c$.

Es gilt $a(x - x_0) + b(y - y_0) \;=\; ax + by - (ax_0 + by_0) \;=\; c - c \;=\; 0$

$\Rightarrow$ $b(y - y_0) \;=\; -a(x - x_0)$.

$\mathrm{ggT}(a, b) = 1 \;\Rightarrow\; b \mid (x - x_0) \;\Rightarrow\; x - x_0 = k \cdot b$ mit geeignetem $k \in \mathbb{Z}$.

$\Rightarrow$ $y - y_0 \;=\; -\frac{a}{b}(x - x_0) \;=\; -\frac{a}{b} \cdot k \cdot b \;=\; -k \cdot a.$

$\Rightarrow$ $y \;=\; y_0 - k \cdot a, \quad x \;=\; x_0 + k \cdot b$

$\Rightarrow$ $(x \mid y)$ wird durch die Formel $(*)$ beschrieben. $\square$

Beispiel: $$110\,x + 32\,y = 8 \tag{1}$$

hat die Lösung $(x_0 \mid y_0) = (28 \mid -96)$.

1) des Satzes: $(x \mid y) = (28 - k \cdot 32 \mid -96 + k \cdot 110)$ mit $k \in \mathbb{Z}$ sind Lösungen.

Teile die Gleichung (1) auf beiden Seiten durch $2 = \mathrm{ggT}(110, 32)$:

$$55\,x + 16\,y \;=\; 4 \tag{2}$$

hat die selben Lösungen wie (1), und $\mathrm{ggT}(55, 16) = 1$.

2) des Satzes: Alle Lösungen von (2) sind

$$(x \mid y) = (28 + k \cdot 16 \mid -96 - k \cdot 55) \text{ mit } k \in \mathbb{Z}.$$

Dies sind auch alle Lösungen von (1).

Anmerkung: Wir können jetzt diophantische Gleichungen vollständig lösen. Entweder besitzt die Gleichung keine Lösung, oder wir können alle berechnen.

Aufgabe 7

Gegeben ist die Gleichung

$$144x + 52y \;=\; 8. \tag{$*$}$$

a) Bestimme $\mathrm{ggT}(144, 52)$ mit Hilfe des euklidischen Algorithmus.

b) Erweitere den euklidischen Algorithmus und berechne eine ganzzahlige Lösung $(x \mid y)$ der Gleichung $144x + 52y = \mathrm{ggT}(144, 52)$.

c) Berechne eine Lösung von $(*)$.

d) Teile die Gleichung $(*)$ auf beiden Seiten durch $\mathrm{ggT}(144, 52)$ und gib die Gleichung an, die dadurch ensteht.

e) Gib alle ganzzahligen Lösungen von $(*)$ an.

Aufgabe 8

Bestimme jeweils alle Lösungen für die Gleichungen aus Aufgabe 5.

5 Kongruenzen

Beginn Online-Einheit 3

Anmerkung: In der nächsten Aufgabe geht es um Teilbarkeit durch 9. Am Ende des nächsten Kapitels kommen wir darauf zurück.

Aufgabe 9

Bestimme den Rest beim Teilen durch 9.

a) 1000: **b)** 2005: **c)** 2050:

d) 1035: **e)** 5103:

Aufgabe 10

Bestimme eine vierstellige, eine fünfstellige und eine sechsstellige Zahl, die beim Teilen durch 9 den Rest 3 lassen.

Definition: Seien a, b ganze Zahlen, $m \in \mathbb{N}_+ = \{1, 2, \ldots\}$. Schreibe

$$a \equiv b \mod m \qquad (a \text{ ist kongruent zu } b \text{ modulo } m),$$

falls $a - b$ durch m teilbar ist.

Beispiel: $15 \equiv 3 \mod 6$, denn $15 - 3 = 12$ ist durch 6 teilbar.

Anmerkung: Im folgenden Satz geben wir andere Bedingungen an, mit deren Hilfe wir feststellen können, ob zwei Zahlen kongruent modulo eines Moduls m sind.

Satz (Kongruenzkriterien): Folgende Aussagen sind äquivalent:

(1) $a \equiv b \mod m$
(2) Es gibt ein $k \in \mathbb{Z}$, so dass $a = b + km$
(3) a und b lassen beim Teilen durch m den selben Rest.

Anmerkung: Äquivalent bedeutet, dass alle drei Aussagen gleichzeitig wahr oder gleichzeitig falsch sind. Für den Beweis verwenden wir einen *Ringschluss*. Dadurch sparen wir Beweisschritte.

Beweisprinzip Ringschluss:

$$\begin{array}{ccc} & (1) & \\ \nearrow & & \searrow \\ (3) & \Longleftarrow & (2) \end{array}$$

Beweis: (1) $\Rightarrow$ (2):

$$\begin{aligned} a \equiv b \mod m &\Leftrightarrow m \mid (a-b) \\ &\Rightarrow \text{Es gibt ein } k \in \mathbb{Z}, \text{ so dass } a - b = k \cdot m \quad \big| + b \\ &\Rightarrow a = km + b = b + km \end{aligned}$$

(2) $\Rightarrow$ (3): Sei r der Rest beim Teilen von b durch m,
d.h. $b = lm + r$ mit einem $l \in \mathbb{Z}$.

$$\begin{aligned} (2) \Rightarrow a &= b + km \\ &= lm + r + km \\ &= \underbrace{(l+k)}_{\in \mathbb{Z}} m + r \end{aligned}$$

$\Rightarrow$ a lässt beim Teilen durch m den selben Rest r wie b.

(3) $\Rightarrow$ (1): $a = km + r,\ b = lm + r$ mit $k, l \in \mathbb{Z}$

$$\begin{aligned} \Rightarrow a - b &= km + r - (lm + r) \\ &= km + \cancel{r} - kl - \cancel{r} \\ &= (k-l)m \\ \Rightarrow m &\mid (a-b) \\ \Leftrightarrow a &\equiv b \mod m \end{aligned}$$

□

Aus Aufgabe 1: b) $2005 : 9 = 222$ R 7
$\Leftrightarrow 2005 = 9 \cdot 222 + 7$
$\Rightarrow 2005 \equiv 7 \mod 9$

c) $2050 \equiv 7 \mod 9$
$\Rightarrow 2050 \equiv 2005 \mod 9$

Aufgabe 11

Bestimme jeweils das Ergebnis beim Teilen mit Rest. Trage Deine Lösungen in die Kästchen ein.

a) $33 = \square \cdot 6 + \square$

$\Rightarrow 33 \equiv \square \mod 6$

b) $-101 = \square \cdot 4 + \square$

$\Rightarrow -101 \equiv \square \mod 4$

Aufgabe 12

Bestimme jeweils möglichst alle ganzzahligen Lösungen x der angegebenen Gleichung.

a) $5 + x \equiv 2 \mod 7$: $L =$

b) $5 \cdot x \equiv 2 \mod 7$: $L =$

c) $5 \cdot x \equiv 2 \mod 10$:

d) $-34 \equiv x \mod 5$:

Satz (Rechenregeln für Kongruenzen):

a) Wenn $a \equiv b \mod m$ und $c \equiv d \mod m$, dann:

$a_1)$ $-a \equiv -b \mod m$

$a_2)$ $a + c \equiv b + d \mod m$

$a_3)$ $ac \equiv bd \mod m$

$a_4)$ $a^2 \equiv b^2 \mod m$, $a^3 \equiv b^3 \mod m$, ...

b) Wenn $a \equiv b \mod m$ und $b \equiv c \mod m$, dann

$b_1)$ $a \equiv a \mod m$

$b_2)$ $b \equiv a \mod m$

$b_3)$ $a \equiv c \mod m$

Anmerkung: Die Rechenoperationen Plus und Mal vertragen sich mit der Kongruenzrelation. Wir beweisen zunächst nur den Teil a_3). Den Beweis anderer Teile kannst Du danach selbst versuchen.

Beweis von a_3): Wir wissen $a = b + km$, $c = d + lm$ mit $k, l \in \mathbb{Z}$.
Wir suchen ein $j \in \mathbb{Z}$, so dass $ac = bd + jm$.

$$\begin{aligned} ac &= (b + km)(d + lm) \\ &= bd + blm + kmd + kmlm \\ &= bd + \underbrace{(bl + kd + klm)}_{\in \mathbb{Z}} m \end{aligned}$$

$\Rightarrow ac = bd + jm$

$\Rightarrow ac \equiv bd \mod m$ $\square$

Aufgabe 13

Beweise die folgenden Aussagen:

a) Wenn $a \equiv b \mod m$ und $c \equiv d \mod m$, dann $a + c \equiv b + d \mod m$.

b) Wenn $a \equiv b \mod m$, dann $-a \equiv -b \mod m$.

c) Wenn $a \equiv b \mod m$ und $b \equiv c \mod m$, dann $a \equiv c \mod m$.

Hinweis: Zum Beweis von Teil a) kannst Du den vorigen Beweis von a$_3$) entsprechend anpassen.

Anmerkung: Nun kommen wir zurück zur Teilbarkeit einer Zahl durch 9.

Satz (Quersummenregel): Wir schreiben $Q(a)$ für die Quersumme einer natürlichen Zahl a. Wir bilden so lange die Quersummen $Q(a),\ Q(Q(a)), \ldots$, bis sich eine Zahl b zwischen 1 und 9 ergibt. Dann gilt $a \equiv b \mod 9$.
Wenn $b = 9$, dann ist a durch 9 teilbar.

Beispiel: $a = 123456$: $Q(a) = 21,\ Q(Q(a)) = 3 \ \Rightarrow\ 123456 \equiv 3 \mod 9$

Anmerkung: Dies bedeutet, dass a zwar nicht durch 9, aber durch 3 teilbar ist.

Beweis 1) $a \equiv Q(a) \mod 9$:

Eine natürliche Zahl a mit $n+1$ Stellen können wir darstellen als

$$a = \boxed{a_n}\boxed{a_{n-1}} \ldots \begin{array}{|c|c|c|}\hline a_2 & a_1 & a_0 \\ \hline \mathsf{H} & \mathsf{Z} & \mathsf{E} \\ \hline \end{array} \ \Rightarrow\ a = \underbrace{a_0 \cdot 1}_{\equiv a_0} + \underbrace{a_1 \cdot 10}_{\equiv a_1} + \underbrace{a_2 \cdot 100}_{\equiv a_2} + \ldots + \underbrace{a_n \cdot 10^n}_{\equiv a_n \bmod 9}.$$

$$\begin{array}{rcl} 10 & \equiv & 1 \bmod 9 \\ \overset{\text{Satz a}_4)}{\Rightarrow}\ 10^2 & \equiv & 1^2 \bmod 9 \\ \vdots & & \\ 10^n & \equiv & 1 \bmod 9 \end{array} \quad \overset{\text{Satz a}_3)}{\Rightarrow} \quad \begin{array}{rcl} a_1 \cdot 10 & \equiv & a_1 \cdot 1 \bmod 9 \\ a_2 \cdot 10^2 & \equiv & a_2 \cdot 1 \bmod 9 \\ \vdots & & \\ a_n \cdot 10^n & \equiv & a_n \cdot 1 \bmod 9 \end{array}$$

$$\overset{\text{Satz a}_2)}{\Rightarrow}\ a \equiv \underbrace{a_0 + a_1 + a_2 + \ldots + a_n}_{=Q(a)} \mod 9.$$

2) $a \equiv Q(a), Q(a) \equiv Q(Q(a)) \overset{\text{Satz b}_3)}{\Rightarrow} a \equiv Q(Q(a)) \Rightarrow a \equiv Q(Q(Q(a)))\ldots$ $\square$

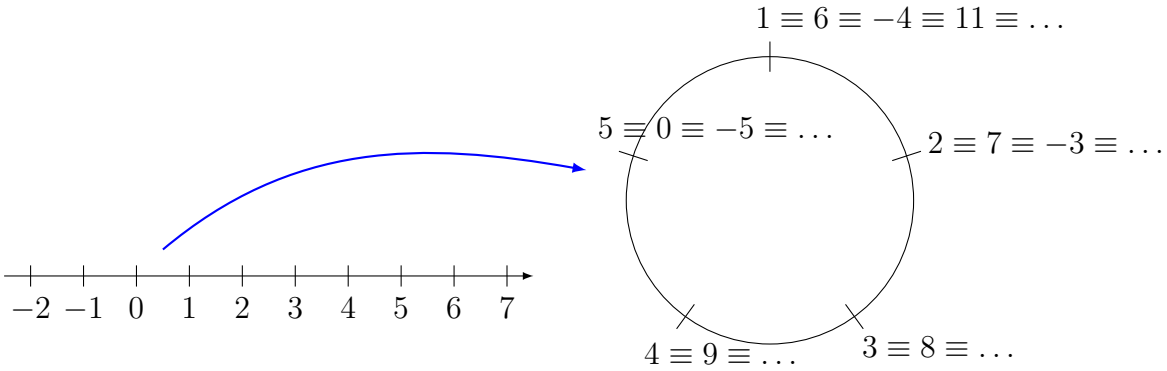
Aufgabe 14

Gib zwei verschiedene 10-stellige Zahlen an, deren Ziffern nur aus Achten und Nullen bestehen, und die beim Teilen durch 9 den Rest 3 ergeben.

