Lineare Algebra
algebraische Strukturen 3

Reinhold Hübl

Wintersemester 2020/21

DHBW
Duale Hochschule
Baden-Württemberg
Mannheim

Teiler und Teilbarkeit

Wir betrachten positive ganze Zahlen k und n.

Definition

k heißt Teiler von n, wenn es eine ganze Zahl l gibt mit $n = k \cdot l$.

Beispiel

Die Zahl 2 ist ein Teiler von 36.

Teiler und Teilbarkeit

Wir betrachten positive ganze Zahlen k und n.

Definition

k heißt Teiler von n, wenn es eine ganze Zahl l gibt mit $n = k \cdot l$.

Beispiel

Die Zahl 2 ist ein Teiler von 36.

Beispiel

Für jede positive ganze Zahl n sind 1 und n Teiler von n. Diese Teiler heißen die **trifivialen Teiler** von n. Alle anderen Teiler heißen **echte Teiler** von n.

Teiler und Teilbarkeit

Wir betrachten positive ganze Zahlen k und n.

Definition

k heißt Teiler von n, wenn es eine ganze Zahl l gibt mit $n = k \cdot l$.

Beispiel

Die Zahl 2 ist ein Teiler von 36.

Beispiel

Für jede positive ganze Zahl n sind 1 und n Teiler von n. Diese Teiler heißen die **trifivialen Teiler** von n. Alle anderen Teiler heißen **echte Teiler** von n.

Primzahlen

Definition

Eine Zahl $p \in \mathbb{N}$, $p \geq 2$ heißt **Primzahl**, wenn p keine echten Teiler hat.

Beispiel

$2, 3, 5, 7$ und 11 sind Primzahlen, 9 ist keine.

Primzahlen

Definition

Eine Zahl $p \in \mathbb{N}$, $p \geq 2$ heißt **Primzahl**, wenn p keine echten Teiler hat.

Beispiel

$2, 3, 5, 7$ und 11 sind Primzahlen, 9 ist keine.

Bemerkung

Eine Zahl $p \in \mathbb{N} \setminus \{0, 1\}$ ist genau dann eine Primzahl, wenn für alle ganzen Zahlen $a, b \in \mathbb{Z}$ gilt

$$p \mid a \cdot b \iff p \mid a \text{ oder } p \mid b$$

also p teilt genau dann ein Produkt von zwei Zahlen, wenn es schon eine der beiden Zahlen teilt.

Primzahlen

Definition

Eine Zahl $p \in \mathbb{N}$, $p \geq 2$ heißt **Primzahl**, wenn p keine echten Teiler hat.

Beispiel

$2, 3, 5, 7$ und 11 sind Primzahlen, 9 ist keine.

Bemerkung

Eine Zahl $p \in \mathbb{N} \setminus \{0, 1\}$ ist genau dann eine Primzahl, wenn für alle ganzen Zahlen $a, b \in \mathbb{Z}$ gilt

$$p | a \cdot b \iff p|a \text{ oder } p|b$$

also p teilt genau dann ein Produkt von zwei Zahlen, wenn es schon eine der beiden Zahlen teilt.

Primzahlen

Bemerkung

Jede ganze Zahle $z \in \mathbb{Z} \setminus \{0\}$ schreibt sich in eindeutiger Weise als

$$z = \varepsilon \cdot p_1^{n_1} \cdot p_2^{n_2} \cdots p_t^{n_t}$$

mit $\varepsilon \in \{-1, 1\}$, Primzahlen $p_1 < p_2 < \ldots < p_t$ und positiven natürlichen Zahlen $n_1, \ldots, n_t$. (Dabei lassen wir den Spezialfall $t = 0$ für $z = \pm 1$ zu).

Beispiel

Die Zahl 36 hat die Primfaktorzerlegung

$$36 = 2^2 \cdot 3^2$$

Der Vorfaktor $\varepsilon = +1$ wird dabei in der Regel weggelassen.

Primzahlen

Bemerkung

Jede ganze Zahle $z \in \mathbb{Z} \setminus \{0\}$ schreibt sich in eindeutiger Weise als

$$z = \varepsilon \cdot p_1^{n_1} \cdot p_2^{n_2} \cdots p_t^{n_t}$$

mit $\varepsilon \in \{-1, 1\}$, Primzahlen $p_1 < p_2 < \ldots < p_t$ und positiven natürlichen Zahlen $n_1, \ldots, n_t$. (Dabei lassen wir den Spezialfall $t = 0$ für $z = \pm 1$ zu).

Beispiel

Die Zahl 36 hat die Primfaktorzerlegung

$$36 = 2^2 \cdot 3^2$$

Der Vorfaktor $\varepsilon = +1$ wird dabei in der Regel weggelassen.

Die Zahl -6615 hat die Primfaktorzerlegung

$$-6615 = (-1) \cdot 3^3 \cdot 5 \cdot 2^7$$

Primzahlen

Bemerkung

Jede ganze Zahle $z \in \mathbb{Z} \setminus \{0\}$ schreibt sich in eindeutiger Weise als

$$z = \varepsilon \cdot p_1^{n_1} \cdot p_2^{n_2} \cdots p_t^{n_t}$$

mit $\varepsilon \in \{-1, 1\}$, Primzahlen $p_1 < p_2 < \ldots < p_t$ und positiven natürlichen Zahlen $n_1, \ldots, n_t$. (Dabei lassen wir den Spezialfall $t = 0$ für $z = \pm 1$ zu).

Beispiel

Die Zahl 36 hat die Primfaktorzerlegung

$$36 = 2^2 \cdot 3^2$$

Der Vorfaktor $\varepsilon = +1$ wird dabei in der Regel weggelassen.
Die Zahl -6615 hat die Primfaktorzerlegung

$$-6615 = (-1) \cdot 3^3 \cdot 5 \cdot 2^7$$

Teiler

Definition

Sind $m, n \in \mathbb{N} \setminus \{0\}$, so heißt eine Zahl $g \in \mathbb{N}$ der **größte gemeinsame Teiler** von m und n, wenn gilt:

- g ist ein Teiler von m und ein Teiler von n.

Teiler

Definition

Sind $m, n \in \mathbb{N} \setminus \{0\}$, so heißt eine Zahl $g \in \mathbb{N}$ der **größte gemeinsame Teiler** von m und n, wenn gilt:

- g ist ein Teiler von m und ein Teiler von n.
- Ist h ein weiterer Teiler von m und n, so ist h auch ein Teiler von g.

Teiler

Definition

Sind $m, n \in \mathbb{N} \setminus \{0\}$, so heißt eine Zahl $g \in \mathbb{N}$ der **größte gemeinsame Teiler** von m und n, wenn gilt:

- g ist ein Teiler von m und ein Teiler von n.
- Ist h ein weiterer Teiler von m und n, so ist h auch ein Teiler von g.

Wir schreiben

$$\mathrm{ggT}(m, n) := g$$

für den größten gemeinsame Teiler von m und n.

