# Informatik-Studium Documentation

**Julian Sobott**

**08.06.2019**

# Vorlesungen:

KAPITEL 1

# Diskrete Mathematik und Lineare Algebra

## 1.1 Zahlentheorie

### 1.1.1 1. Teilbarkeit

In diesem Abschnitt ist $\mathbb{Z}$ die Grundmenge.

#### Definition 1: Teiler

Für zwi Zahlen $m, n \in$ mit $m > 0$ ist m Teiler n, falls es ein $t \in$ gibt, so dass $n = t * m$. Kurzschreibweise: $m \mid n$

#### Beispiel 1:

$2 \mid 6$, da $2 * 3 = 6$

$2 \nmid 6$, da $\forall t \in \ 7 \neq t * 2$

#### Spezialfälle:

$1 \mid n$, da $n = n * 1$

$n \mid n$ für $n > 0$, da $n = 1 * n$ für $n < 0$ gilt das nicht, da lt. *Definition 1: Teiler* der $Teiler > 0$ sein muss.

$m \mid 0$, da $0 = 0 * m$

#### Definition 2: Teilermenge

Für eine Zahl $n \in$ ist $T_n$ die Menge aller Teiler von $n$. Also $T_n = \{k > 0 : k \mid n\}$

#### Beispiel 2:

$T_6 = \{1, 2, 3, 6\}$

$T_7 = \{1, 7\}$

### 1.1.2 Modulo

Ist *m* kein teiler von n, so bleibt bei der Division ein Rest. Für $n, t, m, r \in$ und $m, r > 0$ können wir dann schreiben: $n = t * m + r$. Dabei wählen wir *t* maximal, so dass $t * m \leq n$. Also $t = \lfloor \frac{n}{m} \rfloor$. Eingesetzt $n = \lfloor \frac{n}{m} \rfloor * m + r \Leftrightarrow r = n - \lfloor \frac{n}{m} \rfloor * m$. Da $\lfloor \frac{n}{m} \rfloor * m \leq n$, ist $r \geq 0$. Andererseits ist $r < m$, da $\lfloor \frac{n}{m} \rfloor$ der größte Faktor ist. Somit ist $t * m \leq n \Rightarrow$ Es gilt: $r \in \{0, 1, ..., m - 1\}$

#### Definition 3: Modulo

Die Menge der möglichen Reste ist $Z_m = \{0, 1, ..., m - 1\}$ Bei der ganzzahligen Division von *n* durch *m* bezeichnet man *m* als den underline{Modul} und den Rest *r* als *n* modulo *m*, kurz $n \mod m$.

#### Folgerung 1:

Für $n, m \in$ mit $m > 0$ und $r = n \mod m$

**Beweis:**

---

**Zu tun:** Add Beweis

---

Eine Zahl *n* kann für feste *m* auf viele Arten in der Form $n = t * m + r$ geschrieben werden. Beschränkt man *r* auf $\{0, 1, ..., m - 1\}$, dann gibt es nur noch eine Darstellung.

#### Theorem

Sei $n, m \in$ und $m > 0$. Die Darstellung $n = t * m + r$ ist eindeutig.

### 1.1.3 Teilbarkeit - Fortsetzung

#### Definition 4: Schnittmenge von Teilmengen

Für zwei Zahlen $m, n \in$ ist $T_{m,n} = T_m \cap T_n$

#### Definition 5: Größter gemeinsamer Teiler (ggT)

Für zwei Zahlen $m, n \in$ mit $m, n \neq 0$ ist der größte gemeinsame Teiler, kurz *ggT(m,n)*, die größte Zahl in $T_{m,n}$. Also $max(T_{m,n})$

Formal:

$$ggT(m, n) = max(\{k \in \mathbb{N} : k > 0 \cap k \mid m \cap k \mid n\})$$

### Definition 6: Kleinstes gemeinsames Vielfaches (kgV)

Das kleinste gemeinsame Vielfache von $m, n \in$ mit $m, n >$ ist die kleinste Zahl, die von *m* und *n* geteilt wird.

Formal:

$$kgV(m,n) = min(\{k \in \mathbb{N} : k > 0 \cap m \mid k \cap n \mid k\})$$

### Beispiel:

$$\begin{aligned} T_{12} &= \{1,2,3,4,6,12\} \\ T_{18} &= \{1,2,3,6,9,18\} \\ T_{12,18} &= \{1,2,3,6\} \\ ggT(12,18) &= 6 \\ kgv(12,18) &= 36 \end{aligned}$$

```
Ziel effiziente Berechnung des ggT.
```

### Lemma 1:

Für alle $a, b \in$ ist $T_{m,n} \subseteq T_{a*m+b*n}$

### Beweis:

Sei $k \in T_{m,n}$ ein beliebiger Teiler von *m* und *n*. D.h. es gibt $s, t \in$, so dass $m = s * k$ und $n = t * k$. Dann gilt: $a * m + b * n = a * s * k + b * t * k = k * (a * s + b * t)$. Folglich gilt: $k \mid (a * m + b * n)$.