6 Rechnen mit Restklassen

Beginn Online-Einheit 4

Die Beziehung *kongruent modulo* 5 rollt den Zahlenstrahl zu einem Zahlenring zusammen:



Betrachte alle Zahlen, die beim Teilen durch eine Zahl $m \in \mathbb{N}_+$ den selben Rest lassen. Diese Zahlen werden zu einer Menge zusammengefasst, der Restklasse.

Definition: Die Restklasse $[a]$ von a modulo m ist definiert durch

$$[a] \;:=\; \{b \in \mathbb{Z} : b \equiv a \mod m\}.$$

a heißt Repräsentant der Restklasse $[a]$.

Beispiele modulo 5:

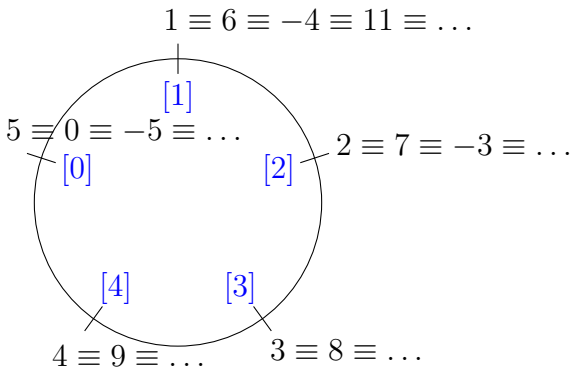
$$\begin{array}{lllllll} [0] & = & \{\ldots,-10,-5,0,5,10,\ldots\} & = & [5] & = & \ldots \\ [1] & = & \{\ldots,-9,-4,1,6,11,\ldots\} & = & [6] & = & [-4] \;=\; \ldots \\ [2] & = & \ldots & & & & \\ [3] & = & \ldots \;=\; [8] \;=\; \ldots & & & & \\ [4] & = & \ldots & & & & \end{array}$$

0 und 5 sind verschiedene Repräsentanten von $[0]$.

Anmerkungen: 1) Bezüglich des Moduls 5 gibt es genau 5 Restklassen.

2) Durch den Begriff *Restklasse* wird aus Kongruenz Gleichheit: $1 \equiv 6 \mod 5$ bedeutet dasselbe wie $[1] = [6]$ in $\mathbb{Z}_5$.

Wir können nun die Restklassen in unserem Zahlenring ergänzen:



Definition: Die Menge aller Restklassen modulo m heißt Restklassenring modulo m, schreibe $\mathbb{Z}_m$.

Beispiel: $\mathbb{Z}_5 \;=\; \big\{[0],[1],[2],[3],[4]\big\}$.

Aufgabe 15

a) Gib die Elemente der Restklasse $[3]$ modulo 7 an.

$[3] = \boxed{}$.

b) Gegeben sind die Restklassen $[49]$, $[16]$ und $[-10]$ modulo 7. Gib jeweils eine möglichst kleine nichtnegative ganze Zahl x an, so dass $[49] = [x]$ bzw. $[16] = [x]$ bzw. $[-10] = [x]$ gilt.

$[49] = \boxed{}$, $[16] = \boxed{}$, $[-10] = \boxed{}$.

c) Gib alle Elemente von $\mathbb{Z}_7$ an.

$\mathbb{Z}_7 = \boxed{}$.

Anmerkung: Wir wollen mit Restklassen rechnen können. Dazu definieren wir nun Addition und Multiplikation von Restklassen.

Definition: Für $a, b \in \mathbb{Z}$ definiert man

$$\begin{aligned} [a] + [b] &:= [a+b] \\ [a] \cdot [b] &:= [ab] \end{aligned}$$

Anmerkung: Man definiert hier eine Addition von Mengen. Das ist eine neue Addition. Weil sie durch die bekannte Addition von ganzen Zahlen definiert wird, verwendet man das selbe Symbol. Genauso für die Multiplikation.

Beispiele modulo 5:

$$\begin{aligned} [2] + [2] &= [4] \\ [3] + [4] &= [7] = [2] \\ [3] \cdot [4] &= [12] = [2] \\ [-2] \cdot [-1] &= [2] \\ [8] \cdot [9] &= [72] = [2] \end{aligned}$$

Anmerkungen: 1) Wir einigen uns darauf, dass die Ergebnisse beim Rechnen modulo 5 immer als Restklassen von Zahlen zwischen 0 und 4 dargestellt werden. Dann können die Ergebnisse besser verglichen werden. Außerdem kann man mit kleineren Zahlen besser weiterrechnen.

2) Wir sehen im Beispiel: $[3] = [-2] = [8]$ und $[4] = [-1] = [9]$, und alle drei Produkte $[3] \cdot [4]$, $[-2] \cdot [-1]$, $[8] \cdot [9]$ ergeben dieselbe Restklasse. Wir klären nun, dass das immer so ist. Erst dann ist die Definition der Multiplikation sinnvoll.

Satz: Ist $[a] = [a']$ und $[b] = [b']$, so gilt $[a \cdot b] = [a' \cdot b']$ und $[a + b] = [a' + b']$.

Beweis: Ist $[a] = [a']$ und $[b] = [b']$, so folgt:

$$\begin{aligned} & a \equiv a' \mod m \quad \text{und} \quad b \equiv b' \mod m \\ \overset{\text{Rechenregeln für Kongruenzen}}{\Rightarrow} \quad & ab \equiv a'b' \mod m \quad \text{und} \quad a + b \equiv a' + b' \mod m \\ \Rightarrow \quad & [ab] = [a'b'] \quad \text{und} \quad [a+b] = [a'+b'] \end{aligned}$$ □

Anmerkung: Es ist also egal, welche Repräsentanten der Restklassen $[a]$ und $[b]$ für die Berechnung von $[a] \cdot [b]$ verwendet werden, als Ergebnis kommt immer die selbe Restklasse heraus.

Aufgabe 16

Fülle die Verknüpfungstabelle für die Addition und Multiplikation in $\mathbb{Z}_5$ aus. Achtung: Es dürfen nur die Bezeichnungen $[0], \ldots, [4]$ verwendet werden, also anstelle von $[8]$ muss $[3]$ geschrieben werden.

$+$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$					
$[1]$					
$[2]$					
$[3]$					
$[4]$					

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$					
$[1]$					
$[2]$					
$[3]$					
$[4]$					

Frage: Wie sieht es nun mit Differenzen und Quotienten aus?

In $\mathbb{Z}_5$: $[1]-[2]=[4]$, denn $[4]+[2]=[1]$ (Verknüpfungstabelle letzte Aufgabe),
$[1]-[4]=[2]$, denn $[2]+[4]=[1]$.
Beachte: $[1]-[2]=[4]=[-1]$, $[1]-[4]=[2]=[-3]$.

Satz: für $a, b \in \mathbb{Z}$ gilt $[a]-[b]=[a-b]$.

Beweis: $[a-b]+[b]=[a-b+b]=[a] \;\Rightarrow\; [a-b]=[a]-[b]$.

Beispiel zur Division: Was ist $\dfrac{[1]}{[2]}$ in $\mathbb{Z}_5$?

$$\frac{[1]}{[2]} \;=\; [x] \;\Leftrightarrow\; [2]\cdot[x] \;=\; [1]$$

Multiplikationstabelle in $\mathbb{Z}_5 \;\Rightarrow\; [x]=[3]$

Genauso: $\dfrac{[2]}{[3]}=[4]$, da $[3]\cdot[4]=[2]$.

Anmerkung: Das ist doch erstaunlich: Eins geteilt durch zwei ergibt drei! Dies gilt nur in $\mathbb{Z}_5$.

Aufgabe 17

Für die Lösung dieser Aufgabe kannst du die folgenden Verknüpfungstabellen verwenden.

Addition in $\mathbb{Z}_9$

$+$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$	$[7]$	$[8]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$	$[7]$	$[8]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$	$[7]$	$[8]$	$[0]$
$[2]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$	$[7]$	$[8]$	$[0]$	$[1]$
$[3]$	$[3]$	$[4]$	$[5]$	$[6]$	$[7]$	$[8]$	$[0]$	$[1]$	$[2]$
$[4]$	$[4]$	$[5]$	$[6]$	$[7]$	$[8]$	$[0]$	$[1]$	$[2]$	$[3]$
$[5]$	$[5]$	$[6]$	$[7]$	$[8]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[6]$	$[6]$	$[7]$	$[8]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[7]$	$[7]$	$[8]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$
$[8]$	$[8]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$	$[7]$

Multiplikation in $\mathbb{Z}_{11}$

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$	$[7]$	$[8]$	$[9]$	$[10]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$	$[7]$	$[8]$	$[9]$	$[10]$
$[2]$	$[0]$	$[2]$	$[4]$	$[6]$	$[8]$	$[10]$	$[1]$	$[3]$	$[5]$	$[7]$	$[9]$
$[3]$	$[0]$	$[3]$	$[6]$	$[9]$	$[1]$	$[4]$	$[7]$	$[10]$	$[2]$	$[5]$	$[8]$
$[4]$	$[0]$	$[4]$	$[8]$	$[1]$	$[5]$	$[9]$	$[2]$	$[6]$	$[10]$	$[3]$	$[7]$
$[5]$	$[0]$	$[5]$	$[10]$	$[4]$	$[9]$	$[3]$	$[8]$	$[2]$	$[7]$	$[1]$	$[6]$
$[6]$	$[0]$	$[6]$	$[1]$	$[7]$	$[2]$	$[8]$	$[3]$	$[9]$	$[4]$	$[10]$	$[5]$
$[7]$	$[0]$	$[7]$	$[3]$	$[10]$	$[6]$	$[2]$	$[9]$	$[5]$	$[1]$	$[8]$	$[4]$
$[8]$	$[0]$	$[8]$	$[5]$	$[2]$	$[10]$	$[7]$	$[4]$	$[1]$	$[9]$	$[6]$	$[3]$
$[9]$	$[0]$	$[9]$	$[7]$	$[5]$	$[3]$	$[1]$	$[10]$	$[8]$	$[6]$	$[4]$	$[2]$
$[10]$	$[0]$	$[10]$	$[9]$	$[8]$	$[7]$	$[6]$	$[5]$	$[4]$	$[3]$	$[2]$	$[1]$

a) Bestimme in $\mathbb{Z}_9$: $[1]-[8]=$ $\square$ und $-[4]=$ $\square$.

b) Bestimme in $\mathbb{Z}_{11}$ die Restklassen der angegebenen Brüche. Lies die Ergebnisse in der unten stehenden Multiplikationstabelle ab und begründe jeweils Dein Ergebnis.

b_1) $\frac{[1]}{[2]}=$ $\square$, denn $[2]\cdot$ $\square$ $=$ $\square$.

b_2) $\frac{[1]}{[4]}=$ $\square$, denn $\square$

b_3) $\frac{[2]}{[4]}=$ $\square$, denn $\square$

Aufgabe 18

a) Fülle die Verknüpfungstabelle für die Multiplikation in $\mathbb{Z}_4$ aus.