Teiler

Definition

Sind $m, n \in \mathbb{N} \setminus \{0\}$, so heißt eine Zahl $g \in \mathbb{N}$ der **größte gemeinsame Teiler** von m und n, wenn gilt:

- g ist ein Teiler von m und ein Teiler von n.
- Ist h ein weiterer Teiler von m und n, so ist h auch ein Teiler von g.

Wir schreiben

$$\mathrm{ggT}(m, n) := g$$

für den größten gemeinsame Teiler von m und n.

Zwei Zahlen $m, n \in \mathbb{N} \setminus \{0\}$ heißen **teilerfremd**, wenn $\mathrm{ggT}(m, n) = 1$, wenn sie also keinen echten gemeinsamen Teiler besitzen.

Teiler

Definition

Sind $m, n \in \mathbb{N} \setminus \{0\}$, so heißt eine Zahl $g \in \mathbb{N}$ der **größte gemeinsame Teiler** von m und n, wenn gilt:

- g ist ein Teiler von m und ein Teiler von n.
- Ist h ein weiterer Teiler von m und n, so ist h auch ein Teiler von g.

Wir schreiben

$$\mathrm{ggT}(m, n) := g$$

für den größten gemeinsame Teiler von m und n.
Zwei Zahlen $m, n \in \mathbb{N} \setminus \{0\}$ heißen **teilerfremd**, wenn $\mathrm{ggT}(m, n) = 1$, wenn sie also keinen echten gemeinsamen Teiler besitzen.

Teiler

Übung

Bestimmen Sie den größten gemeinsamen Teiler von $n = 5040$ und $m = 15288$.

Teiler

Übung

Bestimmen Sie den größten gemeinsamen Teiler von $n = 5040$ und $m = 15288$.

Lösung:

$$\mathrm{ggT}(m, n) = 2^3 \cdot 3 \cdot 7 = 168$$

Teiler

Übung

Bestimmen Sie den größten gemeinsamen Teiler von $n = 5040$ und $m = 15288$.

Lösung:

$$\mathrm{ggT}(m, n) = 2^3 \cdot 3 \cdot 7 = 168$$

Die Bestimmung der Primfaktorzerlegung großer Zahlen ist ein sehr schwieriges Problem, für das kein effizienter Algorithmus bekannt ist. Daher ist diese Methode zur Bestimmung des größten gemeinsamen Teilers ineffizient.

Teiler

Übung

Bestimmen Sie den größten gemeinsamen Teiler von $n = 5040$ und $m = 15288$.

Lösung:

$$\mathrm{ggT}(m, n) = 2^3 \cdot 3 \cdot 7 = 168$$

Die Bestimmung der Primfaktorzerlegung großer Zahlen ist ein sehr schwieriges Problem, für das kein effizienter Algorithmus bekannt ist. Daher ist diese Methode zur Bestimmung des größten gemeinsamen Teilers ineffizient.

euklidischer Algorithmus

- **Vorbereitungsschritt:** Ordne m und n so, dass $m \geq n$. (Vertausche m und n, falls nötig, denn $\mathrm{ggT}(m,n) = \mathrm{ggT}(n,m)$). Setzen $i = 0$ und $r_0 = m$, $r_1 = n$.
- **Verarbeitungsschritt:** Wir dividieren r_i durch r_{i+1} mit Rest:

$$r_i = a \cdot r_{i+1} + b$$

mit einer natürlichen Zahl a und einem Rest $b \in \{0, 1, \ldots, r_{i+1} - 1\}$.

- Falls $b = 0$ (d.h. die Division geht ohne Rest auf) $\longrightarrow$ **STOPP**.
- Falls $b \neq 0$ setze $r_{i+2} = b$ und $i = i + 1$. Wiederhole den Verarbeitungsschritt.

euklidischer Algorithmus

- **Vorbereitungsschritt:** Ordne m und n so, dass $m \geq n$. (Vertausche m und n, falls nötig, denn $\mathrm{ggT}(m,n) = \mathrm{ggT}(n,m)$). Setzen $i = 0$ und $r_0 = m$, $r_1 = n$.
- **Verarbeitungsschritt:** Wir dividieren r_i durch r_{i+1} mit Rest:

$$r_i = a \cdot r_{i+1} + b$$

mit einer natürlichen Zahl a und einem Rest $b \in \{0, 1, \ldots, r_{i+1} - 1\}$.

  - Falls $b = 0$ (d.h. die Division geht ohne Rest auf) $\longrightarrow$ **STOPP**.
  - Falls $b \neq 0$ setze $r_{i+2} = b$ und $i = i + 1$. Wiederhole den Verarbeitungsschritt.

- **Ergebnisschritt:** Nach endlich vielen Verarbeitungsschritten (höchstens m vielen) geht die Division erstmals ohne Rest auf, d.h. $r_i = a \cdot r_{i+1} + 0$ mit $r_{i+1} \neq 0$, Das STOPP–Kriterium wird also immer erreicht und r_{i+1} ist der größte gemeinsame Teiler von m und n, $r_{i+1} = \mathrm{ggT}(m,n)$.

euklidischer Algorithmus

- **Vorbereitungsschritt:** Ordne m und n so, dass $m \geq n$. (Vertausche m und n, falls nötig, denn $\mathrm{ggT}(m,n) = \mathrm{ggT}(n,m)$). Setzen $i = 0$ und $r_0 = m$, $r_1 = n$.
- **Verarbeitungsschritt:** Wir dividieren r_i durch r_{i+1} mit Rest:

$$r_i = a \cdot r_{i+1} + b$$

mit einer natürlichen Zahl a und einem Rest $b \in \{0, 1, \ldots, r_{i+1} - 1\}$.
  - Falls $b = 0$ (d.h. die Division geht ohne Rest auf) $\longrightarrow$ **STOPP**.
  - Falls $b \neq 0$ setze $r_{i+2} = b$ und $i = i + 1$. Wiederhole den Verarbeitungsschritt.
- **Ergebnisschritt:** Nach endlich vielen Verarbeitungsschritten (höchstens m vielen) geht die Division erstmals ohne Rest auf, d.h.$r_i = a \cdot r_{i+1} + 0$ mit $r_{i+1} \neq 0$, Das STOPP–Kriterium wird also immer erreicht und r_{i+1} ist der größte gemeinsame Teiler von m und n, $r_{i+1} = \mathrm{ggT}(m,n)$.

euklidischer Algorithmus

Beispiel

Wir betrachten die Zahlen $m = 222$ und $n = 156$. Hier gilt bereits $m \geq n$, und wir setzen $r_0 = 222$ und $r_1 = 156$.

- $i = 0$: $\quad 222 = 1 \cdot 156 + 66$. Wir setzen $r_2 = 66$.

euklidischer Algorithmus

Beispiel

Wir betrachten die Zahlen $m = 222$ und $n = 156$. Hier gilt bereits $m \geq n$, und wir setzen $r_0 = 222$ und $r_1 = 156$.

