3 Algebra und Zahlentheorie

Themen:

- Elementare Zahlentheorie
- Die Restklassenringe $\mathbb{Z}_n$
- Verschlüsselungstechniken

3.1 Grundlegende Sätze der elementaren Zahlentheorie

a, b meist ganze Zahlen.

3.1 Grundlegende Sätze der elementaren Zahlentheorie

a, b meist ganze Zahlen.

$a \mid b \Leftrightarrow a$ ist ein Teiler von $b \Leftrightarrow b = aq$ für eine ganze Zahl q.

3.1 Grundlegende Sätze der elementaren Zahlentheorie

a, b meist ganze Zahlen.

$a \mid b \Leftrightarrow a$ ist ein Teiler von $b \Leftrightarrow b = aq$ für eine ganze Zahl q.

$p \in \mathbb{N}$ heißt *Primzahl* genau dann, wenn p genau zwei Teiler hat, nämlich 1 und p.

3.1 Grundlegende Sätze der elementaren Zahlentheorie

a, b meist ganze Zahlen.

$a \mid b \Leftrightarrow a$ ist ein Teiler von $b \Leftrightarrow b = aq$ für eine ganze Zahl q.

$p \in \mathbb{N}$ heißt *Primzahl* genau dann, wenn p genau zwei Teiler hat, nämlich 1 und p.

Damit ist 1 keine Primzahl, weil sie nur einen Teiler besitzt.

Fundamentalsatz der Arithmetik

Aus der Schule ist der folgende Satz über die eindeutige Zerlegung einer natürlichen Zahl in ihre Primfaktoren bekannt.

Fundamentalsatz der Arithmetik

Aus der Schule ist der folgende Satz über die eindeutige Zerlegung einer natürlichen Zahl in ihre Primfaktoren bekannt.

Satz Ist $p_1 = 2$, $p_2 = 3$, $p_3 = 5, \ldots$ die Folge der Primzahlen, so gibt es zu jeder natürlichen Zahl $a > 1$ eindeutige Exponenten $r_1, \ldots, r_k \in \mathbb{N}_0$ mit

$$a = p_1^{r_1} p_2^{r_2} \ldots p_k^{r_k}, \quad r_k > 0.$$

Fundamentalsatz der Arithmetik

Aus der Schule ist der folgende Satz über die eindeutige Zerlegung einer natürlichen Zahl in ihre Primfaktoren bekannt.

Satz Ist $p_1 = 2$, $p_2 = 3$, $p_3 = 5, \ldots$ die Folge der Primzahlen, so gibt es zu jeder natürlichen Zahl $a > 1$ eindeutige Exponenten $r_1, \ldots, r_k \in \mathbb{N}_0$ mit

$$a = p_1^{r_1} p_2^{r_2} \ldots p_k^{r_k}, \quad r_k > 0.$$

Wenn wir vor der rechten Seite ein Minuszeichen setzen dürfen, gilt er auch für alle $a \in \mathbb{Z}$ mit $|a| > 1$.

Eine Primzahl als Teiler

Unter den vielen Anwendungen dieses Satzes erwähnen wir: Ist eine Primzahl p Teiler von ab, so ist

$$p \mid a \text{ oder } p \mid b.$$

Eine Primzahl als Teiler

Unter den vielen Anwendungen dieses Satzes erwähnen wir: Ist eine Primzahl p Teiler von ab, so ist

$$p \mid a \text{ oder } p \mid b.$$

Schauen wir uns die Primfaktorzerlegungen von a und b an, so muss p in einer der beiden vorkommen.

Kongruenzen

Wir sagen, a ist *kongruent zu* b *modulo* m, wenn die natürliche Zahl m ein Teiler von $b - a$ ist, also $m \mid b - a$.

Kongruenzen

Wir sagen, a ist *kongruent zu* b *modulo* m, wenn die natürliche Zahl m ein Teiler von $b - a$ ist, also $m \mid b - a$.

Schreiben dafür

$$a \equiv b \mod m.$$

Kongruenzen

Wir sagen, a ist *kongruent zu* b *modulo* m, wenn die natürliche Zahl m ein Teiler von $b - a$ ist, also $m \mid b - a$.

Schreiben dafür

$$a \equiv b \mod m.$$

Die Zahl m heißt *Modul* der Kongruenz.

Kongruenzen

Wir sagen, a ist *kongruent zu b modulo m*, wenn die natürliche Zahl m ein Teiler von $b - a$ ist, also $m \mid b - a$.

Schreiben dafür

$$a \equiv b \mod m.$$

Die Zahl m heißt *Modul* der Kongruenz.

Die Differenz zweier gerader Zahlen ist gerade, sie sind daher kongruent modulo 2.

Kongruenzen

Wir sagen, a ist *kongruent zu b modulo m*, wenn die natürliche Zahl m ein Teiler von $b - a$ ist, also $m \mid b - a$.

Schreiben dafür

$$a \equiv b \mod m.$$

Die Zahl m heißt *Modul* der Kongruenz.

Die Differenz zweier gerader Zahlen ist gerade, sie sind daher kongruent modulo 2.

Ebenso sind zwei ungerade Zahlen kongruent modulo 2, weil ihre Differenz ebenfalls geradzahlig ist.

Kongruenzen

Sind zwei Zahlen kongruent modulo m, so muss die Differenz der beiden Zahlen ein ganzzahliges Vielfaches von m sein, daher

$$a \equiv b \mod m \quad \Leftrightarrow \quad m \mid a-b \quad \Leftrightarrow \quad a = b + qm \text{ für ein } q \in \mathbb{Z}.$$

Kongruenzen

Sind zwei Zahlen kongruent modulo m, so muss die Differenz der beiden Zahlen ein ganzzahliges Vielfaches von m sein, daher

$$a \equiv b \mod m \quad \Leftrightarrow \quad m \mid a-b \quad \Leftrightarrow \quad a = b + qm \text{ für ein } q \in \mathbb{Z}.$$

Eine natürliche Zahl a hinterlässt beim Teilen durch m einen Rest in der Menge

$$\{0, 1, \ldots, m-1\}.$$

Kongruenzen

Sind zwei Zahlen kongruent modulo m, so muss die Differenz der beiden Zahlen ein ganzzahliges Vielfaches von m sein, daher

$$a \equiv b \mod m \quad \Leftrightarrow \quad m \mid a-b \quad \Leftrightarrow \quad a = b + qm \text{ für ein } q \in \mathbb{Z}.$$

Eine natürliche Zahl a hinterlässt beim Teilen durch m einen Rest in der Menge

$$\{0, 1, \ldots, m-1\}.$$

Zwei natürliche Zahlen a, b sind genau dann kongruent modulo m, wenn sie beim Teilen durch m den gleichen Rest besitzen.

Kongruenzen

Sind zwei Zahlen kongruent modulo m, so muss die Differenz der beiden Zahlen ein ganzzahliges Vielfaches von m sein, daher

$$a \equiv b \mod m \quad \Leftrightarrow \quad m \mid a-b \quad \Leftrightarrow \quad a = b + qm \text{ für ein } q \in \mathbb{Z}.$$

Eine natürliche Zahl a hinterlässt beim Teilen durch m einen Rest in der Menge

$$\{0, 1, \ldots, m-1\}.$$

Zwei natürliche Zahlen a, b sind genau dann kongruent modulo m, wenn sie beim Teilen durch m den gleichen Rest besitzen.

Dieser Rest fällt in $b - a$ heraus. Dieses Prinzip lässt sich auch auf negative Zahlen ausdehnen, wenn wir m auf den Rest addieren.

Rechenregeln für Kongruenzen

$$a \equiv b \mod m, \quad c \equiv d \mod m \quad \Rightarrow$$

$$a \pm c \equiv b \pm d \mod m \quad \text{und} \quad ac \equiv bd \mod m.$$

Rechenregeln für Kongruenzen

$$a \equiv b \mod m,\ \ c \equiv d \mod m \quad \Rightarrow$$

$$a \pm c \equiv b \pm d \mod m \ \text{ und } \ ac \equiv bd \mod m.$$

Insbesondere

$$a \equiv b \mod m \quad \Rightarrow \quad a^k \equiv b^k \mod m.$$

Rechenregeln für Kongruenzen

$$a \equiv b \mod m,\ \ c \equiv d \mod m \quad \Rightarrow$$

$$a \pm c \equiv b \pm d \mod m \ \text{ und } \ ac \equiv bd \mod m.$$

Insbesondere

$$a \equiv b \mod m \quad \Rightarrow \quad a^k \equiv b^k \mod m.$$

Zusammenfassung: Ist $p(x)$ ein Polynom mit ganzzahligen Koeffizienten, so gilt

$$a \equiv b \mod m \ \Rightarrow \ p(a) \equiv p(b) \mod m.$$

Teilerfremde Zahlen

Zwei natürliche Zahlen heißen *teilerfremd*, wenn sie nur 1 als gemeinsamen Teiler besitzen.

Teilerfremde Zahlen

Zwei natürliche Zahlen heißen *teilerfremd*, wenn sie nur 1 als gemeinsamen Teiler besitzen.

a und b sind genau dann teilerfremd, wenn ihre Primfakorzerlegungen keine gemeinsamen Primfaktoren besitzen

Division in der Kongruenzrelation

Vorsicht: Es gilt $m \equiv 2m \mod m$, aber

$$1 \not\equiv 2 \mod m.$$

Division in der Kongruenzrelation

Vorsicht: Es gilt $m \equiv 2m \mod m$, aber

$$1 \not\equiv 2 \mod m.$$

Daher

$$ac \equiv bc \mod m,\ c \text{ und } m \text{ teilerfremd } \Rightarrow\ a \equiv b \mod m.$$

Division in der Kongruenzrelation

Vorsicht: Es gilt $m \equiv 2m \mod m$, aber

$$1 \not\equiv 2 \mod m.$$

Daher

$$ac \equiv bc \mod m,\ c \text{ und } m \text{ teilerfremd } \Rightarrow\ a \equiv b \mod m.$$

Beweis

$$ac \equiv bc \mod m \ \Leftrightarrow\ m \mid (b-a)c.$$

Division in der Kongruenzrelation

Vorsicht: Es gilt $m \equiv 2m \mod m$, aber

$$1 \not\equiv 2 \mod m.$$

Daher

$$ac \equiv bc \mod m,\ c \text{ und } m \text{ teilerfremd } \Rightarrow\ a \equiv b \mod m.$$

Beweis

$$ac \equiv bc \mod m \ \Leftrightarrow\ m \mid (b-a)c.$$

Sind m und c teilerfremd, so kommen in den Primfaktorzerlegungen von m und c nur verschiedene Primzahlen vor. Damit muss m ein Teiler von $b-a$ sein.

Kleiner Satz von Fermat

Satz Sei a positiv und p eine Primzahl. Dann gilt

$$a^p \equiv a \mod p.$$

Kleiner Satz von Fermat

Satz Sei a positiv und p eine Primzahl. Dann gilt

$$a^p \equiv a \mod p.$$

Ist p kein Teiler von a, folgt hieraus

$$a^{p-1} \equiv 1 \mod p.$$

Beweis

$$a^p \equiv a \mod p.$$

Vollständige Induktion über a : Für $a = 1$ ist $p \mid 1^p - 1$ richtig.

Beweis

$$a^p \equiv a \mod p.$$

Vollständige Induktion über a : Für $a = 1$ ist $p \mid 1^p - 1$ richtig.

Induktionsvoraussetzung: Behauptung ist für a richtig, also $p \mid a^p - a$.