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	[ ]	[ ]	[ ]	[ ]
$[1]$	[ ]	[ ]	[ ]	[ ]
$[2]$	[ ]	[ ]	[ ]	[ ]
$[3]$	[ ]	[ ]	[ ]	[ ]

b) Versuche, in $\mathbb{Z}_4$ die Restklassen folgender Brüche zu bestimmen.

$\frac{[1]}{[3]}$ $\square$,

$\frac{[1]}{[2]}$ $\square$,

$\frac{[2]}{[2]}$ $\square$.

Anmerkung: Wir sehen, dass Brüche nicht immer definiert sind. Wir untersuchen nun, wann Division in $\mathbb{Z}_m$ definiert ist.

Existenz von Brüchen in $\mathbb{Z}_m$: Sei $m \in \mathbb{N}_+$, $a \in \{0, 1, \ldots, m-1\}$ und $b \in \{1, 2, \ldots, m-1\}$.

$$\begin{aligned} \frac{[a]}{[b]} = [x] &\Leftrightarrow [a] = [b] \cdot [x] = [bx] \\ &\Leftrightarrow a \equiv bx \mod m \\ &\Leftrightarrow a - bx = km \quad \text{für ein } k \in \mathbb{Z} \\ &\Leftrightarrow a = b\underbrace{x}_{\text{gesucht}} + m\underbrace{k}_{\text{unbekannt}} \end{aligned}$$

Dies ist eine diophantische Gleichung für die Unbekannten $x, k \in \mathbb{Z}$.

Wir wissen: Falls ggT$(b, m) \mid a$, ist die Gleichung lösbar.

Sei nun m eine Primzahl. Dann gilt ggT$(b, m) = 1$.

$\Rightarrow$ Für jedes $a \in \mathbb{N}$ existiert eine Lösung $(x_0 \mid k_0)$. Alle Lösungen sind durch

$$(x \mid k) = (x_0 + lm \mid k - lb) \text{ mit } l \in \mathbb{Z}$$

gegeben. Wir suchen nur $x = x_0 + lm$ und sehen $[x] = [x_0]$. Also ist $[x]$ eindeutig.

Damit ist bewiesen:

Satz vom Dividieren: Ist p eine Primzahl, und sind $a \in \{0, 1, \ldots, p-1\}$, $b \in \{1, \ldots, p-1\}$, so besitzt die Gleichung

$$[b] \cdot [x] = [a] \qquad \text{in } \mathbb{Z}_p$$

genau eine Lösung $[x]$, d.h. $\frac{[a]}{[b]} := [x]$ ist definiert.

Aufgabe 19

In $\mathbb{Z}_{37}$ soll der Bruch $\frac{[5]}{[33]}$ bestimmt werden.

a) Führe den euklidischen Algorithmus zur Bestimmung von $\mathrm{ggT}(37, 33)$ durch.

b) Erweitere den euklidischen Algorithmus, um eine Lösung $(k \mid l)$ der diophantischen Gleichung $k \cdot 33 + l \cdot 37 = 1$ zu berechnen.

c) Sei $(k \mid l)$ die in b) bestimmte Lösung. Bestimme mit dem k aus dieser Lösung die Restklasse $[x] = [k] \cdot [33]$ in $\mathbb{Z}_{37}$, wobei $0 \leq x < 37$ gelten soll.

d) Bestimme die Restklasse $[y] = \frac{[1]}{[33]}$, wobei $0 \leq y < 37$ gelten soll.

e) Bestimme die Restklasse $[z] = \frac{[5]}{[33]}$, wobei $0 \leq z < 37$ gelten soll.

7 Die Vigenère-Verschlüsselung

Beginn Online-Einheit 5

Diese Verschlüsselung arbeitet mit einem Passwort und einer Tabelle. Man schreibt das Passwort Buchstabe für Buchstabe unter den Originaltext und wiederholt dies so lange, bis der Text zu Ende ist.

Verschlüsselung von „HEUTE IST ES SEHR HEISS“ mit dem Passwort „primzahl“:

Klartext:	H	E	U	T	E	I	S	T	E	S	S	E	H	R	H	E	I	S	S
	p	r	i	m	z	a	h	l	p	r	i	m	z	a	h	l	p	r	i
Chiffretext:	w	v	c	f	d	i	z	e	t	j	a	q	g	r	o	p	x	j	a

Der Buchstabe H wird nun mit p verschlüsselt. Das bedeutet, man geht in die Zeile, die links mit p beginnt. Der verschlüsselte Buchstabe ist der, der in dieser Zeile in der H-Spalte steht. Entsprechend wird der Buchstabe E mit r verschlüsselt.

Vigenère-Quadrat:

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
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
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	a
c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	k	k
m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	l	l	m	n	o
q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
z	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

Zum Entschlüsseln muss man nun entsprechend vorgehen. Man schreibt wieder das Passwort Wort für Wort unter den verschlüsselten Text. Erhält man oben im Beispiel als erstes den Buchstaben w, so geht man in der p-Zeile zum Buchstaben w und dann nach oben zum H.

Aufgabe 20

Entschlüssle mit dem Passwort „dreieck“ den Text

h e x a g j v x v w a i n x l j x m m p p d t l

Anmerkung: Als die Vigenère-Verschlüsselung entwickelt wurde, galt sie als sehr sicher. Mit einem entsprechenden Computerprogramm ist sie heutzutage einfach zu knacken, wenn das Passwort nicht zu lange ist. Wie man das macht, kannst Du im Online-Kurs sehen.

8 Potenzen im Restklassenring

Beginn Online-Einheit 6

Aufgabe 21

In dieser Aufgabe soll in $\mathbb{Z}_7 = \{[0], [1], [2], \ldots, [6]\}$ gerechnet werden. Das bedeutet, dass als Ergebnisse nur die Zahlen $0, 1, 2, 3, 4, 5, 6$ eingetragen werden sollen.

Bestimme die Potenzen $[a]^k$ in $\mathbb{Z}_7$ und trage Deine Ergebnisse in die Tabelle ein.
Hinweise: Du kannst die unten stehende Verknüpfungstabelle benützen. Wenn Du die Beziehung $[a]^{k+1} = [a] \cdot [a]^k$ verwendest, geht es leichter.

$k =$	1	2	3	4	5	6
$[2]^k =$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
$[3]^k =$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
$[4]^k =$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
$[5]^k =$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
$[6]^k =$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
$[0]^k =$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

Verknüpfungstabelle für die Multiplikation in $\mathbb{Z}_7$:

$\cdot$	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[2]	[0]	[2]	[4]	[6]	[1]	[3]	[5]
[3]	[0]	[3]	[6]	[2]	[5]	[1]	[4]
[4]	[0]	[4]	[1]	[5]	[2]	[6]	[3]
[5]	[0]	[5]	[3]	[1]	[6]	[4]	[2]
[6]	[0]	[6]	[5]	[4]	[3]	[2]	[1]

Frage: Fällt Dir an der Potenztabelle etwas auf? Erkennst Du ein Muster oder eine Regelmäßigkeit?

Kleiner Satz von Fermat: Sei p Primzahl, $a \in \mathbb{Z}$ kein Vielfaches von p. Dann gilt

$$[a]^{p-1} = [1] \text{ in } \mathbb{Z}_p \qquad \text{bzw.} \qquad a^{p-1} \equiv 1 \mod p.$$

Anmerkungen:
1) Die beiden Gleichungen sind nur verschiedene Schreibweisen für denselben Sachverhalt.
2) Du kannst nun in der Tabelle der letzten Aufgabe die Restklassen $[1]$ rot umkringeln, die der kleine Satz von Fermat behauptet.
3) Falls a Vielfaches von p ist, gilt $[a] = [0]$. Dann folgt $[a]^k = 0$ in $\mathbb{Z}_p$ bzw. $a^k \equiv 0 \mod p$ für alle $k \in \mathbb{N}_+$.

Beispiel: $2^{40} \equiv ? \mod 19$:
Kleiner Fermat: $2^{19-1} \equiv 1 \mod 19$
$\Rightarrow\ 2^{40} = 2^{18} \cdot 2^{18} \cdot 2^4 \equiv 1 \cdot 1 \cdot 16 = 16 \mod 19$

Anmerkung: Wir beweisen nun, dass die Aussage des Satzes richtig ist.

Beweis: Wir untersuchen die Teilmenge
$A = \{[0a], [1a], [2a], \ldots, [(p-1)a]\}$
von $\mathbb{Z}_p = \{[0], [1], \ldots, [p-1]\}$.

Anmerkung: Dass A Teilmenge von $\mathbb{Z}_p$ ist bedeutet, dass alle Elemente der Menge A auch Elemente der Menge $\mathbb{Z}_p$ sind. In der Aufzählung der Restklassen, die in der Menge A liegen, stehen eventuell andere Repräsentanten als bei den Elementen von $\mathbb{Z}_p$.

Schritt 1: Wir beweisen, dass alle p Restklassen $[0a]$, $[1a]$, $[2a]$, $\ldots$, $[(p-1)a]$ verschieden sind.

Annahme: $[ja] = [ka]$ für zwei dieser Restklassen mit $j < k$. Dann folgt

$[0] = [ka] - [ja] = [ka - ja] = \big[(k-j)a\big] = [k-j] \cdot [a]$ mit $[k-j] \neq [0]$
$\underset{\text{Dividieren}}{\overset{\text{Satz vom}}{\Rightarrow}} [a] = [0]$, d.h. a ist Vielfaches von p $\Rightarrow$ Widerspruch
Also muss $[ja] \neq [ka]$ für $j \neq k$ gelten.

Schritt 2: Die Menge A hat p verschiedene Elemente und ist Teilmenge der p-elementigen Menge $\mathbb{Z}_p$. Also sind die Mengen gleich.

Schritt 3: Es ist klar, das $[0a] = [0]$ gilt. Wir entfernen nun dieses Element aus beiden Mengen. Das Produkt der restlichen Elemente muss gleich sein:

$$\begin{array}{rcl} & [a] \cdot [2a] \cdot [3a] \cdots [(p-1)a] &=& [1] \cdot [2] \cdot [3] \cdots [p-1] \\ \underset{\text{Satz vom Dividieren}}{\overset{\text{Satz vom}}{\Leftrightarrow}} & [1] \cdot [2] \cdot [3] \cdots [p-1] \cdot [a]^{p-1} &=& [1] \cdot [2] \cdot [3] \cdots [p-1] \\ \Rightarrow & [a]^{p-1} = [1] \text{ in } \mathbb{Z}_p. & & \end{array}$$ □

Satz (Brüche berechnen): Sei p eine Primzahl und $[a] \in \mathbb{Z}_p$, $[a] \neq [0]$. Dann gelten:

1) $\dfrac{[1]}{[a]} \underset{\text{Fermat}}{\overset{\text{Kleiner}}{=}} \dfrac{[a]^{p-1}}{[a]} = [a]^{p-2}$,

2) $\dfrac{[1]}{[a]^k} = \dfrac{[a]^{p-1}}{[a]^k} = [a]^{p-1-k}$ für $k = 1, 2, \ldots, p-2$.

Brüche können also durch Potenzen berechnet werden.

Aufgabe 22

Berechne die folgenden Brüche jeweils im angegebenen Restklassenring.

a) $\dfrac{[1]}{[5]^{20}}$ in $\mathbb{Z}_{23}$:

b) $\dfrac{[13]}{[5]^{20}}$ in $\mathbb{Z}_{23}$:

c) $\dfrac{[1]}{[4]^6}$ in $\mathbb{Z}_{13}$:

d) $\dfrac{[10]}{[4]^5}$ in $\mathbb{Z}_{13}$:

Aufgabe 23

Bestimme jeweils alle Lösungen der angegebenen Gleichung.

a) $[2] \cdot [x] = [5]$ in $\mathbb{Z}_7$,

b) $2 \cdot x \equiv 5 \mod 7$,

c) $4 \cdot x \equiv 3 \mod 11$.