- $i = 0$: $222 = 1 \cdot 156 + 66$. Wir setzen $r_2 = 66$.
- $i = 1$: $156 = 2 \cdot 66 + 24$. Wir setzen $r_3 = 24$.

euklidischer Algorithmus

Beispiel

Wir betrachten die Zahlen $m = 222$ und $n = 156$. Hier gilt bereits $m \geq n$, und wir setzen $r_0 = 222$ und $r_1 = 156$.

- $i = 0$: $222 = 1 \cdot 156 + 66$. Wir setzen $r_2 = 66$.
- $i = 1$: $156 = 2 \cdot 66 + 24$. Wir setzen $r_3 = 24$.
- $i = 2$: $66 = 2 \cdot 24 + 18$. Wir setzen $r_4 = 18$.

euklidischer Algorithmus

Beispiel

Wir betrachten die Zahlen $m = 222$ und $n = 156$. Hier gilt bereits $m \geq n$, und wir setzen $r_0 = 222$ und $r_1 = 156$.

- $i = 0$: $222 = 1 \cdot 156 + 66$. Wir setzen $r_2 = 66$.
- $i = 1$: $156 = 2 \cdot 66 + 24$. Wir setzen $r_3 = 24$.
- $i = 2$: $66 = 2 \cdot 24 + 18$. Wir setzen $r_4 = 18$.
- $i = 3$: $24 = 1 \cdot 18 + 6$. Wir setzen $r_5 = 6$.

euklidischer Algorithmus

Beispiel

Wir betrachten die Zahlen $m = 222$ und $n = 156$. Hier gilt bereits $m \geq n$, und wir setzen $r_0 = 222$ und $r_1 = 156$.

- $i = 0$: $222 = 1 \cdot 156 + 66$. Wir setzen $r_2 = 66$.
- $i = 1$: $156 = 2 \cdot 66 + 24$. Wir setzen $r_3 = 24$.
- $i = 2$: $66 = 2 \cdot 24 + 18$. Wir setzen $r_4 = 18$.
- $i = 3$: $24 = 1 \cdot 18 + 6$. Wir setzen $r_5 = 6$.
- $i = 4$: $18 = 3 \cdot 6 + 0$. $\longrightarrow$ **STOPP**.

euklidischer Algorithmus

Beispiel

Wir betrachten die Zahlen $m = 222$ und $n = 156$. Hier gilt bereits $m \geq n$, und wir setzen $r_0 = 222$ und $r_1 = 156$.

- $i = 0$: $222 = 1 \cdot 156 + 66$. Wir setzen $r_2 = 66$.
- $i = 1$: $156 = 2 \cdot 66 + 24$. Wir setzen $r_3 = 24$.
- $i = 2$: $66 = 2 \cdot 24 + 18$. Wir setzen $r_4 = 18$.
- $i = 3$: $24 = 1 \cdot 18 + 6$. Wir setzen $r_5 = 6$.
- $i = 4$: $18 = 3 \cdot 6 + 0$. $\longrightarrow$ **STOPP**.

Ergebnis: $\mathrm{ggT}(222, 156) = 6$.

euklidischer Algorithmus

Beispiel

Wir betrachten die Zahlen $m = 222$ und $n = 156$. Hier gilt bereits $m \geq n$, und wir setzen $r_0 = 222$ und $r_1 = 156$.

- $i = 0$: $222 = 1 \cdot 156 + 66$. Wir setzen $r_2 = 66$.
- $i = 1$: $156 = 2 \cdot 66 + 24$. Wir setzen $r_3 = 24$.
- $i = 2$: $66 = 2 \cdot 24 + 18$. Wir setzen $r_4 = 18$.
- $i = 3$: $24 = 1 \cdot 18 + 6$. Wir setzen $r_5 = 6$.
- $i = 4$: $18 = 3 \cdot 6 + 0$. $\longrightarrow$ **STOPP**.

Ergebnis: $\mathrm{ggT}(222, 156) = 6$.

euklidischer Algorithmus

Übung

Bestimmen Sie den größten gemeinsamen Teiler von $m = 239$ und $n = 144$.

euklidischer Algorithmus

Übung

Bestimmen Sie den größten gemeinsamen Teiler von $m = 239$ und $n = 144$.

Lösung:

$\mathrm{ggT}(239, 144) = 1.$

euklidischer Algorithmus

Übung

Bestimmen Sie den größten gemeinsamen Teiler von $m = 239$ und $n = 144$.

Lösung:

$\mathrm{ggT}(239, 144) = 1$.

euklidischer Algorithmus

Satz

Sind $m, n \in \mathbb{N} \setminus \{0\}$ *mit* $\mathrm{ggT}(m, n) = g$, *so gibt es ganze Zahlen* a, b *mit*

$$a \cdot m + b \cdot n = g$$

Das erhält man durch Rückwärtsrechnen aus dem euklidischen Algorithmus.

euklidischer Algorithmus

Satz

Sind $m, n \in \mathbb{N} \setminus \{0\}$ *mit* $\mathrm{ggT}(m, n) = g$, *so gibt es ganze Zahlen* a, b *mit*

$$a \cdot m + b \cdot n = g$$

Das erhält man durch Rückwärtsrechnen aus dem euklidischen Algorithmus.

euklidischer Algorithmus

Beispiel

Wir wollen 6 mit 156 und 222 darstellen.

1. Aus Schritt $i = 3$ erhalte: $6 = 24 - 1 \cdot 18$.

euklidischer Algorithmus

Beispiel

Wir wollen 6 mit 156 und 222 darstellen.

1. Aus Schritt $i = 3$ erhalte: $6 = 24 - 1 \cdot 18$.
2. Aus Schritt $i = 2$ erhaltet $18 = 66 - 2 \cdot 24$. Eingesetzt in (1):

$$6 = 24 - 1 \cdot (66 - 2 \cdot 24) = 3 \cdot 24 - 1 \cdot 66$$

euklidischer Algorithmus

Beispiel

Wir wollen 6 mit 156 und 222 darstellen.

1. Aus Schritt $i = 3$ erhalte: $6 = 24 - 1 \cdot 18$.
2. Aus Schritt $i = 2$ erhaltet $18 = 66 - 2 \cdot 24$. Eingesetzt in (1):

$$6 = 24 - 1 \cdot (66 - 2 \cdot 24) = 3 \cdot 24 - 1 \cdot 66$$

3. Aus Schritt $i = 1$ erhalte zunächst $24 = 156 - 2 \cdot 66$. Eingesetzt in (2):

$$6 = 3 \cdot (156 - 2 \cdot 66) - 1 \cdot 66 = 3 \cdot 156 - 7 \cdot 66$$

euklidischer Algorithmus

Beispiel

Wir wollen 6 mit 156 und 222 darstellen.