Beweis

$$a^p \equiv a \mod p.$$

Vollständige Induktion über a : Für $a = 1$ ist $p \mid 1^p - 1$ richtig.

Induktionsvoraussetzung: Behauptung ist für a richtig, also $p \mid a^p - a$.

Wir müssen zeigen, dass

$$p \mid (a+1)^p - (a+1).$$

Beweis

$$p \mid (a+1)^p - (a+1).$$

Mit der binomischen Formel erhalten wir

$$(a+1)^p - (a+1) = \sum_{i=0}^{p} \binom{p}{i} a^i - (a+1)$$

$$= a^p + 1 + \sum_{i=1}^{p-1} \binom{p}{i} a^i - (a+1)$$

Beweis

$$p \mid (a+1)^p - (a+1).$$

Mit der binomischen Formel erhalten wir

$$\begin{aligned}(a+1)^p - (a+1) &= \sum_{i=0}^{p} \binom{p}{i} a^i - (a+1) \\ &= a^p + 1 + \sum_{i=1}^{p-1} \binom{p}{i} a^i - (a+1) \\ &= a^p - a + \sum_{i=1}^{p-1} \binom{p}{i} a^i.\end{aligned}$$

Beweis

$$p \mid (a+1)^p - (a+1).$$

Mit der binomischen Formel erhalten wir

$$\begin{aligned}(a+1)^p - (a+1) &= \sum_{i=0}^{p} \binom{p}{i} a^i - (a+1) \\ &= a^p + 1 + \sum_{i=1}^{p-1} \binom{p}{i} a^i - (a+1) \\ &= a^p - a + \sum_{i=1}^{p-1} \binom{p}{i} a^i.\end{aligned}$$

Auf der rechten Seite ist $a^p - a$ aufgrund der Induktionsvoraussetzung durch p teilbar.

Beweis

$$(a+1)^p - (a+1) = a^p - a + \sum_{i=1}^{p-1} \binom{p}{i} a^i.$$

Die Binomialkoeffizienten

$$\binom{p}{i} = \frac{p!}{i!(p-i)!}$$

sind ganzzahlig.

Beweis

$$(a+1)^p - (a+1) = a^p - a + \sum_{i=1}^{p-1} \binom{p}{i} a^i.$$

Die Binomialkoeffizienten

$$\binom{p}{i} = \frac{p!}{i!(p-i)!}$$

sind ganzzahlig. Ist p eine Primzahl, so kann der Faktor p im Zähler für $i \neq 0$ und $i \neq p$ nicht herausgekürzt werden.

Beweis

$$(a+1)^p - (a+1) = a^p - a + \sum_{i=1}^{p-1} \binom{p}{i} a^i.$$

Die Binomialkoeffizienten

$$\binom{p}{i} = \frac{p!}{i!(p-i)!}$$

sind ganzzahlig. Ist p eine Primzahl, so kann der Faktor p im Zähler für $i \neq 0$ und $i \neq p$ nicht herausgekürzt werden.

Da die Binomialkoeffizienten hier durch p teilbar sind, ist auch die linke Seite durch p teilbar.

Beispiel

Zeigen Sie, dass für jede positive Zahl n gilt $30 \mid n^5 - n$.

Beispiel

Zeigen Sie, dass für jede positive Zahl n gilt $30 \mid n^5 - n$.

Lösung: Die Teilbarkeit durch 5 folgt aus dem Fermatschen Satz.

Beispiel

Zeigen Sie, dass für jede positive Zahl n gilt $30 \mid n^5 - n$.

Lösung: Die Teilbarkeit durch 5 folgt aus dem Fermatschen Satz.

Wegen

$$n^5 - n = (n-1)n(n+1)(n^2+1)$$

ist $n^5 - n$ außerdem durch 2 und durch 3 teilbar.

Beispiel

Zeigen Sie, dass für jede positive Zahl n gilt $30 \mid n^5 - n$.

Lösung: Die Teilbarkeit durch 5 folgt aus dem Fermatschen Satz.

Wegen

$$n^5 - n = (n-1)n(n+1)(n^2+1)$$

ist $n^5 - n$ außerdem durch 2 und durch 3 teilbar.

Beide Zahlen müssen Teiler einer Zahl in der Folge $n-1, n, n+1$ sein.

Division mit Rest

Sind $a \in \mathbb{N}_0$ und $b \in \mathbb{N}$, so gibt es eindeutig bestimmte Zahlen $m, r \in \mathbb{N}_0$ mit

$$a = mb + r, \quad 0 \leq r < b.$$

Division mit Rest

Sind $a \in \mathbb{N}_0$ und $b \in \mathbb{N}$, so gibt es eindeutig bestimmte Zahlen $m, r \in \mathbb{N}_0$ mit

$$a = mb + r, \quad 0 \leq r < b.$$

Jede nichtnegative ganze Zahl liegt in genau einem Intervall $[0, b), [b, 2b), \ldots$. Daher sind sowohl m als auch r eindeutig bestimmt.

Ganzzahldivision

Für ganzzahliges a existieren eindeutige $b \in \mathbb{Z}$ und $0 \leq r < m$ mit

$$a = mb + r.$$

Ganzzahldivision

Für ganzzahliges a existieren eindeutige $b \in \mathbb{Z}$ und $0 \leq r < m$ mit

$$a = mb + r.$$

Ganzzahldivision: $a \operatorname{div} m = b$.

Ganzzahldivision

Für ganzzahliges a existieren eindeutige $b \in \mathbb{Z}$ und $0 \leq r < m$ mit

$$a = mb + r.$$

Ganzzahldivision: $a \operatorname{div} m = b$.

Beispiel:

$$15 \operatorname{div} 7 = 2, \qquad \text{aber} \quad -15 \operatorname{div} 7 = -3.$$

Ganzzahldivision

Für ganzzahliges a existieren eindeutige $b \in \mathbb{Z}$ und $0 \leq r < m$ mit

$$a = mb + r.$$

Ganzzahldivision: $a \operatorname{div} m = b$.

Beispiel:

$$15 \operatorname{div} 7 = 2, \qquad \text{aber} \quad -15 \operatorname{div} 7 = -3.$$

Der auftretende Rest $r \in \{0, \ldots, m-1\}$ ist der *Rest von a modulo m*.

Ganzzahldivision

Für ganzzahliges a existieren eindeutige $b \in \mathbb{Z}$ und $0 \leq r < m$ mit

$$a = mb + r.$$

Ganzzahldivision: $a \operatorname{div} m = b$.

Beispiel:

$$15 \operatorname{div} 7 = 2, \qquad \text{aber} \quad -15 \operatorname{div} 7 = -3.$$

Der auftretende Rest $r \in \{0, \ldots, m-1\}$ ist der *Rest von a modulo m*.

Schreiben dafür $a \bmod m$. Dann

$$a = m \cdot (a \operatorname{div} m) + (a \bmod m).$$

Größter gemeinsamer Teiler

d heißt *größter gemeinsamer Teiler* von $a \in \mathbb{N}$ und $b \in \mathbb{N}$, wenn

- $d \mid a, b$,

Größter gemeinsamer Teiler

d heißt *größter gemeinsamer Teiler* von $a \in \mathbb{N}$ und $b \in \mathbb{N}$, wenn

- $d \mid a, b$,
- Aus $t \mid a$ und $t \mid b$ folgt, dass $t \mid d$.

Größter gemeinsamer Teiler

d heißt *größter gemeinsamer Teiler* von $a \in \mathbb{N}$ und $b \in \mathbb{N}$, wenn

- $d \mid a, b$,
- Aus $t \mid a$ und $t \mid b$ folgt, dass $t \mid d$.

Schreiben dafür

$$d = ggT(a, b).$$

Größter gemeinsamer Teiler

d heißt *größter gemeinsamer Teiler* von $a \in \mathbb{N}$ und $b \in \mathbb{N}$, wenn

- $d \mid a, b$,
- Aus $t \mid a$ und $t \mid b$ folgt, dass $t \mid d$.

Schreiben dafür

$$d = ggT(a, b).$$

Für teilerfremde Zahlen gilt $ggT(a, b) = 1$.

Größter gemeinsamer Teiler

d heißt *größter gemeinsamer Teiler* von $a \in \mathbb{N}$ und $b \in \mathbb{N}$, wenn

- $d \mid a, b$,
- Aus $t \mid a$ und $t \mid b$ folgt, dass $t \mid d$.

Schreiben dafür

$$d = ggT(a, b).$$

Für teilerfremde Zahlen gilt $ggT(a, b) = 1$.

Den größten gemeinsamen Teiler kann man aus den Primfaktorzerlegungen der Zahlen a und b bestimmen, indem man das Produkt der gemeinsamen Primfaktoren bildet.

Größter gemeinsamer Teiler

d heißt *größter gemeinsamer Teiler* von $a \in \mathbb{N}$ und $b \in \mathbb{N}$, wenn

- $d \mid a, b$,
- Aus $t \mid a$ und $t \mid b$ folgt, dass $t \mid d$.

Schreiben dafür

$$d = ggT(a, b).$$

Für teilerfremde Zahlen gilt $ggT(a, b) = 1$.

Den größten gemeinsamen Teiler kann man aus den Primfaktorzerlegungen der Zahlen a und b bestimmen, indem man das Produkt der gemeinsamen Primfaktoren bildet.

Besser den Beweis des nächsten Satzes nehmen

Satz vom größten gemeinsamen Teiler, Lemma von Bézout

Satz Für
$a, b \in \mathbb{N}$ existiert genau ein größter gemeinsamer Teiler $d \in \mathbb{N}$.

Satz vom größten gemeinsamen Teiler, Lemma von Bézout

Satz Für
$a, b \in \mathbb{N}$ existiert genau ein größter gemeinsamer Teiler $d \in \mathbb{N}$.

Ferner gibt es Zahlen $\alpha, \beta \in \mathbb{Z}$ mit

$$d = \alpha a + \beta b.$$

Beweis

Wir dürfen $a > b$ annehmen. Wir wenden fortgesetzte Division mit Rest nach folgendem Schema solange an, bis der Rest 0 entsteht:

$$
\begin{aligned}
a &= b \cdot q_1 + r_1, & 0 < r_1 < b,\\
b &= r_1 \cdot q_2 + r_2, & 0 < r_2 < r_1,\\
r_1 &= r_2 \cdot q_3 + r_3, & 0 < r_3 < r_2,\\
&\vdots\\
r_{k-4} &= r_{k-3} \cdot q_{k-2} + r_{k-2}, & 0 < r_{k-2} < r_{k-3},\\
r_{k-3} &= r_{k-2} \cdot q_{k-1} + r_{k-1}, & 0 < r_{k-1} < r_{k-2},\\
r_{k-2} &= r_{k-1} \cdot q_k + r_k, & 0 < r_k < r_{k-1},\\
r_{k-1} &= r_k \cdot q_k. &
\end{aligned}
$$

Beweis

Wir dürfen $a > b$ annehmen. Wir wenden fortgesetzte Division mit Rest nach folgendem Schema solange an, bis der Rest 0 entsteht:

$$
\begin{aligned}
a &= b \cdot q_1 + r_1, & 0 < r_1 < b,\\
b &= r_1 \cdot q_2 + r_2, & 0 < r_2 < r_1,\\
r_1 &= r_2 \cdot q_3 + r_3, & 0 < r_3 < r_2,\\
&\vdots\\
r_{k-4} &= r_{k-3} \cdot q_{k-2} + r_{k-2}, & 0 < r_{k-2} < r_{k-3},\\
r_{k-3} &= r_{k-2} \cdot q_{k-1} + r_{k-1}, & 0 < r_{k-1} < r_{k-2},\\
r_{k-2} &= r_{k-1} \cdot q_k + r_k, & 0 < r_k < r_{k-1},\\
r_{k-1} &= r_k \cdot q_k.
\end{aligned}
$$

Da die Folge der Reste nichtnegativ und streng monoton fallend ist, kommen wir nach endlich vielen Schritten zum Rest 0.