Hinweis: Beachte, dass Kongruenz-Gleichungen unendlich viele Lösungen besitzen, so wie jede Restklasse unendlich viele Elemente besitzt.

Definition: Ein Element $[g] \in \mathbb{Z}_m$ heißt Primitivwurzel, falls durch $[g]^k$ alle Elemente von $\mathbb{Z}_m$ außer $[0]$ dargestellt werden können.

Beispiel: In $\mathbb{Z}_5$:

$k =$	1	2	3	4
$[2]^k =$	$[2]$	$[4]$	$[3]$	$[1]$
$[4]^k =$	$[4]$	$[1]$		

$\Rightarrow$ $[2]$ ist eine Primitivwurzel, aber $[4]$ nicht.

Aufgabe 24

a) Bestimme mit Hilfe der Potenztabellen in $\mathbb{Z}_7$ (Aufgabe 21), welche Elemente von $\mathbb{Z}_7$ Primitivwurzeln sind.

Primitivwurzeln in $\mathbb{Z}_7$ sind:

Keine Primitivwurzeln in $\mathbb{Z}_7$ sind:

b) Fülle für $\mathbb{Z}_{11}$ in der folgenden Potenztabelle jede Zeile so weit aus, bis Du das Element $[1]$ erhältst.

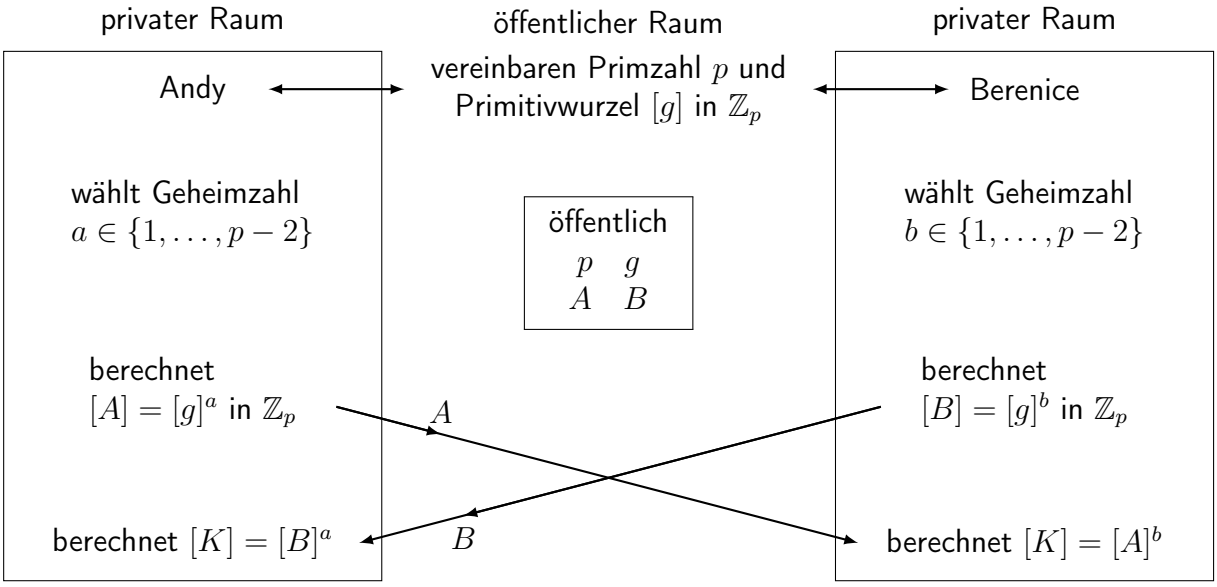
$k =$	1	2	3	4	5	6	7	8	9	10
$[10]^k =$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
$[6]^k =$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
$[3]^k =$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
$[2]^k =$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

c) Welche der Elemente $[10], [6], [3], [2]$ sind Primitivwurzeln?

In $\mathbb{Z}_{11}$ sind Primitivwurzeln:

Anmerkung: Primitivwurzeln bilden eine Grundlage für den ersten Verschlüsselungsalgorithmus, den wir jetzt kennenlernen.

9 Der Diffie-Hellman-Merkle-Schlüsselaustausch



Andy und Berenice erhalten die selbe Schlüsselzahl K, denn es gilt

$[B]^a = \left([g]^b\right)^a = [g]^{ab} = \left([g]^a\right)^b = [A]^b$.

Aufgabe 25

Andy und Berenice vereinbaren $p = 7$ und $g = 3$.

Andy wählt: $a = 3$, berechnet A: $[g]^a =$ in $\mathbb{Z}_7 \Rightarrow A =$

Berenice wählt: $b = 4$, berechnet B: $[g]^b =$ in $\mathbb{Z}_7 \Rightarrow B =$

Hinweis: A, B müssen zwischen 1 und 6 liegen.

Öffentlich bekannt sind also:

$p = 7$, $g = 3$, $A =$, $B =$.

Andy berechnet: $[B]^a =$ in $\mathbb{Z}_7 \Rightarrow K =$

Berenice berechnet: $[A]^b =$ in $\mathbb{Z}_7 \Rightarrow K =$

Hinweis: K muss zwischen 1 und 6 liegen.

Für Andy und Berenice kommt die selbe Zahl K als Ergebnis heraus. Schreibe diese Zahl mit Buchstaben als Wort und verwende dieses Zahlwort als Schlüsselwort für die Vigenère-Entschlüsselung, um die Nachricht `izqtimew` zu entschlüsseln.

Verschlüsselt	i	z	q	t	i	m	e	w
Schlüssel								
Nachricht								

Aufgabe 26

Andy und Berenice vereinbaren $p = 11$ und $g = 2$. Andy schickt an Berenice die Zahl $A = 5$, Berenice meldet $B = 8$. Kurze Zeit später übermittelt Andy die Nachricht

h i x y z q w k n c t v m

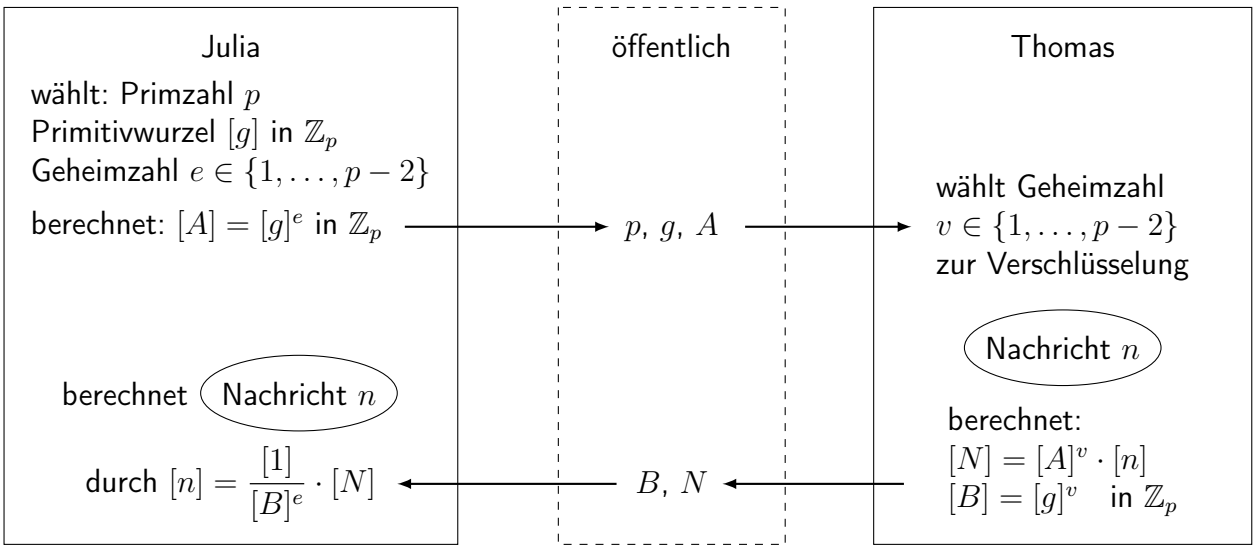
Bestimme a, b und den Schlüssel K, entschlüssle die Nachricht mit dem Zahlwort zu K als Schlüsselwort für Vigenère-Entschlüsselung.

Hinweis: Verwende die Tabelle der Potenzen $[2]^k$ aus Aufgabe 24.

Anmerkung: Die Verschlüsselung kann hier geknackt werden, da für p, g, a, b kleine Zahlen verwendet wurden. In der richtigen Anwendung werden sehr große Zahlen verwendet. Dann ist es schwierig, aus g und A die Zahl a zu berechnen.

10 Die Elgamal-Verschlüsselung

Beginn Online-Einheit 7



Julia berechnet die richtige Nachricht n, denn es gilt

$$\begin{aligned}\frac{[1]}{[B]^e} \cdot [N] &= \frac{[1]}{[B]^e} \cdot [A]^v \cdot [n] \\ &= \frac{[1]}{\left([g]^v\right)^e} \cdot \left([g]^e\right)^v \cdot [n] \\ &= \frac{[1]}{[g]^{ve}} \cdot [g]^{ev} \cdot [n] \\ &= [n] \text{ in } \mathbb{Z}_p.\end{aligned}$$

Wieder beruht die Entschlüsselung auf der Gleichheit $\left([g]^v\right)^e = \left([g]^e\right)^v$.

Anmerkung: Mit der Elgamal-Verschlüsselung können Nachrichten n zwischen 1 und p ver- und entschlüsselt werden.

Aufgabe 27

Julia wählt $p = 23$ und die Primitivwurzel $[5]$ in $\mathbb{Z}_{23}$. Weiter wählt sie den Entschlüsselungsexponent $e = 14$ und berechnet

$$[A] = [5]^{14} = [25]^7 = [25 - 23]^7 = [2]^7 = [128] = [128 - 115] = [13] \text{ in } \mathbb{Z}_{23}.$$

Julia veröffentlicht auf ihrer Homepage $(p, g, A) = (23, 5, 13)$.

a) Thomas möchte die Nachricht $n = 11$ an Julia senden. Dazu wählt er den Verschlüsselungsexponent $v = 3$ und berechnet in $\mathbb{Z}_{23}$

$[B] \;=\; [g]^v \;=\; [5]^3 \;=$ in $\mathbb{Z}_{23}$,

$[A]^v \;=\; [13]^3 \;=$ in $\mathbb{Z}_{23}$,

$[N] \;=\; [A]^v \cdot [n] \;=\; [12] \cdot [11] \;=$ in $\mathbb{Z}_{23}$.

Thomas schickt also $(B = \qquad\qquad , N = \qquad\qquad)$ an Julia.

Julia berechnet als erstes $[B]^{-14} = [B]^{22-14} = [B]^8 = [B^2]^4 = [B^2 - 92]^4 =$

in $\mathbb{Z}_{23}$.

Hinweis: $[18] = [-5]$ kann hilfreich sein.

Dann erhält sie die Nachricht n durch Multiplikation:

$[n] = [B]^{-14} \cdot [N] =$ in $\mathbb{Z}_{23}$.

b) Marc schickt an Julia $(B, N) = (3, 21)$. Welche Nachricht n hat er an Julia geschickt?

$[B]^{-14} =$ in $\mathbb{Z}_{23}$,

$[n] =$ in $\mathbb{Z}_{23}$.

c) Zusatzaufgabe: Erstelle die Potenztabelle für $[5]^k$ um herauszufinden, welchen Verschlüsselungsexponent Marc gewählt hat.
Kennzeichne Marcs Verschlüsselungsexponent durch Umkringeln.

$k =$	1	2	3	4	5	6	7	8	9	10	11
$[5]^k =$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

$k =$	12	13	14	15	16	17	18	19	20	21	22
$[5]^k =$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

11 Kongruenzgleichungen

Beispiel: $x \cdot 9 \equiv 1 \mod 16$ $(*)$

Anmerkung: Man könnte daran denken, die Gleichung als $[x]\cdot[9] = [1]$ in $\mathbb{Z}_{16}$ zu lösen. Aber der kleine Fermat ist nicht anwendbar, da $m = 16$ keine Primzahl ist. Daher müssen wir unsere Kenntnisse über diophantische Gleichungen benützen.