1. Aus Schritt $i = 3$ erhalte: $6 = 24 - 1 \cdot 18$.
2. Aus Schritt $i = 2$ erhaltet $18 = 66 - 2 \cdot 24$. Eingesetzt in (1):

$$6 = 24 - 1 \cdot (66 - 2 \cdot 24) = 3 \cdot 24 - 1 \cdot 66$$

3. Aus Schritt $i = 1$ erhalte zunächst $24 = 156 - 2 \cdot 66$. Eingesetzt in (2):

$$6 = 3 \cdot (156 - 2 \cdot 66) - 1 \cdot 66 = 3 \cdot 156 - 7 \cdot 66$$

4. aus Schritt $i = 0$ erhalte zunächst $66 = 222 - 1 \cdot 156$. Eingesetzt in (3):

$$6 = 3 \cdot 156 - 7 \cdot (222 - 1 \cdot 156) = 10 \cdot 156 - 7 \cdot 222$$

euklidischer Algorithmus

Beispiel

Wir wollen 6 mit 156 und 222 darstellen.

1. Aus Schritt $i = 3$ erhalte: $6 = 24 - 1 \cdot 18$.
2. Aus Schritt $i = 2$ erhaltet $18 = 66 - 2 \cdot 24$. Eingesetzt in (1):

$$6 = 24 - 1 \cdot (66 - 2 \cdot 24) = 3 \cdot 24 - 1 \cdot 66$$

3. Aus Schritt $i = 1$ erhalte zunächst $24 = 156 - 2 \cdot 66$. Eingesetzt in (2):

$$6 = 3 \cdot (156 - 2 \cdot 66) - 1 \cdot 66 = 3 \cdot 156 - 7 \cdot 66$$

4. aus Schritt $i = 0$ erhalte zunächst $66 = 222 - 1 \cdot 156$. Eingesetzt in (3):

$$6 = 3 \cdot 156 - 7 \cdot (222 - 1 \cdot 156) = 10 \cdot 156 - 7 \cdot 222$$

Damit haben wir eine gewünschte Darstellung $6 = 10 \cdot 156 + (-7) \cdot 222$.

euklidischer Algorithmus

Beispiel

Wir wollen 6 mit 156 und 222 darstellen.

1. Aus Schritt $i = 3$ erhalte: $6 = 24 - 1 \cdot 18$.
2. Aus Schritt $i = 2$ erhaltet $18 = 66 - 2 \cdot 24$. Eingesetzt in (1):

$$6 = 24 - 1 \cdot (66 - 2 \cdot 24) = 3 \cdot 24 - 1 \cdot 66$$

3. Aus Schritt $i = 1$ erhalte zunächst $24 = 156 - 2 \cdot 66$. Eingesetzt in (2):

$$6 = 3 \cdot (156 - 2 \cdot 66) - 1 \cdot 66 = 3 \cdot 156 - 7 \cdot 66$$

4. aus Schritt $i = 0$ erhalte zunächst $66 = 222 - 1 \cdot 156$. Eingesetzt in (3):

$$6 = 3 \cdot 156 - 7 \cdot (222 - 1 \cdot 156) = 10 \cdot 156 - 7 \cdot 222$$

Damit haben wir eine gewünschte Darstellung $6 = 10 \cdot 156 + (-7) \cdot 222$.

euklidischer Algorithmus

Übung

Schreiben Sie $1 = \mathrm{ggT}(239, 144)$ in der Form

$$1 = a \cdot 239 + b \cdot 144$$

mit ganzen Zahlen a und b.

euklidischer Algorithmus

Übung

Schreiben Sie $1 = \mathrm{ggT}(239, 144)$ in der Form

$$1 = a \cdot 239 + b \cdot 144$$

mit ganzen Zahlen a und b.

Lösung:

Es gilt

$$1 = 47 \cdot 239 + (-78) \cdot 144$$

euklidischer Algorithmus

Übung

Schreiben Sie $1 = \mathrm{ggT}(239, 144)$ in der Form

$$1 = a \cdot 239 + b \cdot 144$$

mit ganzen Zahlen a und b.

Lösung:

Es gilt

$$1 = 47 \cdot 239 + (-78) \cdot 144$$

Die Ringe $\mathbb{Z}/n\mathbb{Z}$

Die Ringe $\mathbb{Z}/n\mathbb{Z}$ haben wir schon kennengelernt. Zur Vereinfachung der Notation identifizieren wir

$$\mathbb{Z}/n\mathbb{Z} = \{0, 1, \ldots, n-1\}$$

(und schreiben also nicht mehr $[k]$ für die Äquivalenzklasse von k sondern einfach k).

Die Ringe $\mathbb{Z}/n\mathbb{Z}$

Die Ringe $\mathbb{Z}/n\mathbb{Z}$ haben wir schon kennengelernt. Zur Vereinfachung der Notation identifizieren wir

$$\mathbb{Z}/n\mathbb{Z} = \{0, 1, \ldots, n-1\}$$

(und schreiben also nicht mehr $[k]$ für die Äquivalenzklasse von k sondern einfach k).

Dann gilt in $\mathbb{Z}/n\mathbb{Z}$:

- Ist $k + l = q \cdot n + r$, so gilt in $\mathbb{Z}/n\mathbb{Z}$:

$$k + l = r$$

Die Ringe $\mathbb{Z}/n\mathbb{Z}$

Die Ringe $\mathbb{Z}/n\mathbb{Z}$ haben wir schon kennengelernt. Zur Vereinfachung der Notation identifizieren wir

$$\mathbb{Z}/n\mathbb{Z} = \{0, 1, \ldots, n-1\}$$

(und schreiben also nicht mehr $[k]$ für die Äquivalenzklasse von k sondern einfach k).
Dann gilt in $\mathbb{Z}/n\mathbb{Z}$:

- Ist $k + l = q \cdot n + r$, so gilt in $\mathbb{Z}/n\mathbb{Z}$:

$$k + l = r$$

- Ist $k \cdot l = q \cdot n + r$, so gilt in $\mathbb{Z}/n\mathbb{Z}$:

$$k \cdot l = r$$

Die Ringe $\mathbb{Z}/n\mathbb{Z}$

Die Ringe $\mathbb{Z}/n\mathbb{Z}$ haben wir schon kennengelernt. Zur Vereinfachung der Notation identifizieren wir

$$\mathbb{Z}/n\mathbb{Z} = \{0, 1, \ldots, n-1\}$$

(und schreiben also nicht mehr $[k]$ für die Äquivalenzklasse von k sondern einfach k).
Dann gilt in $\mathbb{Z}/n\mathbb{Z}$:

- Ist $k + l = q \cdot n + r$, so gilt in $\mathbb{Z}/n\mathbb{Z}$:

$$k + l = r$$

- Ist $k \cdot l = q \cdot n + r$, so gilt in $\mathbb{Z}/n\mathbb{Z}$:

$$k \cdot l = r$$

Die Ringe $\mathbb{Z}/n\mathbb{Z}$

Beispiel

Für den $R = \mathbb{Z}/31439 \cdot \mathbb{Z}$ gilt

- $11812 + 7403 = 19215 = 0 \cdot 31439 + 19215$. Also gilt in R:

$$11812 + 7403 = 19215$$

Die Ringe $\mathbb{Z}/n\mathbb{Z}$

Beispiel

Für den $R = \mathbb{Z}/31439 \cdot \mathbb{Z}$ gilt

- $11812 + 7403 = 19215 = 0 \cdot 31439 + 19215$. Also gilt in R:

$$11812 + 7403 = 19215$$

- $11812 + 27403 = 39215 = 1 \cdot 31439 + 7786$. Also gilt in R:

$$11812 + 27403 = 7786$$

Die Ringe $\mathbb{Z}/n\mathbb{Z}$

Beispiel

Für den $R = \mathbb{Z}/31439 \cdot \mathbb{Z}$ gilt

- $11812 + 7403 = 19215 = 0 \cdot 31439 + 19215$. Also gilt in R:

$$11812 + 7403 = 19215$$

- $11812 + 27403 = 39215 = 1 \cdot 31439 + 7786$. Also gilt in R:

$$11812 + 27403 = 7786$$

- $11812 \cdot 7403 = 87\,444\,236 = 2781 \cdot 31439 + 12377$. Also gilt in R:

$$11812 \cdot 7403 = 12377$$

Die Ringe $\mathbb{Z}/n\mathbb{Z}$

Beispiel

Für den $R = \mathbb{Z}/31439 \cdot \mathbb{Z}$ gilt

- $11812 + 7403 = 19215 = 0 \cdot 31439 + 19215$. Also gilt in R:

$$11812 + 7403 = 19215$$

- $11812 + 27403 = 39215 = 1 \cdot 31439 + 7786$. Also gilt in R:

$$11812 + 27403 = 7786$$

- $11812 \cdot 7403 = 87\,444\,236 = 2781 \cdot 31439 + 12377$. Also gilt in R:

$$11812 \cdot 7403 = 12377$$

- $117879 \cdot 10579 = 198\,663\,041 = 6319 \cdot 31439 + 0$. Also gilt in R:

$$11879 \cdot 10579 = 0$$

Die Ringe $\mathbb{Z}/n\mathbb{Z}$

Beispiel

Für den $R = \mathbb{Z}/31439 \cdot \mathbb{Z}$ gilt

- $11812 + 7403 = 19215 = 0 \cdot 31439 + 19215$. Also gilt in R:

$$11812 + 7403 = 19215$$

- $11812 + 27403 = 39215 = 1 \cdot 31439 + 7786$. Also gilt in R:

$$11812 + 27403 = 7786$$

- $11812 \cdot 7403 = 87\,444\,236 = 2781 \cdot 31439 + 12377$. Also gilt in R:

$$11812 \cdot 7403 = 12377$$

- $117879 \cdot 10579 = 198\,663\,041 = 6319 \cdot 31439 + 0$. Also gilt in R:

$$11879 \cdot 10579 = 0$$

Die Ringe $\mathbb{Z}/n\mathbb{Z}$

Übung

Berechnen Sie in $\mathbb{Z}/9379$ die Zahl

$$z = 1315 \cdot 6439$$

Die Ringe $\mathbb{Z}/n\mathbb{Z}$

Übung

Berechnen Sie in $\mathbb{Z}/9379$ die Zahl

$$z = 1315 \cdot 6439$$

Lösung:

Es ist

$$1315 \cdot 6439 = 902 \cdot 9379 + 7427$$

und daher

$$z = 7427$$

Die Ringe $\mathbb{Z}/n\mathbb{Z}$

Übung

Berechnen Sie in $\mathbb{Z}/9379$ die Zahl

$$z = 1315 \cdot 6439$$

Lösung:

Es ist

$$1315 \cdot 6439 = 902 \cdot 9379 + 7427$$

und daher

$$z = 7427$$

Die Ringe $\mathbb{Z}/n\mathbb{Z}$

Satz

Genau dann ist $\mathbb{Z}/n\mathbb{Z}$ ein Körper, wenn n eine Primzahl ist.

Bezeichnung

Ist p eine Primzahl, so bezeichnen wir $\mathbb{Z}/p\mathbb{Z}$ mit $\mathbb{F}_p$ und nennen $\mathbb{F}_p$ den Körper mit p Elementen

Die Ringe $\mathbb{Z}/n\mathbb{Z}$

Satz

Genau dann ist $\mathbb{Z}/n\mathbb{Z}$ ein Körper, wenn n eine Primzahl ist.

Bezeichnung

Ist p eine Primzahl, so bezeichnen wir $\mathbb{Z}/p\mathbb{Z}$ mit $\mathbb{F}_p$ und nennen $\mathbb{F}_p$ den Körper mit p Elementen

Beispiel

Der Ring $\mathbb{Z}/17\mathbb{Z}$ ist ein Körper.

Die Ringe $\mathbb{Z}/n\mathbb{Z}$

Satz

Genau dann ist $\mathbb{Z}/n\mathbb{Z}$ ein Körper, wenn n eine Primzahl ist.

Bezeichnung

Ist p eine Primzahl, so bezeichnen wir $\mathbb{Z}/p\mathbb{Z}$ mit $\mathbb{F}_p$ und nennen $\mathbb{F}_p$ den Körper mit p Elementen

Beispiel

Der Ring $\mathbb{Z}/17\mathbb{Z}$ ist ein Körper.

Beispiel

Der Ring $\mathbb{Z}/15\mathbb{Z}$ ist kein Körper.

Die Ringe $\mathbb{Z}/n\mathbb{Z}$

Satz

Genau dann ist $\mathbb{Z}/n\mathbb{Z}$ ein Körper, wenn n eine Primzahl ist.

Bezeichnung

Ist p eine Primzahl, so bezeichnen wir $\mathbb{Z}/p\mathbb{Z}$ mit $\mathbb{F}_p$ und nennen $\mathbb{F}_p$ den Körper mit p Elementen

Beispiel

Der Ring $\mathbb{Z}/17\mathbb{Z}$ ist ein Körper.

Beispiel

Der Ring $\mathbb{Z}/15\mathbb{Z}$ ist kein Körper.

Die Körper $\mathbb{F}_p$

Wir betrachten nun ein Primzahl p. Bei der Division in $\mathbb{F}_p$ hilft der euklidische Algorithmus:
Ist $l \in \mathbb{F}_p \setminus \{0\} = \{1, 2, \ldots, p-1\}$, so sind l und p teilerfremd, dh.

$$1 = \mathrm{ggT}(l, p)$$

Berechnen wir nun $\mathrm{ggT}(l, p)$ mit den euklidischen Algorithmus und führen eine Rückwärtsrechnung durch, so erhalten wir daraus ein Darstelleung

$$1 = a \cdot l + b \cdot p$$

Die Körper $\mathbb{F}_p$

Wir betrachten nun ein Primzahl p. Bei der Division in $\mathbb{F}_p$ hilft der euklidische Algorithmus:
Ist $l \in \mathbb{F}_p \setminus \{0\} = \{1, 2, \ldots, p-1\}$, so sind l und p teilerfremd, dh.