### Spezialfall:

Für den ggT: $ggT(m,n) \mid (a * m + b * n)$.

### Beispiel:

$$\begin{aligned} m = 12,\ n = 18, a = -1,\ b = 2 \\ a * m + b * n = 1 * 12 + 2 * 18 = 24 \\ T_{12,18} = \{1,2,3,6\} \\ T_{24} = \{1,2,3,4,6,8,12,24\} \\ T_{12,18} \subseteq T_{24} \end{aligned}$$

$\Rightarrow$ Teilmenge $T_{a*m+b*n}$ enthält im allgemeinen mehr Zahlen als $T_{m,n}$. Es wäre jedoch von Vorteil, mindestens eine der Zahlen *m*, *n* zu verkleinern, ohne $T_{m,n}$ zu verkleinern.

### Folgerung 2:

Für alle $a \in$ ist $T_{m,n} = T_{m,n-a*m}$

---

**Zu tun:** Beweis: $T_{m,n} \subseteq T_{m,n-a*m}$

---

### Beispiel:

$$
\begin{aligned}
a &= -1 \ \#beliebig \\
T_{12,18} \subseteq T_{12,18-12} &= T_{12,6} \\
T_{12} &= \{1,2,3,4,6,12\} \\
T_{18} &= \{1,2,3,6,9,18\} \\
T_{6} &= \{1,2,3,6\} \\
T_{12,18} &= \{1,2,3,6\} \\
T_{12,6} &= \{1,2,3,6\}
\end{aligned}
$$

---

**Zu tun:** Beweis: $T_{m,n} \supseteq T_{m,n-a*m}$

---

Wählt man in *Folgerung 2:* $a \geq 1$, so verkleinert sich das Zahlenpaar $(m, n)$ zu $(m, n - a * m)$. Trotzdem bleiben die gemeinsamen Teiler die selben. Je kleiner das Zahlenpaar $(m, n - a * m)$ wird, desto einfacher kann der ggT bestimmt werden. Folglich wählen wir *a* maximal, so dass $n - a * m \geq 0$ ist.

*Folgerung 2:* ($T_{m,n} = T_{m,n-a*m}$) gilt unter anderem für $a = \lfloor \frac{n}{m} \rfloor$ (da $\lfloor \frac{n}{m} \rfloor * m \leq n$, deshalb wird *a* maximal). Eingesetzt: $n - a * m = n - \lfloor \frac{n}{m} \rfloor * m = n \mod m$.

### Folgerung 3:

Für $m > 0$ gilt: $T_{m,n} = t_{m,n \mod m}$

### Euklidischer Algorithmus

### Rekursive Formulierung:

```
Euklid(m,n)
    if m=0 then
        return n
    else
        return Euklid(n mod m, m)
```

### Iterative Formulierung:

```
Euklid(m,n)
    while m>0 do
        r <- n mod m
        n <- m
        m <- r
    return n
```

### Folgerung 4:

$T_{m,n} = T_{ggT(m,n)}$. D.h. jeder gemeinsamer Teiler von *n* und *m* teilt folglich auch den *ggT(m,n)*.

### Beispiel: Euklidiescher Algorithmus - kürzen von Brüchen

$\frac{233408}{344512}$ soll auf die kleinstmögliche Form gekürzt werden.

| i | $n_i$ | Berechnung: $m_i$ | $m_i$ |
|---|---|---|---|
| 0 | 344512 | | 233408 |
| 1 | 233407 | $344512 \mod 233408$ | = 111104 |
| 2 | 111104 | $233407 \mod 111104$ | = 11200 |
| 3 | 11200 | $111104 \mod 11200$ | = 896 |
| 4 | 896 | $11200 \mod 896$ | = 448 |
| 5 | 448 | $896 \mod 448$ | = 0 |

$\Rightarrow ggT(233408, 344512) = 448$

$\Rightarrow \frac{233408}{344512} = \frac{\frac{233408}{448}}{\frac{344512}{448}} = \frac{512}{729}$

### Theorem 2:

Es gibt $a, b \in$, so dass $a * m + b * n = ggT(m, n)$.