Lösung: $(*) \Leftrightarrow 9x + 16y = 1$ für ein $y \in \mathbb{Z}$.

Verallgemeinerter euklidischer Algorithmus:

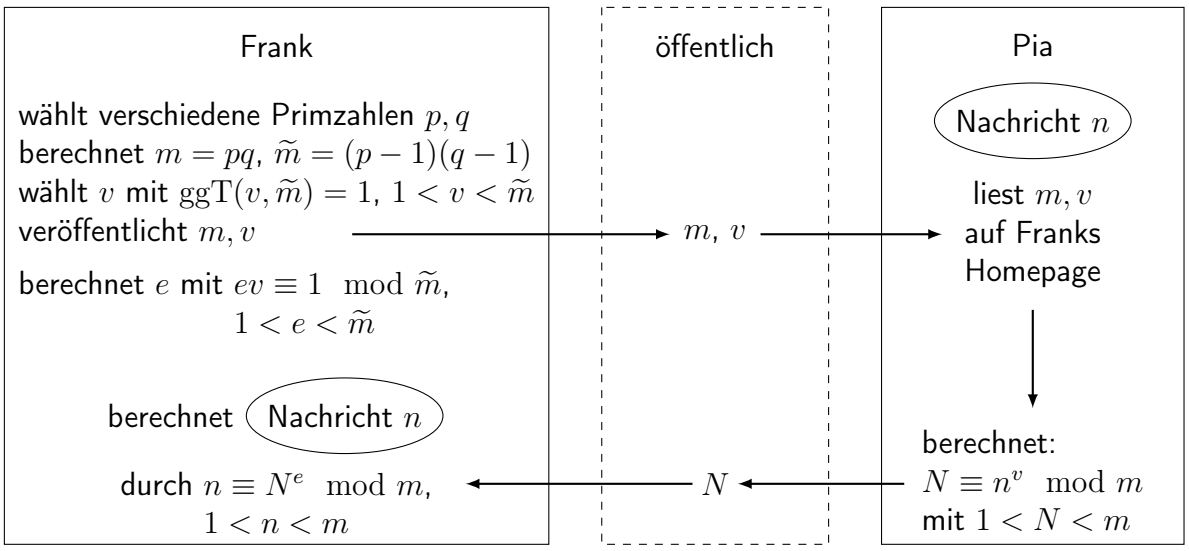
$$\begin{array}{rcl|rcl} 16 &=& 1\cdot 9 + 7 & 7 &=& 16 - 1\cdot 9 \\ 9 &=& 1\cdot 7 + 2 & 2 &=& 9 - 1\cdot 7 \\ 7 &=& 3\cdot 2 + 1 & 1 &=& 7 - 3\cdot 2 = 7 - 3(9 - 1\cdot 7) \\ & & & &=& 4\cdot 7 - 3\cdot 9 = 4(16 - 1\cdot 9) - 3\cdot 9 \\ & & & &=& 4\cdot 16 - 7\cdot 9 \end{array}$$

$\Rightarrow$ $(x, y) = (-7 \mid 4)$ ist eine Lösung.

Alle Lösungen: $(x, y) = (-7 + 16k \mid 4 - 9k)$ mit $k \in \mathbb{Z}$.

$\Rightarrow$ Alle Lösungen von $(*)$: $x = -7 + 16k$ mit $k \in \mathbb{Z}$.

12 Das RSA-Verfahren



Anmerkungen:
1) Ist m das Produkt zweier sehr großer Primzahlen (z.B. je 10 Stellen), dann ist es schwierig, aus m auf p, q zu schließen.
2) Für die Nachricht n steht im Vergleich zum Elgamal-Verfahren ein großer Zahlenraum zur Verfügung. Hier werden Nachrichten n zwischen 2 und $m = pq - 1$ ver- und entschlüsselt.

Aufgabe 28

Frank wählt: $p = 3$, $q = 11$,
berechnet: $m =$, $\widetilde{m} =$
wählt: Verschlüsselungsexponent $v = 7$ (erfüllt $1 < v < \widetilde{m}$ und ggT$(v, \widetilde{m}) = 1$)
veröffentlicht: $m =$ und $v = 7$
berechnet: e:

Pia liest die Homepage von Frank und will ihm die Nachricht $\boxed{n = 6}$ übermitteln. Sie berechnet Modulo 33: $n^v = 6^7 =$

und schickt Frank $\boxed{N =}$. Frank liest in Pias Mail $\boxed{N =}$ und berechnet Modulo 33: $N^e =$

erhält also $\boxed{n =}$ zurück.

Anmerkung: Der Entschlüsselungsexponent e muss zwischen 1 und $m-1$ liegen. Falls der erweiterte euklidische Algorithmus einen negativen Wert für e liefert, muss mit der allgemeinen Formel der richtige Wert für e ermittelt werden.

Aufgabe 29

Frank veröffentlicht auf seiner Homepage die Zahlen $m = 55$ und $v = 7$. Er erhält von Peter die Zahl $N = 25$.

Bestimme $p, q, \widetilde{m}, e$ und die entschlüsselte Botschaft n.

Aufgabe 30

Frank veröffentlicht auf seiner Homepage die Zahlen $m = 51$ und $v = 3$. Er erhält von Jane die Zahl $N = 8$ als verschlüsselte Botschaft.

Bestimme $p, q, \widetilde{m}, e$ und die entschlüsselte Botschaft n.

Beweis, dass Frank die richtige Zahl n berechnet:

Seien $p, q, m, \widetilde{m}, e, v, n, N$ gemäß dem RSA-Algorithmus gewählt bzw. berechnet.

Wir beweisen, dass $\boxed{N^e \equiv n \mod m}$ gilt.

Kleiner Fermat: Ist p Primzahl und $a \in \mathbb{N}$ kein Vielfaches von p, so gilt $a^{p-1} \equiv 1 \mod p$.

Vorbemerkung 1: $\underbrace{a \equiv n \mod p}_{a-n \text{ durch } p \text{ teilbar}}$ und $\underbrace{a \equiv n \mod q}_{a-n \text{ durch } q \text{ teilbar}} \overset{p,q \text{ Primzahlen}}{\Leftrightarrow} a \equiv n \mod \underbrace{pq}_{=m}$.

Vorbemerkung 2: $e \cdot v \equiv 1 \mod \widetilde{m}$
$\Leftrightarrow e \cdot v = 1 + k\widetilde{m} = 1 + k(p-1)(q-1)$ mit einem $k \in \mathbb{Z}$.

Wir rechnen zunächst nur modulo p.
Vorbemerkung 1 $\Rightarrow N^e \equiv (n^v)^e = n^{e \cdot v} \mod p$

Fall $\mathrm{ggT}(n, p) = 1$:

$$n^{e \cdot v} \overset{\text{Vorbemerkung 2}}{=} n^{1+k(p-1)(q-1)} = n \cdot (n^{p-1})^{k(q-1)} \overset{\substack{\text{kleiner} \\ \text{Fermat}}}{\equiv} n \cdot 1^{k(q-1)} = n \mod p$$

Fall $\mathrm{ggT}(n, p) = p$: Dann ist $n = l \cdot p$ und somit $n \equiv 0 \mod p$.
$\Rightarrow n^{e \cdot v} \equiv 0^{e \cdot v} = 0 \equiv n \mod p$.

In beiden Fällen gilt also

$$N^e \equiv n^{e \cdot v} \equiv n \mod p. \tag{1}$$

Nun rechnen wir nur modulo q. Indem man p und q vertauscht, folgt genauso, dass

$$N^e \equiv n^{e \cdot v} \equiv n \mod q \tag{2}$$

gilt.

(1) und (2) $\overset{\substack{\text{Vorbemerkung 1} \\ \Rightarrow \\ pq=m}}{\Rightarrow}$ $\boxed{N^e \equiv n \mod m}$. $\square$

13 Lösungen der Aufgaben

Aufgabe 1

Versuche, jeweils ganzzahlige Lösungen $(x \mid y)$ der angegebenen Gleichung zu finden.
Falls du vermutest, dass es keine Lösung gibt, begründe deine Vermutung.

a) $x + 3y = 10$: $x = 10 - 3y$, z.B. $(x \mid y) = (7 \mid 1), (4 \mid 2), (1 \mid 3), (13 \mid -1)$

b) $3x + 7y = 1$: z.B. $(x \mid y) = (-2 \mid 1), (5 \mid -2), (12 \mid -5), (-9 \mid 4)$

c) $18x + 12y = 3$: Keine Lösung: Linke Seite gerade, rechte ungerade

d) $5x + 5y = 1$: Keine Lösung: Linke Seite ist durch 5 teilbar, rechte nicht

e) $5x + 15y = 50$: Teile die Gleichung auf beiden Seiten durch 5: $x + 3y = 10$
$\Rightarrow$ Gleichung ist die selbe wie in a), also die selben Lösungen

f) $18x + 12y = 66$: Teile Gleichung durch 6: $3x + 2y = 11$,
z.B. $(x \mid y) = (-1 \mid 7), (1 \mid 4), (3 \mid 1), (5 \mid -2)$

Aufgabe 2

Gegeben sind diophantische Gleichungen der Form $ax + by = c$. Bestimme jeweils die Menge der gemeinsamen Teiler von a und b, den $\mathrm{ggT}(a, b)$ und untersuche, ob $\mathrm{ggT}(a, b)$ Teiler von c ist. Falls es Lösungen gibt, vereinfache die Gleichung, indem Du beide Seiten durch die selbe geeignet gewählte Zahl teilst und rate eine Lösung $(x \mid y)$.

a) $18x + 12y = 24$:

Menge der gemeinsamen Teiler von 18 und 12: $\{ \quad 1, 2, 3, 6 \quad \}$,

$\mathrm{ggT}(12, 18) =$ 6.

Die Gleichung ist

	nicht lösbar, denn	
×	lösbar, denn ich habe eine Lösung gefunden:	
	Vereinfachte Gleichung:	$3x + 2y = 4$
	Eine Lösung: $(x \mid y) =$	$(\ 0 \mid 2\ )$

b) $45x + 30y = 5$:

Menge der gemeinsamen Teiler von 45 und 30: $\{ \quad 1, 3, 5, 15 \quad \}$,

$\mathrm{ggT}(45, 30) =$ 15.

Die Gleichung ist

×	nicht lösbar, denn	15 ist kein Teiler von $c = 5$
	lösbar, denn ich habe eine Lösung gefunden:	
	Vereinfachte Gleichung:	
	Eine Lösung: $(x \mid y) =$	$(\quad \mid \quad)$

Aufgabe 3

Teile jeweils a durch b mit Rest und schreibe die Lösung als Gleichung $a = k \cdot b + r$ auf.

a) $a = 143,\ b = 12$: $a = 11b + 11$

b) $a = 14130,\ b = 58$: $a = 243b + 36$

c) $a = 1\,111\,111,\ b = 2\,222$: $a = 500b + 111$

d) $a = 123\,321,\ b = 2\,010$: $a = 61b + 711$

Aufgabe 4

Berechne mit dem Euklidischen Algorithmus:

a) $\mathrm{ggT}(150, 54)$,

b) $\mathrm{ggT}(300, 468)$,

c) $\mathrm{ggT}(2717, 2431)$,

d) $\mathrm{ggT}(4263, 4641)$.