$$1 = \mathrm{ggT}(l, p)$$

Berechnen wir nun $\mathrm{ggT}(l, p)$ mit den euklidischen Algorithmus und führen eine Rückwärtsrechnung durch, so erhalten wir daraus ein Darstelleung

$$1 = a \cdot l + b \cdot p$$

Betrachten wir dann die Restklassen modulo p, so erhalten wir

$$1 = (a \cdot l + b \cdot p) \mod p = a \cdot l \mod p$$

(denn $b \cdot p = 0 \mod p$). Also gilt

$$\frac{1}{l} = a \qquad \text{in } \mathbb{F}_p$$

Die Körper $\mathbb{F}_p$

Wir betrachten nun ein Primzahl p. Bei der Division in $\mathbb{F}_p$ hilft der euklidische Algorithmus:
Ist $l \in \mathbb{F}_p \setminus \{0\} = \{1, 2, \ldots, p-1\}$, so sind l und p teilerfremd, dh.

$$1 = \mathrm{ggT}(l, p)$$

Berechnen wir nun $\mathrm{ggT}(l, p)$ mit den euklidischen Algorithmus und führen eine Rückwärtsrechnung durch, so erhalten wir daraus ein Darstelleung

$$1 = a \cdot l + b \cdot p$$

Betrachten wir dann die Restklassen modulo p, so erhalten wir

$$1 = (a \cdot l + b \cdot p) \mod p = a \cdot l \mod p$$

(denn $b \cdot p = 0 \mod p$). Also gilt

$$\frac{1}{l} = a \qquad \text{in } \mathbb{F}_p$$

Die Körper $\mathbb{F}_p$

Beispiel

Die Zahl $p = 239$ ist eine Primzahl. Wir haben schon gesehen, dass $\mathrm{ggT}(239, 144) = 1$ und dass

$$1 = 47 \cdot 239 + (-78) \cdot 144$$

Damit gilt modulo p

$$1 = (-78) \cdot 144 = (239 - 78) \cdot 144 = 161 \cdot 144$$

Die Körper $\mathbb{F}_p$

Beispiel

Die Zahl $p = 239$ ist eine Primzahl. Wir haben schon gesehen, dass $\mathrm{ggT}(239, 144) = 1$ und dass

$$1 = 47 \cdot 239 + (-78) \cdot 144$$

Damit gilt modulo p

$$1 = (-78) \cdot 144 = (239 - 78) \cdot 144 = 161 \cdot 144$$

Also gilt in $\mathbb{F}_{239}$:

$$\frac{1}{144} = 161$$

Die Körper $\mathbb{F}_p$

Beispiel

Die Zahl $p = 239$ ist eine Primzahl. Wir haben schon gesehen, dass $\mathrm{ggT}(239, 144) = 1$ und dass

$$1 = 47 \cdot 239 + (-78) \cdot 144$$

Damit gilt modulo p

$$1 = (-78) \cdot 144 = (239 - 78) \cdot 144 = 161 \cdot 144$$

Also gilt in $\mathbb{F}_{239}$:

$$\frac{1}{144} = 161$$

Daraus folgt

$$\frac{207}{144} = 207 \cdot \frac{1}{144} = 207 \cdot 161 = 106$$

Die Körper $\mathbb{F}_p$

Beispiel

Die Zahl $p = 239$ ist eine Primzahl. Wir haben schon gesehen, dass $\mathrm{ggT}(239, 144) = 1$ und dass

$$1 = 47 \cdot 239 + (-78) \cdot 144$$

Damit gilt modulo p

$$1 = (-78) \cdot 144 = (239 - 78) \cdot 144 = 161 \cdot 144$$

Also gilt in $\mathbb{F}_{239}$:

$$\frac{1}{144} = 161$$

Daraus folgt

$$\frac{207}{144} = 207 \cdot \frac{1}{144} = 207 \cdot 161 = 106$$

Die Körper $\mathbb{F}_p$

Übung

Berechnen Sie $\frac{13}{74}$ im Körper $\mathbb{F}_{83}$.

Die Körper $\mathbb{F}_p$

Übung

Berechnen Sie $\frac{13}{74}$ im Körper $\mathbb{F}_{83}$.

Lösung:

Es ist

$$1 = 33 \cdot 83 + (-37) \cdot 74$$

also ist

$$\frac{1}{74} = -37 = 46$$

und damit

$$\frac{13}{74} = 13 \cdot 46 = 17$$

Die Körper $\mathbb{F}_p$

Übung

Berechnen Sie $\frac{13}{74}$ im Körper $\mathbb{F}_{83}$.

Lösung:

Es ist

$$1 = 33 \cdot 83 + (-37) \cdot 74$$

also ist

$$\frac{1}{74} = -37 = 46$$

und damit

$$\frac{13}{74} = 13 \cdot 46 = 17$$

Die Körper $\mathbb{F}_p$

Für eine Primzahl p bezeichnen wir mit $E(\mathbb{F}_p) = \mathbb{F}_p \setminus \{0\}$ die **Einheitengruppe** von $\mathbb{F}_p$.

Satz

Die Gruppe $E(\mathbb{F}_p)$ ist zyklisch von der Ordnung $p-1$, dh. es gibt ein Element $g \in \mathbb{F}_p \setminus \{0\}$ mit

$$\mathbb{F}_p \setminus \{0\} = \langle g \rangle = \{g, g^2, \ldots, g^{p-2}, g^{p-1} = 1\}$$

Die Körper $\mathbb{F}_p$

Für eine Primzahl p bezeichnen wir mit $E(\mathbb{F}_p) = \mathbb{F}_p \setminus \{0\}$ die **Einheitengruppe** von $\mathbb{F}_p$.

Satz

Die Gruppe $E(\mathbb{F}_p)$ ist zyklisch von der Ordnung $p-1$, dh. es gibt ein Element $g \in \mathbb{F}_p \setminus \{0\}$ mit

$$\mathbb{F}_p \setminus \{0\} = \langle g \rangle = \{g, g^2, \ldots, g^{p-2}, g^{p-1} = 1\}$$

Bemerkung

Beachten Sie, dass $E(\mathbb{F}_{p-1})$ die Ordnung $p-1$ hat, dass also für alle $a \in E(\mathbb{F}_p)$ gilt

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

Damit gilt auch

$$a^p = a$$

Die Körper $\mathbb{F}_p$

Für eine Primzahl p bezeichnen wir mit $E(\mathbb{F}_p) = \mathbb{F}_p \setminus \{0\}$ die **Einheitengruppe** von $\mathbb{F}_p$.

Satz

Die Gruppe $E(\mathbb{F}_p)$ ist zyklisch von der Ordnung $p-1$, dh. es gibt ein Element $g \in \mathbb{F}_p \setminus \{0\}$ mit

$$\mathbb{F}_p \setminus \{0\} = \langle g \rangle = \{g, g^2, \ldots, g^{p-2}, g^{p-1} = 1\}$$

Bemerkung

Beachten Sie, dass $E(\mathbb{F}_{p-1})$ die Ordnung $p-1$ hat, dass also für alle $a \in E(\mathbb{F}_p)$ gilt

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

Damit gilt auch

$$a^p = a$$

Die Körper $\mathbb{F}_p$

Beispiel

Im Körper $\mathbb{F}_{17}$ wird die Einheitengruppe von dem Element 3 erzeugt. Das Element 5 ist ebenfalls ein Erzeuger der Einheitengruppe, nicht aber das Element 4, denn

$$\langle 4 \rangle = \{4, 16, 13, 1\}$$

Bemerkung

Gilt für ein $g \in E(\mathbb{F}_p)$ für alle echten Teiler n von $p-1$:

$$g^n \neq 1$$

so erzeugt g die Gruppe $E(\mathbb{F}_p)$.