### Beweis:

**Zu tun:** Beweis

### Erweiterter Euklidischer Algorithmus

```
EuklidErweitert(m,n)
    if m = 0 then
        return (n, 0, 1)
    else
        (d, b', a') <- EuklidErweitert(n mod m, m)
        a <- a' - b'(n div m)
        b <- b'
        return (d, a, b)
```

**Beispiel:**

Namen der Variablen sind anders: a=n, b=m, b=s, a=t

| a | b | q | s | t |
|---|---|---|---|---|
| 99 | 78 | 1 | | |
| 78 | 21 | 3 | | |
| 21 | 15 | 1 | | |
| 15 | 6 | 2 | | |
| 6 | 3 | 2 | | |
| 3 | 0 | | | |

| a | b | q | s | t |
|---|---|---|---|---|
| 99 | 78 | 1 | | |
| 78 | 21 | 3 | | |
| 21 | 15 | 1 | | |
| 15 | 6 | 2 | | |
| 6 | 3 | 2 | | |
| 3 | 0 | | 1 | 0 |

| a | b | q | s | t |
|---|---|---|---|---|
| 99 | 78 | 1 | −11 | 14 |
| 78 | 21 | 3 | 3 | −11 |
| 21 | 15 | 1 | −2 | 3 |
| 15 | 6 | 2 | 1 | −2 |
| 6 | 3 | 2 | 0 | 1 |
| 3 | 0 | | 1 | 0 |

Abb. 1: Erweiterter Euklidischer Algorithmus Schema für 99 und 78

$ggT(99, 78) = 99 * (-11) + 78 * 14 = 3$

## 1.2 Primzahlen

### 1.2.1 Definition: Primzahl

$p \in \mathbb{N}$ heißt Primzahl, wenn *p* genau 2 Teiler besitzt. Jede natürliche Zahl *n* hat mindestens die trivialen Teiler 1 und *n*.

**Hinweis:** Die kleinste Zahl, die die Definition erfüllt, ist die 2.

#### Beispiel: Primzahlen

2, 3, 5, 7, 11, 13, ...

### 1.2.2 Primzahlentest:

**Naive Idee:** Teste für alle Zahlen $k = 2, 3, ..., n-1$ ob sie Teiler sind.

**Verbesserung:** Der kleinst mögliche Teiler von n ist 2 (der n als Primzahl ausschließt), daher kann der größte Teiler maximal $\frac{n}{2}$ sein.

**Beobachtung:** Wenn $\frac{n}{2} \mid n$, dann gilt auch $2 \mid n$, denn $n = 2 * \frac{n}{2}$.

**Allgemein gilt:** Für $k \in \mathbb{N}$ gilt, wenn $\frac{n}{k} \mid n$, dann gilt auch $k \mid n$.

Sei $k \neq 1$ der kleinste Teiler von *n*, dann findet der oben beschriebene Algorithmus *k* vor $\frac{n}{k}$, da gilt $k \leq \frac{n}{k}$. Abschätzung für den kleinsten Teiler $k$ : $k \leq \frac{n}{k} \Leftrightarrow k^2 \leq n \Leftrightarrow k \leq \sqrt{n}$. D.h. existiert ein Teiler $k \notin \{1, n\}$, dann ist mindestens ein Teiler von *n* kleiner als $\sqrt{n}$. Um zu zeigen, dass *n* eine Primzahl ist, genügt es also zu zeigen, dass gilt: $\forall k \leq \sqrt{n} : k \nmid n$

**Beobachtung:**

- Wenn $2 \nmid$, dann gilt $\forall a < \sqrt{n}$ ebenfalls $(2a) \nmid n$
- Wenn $3 \nmid$, dann gilt $\forall a < \sqrt{n}$ ebenfalls $(3a) \nmid n$
- **Allgemein: Für $k < \sqrt{n}$ gilt, wenn $k \nmid n$ dann gilt:** $\forall a < \sqrt{n}$ ebenfalls $(k * a) \nmid n$

### 1.2.3 Sieb des Eratosthenes

Algorithmus um herauszufinden, ob eine Zahl *n* eine Primzahl ist. Ist die Zahl keine Primzahl wird ein Teiler zurückgegeben ansonsten 0. Der Algorithmus kann auch genommen werden um Primzahlen zu finden, wenn man anstatt eine Zahl zurückgibt, den prim Array nimmt und schaut wo nach Ende des Durchlaufs noch true drin steht.

```
Sieb_des_eratosthenes(n)
    If n = 2 then return 0
    If 2 | n then return 2
    prim[2] <- true
    // prim ist ein Array in dem steht, welche Zahlen Primzahlen sind
    for k <- 3 to floor(sqrt(n)) do prim[k] <- k ist ungerade?
```

(Fortsetzung auf der nächsten Seite)

(Fortsetzung der vorherigen Seite)

```
    for k <- 3 to floor(sqrt(n)) step 2 do
        if prim[k] then
            if k | n then return k
            j <- k^2
            // Alle kleineren k werden zuvor schon gestrichen
            while j <= floor(sqrt(n))
                prim[j] <- false
                j <- j + 2k
                // ungerade + ungerade wäre gerade
                // und diese wurden schon alle gestrichen
    return 0
```

### 1.2.4 Lemma 2: Primfaktorzerlegung

Jede natürliche Zahl $n \geq 1$ kann als Produkt von Primzahlen geschrieben werden. Ein solches Produkt wird auch als Primfaktorzerlegung bezeichnet. Dabei ist die Primfaktorzerlegung von 1, das leere Produkt, welches auf den Wert 1 definiert ist.