Lösung: **a)**
$$\begin{aligned} 150 &= 2 \cdot 54 + 42 \\ 54 &= 1 \cdot 42 + 12 \\ 42 &= 3 \cdot 12 + 6 \\ 12 &= 2 \cdot 6 \end{aligned} \quad \Rightarrow\ \mathrm{ggT}(150, 54) = 6$$

b)
$$\begin{aligned} 468 &= 1 \cdot 300 + 168 \\ 300 &= 1 \cdot 168 + 132 \\ 168 &= 1 \cdot 132 + 36 \\ 132 &= 3 \cdot 36 + 24 \\ 36 &= 1 \cdot 24 + 12 \\ 24 &= 2 \cdot 12 \end{aligned} \quad \Rightarrow\ \mathrm{ggT}(300, 468) = 12$$

c)
$$\begin{aligned} 2717 &= 1 \cdot 2431 + 286 \\ 2431 &= 8 \cdot 286 + 143 \\ 286 &= 2 \cdot 143 \end{aligned} \quad \Rightarrow\ \mathrm{ggT}(2717, 2431) = 143$$

d)
$$\begin{aligned} 4641 &= 1 \cdot 4263 + 378 \\ 4263 &= 11 \cdot 378 + 105 \\ 378 &= 3 \cdot 105 + 63 \\ 105 &= 1 \cdot 63 + 42 \\ 63 &= 1 \cdot 42 + 21 \\ 42 &= 2 \cdot 21 \end{aligned} \quad \Rightarrow\ \mathrm{ggT}(4263, 4641) = 21$$

Aufgabe 5

Bestimme jeweils eine ganzzahlige Lösung $(x \mid y)$ der angegebenen Gleichung. Berechne dazu in den Aufgabenteilen a) und d) zunächst den ggT der Koeffizienten mit Hilfe des euklidischen Algorithmus. Erweitere dann den Algorithmus, um eine Lösung zu finden.

a) $96x + 66y = 6$,

b) $96x + 66y = 18$ (verwende hierzu die Lösung aus Teil a)),

c) Für beliebiges fest vorgegebenes $n \in \mathbb{N}$: $96x + 66y = n \cdot 6$ (auch hier erweist sich die Lösung aus Teil a) als nützlich),

d) $119x + 143y = 1$,

e) $119x + 143y = 4$.

Lösung: **a)**
$$\begin{array}{rcl|rcl} 96 &=& 1\cdot 66+30 & 30 &=& 96-1\cdot 66\\ 66 &=& 2\cdot 30+6 & 6 &=& 66-2\cdot 30\\ 30 &=& 5\cdot 6 & & & \end{array}$$

$$\Rightarrow \ \mathrm{ggT}(96,66) = 6 = 66-2\cdot(96-1\cdot 66) = 3\cdot 66 - 2\cdot 96$$

$$\Rightarrow \ (x \mid y) = (-2 \mid 3)$$

b) Die Lösung aus a) muss mit 3 multipliziert werden: $(x \mid y) = (-6 \mid 9)$.

c) Die Lösung aus a) muss mit n multipliziert werden: $(x \mid y) = (-2n \mid 3n)$.

d)
$$\begin{array}{rcl|rcl} 143 &=& 1\cdot 119+24 & 24 &=& 143-1\cdot 119\\ 119 &=& 4\cdot 24+23 & 23 &=& 119-4\cdot 24\\ 24 &=& 1\cdot 23+1 & 1 &=& 24-1\cdot 23\\ 23 &=& 23\cdot 1 & & & \end{array}$$

$$\Rightarrow \ \mathrm{ggT}(143,119) = 1 = 24-1\cdot(119-4\cdot 24) = 5\cdot 24-119 = 5\cdot(143-1\cdot 119)-119 = 5\cdot 143-6\cdot 119$$

$\Rightarrow \ 119\cdot(-6)+143\cdot 5 = 1$. Also ist $(x \mid y) = (-6 \mid 5)$ eine Lösung.

e) Da die rechte Seite $= 4\cdot\mathrm{ggT}(119,143)$ ist, müssen die Zahlen aus d) noch mit 4 multipliziert werden (vgl. b), c)).

$\Rightarrow \ (x \mid y) = (-24 \mid 20)$

Aufgabe 6

Bestimme durch Probieren mehrere ganzzahlige Lösungen $(x \mid y)$, möglichst alle.

a) $3x+2y=1$: $(x \mid y) = (-1 \mid 2),\ (1 \mid -1),\ (3 \mid -4),\ (5 \mid -7),\ (7 \mid -10), \ldots$
oder allgemein: $(x \mid y) = (1+2k \mid -1-3k),\ k \in \mathbb{Z}$

b) $3x+9y=3$: $(x \mid y) = (1 \mid 0),\ (4 \mid -1),\ (7 \mid -2),\ (10 \mid -3), \ldots$
oder allgemein: $(x \mid y) = (1+3k \mid 0-k),\ k \in \mathbb{Z}$

Aufgabe 7

Gegeben ist die Gleichung

$$144x+52y = 8. \qquad (*)$$

a) Bestimme $\mathrm{ggT}(144,52)$ mit Hilfe des euklidischen Algorithmus.

b) Erweitere den euklidischen Algorithmus und berechne eine ganzzahlige Lösung $(x \mid y)$ der Gleichung $144x+52y = \mathrm{ggT}(144,52)$.

c) Berechne eine Lösung von $(*)$.

d) Teile die Gleichung $(*)$ auf beiden Seiten durch $\mathrm{ggT}(144,52)$ und gib die Gleichung an, die dadurch ensteht.

e) Gib alle ganzzahligen Lösungen von $(*)$ an.

Lösung: **a)** und **b)**

$$\begin{array}{rcl|rcl} 144 &=& 2\cdot 52+40 & 40 &=& 144-2\cdot 52\\ 52 &=& 1\cdot 40+12 & 12 &=& 52-40\\ 40 &=& 3\cdot 12+4 & 4 &=& 40-3\cdot 12\\ 12 &=& 3\cdot 4 & & & \end{array}$$

$$\begin{aligned} \mathrm{ggT}(144,52) = 4 &= 40-3(52-40)\\ &= 4\cdot 40-3\cdot 52\\ &= 4(144-2\cdot 52)-3\cdot 52\\ &= 4\cdot 144-11\cdot 52 \end{aligned}$$

$\Rightarrow\ (x \mid y) = (4 \mid -11)$ ist eine Lösung von $144x+52y = 4 = \mathrm{ggT}(144,52)$

b) $8 = 2\cdot \mathrm{ggT}(144,52)\ \Rightarrow\ (x \mid y) = (2\cdot 4 \mid 2\cdot(-11)) = (8 \mid -22)$ ist eine Lösung.

c) $36x+13y = 2$.

d) $(x \mid y) = (8+k\cdot 13 \mid -22-k\cdot 36)$ mit $k\in\mathbb{Z}$.

Aufgabe 8

Bestimme jeweils alle Lösungen für die Gleichungen aus Aufgabe 5.

a) $96x+66y = 6$,

b) $96x+66y = 18$,

c) Für beliebiges fest vorgegebenes $n\in\mathbb{N}$: $96x+66y = n\cdot 6$,

d) **Zusatzaufgabe:** $119x+143y = 1$,

e) **Zusatzaufgabe:** $119x+143y = 4$.

Lösung: **a)** Aus der Aufgabe 1a ist bekannt: Eine Lösung ist $(x \mid y) = (-2 \mid 3)$. Teile die Gleichung durch $\mathrm{ggT}(96,66) = 6$:

$$96x+66y = 6 \ \Leftrightarrow\ 16x+11y = 1.$$

Wegen $\mathrm{ggT}(16,11) = 1$ sind nach dem letzten Satz alle Lösungen gegeben durch

$$(x \mid y) \ = \ (-2+11k \mid 3-16k), \quad (k\in\mathbb{Z}).$$

b) Genauso: Eine Lösung ist $(x \mid y) = (-6 \mid 9)$. Teile die Gleichung durch 6: $16x+11y = 3$. Alle Lösungen:

$$(x \mid y) \ = \ (-6+11k \mid 9-16k), \quad (k\in\mathbb{Z}).$$

Beachte, dass nur der Teil der Lösung aus Teil a), der nicht den Faktor k enthält, mit 3 multipliziert wird!

c) Genauso: Alle Lösungen $(x \mid y) = (-2n+11k \mid 3n-16k)$, $(k\in\mathbb{Z})$.

d) Wegen $\mathrm{ggT}(143,119) = 1$ sind bereits die Voraussetzungen des letzten Satzes erfüllt. Eine Lösung ist $(x \mid y) = (-6 \mid 5)$.

$\Rightarrow\ (x \mid y) = (-6+143k \mid 5-119k)$ mit $k\in\mathbb{Z}$ sind alle Lösungen.

e) Alle Lösungen sind $(x \mid y) = (-24+143k \mid 20-119k)$ mit $k\in\mathbb{Z}$.

Aufgabe 9

Bestimme den Rest beim Teilen durch 9.

a) 1000: $R = 1$ **b)** 2005: $R = 7$ **c)** 2050: $R = 7$

d) 1035: $R = 0$ **e)** 5103: $R = 0$

Aufgabe 10

Bestimme eine vierstellige, eine fünfstellige und eine sechsstellige Zahl, die beim Teilen durch 9 den Rest 3 lassen.

Lösung: Z.B. $1\,002 = 999 + 3$, $10\,002 = 9\,999 + 3$, $100\,002 = 99\,999 + 3$.

Aufgabe 11

Bestimme jeweils das Ergebnis beim Teilen mit Rest. Trage Deine Lösungen in die Kästchen ein.

a) $33 = \boxed{5} \cdot 6 + \boxed{3}$

$\Rightarrow 33 \equiv \boxed{3} \mod 6$

b) $-101 = \boxed{-26} \cdot 4 + \boxed{3}$

$\Rightarrow -101 \equiv \boxed{3} \mod 4$

Aufgabe 12

Bestimme jeweils möglichst alle ganzzahligen Lösungen x der angegebenen Gleichung.

a) $5 + x \equiv 2 \mod 7$: $L = \{\ldots, -10, -3, 4, 11, \ldots\}$
$= \{4 + 7k \text{ mit beliebigem } k \in \mathbb{Z}\}$

b) $5 \cdot x \equiv 2 \mod 7$: $L = \{\ldots, -8, -1, 6, 13, \ldots\}$
$= \{6 + 7k \text{ mit beliebigem } k \in \mathbb{Z}\}$

c) $5 \cdot x \equiv 2 \mod 10$: Die Gleichung ist nicht lösbar, da $5 \cdot x \equiv 0 \mod 10$ für gerades x und $5 \cdot x \equiv 5 \mod 10$ für ungerades x

d) $-34 \equiv x \mod 5$: $L = \{\ldots -34, -29, \ldots, -4, 1, 6, \ldots\}$
$= \{1 + 5k \text{ mit beliebigem } k \in \mathbb{Z}\}$

Aufgabe 13

Beweise die folgenden Aussagen:

a) Wenn $a \equiv b \mod m$ und $c \equiv d \mod m$, dann $a + c \equiv b + d \mod m$.

b) Wenn $a \equiv b \mod m$, dann $-a \equiv -b \mod m$.

c) Wenn $a \equiv b \mod m$ und $b \equiv c \mod m$, dann $a \equiv c \mod m$.

Hinweis: Zum Beweis von Teil a) kannst Du den vorigen Beweis von a$_3$) entsprechend anpassen.

Lösung: **a)** $a \equiv b \mod m$ und $c \equiv d \mod m$
$\Leftrightarrow\ a = b + km,\ c = d + lm$ mit geeigneten $k, l \in \mathbb{Z}$
$\Rightarrow\ a + c = b + d + km + lm = b + d + \underbrace{(k+l)}_{=k' \in \mathbb{Z}} m$
$\Rightarrow\ a + c \equiv b + d \mod m$

b) $a \equiv b \mod m \ \Leftrightarrow\ a = b + km$ mit einem geeigneten $k \in \mathbb{Z}$
$\Leftrightarrow\ -a = -b + (-k)m$
$\Rightarrow\ -a \equiv -b \mod m$

Alternative Lösung: $-1 \equiv -1 \mod m$ und $a \equiv b \mod m \overset{\text{Satz a}_2)}{\Rightarrow} -a \equiv -b \mod m$

c) $a \equiv b \mod m \ \Rightarrow\ a, b$ lassen beim Teilen durch m denselben Rest
$b \equiv c \mod m \ \Rightarrow\ b, c$ lassen beim Teilen durch m denselben Rest.
$\Rightarrow\ a, c$ lassen beim Teilen durch m denselben Rest.
$\Rightarrow\ a \equiv c \mod m$

Alternative Lösung: $a \equiv b \mod m$ und $b \equiv c \mod m$
$\Leftrightarrow\ a = b + km,\ b = c + lm$ mit geeigneten $k, l \in \mathbb{Z}$
$\Rightarrow\ a = (c + lm) + km = c + (k + l)m$ mit $k + l \in \mathbb{Z}$
$\Rightarrow\ a \equiv c \mod m$

Aufgabe 14

Gib zwei verschiedene 10-stellige Zahlen an, deren Ziffern nur aus Achten und Nullen bestehen, und die beim Teilen durch 9 den Rest 3 ergeben.