Die Körper $\mathbb{F}_p$

Beispiel

Im Körper $\mathbb{F}_{17}$ wird die Einheitengruppe von dem Element 3 erzeugt. Das Element 5 ist ebenfalls ein Erzeuger der Einheitengruppe, nicht aber das Element 4, denn

$$\langle 4 \rangle = \{4, 16, 13, 1\}$$

Bemerkung

Gilt für ein $g \in E(\mathbb{F}_p)$ für alle echten Teiler n von $p-1$:

$$g^n \neq 1$$

so erzeugt g die Gruppe $E(\mathbb{F}_p)$.

Die Körper $\mathbb{F}_p$

Übung

Bestimmen Sie einen Erzeuger der Einheitengruppe von $\mathbb{F}_{19}$.

Die Körper $\mathbb{F}_p$

Übung

Bestimmen Sie einen Erzeuger der Einheitengruppe von $\mathbb{F}_{19}$.

Lösung:

Das Element 2 ist ein Erzeuger von $E(\mathbb{F}_{19})$.

Die Körper $\mathbb{F}_p$

Übung

Bestimmen Sie einen Erzeuger der Einheitengruppe von $\mathbb{F}_{19}$.

Lösung:

Das Element 2 ist ein Erzeuger von $E(\mathbb{F}_{19})$.

Ausblick - Verschlüsselung

Rechnen mit ganzen Zahlen und Restklassen und der euklidische Algorithmus spielen eine wichtige Rolle in vielen Verfahren der sogenannenten **asymmetrischen Verschlüsselung**.

Bei diesen asymmetrischen Verfahren kommen zwei Schlüssel zur Anwendung, ein öffentlicher Schlüssel (*public key*), der zum Verschlüsseln benutzt wird, und ein geheimer Schlüssel (*private key*), der zum Entschlüsseln verwendet wird.

Ausblick - Verschlüsselung

Rechnen mit ganzen Zahlen und Restklassen und der euklidische Algorithmus spielen eine wichtige Rolle in vielen Verfahren der sogenannenten **asymmetrischen Verschlüsselung**.
Bei diesen asymmetrischen Verfahren kommen zwei Schlüssel zur Anwendung, ein öffentlicher Schlüssel (*public key*), der zum Verschlüsseln benutzt wird, und ein geheimer Schlüssel (*private key*), der zum Entschlüsseln verwendet wird.
Der öffentliche Schlüssel ist allgemein bekannt. Die Sicherheit dieser Verfahren beruht also darauf, dass der private Schlüssel aus dem öffentlichen Schlüssel nicht berechnet werden kann.

Ausblick - Verschlüsselung

Rechnen mit ganzen Zahlen und Restklassen und der euklidische Algorithmus spielen eine wichtige Rolle in vielen Verfahren der sogenannenten **asymmetrischen Verschlüsselung**.
Bei diesen asymmetrischen Verfahren kommen zwei Schlüssel zur Anwendung, ein öffentlicher Schlüssel (*public key*), der zum Verschlüsseln benutzt wird, und ein geheimer Schlüssel (*private key*), der zum Entschlüsseln verwendet wird.
Der öffentliche Schlüssel ist allgemein bekannt. Die Sicherheit dieser Verfahren beruht also darauf, dass der private Schlüssel aus dem öffentlichen Schlüssel nicht berechnet werden kann.

Eines der bekanntesten asymmetrischen Verfahren ist das **RSA–Verfahren**.

Ausblick - Verschlüsselung

Rechnen mit ganzen Zahlen und Restklassen und der euklidische Algorithmus spielen eine wichtige Rolle in vielen Verfahren der sogenannenten **asymmetrischen Verschlüsselung**.
Bei diesen asymmetrischen Verfahren kommen zwei Schlüssel zur Anwendung, ein öffentlicher Schlüssel (*public key*), der zum Verschlüsseln benutzt wird, und ein geheimer Schlüssel (*private key*), der zum Entschlüsseln verwendet wird.
Der öffentliche Schlüssel ist allgemein bekannt. Die Sicherheit dieser Verfahren beruht also darauf, dass der private Schlüssel aus dem öffentlichen Schlüssel nicht berechnet werden kann.

Eines der bekanntesten asymmetrischen Verfahren ist das **RSA–Verfahren**.

Das RSA–Verfahren

Der öffentliche Schlüssel des RSA–Verfahrens besteht aus einem Paar (e, N) positiver ganzer Zahlen, der private Schlüssel besteht ebenfalls aus einem Paar (d, N) positiver ganzer Zahlen, wobei diese Zahlen wie folgt zu konstruieren sind:

- Wähle zwei große Primzahlen p und q mit $p \neq q$ und setze $N = p \cdot q$.

Das RSA–Verfahren

Der öffentliche Schlüssel des RSA–Verfahrens besteht aus einem Paar (e, N) positiver ganzer Zahlen, der private Schlüssel besteht ebenfalls aus einem Paar (d, N) positiver ganzer Zahlen, wobei diese Zahlen wie folgt zu konstruieren sind:

- Wähle zwei große Primzahlen p und q mit $p \neq q$ und setze $N = p \cdot q$.
- Wähle eine zu $(p-1) \cdot (q-1)$ teilerfremde Zahl e.

Das RSA–Verfahren

Der öffentliche Schlüssel des RSA–Verfahrens besteht aus einem Paar (e, N) positiver ganzer Zahlen, der private Schlüssel besteht ebenfalls aus einem Paar (d, N) positiver ganzer Zahlen, wobei diese Zahlen wie folgt zu konstruieren sind:

- Wähle zwei große Primzahlen p und q mit $p \neq q$ und setze $N = p \cdot q$.
- Wähle eine zu $(p-1) \cdot (q-1)$ teilerfremde Zahl e.
- Bestimme d mit $0 < d < N$ so, dass $d \cdot e \equiv 1 \mod (p-1) \cdot (q-1)$.

Das RSA–Verfahren

Der öffentliche Schlüssel des RSA–Verfahrens besteht aus einem Paar (e, N) positiver ganzer Zahlen, der private Schlüssel besteht ebenfalls aus einem Paar (d, N) positiver ganzer Zahlen, wobei diese Zahlen wie folgt zu konstruieren sind:

- Wähle zwei große Primzahlen p und q mit $p \neq q$ und setze $N = p \cdot q$.
- Wähle eine zu $(p-1) \cdot (q-1)$ teilerfremde Zahl e.
- Bestimme d mit $0 < d < N$ so, dass $d \cdot e \equiv 1 \mod (p-1) \cdot (q-1)$.