Beweis

$$
\begin{aligned}
a &= b \cdot q_1 + r_1, && 0 < r_1 < b, \\
b &= r_1 \cdot q_2 + r_2, && 0 < r_2 < r_1, \\
r_1 &= r_2 \cdot q_3 + r_3, && 0 < r_3 < r_2, \\
&\vdots \\
r_{k-4} &= r_{k-3} \cdot q_{k-2} + r_{k-2}, && 0 < r_{k-2} < r_{k-3}, \\
r_{k-3} &= r_{k-2} \cdot q_{k-1} + r_{k-1}, && 0 < r_{k-1} < r_{k-2}, \\
r_{k-2} &= r_{k-1} \cdot q_k + r_k, && 0 < r_k < r_{k-1}, \\
r_{k-1} &= r_k \cdot q_k. &&
\end{aligned}
$$

Beweis

$$
\begin{aligned}
a &= b \cdot q_1 + r_1, & 0 < r_1 < b,\\
b &= r_1 \cdot q_2 + r_2, & 0 < r_2 < r_1,\\
r_1 &= r_2 \cdot q_3 + r_3, & 0 < r_3 < r_2,\\
&\vdots & \\
r_{k-4} &= r_{k-3} \cdot q_{k-2} + r_{k-2}, & 0 < r_{k-2} < r_{k-3},\\
r_{k-3} &= r_{k-2} \cdot q_{k-1} + r_{k-1}, & 0 < r_{k-1} < r_{k-2},\\
r_{k-2} &= r_{k-1} \cdot q_k + r_k, & 0 < r_k < r_{k-1},\\
r_{k-1} &= r_k \cdot q_k. &
\end{aligned}
$$

r_k ist der größte gemeinsame Teiler von a und b:

Beweis

$$
\begin{aligned}
a &= b \cdot q_1 + r_1, & 0 < r_1 < b,\\
b &= r_1 \cdot q_2 + r_2, & 0 < r_2 < r_1,\\
r_1 &= r_2 \cdot q_3 + r_3, & 0 < r_3 < r_2,\\
&\vdots\\
r_{k-4} &= r_{k-3} \cdot q_{k-2} + r_{k-2}, & 0 < r_{k-2} < r_{k-3},\\
r_{k-3} &= r_{k-2} \cdot q_{k-1} + r_{k-1}, & 0 < r_{k-1} < r_{k-2},\\
r_{k-2} &= r_{k-1} \cdot q_k + r_k, & 0 < r_k < r_{k-1},\\
r_{k-1} &= r_k \cdot q_k.
\end{aligned}
$$

r_k ist der größte gemeinsame Teiler von a und b: Liest man nämlich die Gleichungen von unten nach oben, so kommt man auf die Beziehungen

$$r_k \mid r_{k-1},\ r_k \mid r_{k-2}, \ldots\ r_k \mid b,\ r_k \mid a,$$

womit r_k ein gemeinsamer Teiler von b und a ist.

Beweis

$$
\begin{aligned}
a &= b \cdot q_1 + r_1, && 0 < r_1 < b,\\
b &= r_1 \cdot q_2 + r_2, && 0 < r_2 < r_1,\\
r_1 &= r_2 \cdot q_3 + r_3, && 0 < r_3 < r_2,\\
&\vdots\\
r_{k-4} &= r_{k-3} \cdot q_{k-2} + r_{k-2}, && 0 < r_{k-2} < r_{k-3},\\
r_{k-3} &= r_{k-2} \cdot q_{k-1} + r_{k-1}, && 0 < r_{k-1} < r_{k-2},\\
r_{k-2} &= r_{k-1} \cdot q_k + r_k, && 0 < r_k < r_{k-1},\\
r_{k-1} &= r_k \cdot q_k.
\end{aligned}
$$

Beweis

$$
\begin{aligned}
a &= b \cdot q_1 + r_1, && 0 < r_1 < b,\\
b &= r_1 \cdot q_2 + r_2, && 0 < r_2 < r_1,\\
r_1 &= r_2 \cdot q_3 + r_3, && 0 < r_3 < r_2,\\
&\vdots\\
r_{k-4} &= r_{k-3} \cdot q_{k-2} + r_{k-2}, && 0 < r_{k-2} < r_{k-3},\\
r_{k-3} &= r_{k-2} \cdot q_{k-1} + r_{k-1}, && 0 < r_{k-1} < r_{k-2},\\
r_{k-2} &= r_{k-1} \cdot q_k + r_k, && 0 < r_k < r_{k-1},\\
r_{k-1} &= r_k \cdot q_k.
\end{aligned}
$$

Für einen beliebigen gemeinsamen Teiler t von a und b kommt man, wenn man die Gleichungen von oben nach unten liest, auf

$$t \mid r_1,\ t \mid r_2, \ldots,\ t \mid r_k.$$

Beweis

$$
\begin{aligned}
a &= b \cdot q_1 + r_1, && 0 < r_1 < b,\\
b &= r_1 \cdot q_2 + r_2, && 0 < r_2 < r_1,\\
r_1 &= r_2 \cdot q_3 + r_3, && 0 < r_3 < r_2,\\
&\vdots\\
r_{k-4} &= r_{k-3} \cdot q_{k-2} + r_{k-2}, && 0 < r_{k-2} < r_{k-3},\\
r_{k-3} &= r_{k-2} \cdot q_{k-1} + r_{k-1}, && 0 < r_{k-1} < r_{k-2},\\
r_{k-2} &= r_{k-1} \cdot q_k + r_k, && 0 < r_k < r_{k-1},\\
r_{k-1} &= r_k \cdot q_k.
\end{aligned}
$$

Für einen beliebigen gemeinsamen Teiler t von a und b kommt man, wenn man die Gleichungen von oben nach unten liest, auf

$$t \mid r_1,\ t \mid r_2, \ldots,\ t \mid r_k.$$

Damit ist in der Tat $r_k = ggT(a, b)$.

Beweis

$$
\begin{aligned}
a &= b \cdot q_1 + r_1, & 0 < r_1 < b,\\
b &= r_1 \cdot q_2 + r_2, & 0 < r_2 < r_1,\\
r_1 &= r_2 \cdot q_3 + r_3, & 0 < r_3 < r_2,\\
&\vdots\\
r_{k-4} &= r_{k-3} \cdot q_{k-2} + r_{k-2}, & 0 < r_{k-2} < r_{k-3},\\
r_{k-3} &= r_{k-2} \cdot q_{k-1} + r_{k-1}, & 0 < r_{k-1} < r_{k-2},\\
r_{k-2} &= r_{k-1} \cdot q_k + r_k, & 0 < r_k < r_{k-1},\\
r_{k-1} &= r_k \cdot q_k.
\end{aligned}
$$

$r_k = \alpha a + \beta b$: Aus der vorletzten und drittletzten Gleichung ergibt sich

$$r_k = r_{k-2} - r_{k-1} q_k, \quad r_k = (1 + q_{k-1} q_k) r_{k-2} - q_k r_{k-3}.$$

Beweis

$$
\begin{aligned}
a &= b \cdot q_1 + r_1, & 0 < r_1 < b,\\
b &= r_1 \cdot q_2 + r_2, & 0 < r_2 < r_1,\\
r_1 &= r_2 \cdot q_3 + r_3, & 0 < r_3 < r_2,\\
&\vdots\\
r_{k-4} &= r_{k-3} \cdot q_{k-2} + r_{k-2}, & 0 < r_{k-2} < r_{k-3},\\
r_{k-3} &= r_{k-2} \cdot q_{k-1} + r_{k-1}, & 0 < r_{k-1} < r_{k-2},\\
r_{k-2} &= r_{k-1} \cdot q_k + r_k, & 0 < r_k < r_{k-1},\\
r_{k-1} &= r_k \cdot q_k.
\end{aligned}
$$

$r_k = \alpha a + \beta b$: Aus der vorletzten und drittletzten Gleichung ergibt sich

$$r_k = r_{k-2} - r_{k-1} q_k, \quad r_k = (1 + q_{k-1} q_k) r_{k-2} - q_k r_{k-3}.$$

Stelle r_{k-2} als Kombination von r_{k-4} und r_{k-3} dar:

$$r_k = \alpha a + \beta b.$$

Beispiel

Das im letzten Beweis dargestellte Verfahren ist deshalb so effektiv, weil sich die r_i in jedem Schritt mindestens halbieren.

Beispiel

Das im letzten Beweis dargestellte Verfahren ist deshalb so effektiv, weil sich die r_i in jedem Schritt mindestens halbieren.

Für $a = 38$ und $b = 10$ erhält man

$$38 = 10 \cdot 3 + 8$$

$$10 = 8 \cdot 1 + 2$$

$$8 = 2 \cdot 4,$$

also $ggT(38, 10) = 2$..

Beispiel

Das im letzten Beweis dargestellte Verfahren ist deshalb so effektiv, weil sich die r_i in jedem Schritt mindestens halbieren.

Für $a = 38$ und $b = 10$ erhält man

$$38 = 10 \cdot 3 + 8$$

$$10 = 8 \cdot 1 + 2$$

$$8 = 2 \cdot 4,$$

also $ggT(38, 10) = 2$..

α, β bestimmt man aus

$$\begin{aligned} 2 &= 10 - 1 \cdot 8 \\ &= 10 - 1 \cdot (38 - 10 \cdot 3) = 4 \cdot 10 - 1 \cdot 38, \end{aligned}$$

also $\alpha = -1$ und $\beta = 4$.

3.2 Stellenwertsysteme

Sei $g \in \mathbb{N} \setminus \{1\}$. Die *g-adische Darstellung* einer natürlichen Zahl n ist von der Form

$$n = a_0 \cdot g^0 + a_1 \cdot g^1 + \ldots + a_s g^s = \sum_{k=0}^{s} a_k g^k$$

mit „Ziffern“ $a_k \in \{0, 1, \ldots, g-1\}$.

3.2 Stellenwertsysteme

Sei $g \in \mathbb{N} \setminus \{1\}$. Die *g-adische Darstellung* einer natürlichen Zahl n ist von der Form

$$n = a_0 \cdot g^0 + a_1 \cdot g^1 + \ldots + a_s g^s = \sum_{k=0}^{s} a_k g^k$$

mit „Ziffern“ $a_k \in \{0, 1, \ldots, g-1\}$.

Für die *Basis* g hat sich im täglichen Gebrauch $g = 10$ durchgesetzt, wir schreiben ja

$$a_s \ldots a_0.$$

3.2 Stellenwertsysteme

Sei $g \in \mathbb{N} \setminus \{1\}$. Die *g-adische Darstellung* einer natürlichen Zahl n ist von der Form

$$n = a_0 \cdot g^0 + a_1 \cdot g^1 + \ldots + a_s g^s = \sum_{k=0}^{s} a_k g^k$$

mit „Ziffern“ $a_k \in \{0, 1, \ldots, g-1\}$.