Lösung: Z.B. $a = 8\,888\,880\,000$, $b = 8\,800\,880\,088$.

Aufgabe 15

a) Gib die Elemente der Restklasse $[3]$ modulo 7 an.

$[3] =$ $\{\ldots, -11, -4, 3, 10, 17, \ldots\}$. oder $\{3 + 7k : k \in \mathbb{Z}\}$

b) Gegeben sind die Restklassen $[49]$, $[16]$ und $[-10]$ modulo 7. Gib jeweils eine möglichst kleine nichtnegative ganze Zahl x an, so dass $[49] = [x]$ bzw. $[16] = [x]$ bzw. $[-10] = [x]$ gilt.

$[49] =$ $[0]$, $[16] =$ $[2]$, $[-10] =$ $[4]$.

c) Gib alle Elemente von $\mathbb{Z}_7$ an.

$\mathbb{Z}_7 =$ $\{[0], [1], [2], [3], [4], [5], [6]\}$.

Aufgabe 16

Fülle die Verknüpfungstabelle für die Addition und Multiplikation in $\mathbb{Z}_5$ aus. Achtung: Es dürfen nur die Bezeichnungen $[0], \ldots, [4]$ verwendet werden, also anstelle von $[8]$ muss $[3]$ geschrieben werden.

Lösung:

$+$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$	$[0]$
$[2]$	$[2]$	$[3]$	$[4]$	$[0]$	$[1]$
$[3]$	$[3]$	$[4]$	$[0]$	$[1]$	$[2]$
$[4]$	$[4]$	$[0]$	$[1]$	$[2]$	$[3]$

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[2]$	$[0]$	$[2]$	$[4]$	$[1]$	$[3]$
$[3]$	$[0]$	$[3]$	$[1]$	$[4]$	$[2]$
$[4]$	$[0]$	$[4]$	$[3]$	$[2]$	$[1]$

Aufgabe 17

a) Bestimme in $\mathbb{Z}_9$: $[1]-[8]=$ $\boxed{[2]}$ und $-[4]=$ $\boxed{[5]}$.

b) Bestimme in $\mathbb{Z}_{11}$ die Restklassen der angegebenen Brüche. Lies die Ergebnisse in der unten stehenden Multiplikationstabelle ab und begründe jeweils Dein Ergebnis.

b_1) $\frac{[1]}{[2]}=$ $\boxed{[6]}$, denn $[2]\cdot$ $\boxed{[6]}$ $=$ $\boxed{[1]}$.

b_2) $\frac{[1]}{[4]}=$ $\boxed{[3]}$, denn $\boxed{[4]\cdot[3]=[1]}$

b_3) $\frac{[2]}{[4]}=$ $\boxed{[6]}$, denn $\boxed{[4]\cdot[6]=[2]}$

Aufgabe 18

a) Fülle die Verknüpfungstabelle für die Multiplikation in $\mathbb{Z}_4$ aus.

b) Versuche, in $\mathbb{Z}_4$ die Restklassen folgender Brüche zu bestimmen.

$\frac{[1]}{[3]}$ $\boxed{=[3]}$,

$\frac{[1]}{[2]}$ $\boxed{\text{gibt es nicht, denn es gibt keine Restklasse } [x] \text{ mit } [x]\cdot[2]=[1]}$,

$\frac{[2]}{[2]}$ $\boxed{\begin{array}{l}\text{Für } \frac{[2]}{[2]} \text{ gibt es zwei Möglichkeiten: } [1] \text{ oder } [3].\\ \text{Dieser Bruch kann also nicht definiert werden.}\end{array}}$.

Aufgabe 19

In $\mathbb{Z}_{37}$ soll der Bruch $\frac{[5]}{[33]}$ bestimmt werden.

a) Führe den euklidischen Algorithmus zur Bestimmung von $\mathrm{ggT}(37,33)$ durch.

b) Erweitere den euklidischen Algorithmus, um eine Lösung $(k \mid l)$ der diophantischen Gleichung $k\cdot 33+l\cdot 37=1$ zu berechnen.

c) Sei $(k \mid l)$ die in b) bestimmte Lösung. Bestimme mit dem k aus dieser Lösung die Restklasse $[x]=[k]\cdot[33]$ in $\mathbb{Z}_{37}$, wobei $0\le x<37$ gelten soll.

d) Bestimme die Restklasse $[y]=\frac{[1]}{[33]}$, wobei $0\le y<37$ gelten soll.

e) Bestimme die Restklasse $[z]=\frac{[5]}{[33]}$, wobei $0\le z<37$ gelten soll.

Lösung: **a)** und **b)**:

$$\begin{array}{rcl|rcl} 37 &=& 1\cdot 33+4 & 4 &=& 37-1\cdot 33\\ 33 &=& 8\cdot 4+1 & 1 &=& 33-8\cdot 4\\ 4 &=& 4\cdot 1 & &=& 33-8(37-1\cdot 33) \;=\; 9\cdot 33+8\cdot 37 \end{array}$$

$\Rightarrow$ $(k \mid l)=(9 \mid 8)$ ist eine Lösung der Gleichung $k\cdot 33+l\cdot 37=1$.

c) Nach b) gilt $9 \cdot 33 \equiv 1 \mod 37 \Rightarrow [9 \cdot 33] = [1]$, also $[x] = [1]$.

d) Aus c) folgt $[y] = \dfrac{[1]}{[33]} = [9]$, denn $[9] \cdot [33] = [9 \cdot 33] = [1]$.

e) Aus d) folgt $[z] = [5] \cdot [9] = [45] = [45 - 37] = [8]$.
Probe: $[8] \cdot [33] = [264] = [264 - 7 \cdot 37] = [264 - 259] = [5]$. ✓

Aufgabe 20

Entschlüssle mit dem Passwort „dreieck“ den Text

h	e	x	a	g	j	v	x	v	w	a	i	n	x	l	j	x	m	m	p	p	d	t	l
d	r	e	i	e	c	k	d	r	e	i	e	c	k	d	r	e	i	e	c	k	d	r	e
E	N	T	S	C	H	L	U	E	S	S	E	L	N	I	S	T	E	I	N	F	A	C	H

Aufgabe 21

In dieser Aufgabe soll in $\mathbb{Z}_7 = \{[0], [1], [2], \ldots, [6]\}$ gerechnet werden. Das bedeutet, dass als Ergebnisse nur die Zahlen $0, 1, 2, 3, 4, 5, 6$ eingetragen werden sollen.

Bestimme die Potenzen $[a]^k$ in $\mathbb{Z}_7$ und trage Deine Ergebnisse in die Tabelle ein.
Hinweise: Du kannst die unten stehende Verknüpfungstabelle benützen. Wenn Du die Beziehung $[a]^{k+1} = [a] \cdot [a]^k$ verwendest, geht es leichter.

Lösung:

$k =$	1	2	3	4	5	6
$[2]^k =$	$[2]$	$[4]$	$[1]$	$[2]$	$[4]$	$[1]$
$[3]^k =$	$[3]$	$[2]$	$[6]$	$[4]$	$[5]$	$[1]$
$[4]^k =$	$[4]$	$[2]$	$[1]$	$[4]$	$[2]$	$[1]$
$[5]^k =$	$[5]$	$[4]$	$[6]$	$[2]$	$[3]$	$[1]$
$[6]^k =$	$[6]$	$[1]$	$[6]$	$[1]$	$[6]$	$[1]$
$[0]^k =$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$

Aufgabe 22

Berechne die folgenden Brüche jeweils im angegebenen Restklassenring.

a) $\dfrac{[1]}{[5]^{20}}$ in $\mathbb{Z}_{23}$: $\quad \dfrac{[1]}{[5]^{20}} = [5]^{23-1-20} = [5]^2 = [25] = [2]$

b) $\dfrac{[13]}{[5]^{20}}$ in $\mathbb{Z}_{23}$: $\quad \dfrac{[13]}{[5]^{20}} = [13] \cdot \dfrac{[1]}{[5]^{20}} = [13] \cdot [2] = [26] = [3]$

c) $\dfrac{[1]}{[4]^6}$ in $\mathbb{Z}_{13}$: $\quad \dfrac{[1]}{[4]^6} = \dfrac{[4]^{12}}{[4]^6} = [4]^6 = \left([4]^2\right)^3 = [16]^3 = [3]^3 = [27] = [1]$

oder $\quad \dfrac{[1]}{[4]^6} = \dfrac{[1]}{[2]^{12}} = \dfrac{[1]}{[1]} = [1]$

d) $\dfrac{[10]}{[4]^5}$ in $\mathbb{Z}_{13}$: $\quad \dfrac{[10]}{[4]^5} = \dfrac{[10] \cdot [4]}{[4]^6} \overset{\text{Teil c)}}{=} [10] \cdot [4] \cdot [1] = [40] = [1]$

Aufgabe 23

Bestimme jeweils alle Lösungen der angegebenen Gleichung.

a) $[2] \cdot [x] = [5]$ in $\mathbb{Z}_7$,

b) $2 \cdot x \equiv 5 \mod 7$,

c) $4 \cdot x \equiv 3 \mod 11$.

Lösung: **a)** $[x] = \dfrac{[5]}{[2]} = [5] \cdot \dfrac{[1]}{[2]} = [5] \cdot [2]^{7-2} = [5] \cdot [32] = [5 \cdot 4] = [20] = [6]$,

b) Aus a): $x \equiv 6 \mod 7$, d.h. $x \in \{\ldots, -8, -1, 6, 13, \ldots\}$,

c) $4 \cdot x \equiv 3 \equiv 3 \cdot 4^{10} \mod 11$
$\Rightarrow \; x \equiv 3 \cdot 4^9 = 3 \cdot 64^3 \equiv 3 \cdot 9^3 = 27 \cdot 81 \equiv 5 \cdot 4 = 20 \equiv 9 \mod 11$,
d.h. $x \in \{\ldots, -13, -2, 9, 20, \ldots\}$.

Aufgabe 24

a) Bestimme mit Hilfe der Potenztabellen in $\mathbb{Z}_7$ (Aufgabe 21), welche Elemente von $\mathbb{Z}_7$ Primitivwurzeln sind.

Primitivwurzeln in $\mathbb{Z}_7$ sind: $[3], [5]$

Keine Primitivwurzeln in $\mathbb{Z}_7$ sind: $[2], [4], [6]$

b) Fülle für $\mathbb{Z}_{11}$ in der folgenden Potenztabelle jede Zeile so weit aus, bis Du das Element $[1]$ erhältst.

$k =$	1	2	3	4	5	6	7	8	9	10
$[10]^k =$	$[10]$	$[1]$	$[\ ]$	$[\ ]$	$[\ ]$	$[\ ]$	$[\ ]$	$[\ ]$	$[\ ]$	$[\ ]$
$[6]^k =$	$[6]$	$[3]$	$[7]$	$[9]$	$[10]$	$[5]$	$[8]$	$[4]$	$[2]$	$[1]$
$[3]^k =$	$[3]$	$[9]$	$[5]$	$[4]$	$[1]$	$[\ ]$	$[\ ]$	$[\ ]$	$[\ ]$	$[\ ]$
$[2]^k =$	$[2]$	$[4]$	$[8]$	$[5]$	$[10]$	$[9]$	$[7]$	$[3]$	$[6]$	$[1]$

c) Welche der Elemente $[10], [6], [3], [2]$ sind Primitivwurzeln?

In $\mathbb{Z}_{11}$ sind Primitivwurzeln: $[6], [2]$

Aufgabe 25

Andy und Berenice vereinbaren $p = 7$ und $g = 3$.