#### Beweis:

---

**Zu tun:** Beweis

---

#### Beispiele:

$$10 = 2 * 5$$
$$24 = 2 * 2 * 2 * 3 = 2^3 * 3$$
$$29 = 29$$

### 1.2.5 Theorem 3:

Für $n \geq 1$ gilt: Die Darstellung von $n = p_0 * p_1 * ... * p_n$ mit Primzahlen $p_i$ und $p_0 \leq p_1 \leq ... \leq p_n$ ist eindeutig.

#### Beweis:

---

**Zu tun:** Beweis

---

### 1.2.6 Folgerung 5:

Es gibt unendlich viele Primzahlen.

**Beweis:**

**Zu tun:** Beweis

### 1.2.7 Theorem 4: Primzahlsatz der Zahlentheorie

Sei $\pi(n) := \{p \leq n : n\, ist\, prim\}$, dann gilt: $\pi(n)\ \frac{n}{log(n)}$

### 1.2.8 Folgerung 6:

Die Primfaktorzerlegung des ggT zweier Zahlen $a, b \neq 0$ enthält genau die Faktoren der Primfaktorzerlegung von $a$ und $b$, die in beiden enthalten sind.

**Beweis:**

**Zu tun:** Beweis

**Beispiel:**

$$\begin{aligned} a = 12 &= 2 * 2 * 3 \\ b = 18 &= 2 * 3 * 3 \\ ggT(12, 18) &= 6 = 2 * 3 \end{aligned}$$

### 1.2.9 Folgerung 7:

Das kgV zweier Zahlen $a, b > 0$ kann mit $\frac{a*b}{ggT(a,b)}$ berechnet werden.

**Beweis:**

**Zu tun:** Beweis

**Beispiel:**

$$\begin{aligned} a = 12 &= 2 * 2 * 3 \\ b = 18 &= 2 * 3 * 3 \\ ggT(12, 18) &= 6 = 2 * 3 \\ kgV(12, 18) &= \frac{a * b}{ggT(a, b)} = \frac{2 * 2 * 3 * 2 * 3 * 3}{2 * 3} = 2 * 2 * 3 * 3 = 36 \end{aligned}$$

### 1.2.10 Definition 8: Teilerfremd

Die Zahlen $a, b \in \mathbb{Z}$ heißen Teilerfremd, wenn $ggT(a, b) = 1$. Schreibweise: $a \perp b$

#### Beispiel:

$$\begin{aligned} a &= 2, & b &= 3 \\ T_2 &= \{1, 2\}, & T_3 &= \{1, 3\} \\ ggT(2, 3) &= 1 \\ &\Rightarrow a \perp b \end{aligned}$$

#### Beobachtung:

- $a \perp b \Rightarrow a$ und $b$ haben keine gemeinsamen Primfaktoren > 1
- $a \perp b$ und $a \perp c \Leftrightarrow a \perp b * c$
- $p$ is prim $\cap\ p \mid (a * b) \Rightarrow p \mid a\ \cup\ p \mid b$

## 1.3 Kongruenzen

Die Kongruenz-Relation $\equiv_m$ setzt ganze Zahlen, die den gleichen rest bei der Division durch eine natürliche Zahl $n \geq 1$ haben, in Relation.

### 1.3.1 Definition 9: Kongruenz

Sei $m, a, b \in \mathbb{Z}, m \geq 1$.

$a \equiv_m b \Leftrightarrow a \equiv b (mod\ m) \Leftrightarrow a\ mod\ m = b\ mod\ m$

#### Beispiel:

$1 \equiv 4 \equiv 7 \equiv -2 \equiv -5\ (mod\ 3)$ //$(-5 + 2 * 3 = 1)$

### 1.3.2 Äquivalenzklassen und -relationen

Da die Kongruenz mittels Gleichheit definiert ist, handelst es sich um eine Äquivalenzrelation (R, S, T). Daher gibt es sogenannte Äquivalenzklassen. Eine Äquivalenzklasse ist eine Menge, die alle Zahlen enthält, die modulo eines bestimmten Modulos einen bestimmten Rest ergeben.