Für die *Basis* g hat sich im täglichen Gebrauch $g = 10$ durchgesetzt, wir schreiben ja

$$a_s \ldots a_0.$$

Relikte anderer Basen sind bei uns noch erkennbar: Stunden, Minuten und Sekunden sind im 60er System strukturiert, das Dutzend und das Gros erinnern an die Basis 12.

Bestimmung der Ziffern

Für die Darstellung

$$n = a_0 \cdot g^0 + a_1 \cdot g^1 + \ldots + a_s g^s = \sum_{k=0}^{s} a_k g^k$$

schreiben wir

$$n = a_s a_{s-1} \ldots a_0{}_g.$$

Bestimmung der Ziffern

Für die Darstellung

$$n = a_0 \cdot g^0 + a_1 \cdot g^1 + \ldots + a_s g^s = \sum_{k=0}^{s} a_k g^k$$

schreiben wir

$$n = a_s a_{s-1} \ldots a_0{}_g.$$

Diese Darstellung ist offenbar eindeutig und es gilt

$$a_k = (n \operatorname{div} g^k) \mod g \quad \text{für } k = 0, 1, \ldots.$$

Bestimmung der Ziffern

Für die Darstellung

$$n = a_0 \cdot g^0 + a_1 \cdot g^1 + \ldots + a_s g^s = \sum_{k=0}^{s} a_k g^k$$

schreiben wir

$$n = a_s a_{s-1} \ldots a_0{}_g.$$

Diese Darstellung ist offenbar eindeutig und es gilt

$$a_k = (n \operatorname{div} g^k) \mod g \quad \text{für } k = 0, 1, \ldots.$$

Für die praktische Rechnung dividiert man fortgesetzt ganzzahlig durch g und nimmt anschließend die Ergebnisse modulo g.

Beispiel

Für $n = 50$ und $g = 2$ gilt

$$50 \operatorname{div} 1 = 50,\ 50 \operatorname{div} 2 = 25,\ 25 \operatorname{div} 2 = 12,$$

$$12 \operatorname{div} 2 = 6,\ 6 \operatorname{div} 2 = 3,\ 3 \operatorname{div} 2 = 1,$$

daher $50_{10} = 110010_2$.

Darstellung ganzer Zahlen im Rechner

Stehen uns $s+1$ Bits im Binärsystem $g=2$ zur Verfügung, so geht ein Bit für das Vorzeichen verloren.

Darstellung ganzer Zahlen im Rechner

Stehen uns $s+1$ Bits im Binärsystem $g=2$ zur Verfügung, so geht ein Bit für das Vorzeichen verloren.

Es ist aber ungünstig, explizit das Vorzeichen zu codieren, weil das bei der Addition zu Fallunterscheidungen führt.

Darstellung ganzer Zahlen im Rechner

Stehen uns $s+1$ Bits im Binärsystem $g=2$ zur Verfügung, so geht ein Bit für das Vorzeichen verloren.

Es ist aber ungünstig, explizit das Vorzeichen zu codieren, weil das bei der Addition zu Fallunterscheidungen führt.

Die Vorzeichen der beiden zu addierenden Zahlen entscheiden darüber, ob addiert oder subtrahiert wird.

Zweierkomplemente

Besser ist es daher, *Zweierkomplemente* zu verwenden, nämlich

$$[a_s a_{s-1} \dots a_0]_2 = a_{s-1} \dots a_{02} - 2^s a_s.$$

Zweierkomplemente

Besser ist es daher, *Zweierkomplemente* zu verwenden, nämlich

$$[a_s a_{s-1} \dots a_0]_2 = a_{s-1} \dots a_{02} - 2^s a_s.$$

Bei $a_s = 0$ laufen die nichtnegativen ganzen Zahlen von

$$0 = [0 \dots 0]_2 \quad \text{bis} \quad 2^s - 1 = [011 \dots 1]_2$$

Zweierkomplemente

Besser ist es daher, *Zweierkomplemente* zu verwenden, nämlich

$$[a_s a_{s-1} \dots a_0]_2 = a_{s-1} \dots a_{02} - 2^s a_s.$$

Bei $a_s = 0$ laufen die nichtnegativen ganzen Zahlen von

$$0 = [0 \dots 0]_2 \quad \text{bis} \quad 2^s - 1 = [011 \dots 1]_2$$

Die negativen Zahlen laufen von

$$-1 = [11 \dots 1]_2 \quad \text{bis} \quad -2^s = [10 \dots 0]_2.$$

Zweierkomplemente

Besser ist es daher, *Zweierkomplemente* zu verwenden, nämlich

$$[a_s a_{s-1} \dots a_0]_2 = a_{s-1} \dots a_{02} - 2^s a_s.$$

Bei $a_s = 0$ laufen die nichtnegativen ganzen Zahlen von

$$0 = [0 \dots 0]_2 \quad \text{bis} \quad 2^s - 1 = [011 \dots 1]_2$$

Die negativen Zahlen laufen von

$$-1 = [11 \dots 1]_2 \quad \text{bis} \quad -2^s = [10 \dots 0]_2.$$

Bei der Addition solcher Zahlen führt man eine normale binäre Addition durch, ohne die besondere Bedeutung der Stelle s zu berücksichtigen.

Zweierkomplemente

Besser ist es daher, *Zweierkomplemente* zu verwenden, nämlich

$$[a_s a_{s-1} \dots a_0]_2 = a_{s-1} \dots a_{02} - 2^s a_s.$$

Bei $a_s = 0$ laufen die nichtnegativen ganzen Zahlen von

$$0 = [0 \dots 0]_2 \quad \text{bis} \quad 2^s - 1 = [011 \dots 1]_2$$

Die negativen Zahlen laufen von

$$-1 = [11 \dots 1]_2 \quad \text{bis} \quad -2^s = [10 \dots 0]_2.$$

Bei der Addition solcher Zahlen führt man eine normale binäre Addition durch, ohne die besondere Bedeutung der Stelle s zu berücksichtigen.

Allerdings fällt ein Übertrag von der Stelle s unter den Tisch. Solange sich die Zahlen im angegebenen Bereich bewegen, ist diese Addition korrekt:

Beispiel

Für $s = 3$ können die Zahlen von

$$-2^3 = -8 \text{ bis } 2^3 - 1 = 7$$

dargestellt werden.

Beispiel

Für $s = 3$ können die Zahlen von

$$-2^3 = -8 \text{ bis } 2^3 - 1 = 7$$

dargestellt werden.

Es ist klar, dass zwei nichtnegative Zahlen korrekt addiert werden, solange die 7 nicht überschritten wird.

Beispiel

Für $s = 3$ können die Zahlen von

$$-2^3 = -8 \text{ bis } 2^3 - 1 = 7$$

dargestellt werden.

Es ist klar, dass zwei nichtnegative Zahlen korrekt addiert werden, solange die 7 nicht überschritten wird.

Andernfalls erhalten wir z.B.

$$4 + 4 = [0100]_2 + [0100]_2 \stackrel{?}{=} [1000]_2 = -8.$$

Beispiel

Für $s = 3$ können die Zahlen von

$$-2^3 = -8 \text{ bis } 2^3 - 1 = 7$$

dargestellt werden.

Es ist klar, dass zwei nichtnegative Zahlen korrekt addiert werden, solange die 7 nicht überschritten wird.

Andernfalls erhalten wir z.B.

$$4 + 4 = [0100]_2 + [0100]_2 \stackrel{?}{=} [1000]_2 = -8.$$

Bei der Summe zweier negativer Zahlen darf die Summe nicht kleiner als -8 werden, z.B

$$-1 - 1 = [1111]_2 + [1111]_2 = [1110]_2 = -2,$$

$$-4 - 5 = [1100]_2 + [1011]_2 \stackrel{?}{=} [0111]_2 = 7.$$

3.3 Untergruppen und der Satz von Lagrange

Wir hatten $\mathbb{G} = (G, e, \circ)$ eine Gruppe genannt, wenn

- die zweistellige Operation $\circ$ assoziativ ist,
- es ein neutrales Element e gibt,
- es zu jedem x ein x^{-1} gibt mit $x \circ x^{-1} = x^{-1} \circ x = e$.

Untergruppen

$U \subset G$ heißt *Untergruppe* von G, wenn:

$(U, e, \circ)$ ist Gruppe ist mit der gleichen Operation „$\circ$“ eingeschränkt auf $U \times U$.

Untergruppen

$U \subset G$ heißt *Untergruppe* von G, wenn:

$(U, e, \circ)$ ist Gruppe ist mit der gleichen Operation „$\circ$“ eingeschränkt auf $U \times U$.

In diesem Fall schreiben wir $U \leq G$ und, falls $U \neq G$, $U < G$.

Untergruppenkriterium

Satz $(G, e, \circ)$ sei eine Gruppe. $U \subset G$ ist genau dann eine Untergruppe von G, wenn

(a) $U \neq \emptyset$,

(b) Mit $x, y \in U$ ist auch $x \circ y \in U$.

(c) Zu jedem $x \in U$ existiert $x^{-1} \in U$.

Untergruppenkriterium

Satz $(G, e, \circ)$ sei eine Gruppe. $U \subset G$ ist genau dann eine Untergruppe von G, wenn

(a) $U \neq \emptyset$,

(b) Mit $x, y \in U$ ist auch $x \circ y \in U$.

(c) Zu jedem $x \in U$ existiert $x^{-1} \in U$.

Beweis Eine Untergruppe erfüllt (a),(b),(c).

Untergruppenkriterium

Satz $(G, e, \circ)$ sei eine Gruppe. $U \subset G$ ist genau dann eine Untergruppe von G, wenn

(a) $U \neq \emptyset$,

(b) Mit $x, y \in U$ ist auch $x \circ y \in U$.

(c) Zu jedem $x \in U$ existiert $x^{-1} \in U$.

Beweis Eine Untergruppe erfüllt (a),(b),(c).

Wegen (a) gibt es ein $x \in U$, das nach (c) ein inverses Element $x^{-1} \in U$ besitzt.

Untergruppenkriterium

Satz $(G, e, \circ)$ sei eine Gruppe. $U \subset G$ ist genau dann eine Untergruppe von G, wenn

(a) $U \neq \emptyset$,

(b) Mit $x, y \in U$ ist auch $x \circ y \in U$.

(c) Zu jedem $x \in U$ existiert $x^{-1} \in U$.

Beweis Eine Untergruppe erfüllt (a),(b),(c).

Wegen (a) gibt es ein $x \in U$, das nach (c) ein inverses Element $x^{-1} \in U$ besitzt.

Nach (b) ist dann auch $x \circ x^{-1} = e \in U$. Das Assoziativgesetz gilt in U, weil es in G gilt.

Beispiele

$U = \{e\}$ und $U = G$ sind immer Untergruppen einer Gruppe G, man nennt sie die *trivialen Untergruppen*.

Beispiele

$U = \{e\}$ und $U = G$ sind immer Untergruppen einer Gruppe G, man nennt sie die *trivialen Untergruppen*.

Weitere Beispiele:

- Die ganzen Zahlen sind mit der üblichen Addition eine Untergruppe der rationalen Zahlen. Die geraden Zahlen sind wiederum eine Untergruppe der ganzen Zahlen.

Beispiele

$U = \{e\}$ und $U = G$ sind immer Untergruppen einer Gruppe G, man nennt sie die *trivialen Untergruppen*.