Andy wählt: $a = 3$, berechnet A: $[g]^a = [3]^3 = [27] = [6]$ in $\mathbb{Z}_7 \;\Rightarrow\; A = 6$

Berenice wählt: $b = 4$, berechnet B: $[g]^b = [3]^4 = [81] = [4]$ in $\mathbb{Z}_7 \;\Rightarrow\; B = 4$

Hinweis: A, B müssen zwischen 1 und 6 liegen.

Öffentlich bekannt sind also:

$$\boxed{p = 7,\ g = 3,\ A = 6,\ B = 4.}$$

Andy berechnet: $[B]^a = [4]^3 = [64] = [1]$ in $\mathbb{Z}_7 \Rightarrow K = 1$

Berenice berechnet: $[A]^b = [6]^4 = [36]^2 = [1]^2 = [1]$ in $\mathbb{Z}_7 \Rightarrow K = 1$

Hinweis: K muss zwischen 1 und 6 liegen.

Für Andy und Berenice kommt die selbe Zahl K als Ergebnis heraus. Schreibe diese Zahl mit Buchstaben als Wort und verwende dieses Zahlwort als Schlüsselwort für die Vigenère-Entschlüsselung, um die Nachricht `izqtimew` zu entschlüsseln.

Verschlüsselt	i	z	q	t	i	m	e	w
Schlüssel	e	i	n	s	e	i	n	s
Nachricht	E	R	D	B	E	E	R	E

Aufgabe 26

Andy und Berenice vereinbaren $p = 11$ und $g = 2$. Andy schickt an Berenice die Zahl $A = 5$, Berenice meldet $B = 8$. Kurze Zeit später übermittelt Andy die Nachricht

h	i	x	y	z	q	w	k	n	c	t	v	m
v	i	e	r	v	i	e	r	v	i	e	r	v
M	A	T	H	E	I	S	T	S	U	P	E	R

Bestimme a, b und den Schlüssel K, entschlüssle die Nachricht mit dem Zahlwort zu K als Schlüsselwort für Vigenère-Entschlüsselung.

Hinweis: Verwende die Tabelle der Potenzen $[2]^k$ aus Aufgabe 3b (Arbeitsblatt 6.3).

Anmerkung: Die Verschlüsselung kann hier geknackt werden, da für p, g, a, b kleine Zahlen verwendet wurden. In der richtigen Anwendung werden sehr große Zahlen verwendet. Dann ist es schwierig, aus g und A die Zahl a zu berechnen.

Lösung: Aus $A = 5$ und $[2]^a = [5]$ liest man aus der Tabelle $a = 4$ ab.

Aus $B = 8$ und $[2]^b = [8]$ liest man aus der Tabelle $b = 3$ ab.

$\Rightarrow\ A^b = 5^3 = 125 \equiv 125 - 121 = 4 \mod 11 \Rightarrow K = 4.$

Entschlüsselung siehe Aufgabentext.

Aufgabe 27

Julia wählt $p = 23$ und die Primitivwurzel $[5]$ in $\mathbb{Z}_{23}$. Weiter wählt sie den Entschlüsselungsexponent $e = 14$ und berechnet

$$[A] = [5]^{14} = [25]^7 = [25 - 23]^7 = [2]^7 = [128] = [128 - 115] = [13] \text{ in } \mathbb{Z}_{23}.$$

Julia veröffentlicht auf ihrer Homepage $(p, g, A) = (23, 5, 13)$.

a) Thomas möchte die Nachricht $n = 11$ an Julia senden. Dazu wählt er den Verschlüsselungsexponent $v = 3$ und berechnet in $\mathbb{Z}_{23}$

$$[B] = [g]^v = [5]^3 = [125 - 115] = [10] \quad \text{in } \mathbb{Z}_{23},$$
$$[A]^v = [13]^3 = [169 - 161] \cdot [13] = [8] \cdot [13] = [104 - 92] = [12] \quad \text{in } \mathbb{Z}_{23},$$
$$[N] = [A]^v \cdot [n] = [12] \cdot [11] = [132 - 115] = [17] \quad \text{in } \mathbb{Z}_{23}.$$

Thomas schickt also $(B = 10\,, N = 17\,)$ an Julia.

Julia berechnet als erstes $[B]^{-14} = [B]^{22-14} = [B]^8 = [B^2]^4 = [B^2 - 92]^4 =$

$= [100 - 92]^4 = [8]^4 = [64 - 46]^2 = \ [18]^2 = [-5]^2 = [25] = [2]$ in $\mathbb{Z}_{23}$.

Hinweis: $[18] = [-5]$ kann hilfreich sein.

Dann erhält sie die Nachricht n durch Multiplikation:

$[n] = [B]^{-14} \cdot [N] = [2] \cdot [17] = [34 - 23] = [11]$ in $\mathbb{Z}_{23}$.

b) Marc schickt an Julia $(B, N) = (3, 21)$. Welche Nachricht n hat er an Julia geschickt?

$[B]^{-14} = [B]^8 = [3]^8 = [9]^4 = [81]^2 = [81 - 69]^2 = [144 - 138] = [6]$ in $\mathbb{Z}_{23}$,

$[n] = [6] \cdot [21] = [126] = [126 - 115] = [11]$ in $\mathbb{Z}_{23}$.

c) Zusatzaufgabe: Erstelle die Potenztabelle für $[5]^k$ um herauszufinden, welchen Verschlüsselungsexponent Marc gewählt hat.

Kennzeichne Marcs Verschlüsselungsexponent durch Umkringeln.

$k =$	1	2	3	4	5	6	7	8	9	10	11
$[5]^k =$	$[5]$	$[2]$	$[10]$	$[4]$	$[20]$	$[8]$	$[17]$	$[16]$	$[11]$	$[9]$	$[22]$
$k =$	12	13	14	15	16	17	18	19	20	21	22
$[5]^k =$	$[18]$	$[21]$	$[13]$	$[19]$	$[3]$	$[15]$	$[6]$	$[7]$	$[12]$	$[14]$	$[1]$

Aufgabe 28

Frank wählt: $p = 3$, $q = 11$,

berechnet: $m = 3 \cdot 11 = 33$, $\widetilde{m} = 2 \cdot 10 = 20$,

wählt: Verschlüsselungsexponent $v = 7$ (erfüllt $1 < v < \widetilde{m}$ und ggT$(v, \widetilde{m}) = 1$)

veröffentlicht: $m = 33$ und $v = 7$

berechnet: e: mit $7e \equiv 1 \mod 20$, d.h. $\mathbf{7}e + \mathbf{20}k = 1$ für ein $k \in \mathbb{Z}$.

Verallgemeinerter Euklidischer Algorithmus:

$$\begin{array}{rcl|rcl} 20 & = & 2 \cdot 7 + 6 & 6 & = & 1 \cdot 20 - 2 \cdot 7 \\ 7 & = & 1 \cdot 6 + 1 & 1 & = & 7 - 1 \cdot 6 \ = \ 7 - 1 \cdot (1 \cdot 20 - 2 \cdot 7) \\ & & & & = & 3 \cdot 7 + (-1) \cdot 20 \end{array}$$

Also $e = 3$. (Allgemein $e = 3 + 20l$, $l \in \mathbb{Z}$)

Pia liest die Homepage von Frank und will ihm die Nachricht $\boxed{n = 6}$ übermitteln. Sie berechnet

Modulo 33: $n^v = 6^7 = \ 36^3 \cdot 6 \ \equiv \ 3^3 \cdot 6 \ = 27 \cdot 6 \ = \ 54 \cdot 3$

$\equiv \ 21 \cdot 3 \ = \ 63 \ \equiv \ 30 \mod 33$

und schickt Frank $\boxed{N = 30}$. Frank liest in Pias Mail $\boxed{N = 30}$ und berechnet

Modulo 33: $N^e = 30^3 \ \equiv (-3)^3 = -27 \equiv 6 \mod 33$

erhält also $\boxed{n = 6}$ zurück.

Aufgabe 29

Frank veröffentlicht auf seiner Homepage die Zahlen $m = 55$ und $v = 7$. Er erhält von Peter die Zahl $N = 25$.

Bestimme $p, q, \widetilde{m}, e$ und die entschlüsselte Botschaft n.

Lösung: $m = 55 = 5 \cdot 11 \Rightarrow p = 5$, $q = 11$, $\widetilde{m} = 4 \cdot 10 = 40$,

Berechne e mit $7e \equiv 1 \mod 40$, d.h. $\mathbf{7}e + \mathbf{40}k = 1$ für ein $k \in \mathbb{Z}$.

Verallgemeinerter Euklidischer Algorithmus:

$$\begin{array}{rcl|rcl} \mathbf{40} & = & 5 \cdot \mathbf{7} + 5 & 5 & = & 1 \cdot \mathbf{40} - 5 \cdot \mathbf{7} \\ \mathbf{7} & = & 1 \cdot 5 + 2 & 2 & = & \mathbf{7} - 1 \cdot 5 \\ 5 & = & 2 \cdot 2 + 1 & 1 & = & 5 - 2 \cdot 2 \;=\; 5 - 2 \cdot (\mathbf{7} - 1 \cdot 5) \;=\; 3 \cdot 5 - 2 \cdot \mathbf{7} \\ & & & & & = \; 3(1 \cdot \mathbf{40} - 5 \cdot \mathbf{7}) - 2 \cdot \mathbf{7} \;=\; 3 \cdot \mathbf{40} - 17 \cdot \mathbf{7} \end{array}$$

Damit wäre $e = -17$.

Das passt nicht, wir suchen eine Lösung von $7e \equiv 1 \mod 40$ mit $1 < e < 40$.

Mit $-17 \equiv 23 \mod 40$ folgt $e = 23$.

Damit:

$$\begin{aligned} N^e &= 25^{23} = 625^{11} \cdot 25 \equiv 20^{11} \cdot 25 = 400^5 \cdot 20 \cdot 25 \equiv 15^5 \cdot 500 \\ &\equiv 225^2 \cdot 15 \cdot 5 \equiv 5^2 \cdot 75 = 25 \cdot 20 = 500 \equiv 5 \mod 55, \end{aligned}$$

also $n = 5$. Probe:

$$n^v = 5^7 = 125^2 \cdot 5 \equiv 15^2 \cdot 5 \equiv 225 \cdot 5 \equiv 5 \cdot 5 = 25 = N \mod 55.$$

Aufgabe 30

Frank veröffentlicht auf seiner Homepage die Zahlen $m = 51$ und $v = 3$. Er erhält von Jane die Zahl $N = 8$ als verschlüsselte Botschaft.

Bestimme $p, q, \widetilde{m}, e$ und die entschlüsselte Botschaft n.

Lösung: $m = 51 = 3 \cdot 17 \Rightarrow p = 3,\ q = 17,\ \widetilde{m} = 2 \cdot 16 = 32.$

Berechne e mit mit $3e \equiv 1 \mod 32$, d.h. $\mathbf{3}e + \mathbf{32}k = 1$ für ein $k \in \mathbb{Z}$.

Verallgemeinerter Euklidischer Algorithmus:

$$\begin{array}{rcl|rcl} \mathbf{32} & = & 10 \cdot \mathbf{3} + 2 & 2 & = & 1 \cdot \mathbf{32} - 10 \cdot \mathbf{3} \\ \mathbf{3} & = & 1 \cdot 2 + 1 & 1 & = & \mathbf{3} - 1 \cdot 2 \;=\; \mathbf{3} - (1 \cdot \mathbf{32} - 10 \cdot \mathbf{3}) \;=\; 11 \cdot \mathbf{3} - 1 \cdot \mathbf{32} \end{array}$$

Also $e = 11$.

Damit folgt $N^e = 8^{11} = 64^5 \cdot 8 \equiv 13^5 \cdot 8 = 169^2 \cdot 13 \cdot 8 \equiv 16^2 \cdot 104 \equiv 1 \cdot 2 = 2 \mod 51$.

Also gilt $n = 2$. (Probe: $n^v = 2^3 = 8 = N$.)