#### Beispiel:

$[2]_5 = \{..., -8, -3, 2, 7, 12, ...\} = \{5 * t + 2 \mid t \in \mathbb{Z}\}$

$[r]_m = \{k * m + r \mid k \in \mathbb{Z}\}$

### 1.3.3 Rechenregeln für Kongruenzen

- $a \equiv_m 0 \Leftrightarrow m \mid a$

### 1.3.4 Theorem 5:

Sei $a, b \in \mathbb{Z}$, dann gilt für $m \geq 1$: $a \equiv_m b \Leftrightarrow m \mid (a - b)$

---

**Zu tun:** Beweis

---

#### Beispiel:

$a = 22, b = 7$

$7 \equiv_m 22$

$a - b = 22 - 7 = 15 \Rightarrow 5 \mid 15$

### 1.3.5 Folgerung 8:

$a \equiv_m b \Leftrightarrow a - b \equiv_m 0$

### 1.3.6 Lemma 3:

Sei $a \equiv_m b$ und $c \equiv_m d$, dann gilt:

1. $a + c \equiv_m b + d$
2. $a - c \equiv_m b - d$
3. $a * c \equiv_m b * d$

**Hinweis:** Dies gilt insbesondere auch wenn $c = d$. D.h. ähnlich wie bei Gleichungen können beide Seiten der Kongruenz gleichmäßig erhöht, verringert oder multipliziert werden. Vorsicht: für die Division gilt dies nicht!

Weiterhin gelten obige Regeln auch für z.B. $c = m$ und $d = 0$. D.h. der Modul kann zu einer Seite der Kongruenz addiert, subtrahiert oder multipliziert werden, ohne die andere Seite zu verändern.

---

**Zu tun:** Beweis

---

#### Beispiel:

1.

$$69 + 53 = 122 \equiv 3 \ (mod\, 7)$$
$$69 + 53 \equiv 6 + 4 = 10 \equiv 3 \ (mod\, 7)$$

2.

$$69 * 53 = 3657 \equiv 3 \ (mod\, 7)$$
$$69 * 53 \equiv 6 * 4 = 24 \equiv 3 \ (mod\, 7)$$

2.

$$69 * 53 + 29 * 23 = 4324 \equiv 5 \ (mod\, 7)$$
$$\equiv 6 * 4 + 1 * 2 \equiv 3 + 2 \equiv 5 \ (mod\, 7)$$

### 1.3.7 Folgerung 9:

Ist $a \equiv_m b$, dann ist auch $a^n \equiv_m b^n \ \ \forall n \geq 0$

### 1.3.8 Folgerung 10:

Kongruenzen können bis auf die Division, wie normale Gleichungen umgeformt werden.

#### Beispiel:

$$\begin{aligned} x - 4 &\equiv_7 6 \\ x &\equiv_7 6 + 4 \\ x &\equiv_7 3 \end{aligned}$$

---

**Zu tun:** Beispiel: durch 3 teilbar

---

### 1.3.9 Divisions Alternative:

Die oben genannten Rechenregeln erlauben keine herkömmliche Division. Es gilt z.B $6 = 2*3 \equiv 10 = 2*5 \ (mod\, 4)$. Beide Seiten enthalten den Faktor 2. Teilt man jedoch beide Seiten durch 2, gilt die Kongruenz nicht mehr. Allerdings kann in bestimmten Fällen ein Faktor durch eine entsprechende Multiplikation entfernt werden.

#### Beispiel:

$$\begin{aligned} 32 = 2*2*2*2*2 &\equiv 22 = 2*11 \pmod 5 \\ \Leftrightarrow 2*2*2*2*(2*3) &\equiv (2*3)*11 \pmod 5 \\ \Leftrightarrow 2*2*2*2*1 &\equiv 1*11 \pmod 5 \end{aligned}$$

**Hinweis:** $2*3 \mod 5 = 1$

### 1.3.10 Definition 10: Inverses

Ein Faktor $x \in \mathbb{Z}_m$ (*Def. 3: mögliche Reste*) für den gilt $a*x \equiv 1 \pmod m$ nennt man Inverses zu a modulo m. Man schreibt für x dann $a^{-1}$.

### 1.3.11 Definition 11: teilerfremde Menge

Die Menge der zu m teilerfremden Zahlen wird als $Z_m^*$ bezeichnet. $Z_m^* \subseteq Z_m$

#### Beispiel:

$Z_2^* = \{1\}$, $Z_3^* = \{1, 2\}$, $Z_4^* = \{1, 3\}$, $Z_5^* = \{1, 2, 3, 4\}$, $Z_6^* = \{1, 5\}$

### 1.3.12 Theorem 6:

$a \perp m \Rightarrow \exists! z \in Z_m^* : z = a^{-1} * b \pmod{m}$

**Hinweis:** $\exists! z \in Z_m^* \widehat{=}$ „Es gibt genau ein z in $Z_m^*$“. D.h. z ist eindeutig.‘

#### Beweis:

1. Zeigen, dass eine Lösung existiert

$$\exists a^{-1} : a * a^{-1} \equiv 1 \pmod{m} \Rightarrow d \in \mathbb{Z} : a * a^{-1} = todo(d * m + 1) \pmod{m}$$
$$\Rightarrow 1 \equiv todoa * a^{-1} - d * m.$$

$$a \perp m \overset{Folgerung6}{\Rightarrow} ggT(a, m) = 1$$
$$\overset{Theorem2}{\Rightarrow} \exists \text{ eine Linearkombination der Form: } 1 = c * a + d * m$$