Weitere Beispiele:

- Die ganzen Zahlen sind mit der üblichen Addition eine Untergruppe der rationalen Zahlen. Die geraden Zahlen sind wiederum eine Untergruppe der ganzen Zahlen.
- Die Menge der Permutationen von $A_n = \{1, 2, \ldots, n\}$ mit $p(1) = 1$ ist eine Untergruppe, die die gleiche Struktur wie die Permutationen der Menge A_{n-1} besitzt.

Satz von Lagrange

Satz Sei G eine endliche Gruppe. Ist U eine Untergruppe von G, so ist ihre Kardinalität $|U|$ ein Teiler von $|G|$.

Beweis

Sei U Untergruppe der endlichen Gruppe G. Für jedes $x \in G$ betrachten wir die *Nebenklasse*

$$xU = \{xy : y \in U\}.$$

Beweis

Sei U Untergruppe der endlichen Gruppe G. Für jedes $x \in G$ betrachten wir die *Nebenklasse*

$$xU = \{xy : y \in U\}.$$

$$xy_1 = xy_2 \quad \text{für} \quad y_1, y_2 \in U \;\Leftrightarrow\; y_1 = y_2.$$

Beweis

Sei U Untergruppe der endlichen Gruppe G. Für jedes $x \in G$ betrachten wir die *Nebenklasse*

$$xU = \{xy : y \in U\}.$$

$$xy_1 = xy_2 \quad \text{für} \quad y_1, y_2 \in U \;\Leftrightarrow\; y_1 = y_2.$$

Damit sind alle Nebenklassen gleich groß und haben $|U|$ viele Elemente.

Beweis

Sei U Untergruppe der endlichen Gruppe G. Für jedes $x \in G$ betrachten wir die *Nebenklasse*

$$xU = \{xy : y \in U\}.$$

$$xy_1 = xy_2 \quad \text{für} \quad y_1, y_2 \in U \;\Leftrightarrow\; y_1 = y_2.$$

Damit sind alle Nebenklassen gleich groß und haben $|U|$ viele Elemente.

Haben zwei Nebenklassen x_1U, x_2U ein Element $x_1y_1 = x_2y_2$ gemeinsam, so sind die Nebenklassen gleich wegen

$$x_1U = x_1(y_1U) = (x_1y_1)U = x_2y_2U = x_2U.$$

Beweis

Sei U Untergruppe der endlichen Gruppe G. Für jedes $x \in G$ betrachten wir die *Nebenklasse*

$$xU = \{xy : y \in U\}.$$

$$xy_1 = xy_2 \quad \text{für} \quad y_1, y_2 \in U \;\Leftrightarrow\; y_1 = y_2.$$

Damit sind alle Nebenklassen gleich groß und haben $|U|$ viele Elemente.

Haben zwei Nebenklassen x_1U, x_2U ein Element $x_1y_1 = x_2y_2$ gemeinsam, so sind die Nebenklassen gleich wegen

$$x_1U = x_1(y_1U) = (x_1y_1)U = x_2y_2U = x_2U.$$

Wegen $x = xe \in xU$ kommt jedes $x \in G$ in einer Nebenklasse vor.

3.4 Restklassenkörper und der Satz von Wilson

$\mathbb{K} = (K, 0, 1, +, \cdot)$ heißt Körper, wenn

- $(K, 0, +)$ und $(K \setminus 0, 1, \cdot)$ abelsche Gruppen sind,
- das Distributivgesetz $a \cdot (b + c) = a \cdot b + a \cdot c$ gilt.

3.4 Restklassenkörper und der Satz von Wilson

$\mathbb{K} = (K, 0, 1, +, \cdot)$ heißt Körper, wenn

- $(K, 0, +)$ und $(K \setminus 0, 1, \cdot)$ abelsche Gruppen sind,
- das Distributivgesetz $a \cdot (b + c) = a \cdot b + a \cdot c$ gilt.

Das inverse Element von a bezüglich der Addition schreiben wir als $-a$, das der Multiplikation als a^{-1}.

3.4 Restklassenkörper und der Satz von Wilson

$\mathbb{K} = (K, 0, 1, +, \cdot)$ heißt Körper, wenn

- $(K, 0, +)$ und $(K \setminus 0, 1, \cdot)$ abelsche Gruppen sind,
- das Distributivgesetz $a \cdot (b + c) = a \cdot b + a \cdot c$ gilt.

Das inverse Element von a bezüglich der Addition schreiben wir als $-a$, das der Multiplikation als a^{-1}.

Üblicherweise verwendet man $a - b$ statt $a + (-b)$ und ab statt $a \cdot b$. Weiter gilt die bekannte Regel „Punktrechnung geht vor Strichrechnung“.

Rechenregeln

Sei $(K, 0, 1, +, \cdot)$ ein Körper. Dann gilt:

(a) Die neutralen Elemente der Addition und der Multiplikation sind eindeutig bestimmt.

Rechenregeln

Sei $(K, 0, 1, +, \cdot)$ ein Körper. Dann gilt:

(a) Die neutralen Elemente der Addition und der Multiplikation sind eindeutig bestimmt.

(b) Das inverse Element $-a$ der Addition und das inverse Element a^{-1}, $a \neq 0$, der Multiplikation sind eindeutig bestimmt.

Rechenregeln

Sei $(K, 0, 1, +, \cdot)$ ein Körper. Dann gilt:

(a) Die neutralen Elemente der Addition und der Multiplikation sind eindeutig bestimmt.

(b) Das inverse Element $-a$ der Addition und das inverse Element a^{-1}, $a \neq 0$, der Multiplikation sind eindeutig bestimmt.

(c) Es gilt $a \cdot 0 = 0$, $(-1)a = -a$, $(-a)b = -ab$.

Rechenregeln

Sei $(K, 0, 1, +, \cdot)$ ein Körper. Dann gilt:

(a) Die neutralen Elemente der Addition und der Multiplikation sind eindeutig bestimmt.

(b) Das inverse Element $-a$ der Addition und das inverse Element a^{-1}, $a \neq 0$, der Multiplikation sind eindeutig bestimmt.

(c) Es gilt $a \cdot 0 = 0$, $(-1)a = -a$, $(-a)b = -ab$.

(d) Ist $a \neq 0$, so folgt aus $ab = ac$, dass $b = c$.

Rechenregeln

Sei $(K, 0, 1, +, \cdot)$ ein Körper. Dann gilt:

(a) Die neutralen Elemente der Addition und der Multiplikation sind eindeutig bestimmt.

(b) Das inverse Element $-a$ der Addition und das inverse Element a^{-1}, $a \neq 0$, der Multiplikation sind eindeutig bestimmt.

(c) Es gilt $a \cdot 0 = 0$, $(-1)a = -a$, $(-a)b = -ab$.

(d) Ist $a \neq 0$, so folgt aus $ab = ac$, dass $b = c$.

(e) Ein Körper ist *nullteilerfrei*, d.h. aus $ab = 0$ folgt $a = 0$ oder $b = 0$.

Beweis

(c) Aus $a0 = a(0 + 0) = a0 + a0$ folgt $a0 = 0$.

Beweis

(c) Aus $a0 = a(0+0) = a0 + a0$ folgt $a0 = 0$.

$$0 = 0a = (1 + (-1))a = a + (-1)a \;\Rightarrow\; (-1)a = -a.$$

Beweis

(c) Aus $a0 = a(0+0) = a0 + a0$ folgt $a0 = 0$.

$$0 = 0a = (1 + (-1))a = a + (-1)a \;\Rightarrow\; (-1)a = -a.$$

Mit $(-1)a = -a$ folgt

$$(-a)b = (-1)ab = (-1)(ab) = -ab.$$

Beweis

(c) Aus $a0 = a(0+0) = a0 + a0$ folgt $a0 = 0$.

$$0 = 0a = (1 + (-1))a = a + (-1)a \;\Rightarrow\; (-1)a = -a.$$

Mit $(-1)a = -a$ folgt

$$(-a)b = (-1)ab = (-1)(ab) = -ab.$$

(e) Ist $ab = 0$ und $b \neq 0$, so $a = abb^{-1} = 0b^{-1} = 0$ wegen (c).

Restklassen

Sei $n > 1$ eine natürliche Zahl. Dann ist die auf $\mathbb{Z} \times \mathbb{Z}$ erklärte Relation $a \equiv b \mod n$ eine Äquivalenzrelation.

Restklassen

Sei $n > 1$ eine natürliche Zahl. Dann ist die auf $\mathbb{Z} \times \mathbb{Z}$ erklärte Relation $a \equiv b \mod n$ eine Äquivalenzrelation.

Denn sie ist reflexiv und symmetrisch sowie transitiv wegen

$$\begin{aligned} a \equiv b \mod n,\ b \equiv c \mod n \quad &\Rightarrow \quad a = b + qm,\ b = c + q'm \\ &\Rightarrow \quad a = c + (q + q')m. \end{aligned}$$

Restklassen

Zwei ganze Zahlen sind daher äquivalent, wenn sie bei der Division durch n den gleichen Rest modulo n besitzen.

Restklassen

Zwei ganze Zahlen sind daher äquivalent, wenn sie bei der Division durch n den gleichen Rest modulo n besitzen.

Die zugehörigen Äquivalenzklassen besitzen daher die natürlichen Vertreter $0, 1, \ldots, n-1$.

Restklassen

Zwei ganze Zahlen sind daher äquivalent, wenn sie bei der Division durch n den gleichen Rest modulo n besitzen.

Die zugehörigen Äquivalenzklassen besitzen daher die natürlichen Vertreter $0, 1, \ldots, n-1$.

Die Menge

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

bildet eine Partition von $\mathbb{Z}$.

Restklassen

Auf $\mathbb{Z}_n$ können wir die Operationen

$$\overline{a} + \overline{b} = \overline{a + b}, \quad \overline{a} \cdot \overline{b} = \overline{a \cdot b}$$

definieren.

Restklassen

Auf $\mathbb{Z}_n$ können wir die Operationen

$$\overline{a} + \overline{b} = \overline{a + b}, \quad \overline{a} \cdot \overline{b} = \overline{a \cdot b}$$

definieren.

Wir beweisen die Korrektheit dieser Definitionen, also die Unabhängigkeit von den Vertretern der jeweiligen Äquivalenzklasse.

Restklassen

Auf $\mathbb{Z}_n$ können wir die Operationen

$$\overline{a} + \overline{b} = \overline{a+b}, \quad \overline{a} \cdot \overline{b} = \overline{a \cdot b}$$

definieren.

Wir beweisen die Korrektheit dieser Definitionen, also die Unabhängigkeit von den Vertretern der jeweiligen Äquivalenzklasse.

Ist $a' \in \overline{a}$, $b' \in \overline{b}$, so $a' = a + pn$, $b' = b + qn$. Dann

$$a'+b' = a+b+(p+q)n \in \overline{a+b}, \quad a' \cdot b' = ab+aqn+bpn+pqn^2 \in \overline{a \cdot b}.$$

Alternative

Alternativ wird auch

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

geschrieben.

Alternative

Alternativ wird auch

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

geschrieben.

Man addiert und multipliziert diese Zahlen „normal“ in $\mathbb{N}_0$ und ordnet das Ergebnis der zugehörigen Äquivalenzklasse beziehungsweise ihrem Vertreter in $\mathbb{Z}_n$ zu.

Alternative

Alternativ wird auch

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

geschrieben.

Man addiert und multipliziert diese Zahlen „normal“ in $\mathbb{N}_0$ und ordnet das Ergebnis der zugehörigen Äquivalenzklasse beziehungsweise ihrem Vertreter in $\mathbb{Z}_n$ zu.