Dann kann (e, N) als öffentlicher Schlüssel und (d, N) als privater Schlüssel benutzt werden.

Das RSA–Verfahren

Der öffentliche Schlüssel des RSA–Verfahrens besteht aus einem Paar (e, N) positiver ganzer Zahlen, der private Schlüssel besteht ebenfalls aus einem Paar (d, N) positiver ganzer Zahlen, wobei diese Zahlen wie folgt zu konstruieren sind:

- Wähle zwei große Primzahlen p und q mit $p \neq q$ und setze $N = p \cdot q$.
- Wähle eine zu $(p-1) \cdot (q-1)$ teilerfremde Zahl e.
- Bestimme d mit $0 < d < N$ so, dass $d \cdot e \equiv 1 \mod (p-1) \cdot (q-1)$.

Dann kann (e, N) als öffentlicher Schlüssel und (d, N) als privater Schlüssel benutzt werden.

Das RSA–Verfahren

Die Wirkungsweise des RSA–Verfahrens beruht auf folgender Aussage (einer Folgerung aus der Aussage, dass die Ordnung eines Elements immer die Gruppenordnung teilt):

Satz

Für jede ganze Zahl m mit $1 \leq m \leq N$ gilt

$$(m^e)^d \equiv m \mod N$$

Das RSA–Verfahren

Damit funktioniert das RSA–Verfahren wie folgt:
Alice will Bob eine Nachricht schicken, die durch eine Zahl m mit $1 < m < N$ dargestellt wird.

- Alice benutzt den öffentlichen Schlüssel und berechnet $b = m^e \mod N$.

Das RSA–Verfahren

Damit funktioniert das RSA–Verfahren wie folgt:
Alice will Bob eine Nachricht schicken, die durch eine Zahl m mit $1 < m < N$ dargestellt wird.

- Alice benutzt den öffentlichen Schlüssel und berechnet $b = m^e \mod N$.
- Alice schickt b über einen öffentlichen Kanal an Bob.

Das RSA–Verfahren

Damit funktioniert das RSA–Verfahren wie folgt:
Alice will Bob eine Nachricht schicken, die durch eine Zahl m mit $1 < m < N$ dargestellt wird.

- Alice benutzt den öffentlichen Schlüssel und berechnet $b = m^e \mod N$.
- Alice schickt b über einen öffentlichen Kanal an Bob.
- Bob benutzt seinen privaten Schlüssel und berechnet $c = b^d \mod N$.

Das RSA–Verfahren

Damit funktioniert das RSA–Verfahren wie folgt:
Alice will Bob eine Nachricht schicken, die durch eine Zahl m mit $1 < m < N$ dargestellt wird.

- Alice benutzt den öffentlichen Schlüssel und berechnet $b = m^e \mod N$.
- Alice schickt b über einen öffentlichen Kanal an Bob.
- Bob benutzt seinen privaten Schlüssel und berechnet $c = b^d \mod N$.
- Wegen $b \equiv m \mod N$ hat Bob die Nachricht entschlüsselt.

Das RSA–Verfahren

Damit funktioniert das RSA–Verfahren wie folgt:
Alice will Bob eine Nachricht schicken, die durch eine Zahl m mit $1 < m < N$ dargestellt wird.

- Alice benutzt den öffentlichen Schlüssel und berechnet $b = m^e \mod N$.
- Alice schickt b über einen öffentlichen Kanal an Bob.
- Bob benutzt seinen privaten Schlüssel und berechnet $c = b^d \mod N$.
- Wegen $b \equiv m \mod N$ hat Bob die Nachricht entschlüsselt.

Das RSA–Verfahren

Beispiel

Wir wählen die Primzahlen $p = 137$ und $q = 89$ und erhalten

$$N = p \cdot q = 12\,193$$

Ferner ist

$$(p-1) \cdot (q-1) = 136 \cdot 88 = 11\,968$$

Ferner wählen wir $e = 97$. Dann ist e teilerfremd zu $11\,968$ und für $d = 9377$ gilt

$$d \cdot e \equiv 1 \mod 11\,968$$

Das Paar $(97, 12\,193)$ ist unser öffentlicher Schlüssel, das Paar $(9377, 12\,193)$ ist unser privater Schlüssel.

Das RSA–Verfahren

Beispiel

Alice will Bob eine Nachricht m senden, die durch die Zahl $m = 7842$ repäsentiert wird.

- Alice berechnet $b = 7842^{97} \mod 12193$.

Das RSA–Verfahren

Beispiel

Alice will Bob eine Nachricht m senden, die durch die Zahl $m = 7842$ repäsentiert wird.

- Alice berechnet $b = 7842^{97} \mod 12193$.
- Sie erhält $b = 2853$ und schickt $b = 2853$ an Bob.

Das RSA–Verfahren

Beispiel

Alice will Bob eine Nachricht m senden, die durch die Zahl $m = 7842$ repäsentiert wird.

- Alice berechnet $b = 7842^{97} \mod 12193$.
- Sie erhält $b = 2853$ und schickt $b = 2853$ an Bob.
- Bob berechnet $m = 2853^{9377} = 7842 \mod 12193$.

Das RSA–Verfahren

Beispiel

Alice will Bob eine Nachricht m senden, die durch die Zahl $m = 7842$ repäsentiert wird.

- Alice berechnet $b = 7842^{97} \mod 12193$.
- Sie erhält $b = 2853$ und schickt $b = 2853$ an Bob.
- Bob berechnet $m = 2853^{9377} = 7842 \mod 12193$.
- Bob hat die Nachricht korrekt entschlüsselt.

Das RSA–Verfahren

Beispiel

Alice will Bob eine Nachricht m senden, die durch die Zahl $m = 7842$ repäsentiert wird.

- Alice berechnet $b = 7842^{97} \mod 12193$.
- Sie erhält $b = 2853$ und schickt $b = 2853$ an Bob.
- Bob berechnet $m = 2853^{9377} = 7842 \mod 12193$.
- Bob hat die Nachricht korrekt entschlüsselt.

Die Sicherheit des Verfahrens beruht darauf, dass zwar Bob die Zahl d über Euklid berechnen kann (da er p und q kennt), nicht jedoch ein Angreifer. Es gibt nämlich kein bekanntes effizientes Verfahren, dass aus einer (großen) Zahl N ihre Primfaktoren ermittelt.

Das RSA–Verfahren

Beispiel

Alice will Bob eine Nachricht m senden, die durch die Zahl $m = 7842$ repäsentiert wird.

- Alice berechnet $b = 7842^{97} \mod 12193$.
- Sie erhält $b = 2853$ und schickt $b = 2853$ an Bob.
- Bob berechnet $m = 2853^{9377} = 7842 \mod 12193$.
- Bob hat die Nachricht korrekt entschlüsselt.

Die Sicherheit des Verfahrens beruht darauf, dass zwar Bob die Zahl d über Euklid berechnen kann (da er p und q kennt), nicht jedoch ein Angreifer. Es gibt nämlich kein bekanntes effizientes Verfahren, dass aus einer (großen) Zahl N ihre Primfaktoren ermittelt.