Ersetze: $c = a^{-1}$ und $d = -d \Rightarrow 1 = a * a^{-1} - d * m$
$\Rightarrow$ Da c und d mittels des euklidschen Algorithmus berechnet werden können, muss mindestens eine Lösung existieren, die Kongruent zu c in $Z_m$ ist.

2. Zeigen, dass die Lösung eindeutig ist

Angenommen es gibt die Lösungen $e, f \in Z_m$.Dann muss gelten:
$$a * e \equiv b \equiv a * f \pmod{m}$$
$$\Leftrightarrow a^{-1} * a * e \equiv a^{-1} * b \equiv a^{-1} * a * f \pmod{m}$$
$$\Leftrightarrow e \equiv a^{-1} * b \equiv f \pmod{m}$$
$$\Leftrightarrow e \equiv f \pmod{m}$$

**Hinweise:**

- Wenn gilt $a \not\perp m$, also insbesondere wenn $ggT(a, m) > 1$, gilt das obige Theorem nicht.
- Außerhalb von $Z_m$ existieren unendlich viele Lösungen

Damit lassen sich nun Kongruenzen der Form $a * x \equiv b \pmod{m}$ für $a \in Z_m^*$ nach x auflösen: $x \equiv a^{-1} * b \pmod{m}$

---

**Zu tun:** Beispiel

---

### 1.3.13 Folgerung 11:

$p$ prim $\cap\, a * x \equiv b \pmod{p} \Rightarrow \forall a : \exists a^{-1} \in Z_m$

### 1.3.14 Folgerung 12:

$(a)^{-1}_{\mod m} \in Z^*_m$

$(a)^{-1}_{\mod m} \widehat{=}$ das Inverse von a modulo m.

Für die Kongruenz $a * x \equiv b \pmod m$ mit $a \perp m$ und $a \in Z^*_m$ lässt sich das Inverse zu a mittels des erweiterten euklidschen Algorithmus errechnen. Vertauscht man die Rollen von $a$ und $a^{-1}$ und $d$ mit $m$ erhält man durch den erweiterten euklidschen Algorithmus die selbe Linearkombination: $1 = a * a^{-1} + d * m$. Daher gilt, dass auch das Inverse zu a modulo m in $Z^*_m$ enthalten sein muss.

### 1.3.15 Simultane Kongruenz:

Eine simultane Kongruenz ganzer Zahlen ist ein System von linearen Kongruenzen.

Betrachten wir nun den Fall, dass zwei lineare Kongruenzen gegeben sind:

$$\begin{aligned} a_1 * x &\equiv b_1 \pmod m \\ a_2 * x &\equiv b_2 \pmod h \end{aligned}$$

Angenommen es gilt: $a_1 \perp m$ und $a_2 \perp h$. Mithilfe von *Theorem 6*:

$$\begin{aligned} x &\equiv a_1^{-1} * b_1 \pmod m \\ x &\equiv a_2^{-1} * b_2 \pmod h \end{aligned}$$

Gesucht werden also Werte für x, die modulo m und modulo h gleich sind.

### 1.3.16 Theorem 7: Chinesischer Restsatz

Sei $m \perp h$. Für $a \in Z_m$ und $b \in Z_h$ haben die beiden Kongruenzen

$$\begin{aligned} x &\equiv a \pmod m \\ x &\equiv b \pmod h \end{aligned}$$

, die eindeutige gemeinsame Lösung:

$$x = (a * h' * h + b * m' * m) \mod m * h$$

Dabei gilt:

$x \in Z_{mh}$,

$h' = (h)^{-1}_{\mod m} =$ Inverse zu h modulo m,

$m' = (m)^{-1}_{\mod h} =$ Inverse zu m modulo h

---

**Zu tun:** Beweis

---

**Zu tun:** Beispiel

---

### 1.3.17 Theorem 8: Verallgemeinerter Chinesischer Restsatz

Gegeben sind die Kongruenzen:

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ ...x & \qquad\qquad \equiv a_k \pmod{n_k} \end{aligned}$$

Dabei sind die $n_i$'s paarweise teilerfremd. Dann kann man mit $n = \prod_{i=1}^{k} n_i$, eine Lösung x wie folgt berechnet werden:

$$x = (\sum_{i=1}^{k} a_i * (\frac{n}{n_i})^{-1}_{\bmod n_i} * \frac{n}{n_i}) \mod n$$