Schreibe $+_n$ und $\cdot_n$ für die so definierten Operationen.

Alternative

Alternativ wird auch

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

geschrieben.

Man addiert und multipliziert diese Zahlen „normal“ in $\mathbb{N}_0$ und ordnet das Ergebnis der zugehörigen Äquivalenzklasse beziehungsweise ihrem Vertreter in $\mathbb{Z}_n$ zu.

Schreibe $+_n$ und $\cdot_n$ für die so definierten Operationen.

Beispielsweise gilt in $\mathbb{Z}_4$ $2 \cdot 3 = 6 \equiv 2 \mod 4$, daher

$$2 \cdot_4 3 = 2.$$

$n = 2$

$+_2$	0	1
0	0	1
1	1	0

$\cdot_2$	0	1
0	0	0
1	0	1

$n = 4$

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Algebraischen Eigenschaften von $\mathbb{Z}_n$

Beide Operationen $+_n$ und $\cdot_n$ sind assoziativ und kommutativ.

Algebraischen Eigenschaften von $\mathbb{Z}_n$

Beide Operationen $+_n$ und $\cdot_n$ sind assoziativ und kommutativ.

0 ist neutral bezüglich der Addition.

Algebraischen Eigenschaften von $\mathbb{Z}_n$

Beide Operationen $+_n$ und $\cdot_n$ sind assoziativ und kommutativ.

0 ist neutral bezüglich der Addition.

Zu $a \in \mathbb{Z}_n$ ist $n - a$ das inverse Element bezüglich der Addition, denn es gilt

$$a + (n - a) = n \equiv 0 \mod n.$$

Algebraischen Eigenschaften von $\mathbb{Z}_n$

Beide Operationen $+_n$ und $\cdot_n$ sind assoziativ und kommutativ.

0 ist neutral bezüglich der Addition.

Zu $a \in \mathbb{Z}_n$ ist $n - a$ das inverse Element bezüglich der Addition, denn es gilt

$$a + (n - a) = n \equiv 0 \mod n.$$

Damit ist $(\mathbb{Z}_n, 0, +)$ eine kommutative Gruppe.

Algebraischen Eigenschaften von $\mathbb{Z}_n$

Beide Operationen $+_n$ und $\cdot_n$ sind assoziativ und kommutativ.

0 ist neutral bezüglich der Addition.

Zu $a \in \mathbb{Z}_n$ ist $n - a$ das inverse Element bezüglich der Addition, denn es gilt

$$a + (n - a) = n \equiv 0 \mod n.$$

Damit ist $(\mathbb{Z}_n, 0, +)$ eine kommutative Gruppe.

Das Distributivgesetz wird von der Rechnung mit ganzen Zahlen geerbt und ist daher ebenfalls gültig.

Algebraischen Eigenschaften von $\mathbb{Z}_n$

Beide Operationen $+_n$ und $\cdot_n$ sind assoziativ und kommutativ.

0 ist neutral bezüglich der Addition.

Zu $a \in \mathbb{Z}_n$ ist $n - a$ das inverse Element bezüglich der Addition, denn es gilt

$$a + (n - a) = n \equiv 0 \mod n.$$

Damit ist $(\mathbb{Z}_n, 0, +)$ eine kommutative Gruppe.

Das Distributivgesetz wird von der Rechnung mit ganzen Zahlen geerbt und ist daher ebenfalls gültig.

1 ist neutrales Element der Multiplikation, was $\mathbb{Z}_n$ zu einem kommutativen Ring macht.

Noch einmal $n = 4$

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Wie die Tafel oben rechts zeigt, gibt es für die 2 bei $n = 4$ kein inverses Element.

Noch einmal $n = 4$

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Wie die Tafel oben rechts zeigt, gibt es für die 2 bei $n = 4$ kein inverses Element.

Allgemein ist für zusammengesetztes $n = kl$ die Struktur kein Körper wegen $k \cdot_n l = n \equiv 0 \mod n$, sie ist damit nicht nullteilerfrei.

Restklassenkörper

Satz Ist p eine Primzahl, so ist $\mathbb{Z}_p$ zusammen mit den Operationen $+_p$ und $\cdot_p$ ein Körper, der *Restklassenkörper modulo p* genannt wird.

Restklassenkörper

Satz Ist p eine Primzahl, so ist $\mathbb{Z}_p$ zusammen mit den Operationen $+_p$ und $\cdot_p$ ein Körper, der *Restklassenkörper modulo p* genannt wird.

Für $a \neq 0$ gilt $-a = p - a$ sowie $a^{-1} \equiv a^{p-2} \mod p$.

Satz Ist p eine Primzahl, so ist $\mathbb{Z}_p$ zusammen mit den Operationen $+_p$ und $\cdot_p$ ein Körper, der *Restklassenkörper modulo p* genannt wird.

Für $a \neq 0$ gilt $-a = p - a$ sowie $a^{-1} \equiv a^{p-2} \mod p$.

Genau die Elemente 1 und $p - 1$ sind zu sich selbst invers bezüglich der Multiplikation $\cdot_p$.

Satz Ist p eine Primzahl, so ist $\mathbb{Z}_p$ zusammen mit den Operationen $+_p$ und $\cdot_p$ ein Körper, der *Restklassenkörper modulo p* genannt wird.

Für $a \neq 0$ gilt $-a = p - a$ sowie $a^{-1} \equiv a^{p-2} \mod p$.

Genau die Elemente 1 und $p - 1$ sind zu sich selbst invers bezüglich der Multiplikation $\cdot_p$.

Alle anderen Elemente $\neq 0$ lassen sich zu Paaren a, a', $a \neq a'$, zusammenfassen mit $a \cdot_p a' = 1$.

Beweis

Nach dem kleinen Satz von Fermat gilt

$$a^{p-1} \equiv 1 \mod p \text{ für alle } a \in \{1, \ldots, p-1\}.$$

Beweis

Nach dem kleinen Satz von Fermat gilt

$$a^{p-1} \equiv 1 \mod p \text{ für alle } a \in \{1, \ldots, p-1\}.$$

Somit $a \cdot a^{p-2} \equiv 1 \mod p$ und die Restklasse modulo p von a^{p-2} ist das inverse Element von a bezüglich $\cdot_p$.

Beweis

Nach dem kleinen Satz von Fermat gilt

$$a^{p-1} \equiv 1 \mod p \text{ für alle } a \in \{1, \ldots, p-1\}.$$

Somit $a \cdot a^{p-2} \equiv 1 \mod p$ und die Restklasse modulo p von a^{p-2} ist das inverse Element von a bezüglich $\cdot_p$.

$$a^2 \equiv 1 \mod p \Rightarrow (a-1)(a+1) \equiv 0 \mod p,$$

was genau für $a = 1$ oder $a = p-1$ erfüllt ist.

Satz von Wilson

Satz Für jede Primzahl p gilt

$$(p-2)! \equiv 1 \mod p, \quad (p-1)! \equiv -1 \mod p.$$

Satz von Wilson

Satz Für jede Primzahl p gilt

$$(p-2)! \equiv 1 \mod p, \quad (p-1)! \equiv -1 \mod p.$$

Beweis Es gilt

$$(p-2)! = 2 \cdot \ldots \cdot (p-2).$$

Satz von Wilson

Satz Für jede Primzahl p gilt

$$(p-2)! \equiv 1 \mod p, \quad (p-1)! \equiv -1 \mod p.$$

Beweis Es gilt

$$(p-2)! = 2 \cdot \ldots \cdot (p-2).$$

Nach dem letzten Satz wird dieses Produkt von Paaren mit $aa' \equiv 1 \mod p$ gebildet, daher $(p-2)! \equiv 1 \mod p$.

Satz von Wilson

Satz Für jede Primzahl p gilt

$$(p-2)! \equiv 1 \mod p, \quad (p-1)! \equiv -1 \mod p.$$

Beweis Es gilt

$$(p-2)! = 2 \cdot \ldots \cdot (p-2).$$

Nach dem letzten Satz wird dieses Produkt von Paaren mit $aa' \equiv 1 \mod p$ gebildet, daher $(p-2)! \equiv 1 \mod p$.

Wir multiplizieren dies mit $p-1$ und erhalten den zweiten Teil der Behauptung.

3.5 Geheimcodes

Wir untersuchen

- Substitution
- Vignére-Verschlüsselung
- RSA-Verschlüsselung

Die Substitution

besteht darin, jeden Buchstaben eines Textes durch einen anderen zu ersetzen.

Die Substitution

besteht darin, jeden Buchstaben eines Textes durch einen anderen zu ersetzen.

Kleine Buchstaben = zu verschlüsselnder Text (=Klartext)

Die Substitution

besteht darin, jeden Buchstaben eines Textes durch einen anderen zu ersetzen.

Kleine Buchstaben = zu verschlüsselnder Text (=Klartext)

Große Buchstaben = verschlüsselte Nachricht (=Geheimtext).

Die Substitution

besteht darin, jeden Buchstaben eines Textes durch einen anderen zu ersetzen.

Kleine Buchstaben = zu verschlüsselnder Text (=Klartext)

Große Buchstaben = verschlüsselte Nachricht (=Geheimtext).

Beispiel

Klartextalphabet: `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`

Geheimtextalphabet: `J L P A W I Q B C T R Z Y D S K E G F X H U O N V M`

Die Substitution

besteht darin, jeden Buchstaben eines Textes durch einen anderen zu ersetzen.

Kleine Buchstaben = zu verschlüsselnder Text (=Klartext)

Große Buchstaben = verschlüsselte Nachricht (=Geheimtext).

Beispiel

Klartextalphabet: `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`

Geheimtextalphabet: `J L P A W I Q B C T R Z Y D S K E G F X H U O N V M`

Dann

Klartext: `gehen wir aus?`

Geheimtext: `QWBWD OCG JHF?`

Häufigkeiten

Buchstabe	Häufigkeit in %	Buchstabe	Häufigkeit in %
a	6,51	n	9,78
b	1,89	o	2,51
c	3,06	p	0,79
d	5,08	q	0,02
e	17,40	r	7,00
f	1,66	s	7,27
g	3,01	t	6,15
h	4,76	u	4,35
i	7,55	v	0,67
j	0,27	w	1,89
k	1,21	x	0,03
l	3,44	y	0,04
m	2,53	z	1,13

Vignère-Verschlüsselung

Bei der Vignère-Verschlüsselung nimmt man für jeden Buchstaben in Abhängigkeit seiner Position im Klartext einen anderen Schlüssel.

Vignère-Verschlüsselung

Bei der Vignère-Verschlüsselung nimmt man für jeden Buchstaben in Abhängigkeit seiner Position im Klartext einen anderen Schlüssel.

Im einfachsten Fall vereinbart man ein Schlüsselwort, beispielsweise `LICHT`, das wiederholt über den Klartext geschrieben wird.

Schlüsselwort	`LICHTLICHTLICHTLICHTL`
Klartext	`truppenabzugnachosten`
Geheimtext	`EZWWIPVCISFOEHVSWUAXY`

Vignère-Verschlüsselung

Schlüsselwort	`LICHTLICHTLICHTLICHTL`
Klartext	`truppenabzugnachosten`
Geheimtext	`EZWWIPVCISFOEHVSWUAXY`

Der Buchstabe des Schlüsselworts gibt an, wieweit der Buchstabe des Klartextes im Alphabet verschoben werden muss.

Vignère-Verschlüsselung

Schlüsselwort	`LICHTLICHTLICHTLICHTL`
Klartext	`truppenabzugnachosten`
Geheimtext	`EZWWIPVCISFOEHVSWUAXY`

Der Buchstabe des Schlüsselworts gibt an, wieweit der Buchstabe des Klartextes im Alphabet verschoben werden muss.

Im obigen Beispiel ist L der 12. Buchstabe des Alphabets und man verschiebt das t des Klartexts um $12 - 1 = 11$ Positionen nach rechts modulo 26, das ist gerade E.

Vignère-Verschlüsselung

Schlüsselwort	`LICHTLICHTLICHTLICHTL`
Klartext	`truppenabzugnachosten`
Geheimtext	`EZWWIPVCISFOEHVSWUAXY`

Der Buchstabe des Schlüsselworts gibt an, wieweit der Buchstabe des Klartextes im Alphabet verschoben werden muss.

Im obigen Beispiel ist L der 12. Buchstabe des Alphabets und man verschiebt das t des Klartexts um $12 - 1 = 11$ Positionen nach rechts modulo 26, das ist gerade E.

Der nächste Buchstabe r wird wegen des an 9. Position stehenden I um 8 Positionen nach rechts verschoben, das ist Z.

Vignère-Verschlüsselung

Damit wird jeder Buchstabe auf 5 verschiedene Arten verschlüsselt, eine Häufigkeitsanalyse der Buchstaben ist zur Entschlüsselung nicht mehr möglich.

Vignère-Verschlüsselung

Damit wird jeder Buchstabe auf 5 verschiedene Arten verschlüsselt, eine Häufigkeitsanalyse der Buchstaben ist zur Entschlüsselung nicht mehr möglich.

Allerdings kann bei kurzen Schlüsselwörtern eine Häufigkeitsanalyse nach Sequenzen vorgenommen werden wie etwa nach dem häufigsten dreibuchstabigen Wort „die“.

Vignère-Verschlüsselung

Damit wird jeder Buchstabe auf 5 verschiedene Arten verschlüsselt, eine Häufigkeitsanalyse der Buchstaben ist zur Entschlüsselung nicht mehr möglich.

Allerdings kann bei kurzen Schlüsselwörtern eine Häufigkeitsanalyse nach Sequenzen vorgenommen werden wie etwa nach dem häufigsten dreibuchstabigen Wort „die“.

Auch nach Verschlüsselung werden die zugehörigen verschlüsselten Sequenzen immer noch häufig sein und führen somit auf das Schlüsselwort.

Vignère-Verschlüsselung

Man kann die Vignère-Verschlüsselung dahingehend verbessern, dass an Stelle eines Schlüsselwortes ein ganzer Text vereinbart wird, beispielsweise ein Abschnitt eines Romans.

Vignère-Verschlüsselung

Man kann die Vignère-Verschlüsselung dahingehend verbessern, dass an Stelle eines Schlüsselwortes ein ganzer Text vereinbart wird, beispielsweise ein Abschnitt eines Romans.

In diesem Fall muss der Entschlüssler den Text kennen.

Vignère-Verschlüsselung

Man kann die Vignère-Verschlüsselung dahingehend verbessern, dass an Stelle eines Schlüsselwortes ein ganzer Text vereinbart wird, beispielsweise ein Abschnitt eines Romans.

In diesem Fall muss der Entschlüssler den Text kennen.

Eine moderne Version dieser Technik verwendet einen Zufallsgenerator an Stelle eines Textes. Vor der Verschlüsselung müssen daher nur die Daten des Generators festgelegt werden.

Involutorische und fixpunktfreie Permutationen

Eine Permutation $p : A_n \to A_n$ heißt *involutorisch*, wenn

$$p^2 = p \circ p = id_{A_n}.$$

Involutorische und fixpunktfreie Permutationen

Eine Permutation $p : A_n \to A_n$ heißt *involutorisch*, wenn

$$p^2 = p \circ p = id_{A_n}.$$

Beispiel $n = 3$

$$f(1) = f(3), \quad f(2) = 2, \quad f(3) = 1.$$

Involutorische und fixpunktfreie Permutationen

Eine Permutation $p : A_n \to A_n$ heißt *involutorisch*, wenn

$$p^2 = p \circ p = id_{A_n}.$$

Beispiel $n = 3$

$$f(1) = f(3), \quad f(2) = 2, \quad f(3) = 1.$$

Eine Permutation $p : A_n \to A_n$ heißt *fixpunktfrei*, wenn

$$p(i) \neq i \quad \text{für alle } i = 1, \ldots, n.$$

Involutorische und fixpunktfreie Permutationen

Eine Permutation $p : A_n \to A_n$ heißt *involutorisch*, wenn

$$p^2 = p \circ p = id_{A_n}.$$

Beispiel $n = 3$

$$f(1) = f(3), \quad f(2) = 2, \quad f(3) = 1.$$

Eine Permutation $p : A_n \to A_n$ heißt *fixpunktfrei*, wenn

$$p(i) \neq i \quad \text{für alle } i = 1, \ldots, n.$$

Beispiel Wichtelproblem: Wahrscheinlichkeit einer Nicht-Selbstbewichtelung ist

$$\frac{|\text{fixpunktfreie Permutationen}|}{|\text{Permutationen}|} \to 1 - e^{-1}.$$

Involutorische und fixpunktfreie Permutationen

Eine Permutation $p : A_n \to A_n$ heißt *involutorisch*, wenn

$$p^2 = p \circ p = id_{A_n}.$$

Beispiel $n = 3$

$$f(1) = f(3), \quad f(2) = 2, \quad f(3) = 1.$$

Eine Permutation $p : A_n \to A_n$ heißt *fixpunktfrei*, wenn

$$p(i) \neq i \quad \text{für alle } i = 1, \ldots, n.$$

Beispiel Wichtelproblem: Wahrscheinlichkeit einer Nicht-Selbstbewichtelung ist

$$\frac{|\text{fixpunktfreie Permutationen}|}{|\text{Permutationen}|} \to 1 - e^{-1}.$$

Im Folgenden ist $n = 26$.

Enigma

Die Enigma-Chiffriermaschine besteht aus einer Tastatur sowie

- einem Satz von Steckverbindungen, die eine involutorische Permutation r der 26 Buchstaben bewirken,

Enigma

Die Enigma-Chiffriermaschine besteht aus einer Tastatur sowie

- einem Satz von Steckverbindungen, die eine involutorische Permutation r der 26 Buchstaben bewirken,
- 3-5 rotierenden Walzen mit 26 Zuständen $a - z$, deren Position sich nach jedem eingegebenen Buchstaben ändert (=vom Zustand z abhängige Permutation p_z),

Enigma

Die Enigma-Chiffriermaschine besteht aus einer Tastatur sowie

- einem Satz von Steckverbindungen, die eine involutorische Permutation r der 26 Buchstaben bewirken,
- 3-5 rotierenden Walzen mit 26 Zuständen $a - z$, deren Position sich nach jedem eingegebenen Buchstaben ändert (=vom Zustand z abhängige Permutation p_z),
- einer „Umkehrwalze“, die wieder eine involutorische Permutation u der 26 Buchstaben darstellt.

Enigma

Wird eine Taste gedruckt, so fließt ein Strom durch die Steckverbindungen, die Walzen und die Umkehrwalze. Anschließend fließt der Strom durch die Walzen und die Steckverbindungen wieder zurück.

Enigma

Wird eine Taste gedruckt, so fließt ein Strom durch die Steckverbindungen, die Walzen und die Umkehrwalze. Anschließend fließt der Strom durch die Walzen und die Steckverbindungen wieder zurück.

Ein Lämpchen leuchtet mit dem zugehörigen Buchstaben des Geheimtextes auf.

Enigma

Wird eine Taste gedruckt, so fließt ein Strom durch die Steckverbindungen, die Walzen und die Umkehrwalze. Anschließend fließt der Strom durch die Walzen und die Steckverbindungen wieder zurück.

Ein Lämpchen leuchtet mit dem zugehörigen Buchstaben des Geheimtextes auf.

$$b_i = R_z(a_i) = r^{-1} \circ p_z^{-1} \circ u \circ p_z \circ r(a_i), \quad i = 1, \ldots 26,$$

Enigma

Wird eine Taste gedruckt, so fließt ein Strom durch die Steckverbindungen, die Walzen und die Umkehrwalze. Anschließend fließt der Strom durch die Walzen und die Steckverbindungen wieder zurück.

Ein Lämpchen leuchtet mit dem zugehörigen Buchstaben des Geheimtextes auf.

$$b_i = R_z(a_i) = r^{-1} \circ p_z^{-1} \circ u \circ p_z \circ r(a_i), \quad i = 1, \ldots 26,$$

a_i Buchstabe des Klartexte,
b_i zugehöriger Buchstabe des Geheimtextes

Enigma

$$b_i = R_z(a_i) = r^{-1} \circ p_z^{-1} \circ u \circ p_z \circ r(a_i), \quad i = 1, \ldots 26.$$

$$(r^{-1} \circ p_z^{-1} \circ u \circ p_z \circ r) \circ (r^{-1} \circ p_z^{-1} \circ u \circ p_z \circ r)$$

$$= r^{-1} \circ p_z^{-1} \circ u \circ u \circ p_z \circ r$$

Enigma

$$b_i = R_z(a_i) = r^{-1} \circ p_z^{-1} \circ u \circ p_z \circ r(a_i), \quad i = 1, \ldots 26.$$

$$\begin{aligned}(r^{-1} \circ p_z^{-1} \circ u \circ p_z \circ r) \circ (r^{-1} \circ p_z^{-1} \circ u \circ p_z \circ r) \\ = r^{-1} \circ p_z^{-1} \circ u \circ u \circ p_z \circ r \\ = r^{-1} \circ p_z^{-1} \circ p_z \circ r = id_{A_{26}}.\end{aligned}$$

Enigma

$$b_i = R_z(a_i) = r^{-1} \circ p_z^{-1} \circ u \circ p_z \circ r(a_i), \quad i = 1, \ldots 26.$$

$$\begin{aligned}(r^{-1} \circ p_z^{-1} \circ u \circ p_z \circ r) \circ (r^{-1} \circ p_z^{-1} \circ u \circ p_z \circ r) \\ = r^{-1} \circ p_z^{-1} \circ u \circ u \circ p_z \circ r \\ = r^{-1} \circ p_z^{-1} \circ p_z \circ r = id_{A_{26}}.\end{aligned}$$

Vorteil: Dechiffrierung kann mit der gleichen Maschine erfolgen, wenn Anfangsstellung der Walzen und der Steckverbindungen bekannt.

Enigma

$$b_i = R_z(a_i) = r^{-1} \circ p_z^{-1} \circ u \circ p_z \circ r(a_i), \quad i = 1, \ldots 26.$$

$$\begin{aligned}(r^{-1} \circ p_z^{-1} \circ u \circ p_z \circ r) \circ (r^{-1} \circ p_z^{-1} \circ u \circ p_z \circ r) \\ = r^{-1} \circ p_z^{-1} \circ u \circ u \circ p_z \circ r \\ = r^{-1} \circ p_z^{-1} \circ p_z \circ r = id_{A_{26}}.\end{aligned}$$

Vorteil: Dechiffrierung kann mit der gleichen Maschine erfolgen, wenn Anfangsstellung der Walzen und der Steckverbindungen bekannt.

Wichtig: R_z ist fixpunktfrei, d.h. ein Buchstabe wird nie durch sich selbst verschlüsselt.