### 1.3.18 Theorem 9: Eulersche $\varphi$-Funktion

Die Eulersche $\varphi$-Funktion ist:

$$\varphi(m) = |Z_m^*|$$

Für *p* prim gilt:

$$\varphi(m) = m * \prod_{p|m}(1 - \frac{1}{p})$$

---

**Zu tun:** BSP.

---

### 1.3.19 Theorem 10: Satz von Euler

Für alle $n \geq 2$ und alle $a \in Z_m^*$ ist:

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

---

**Zu tun:** Beweis

---

### 1.3.20 Folgerung 13:

Für alle Primzahlen *p* und $a \in \{1, ..., p\}$ gilt:

$$a^{p-1} \equiv 1 \pmod{p},$$

da nach *Theorem 9*: $\varphi(p) = p - 1$

### 1.3.21 Theorem 11: Kleiner Satz von Fermat

Für eine Primzahl $p$ und eine beliebige ganze Zahl $a$ gilt:

$$a^p \equiv a \pmod{p}$$

---

**Zu tun:** RSA

---

KAPITEL 2

# Wahrscheinlichkeitstheorie und Statistik

## 2.1 Wahrscheinlichkeitsräume

### 2.1.1 Definition 1: Wahrscheinlichkeitsraum

Ein (diskreter[1]) Wahrscheinlichkeitsraum ist eine Ergebnissmenge $\Omega = \{\omega_1, \omega_2\, \omega_3, ...\}$[2] von Elementarerignissen $\omega_1, \omega_2\, \omega_3, ...$ . Jedem $\omega_i$ ist eine Wahrscheinlichkeit $Pr[\omega_i]$ zugeordnet, so dass gilt:

- $0 \leq Pr[\omega_i] \leq 1$
- $\sum_{\omega_i \in \Omega} Pr[\omega_i] = 1$

### 2.1.2 Definition 2: Ereignis

Die Wahrscheinlichkeit von Ereignis $E \subseteq \Omega$ ist:

$$Pr[E] = \sum_{\omega \in E} Pr[\omega]$$

Ein Ereignis E tritt ein, wenn eines der Elementarereignissen aus E eintritt.

#### Speziell:

- $\emptyset$ - das unmögliche Ereignis
- $\Omega$ - das sichere Ereignis

### 2.1.3 Definition 3: Komplementär Ereignis

Das komplementäre Ereignis zu E ist $\bar{E} = \Omega - E$.

### 2.1.4 Definition 4: Relative Häufigkeit bzw. Wahrscheinlichkeit

Statistik über die Häufigkeit von Ereignis E.

Relative Häufigkeit (E) $= \frac{absoluteHufigkeit(E)}{AnzahlMessungen}$

Relative Häufigkeiten gelten als Erwartungen für die Zukunft und können als Wahrscheinlichkeiten (Wk., en: *propability*) betrachtet werden.

Für die Wahrscheinlichkeit eines Ereignisses E, werden die Wahrscheinlichkeiten der Elementarereignissen in E aufsummiert.

### 2.1.5 Definition 5: Laplace Experiment:

Alle Elementarereignisse $\omega_i$ einer endlichen Ergebnismenge $\Omega$ sind gleich wahrscheinlich.

$$Pr[\omega] = \frac{1}{|\Omega|}, \quad \forall \omega \in \Omega$$

Allgemein für ein Ereignis E:

$$Pr[E] = \frac{|E|}{|\Omega|}$$

[1] Aufzählbar und isolierte Objekte
[2] Unendlich viele Objekte möglich

### Lemma:

$0 \leq \frac{1}{|\Omega|} \leq 1$ und

$\sum_{\omega \in \Omega} Pr[\omega] = \sum_{\omega \in \Omega} \frac{1}{|\Omega|} = \frac{1}{|\Omega|} \sum_{\omega \in \Omega} 1 = \frac{1}{|\Omega|} * |\Omega| = 1$

### Beispiele:

1. Würfel (Laplace Experiment)

   $\Omega = \{1, 2, 3, 4, 5, 6\}$

   $Pr[k] = \frac{1}{6}$ mit $1 \leq k \leq 6$

   Ereignis $P = \{k \in \Omega \mid k\ ist\ prim\} = \{2, 3, 5\}$

   $Pr[P] = 3 * \frac{1}{6} = \frac{1}{2}$

2. Münze: 3-mal werfen (Laplace Experiment)

   $\Omega = \{k, z\}^3$ , $|\Omega| = 8$

   $Pr[\omega] = \frac{1}{8}$

   E = genau einmal k

   $Pr[E] = 3 * \frac{1}{8} = \frac{3}{8}$

3. Urne:

   5 Bälle, 2 rot (r) und 3 schwarz (s)

   Ziehe 2 mal ohne Zurücklegen.