Enigma

$$b_i = R_z(a_i) = r^{-1} \circ p_z^{-1} \circ u \circ p_z \circ r(a_i), \quad i = 1, \ldots 26.$$

$$\begin{aligned}(r^{-1} \circ p_z^{-1} \circ u \circ p_z \circ r) \circ (r^{-1} \circ p_z^{-1} \circ u \circ p_z \circ r) \\ = r^{-1} \circ p_z^{-1} \circ u \circ u \circ p_z \circ r \\ = r^{-1} \circ p_z^{-1} \circ p_z \circ r = id_{A_{26}}.\end{aligned}$$

Vorteil: Dechiffrierung kann mit der gleichen Maschine erfolgen, wenn Anfangsstellung der Walzen und der Steckverbindungen bekannt.

Wichtig: R_z ist fixpunktfrei, d.h. ein Buchstabe wird nie durch sich selbst verschlüsselt.

Die Amerikaner waren auch nicht besser.

Satz (Existenz der modularen Inversen) Sind a und n teilerfremde natürliche Zahlen, so gibt es eine ganze Zahl b mit der Eigenschaft

$$ab \equiv 1 \mod n.$$

Beweis

Nach dem Satz über den größten gemeinsamen Teiler gibt es Zahlen $\alpha, \beta \in \mathbb{Z}$ mit

$$1 = ggT(a, n) = \alpha a + \beta n,$$

also $\alpha a \equiv 1 \mod n$.

Beweis

Nach dem Satz über den größten gemeinsamen Teiler gibt es Zahlen $\alpha, \beta \in \mathbb{Z}$ mit

$$1 = ggT(a, n) = \alpha a + \beta n,$$

also $\alpha a \equiv 1 \mod n$.

Die Zahl $b = \alpha$ erfüllt daher die Behauptung.

Variante des kleinen Satzes von Fermat

Satz Seien p und q zwei verschiedenen Primzahlen und sei a teilerfremd zu pq. Dann gilt

$$a^{(p-1)(q-1)} \equiv 1 \mod pq.$$

Beweis

Mit a teilerfremd zu q ist auch a^{p-1} teilerfremd zu q.

Beweis

Mit a teilerfremd zu q ist auch a^{p-1} teilerfremd zu q.

Mit dem kleinen Satz von Fermat folgt

$$a^{(p-1)(q-1)} \equiv 1 \mod q \Leftrightarrow a^{(p-1)(q-1)} = kq + 1$$

Beweis

Mit a teilerfremd zu q ist auch a^{p-1} teilerfremd zu q.

Mit dem kleinen Satz von Fermat folgt

$$a^{(p-1)(q-1)} \equiv 1 \mod q \Leftrightarrow a^{(p-1)(q-1)} = kq + 1$$

Auf die gleiche Weise $a^{(p-1)(q-1)} = lp + 1$, daher $kq = lp$.

Beweis

Mit a teilerfremd zu q ist auch a^{p-1} teilerfremd zu q.

Mit dem kleinen Satz von Fermat folgt

$$a^{(p-1)(q-1)} \equiv 1 \mod q \Leftrightarrow a^{(p-1)(q-1)} = kq + 1$$

Auf die gleiche Weise $a^{(p-1)(q-1)} = lp + 1$, daher $kq = lp$.

Also ist $kq = lp$ sowohl durch q als auch durch p teilbar.

Beweis

Mit a teilerfremd zu q ist auch a^{p-1} teilerfremd zu q.

Mit dem kleinen Satz von Fermat folgt

$$a^{(p-1)(q-1)} \equiv 1 \mod q \Leftrightarrow a^{(p-1)(q-1)} = kq + 1$$

Auf die gleiche Weise $a^{(p-1)(q-1)} = lp + 1$, daher $kq = lp$.

Also ist $kq = lp$ sowohl durch q als auch durch p teilbar.

Somit $kq = lp = mqp$ und

$$a^{(p-1)(q-1)} = mpq + 1 \text{ oder } a^{(p-1)(q-1)} \equiv 1 \mod pq.$$

Die RSA-Verschlüsselung

Die RSA-Verschlüsselung ist asymmetrisch. Wer mir eine verschlüsselte Nachricht senden will, verschlüsselt sie mit einem öffentlichen Schlüssel, den ich beispielsweise im Internet zur Verfügung stelle.

Die RSA-Verschlüsselung

Die RSA-Verschlüsselung ist asymmetrisch. Wer mir eine verschlüsselte Nachricht senden will, verschlüsselt sie mit einem öffentlichen Schlüssel, den ich beispielsweise im Internet zur Verfügung stelle.

Das Entschlüsseln geschieht mit einer geheimen Zahl, die nicht versendet werden muss und auch dem Sender der Nachricht unbekannt ist.

Vorgehensweise

- Es werden zwei Primzahlen p und q gewählt und $n = pq$ berechnet.

Vorgehensweise

- Es werden zwei Primzahlen p und q gewählt und $n = pq$ berechnet.
- Mit einer weiteren frei gewählten Zahl e, die teilerfremd zu $(p-1)(q-1)$ ist, wird d so berechnet, dass

$$ed \equiv 1 \mod (p-1)(q-1) \quad \text{oder} \quad ed = 1 + k(p-1)(q-1).$$

Vorgehensweise

- Es werden zwei Primzahlen p und q gewählt und $n = pq$ berechnet.
- Mit einer weiteren frei gewählten Zahl e, die teilerfremd zu $(p-1)(q-1)$ ist, wird d so berechnet, dass

  $$ed \equiv 1 \mod (p-1)(q-1) \quad \text{oder} \quad ed = 1 + k(p-1)(q-1).$$

  Dies ist die modulare Inverse. d kann mit Hilfe des erweiterten euklidischen Algorithmus aus dem Satz von Bézout effektiv berechnet werden.

Vorgehensweise

- Es werden zwei Primzahlen p und q gewählt und $n = pq$ berechnet.
- Mit einer weiteren frei gewählten Zahl e, die teilerfremd zu $(p-1)(q-1)$ ist, wird d so berechnet, dass

  $$ed \equiv 1 \mod (p-1)(q-1) \quad \text{oder} \quad ed = 1 + k(p-1)(q-1).$$

  Dies ist die modulare Inverse. d kann mit Hilfe des erweiterten euklidischen Algorithmus aus dem Satz von Bézout effektiv berechnet werden.
- Öffentlicher Schlüssel: e und n.

Vorgehensweise

- Es werden zwei Primzahlen p und q gewählt und $n = pq$ berechnet.
- Mit einer weiteren frei gewählten Zahl e, die teilerfremd zu $(p-1)(q-1)$ ist, wird d so berechnet, dass

  $$ed \equiv 1 \mod (p-1)(q-1) \quad \text{oder} \quad ed = 1 + k(p-1)(q-1).$$

  Dies ist die modulare Inverse. d kann mit Hilfe des erweiterten euklidischen Algorithmus aus dem Satz von Bézout effektiv berechnet werden.
- Öffentlicher Schlüssel: e und n.
- Privater Schlüssel: d.

Vorgehensweise

- Es werden zwei Primzahlen p und q gewählt und $n = pq$ berechnet.
- Mit einer weiteren frei gewählten Zahl e, die teilerfremd zu $(p-1)(q-1)$ ist, wird d so berechnet, dass

  $$ed \equiv 1 \mod (p-1)(q-1) \quad \text{oder} \quad ed = 1 + k(p-1)(q-1).$$

  Dies ist die modulare Inverse. d kann mit Hilfe des erweiterten euklidischen Algorithmus aus dem Satz von Bézout effektiv berechnet werden.
- Öffentlicher Schlüssel: e und n.
- Privater Schlüssel: d.
- p, q und $(p-1)(q-1)$ werden nicht mehr benötigt und sollten sicherheitshalber vernichtet werden.

Vorgehensweise

Nun gibt man die Zahlen n und e öffentlich bekannt. Die „geheime“ Zahl d wird nicht bekannt gegeben.

Vorgehensweise

Nun gibt man die Zahlen n und e öffentlich bekannt. Die „geheime“ Zahl d wird nicht bekannt gegeben.

Will jemand eine Nachricht $m < n$ an uns senden, so übermittelt er

$$c \equiv m^e \mod n.$$

Vorgehensweise

Nun gibt man die Zahlen n und e öffentlich bekannt. Die „geheime“ Zahl d wird nicht bekannt gegeben.

Will jemand eine Nachricht $m < n$ an uns senden, so übermittelt er

$$c \equiv m^e \mod n.$$

Die Zahl c wird entschlüsselt durch

$$m' \equiv c^d \mod n.$$

Vorgehensweise

Nun gibt man die Zahlen n und e öffentlich bekannt. Die „geheime“ Zahl d wird nicht bekannt gegeben.

Will jemand eine Nachricht $m < n$ an uns senden, so übermittelt er

$$c \equiv m^e \mod n.$$

Die Zahl c wird entschlüsselt durch

$$m' \equiv c^d \mod n.$$

Wir müssen zeigen, dass

$$m' = m^{ed} \equiv m \mod n.$$

Beweis

$$m^{ed} \equiv m \mod n.$$

Beweis

$$m^{ed} \equiv m \mod n.$$

Nach Definition von e und d ist $ed = 1 + k(p-1)(q-1)$, also

$$m^{ed} = m^{1+k(p-1)(q-1)} \equiv m \cdot m^{k(p-1)(q-1)} \mod n.$$

Beweis

$$m^{ed} \equiv m \mod n.$$

Nach Definition von e und d ist $ed = 1 + k(p-1)(q-1)$, also

$$m^{ed} = m^{1+k(p-1)(q-1)} \equiv m \cdot m^{k(p-1)(q-1)} \mod n.$$

Wegen $m < n$ gilt $m \equiv m \mod n$ und wegen obigem Satz

$$m^{k(p-1)(q-1)} \equiv 1 \mod n.$$

Beweis

$$m^{ed} \equiv m \mod n.$$

Nach Definition von e und d ist $ed = 1 + k(p-1)(q-1)$, also

$$m^{ed} = m^{1+k(p-1)(q-1)} \equiv m \cdot m^{k(p-1)(q-1)} \mod n.$$

Wegen $m < n$ gilt $m \equiv m \mod n$ und wegen obigem Satz

$$m^{k(p-1)(q-1)} \equiv 1 \mod n.$$

Bilden wir das Produkt dieser Kongruenzen, so

$$m \cdot m^{k(p-1)(q-1)} \equiv m \cdot 1 \equiv m \mod n.$$

Eigenschaften der RSA-Verschlüsselung

Im Gegensatz zu den in den vorigen Abschnitten beschriebenen Verfahren werden keine Schlüssel ausgetauscht.

Eigenschaften der RSA-Verschlüsselung

Im Gegensatz zu den in den vorigen Abschnitten beschriebenen Verfahren werden keine Schlüssel ausgetauscht.

Jeder kann mir eine verschlüsselte Nachricht senden, wenn er sich die von mir bekannt gegebenen Zahlen n und e verschafft. Das Verfahren ist daher abhörsicher.

Sicherheit der RSA-Verschlüsselung

Die RSA-Verschlüsselung beruht auf dem Glauben, dass aus den öffentlichen Zahlen n und e der Schlüssel d nicht in vernünftiger Zeit rekonstruiert werden kann.

Sicherheit der RSA-Verschlüsselung

Die RSA-Verschlüsselung beruht auf dem Glauben, dass aus den öffentlichen Zahlen n und e der Schlüssel d nicht in vernünftiger Zeit rekonstruiert werden kann.

d kann nur über die Faktoren in $n = pq$ bestimmt werden.