   $\Omega = \{r, s\}^2$ , $|\Omega| = 4$

   E = 2. Kugel ist rot $= \{sr, rr\}$

   $Pr[E] = \frac{3}{10} + \frac{1}{10} = \frac{4}{10} = \frac{2}{5}$

### Beispiel: Nachweis für Wk.-Raum

Signalübertragung über Kanal. Erfolgreiche Übertragung mit Wk. $p$. Mit welcher Wk. braucht man $k$ Versuche bis zu einer erfolgreichen Übertragung?

Definiere Elementarereignisse:

$\omega_i =$ erfolgreiche Übertragung erstmals beim $i$-ten Versuch

$\Omega = \{\omega_1, \omega_2, \omega_3, ...\}$

Übertragung schlägt fehl mit Wk. $q = 1 - p$.

$Pr[\omega_i] = q^{i-1} * p$

$\sum_{i=1}^{\infty} Pr[\omega_i] = \sum_{i=1}^{\infty} q^{i-1} p = p * \sum_{i=0}^{\infty} q^i = p * \frac{1}{1-q} = p * \frac{1}{p} = 1$

$\Rightarrow$ Wk.-Raum

**Bsp.**

Ereignis $A_k =$ Erfolg in weniger gleich $k$ Versuchen $= \{\omega_1, \omega_2, ..., \omega_k\}$

$Pr[A_k] = \sum_{i=1}^{k} Pr[\omega_i] = \sum_{i=1}^{k} q^{i-1} p = p * \sum_{i=0}^{k-1} q^i = p * \frac{1-q^k}{1-q} = 1 - q^k = 1 - (1-p)^k$

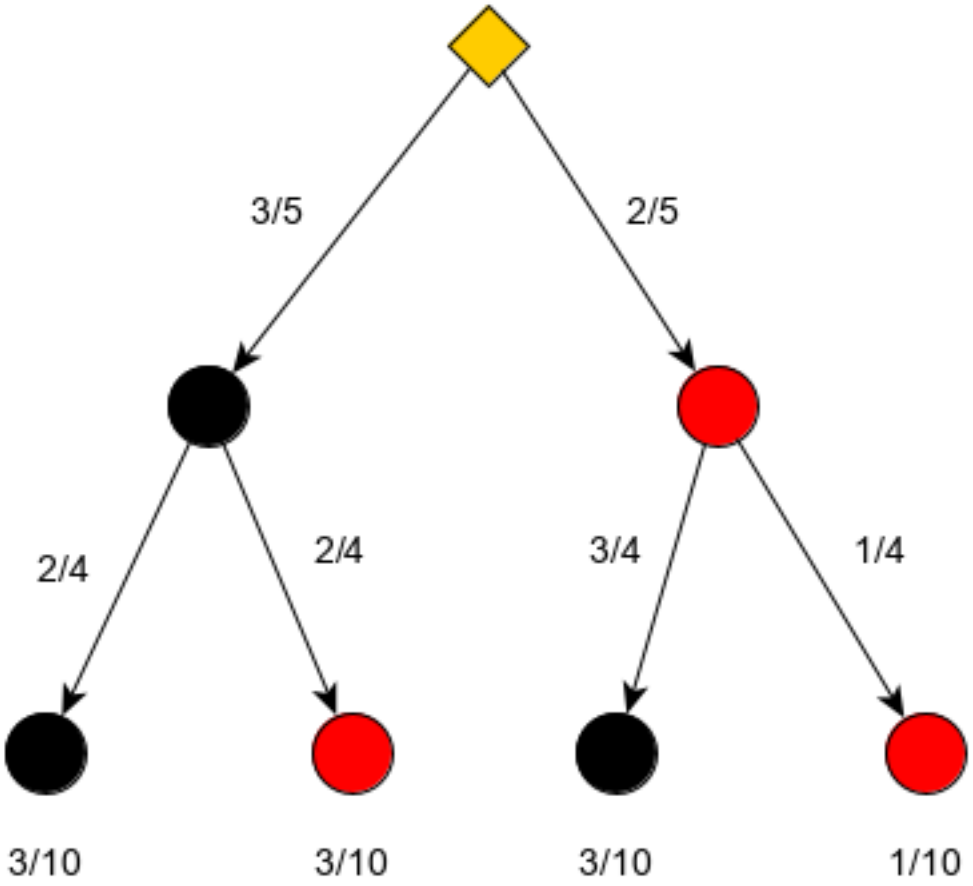


Abb. 1: Baumdiagramm: 5 Bälle, 2 rot (r) und 3 schwarz (s), 2 mal ziehen ohne Zurücklegen

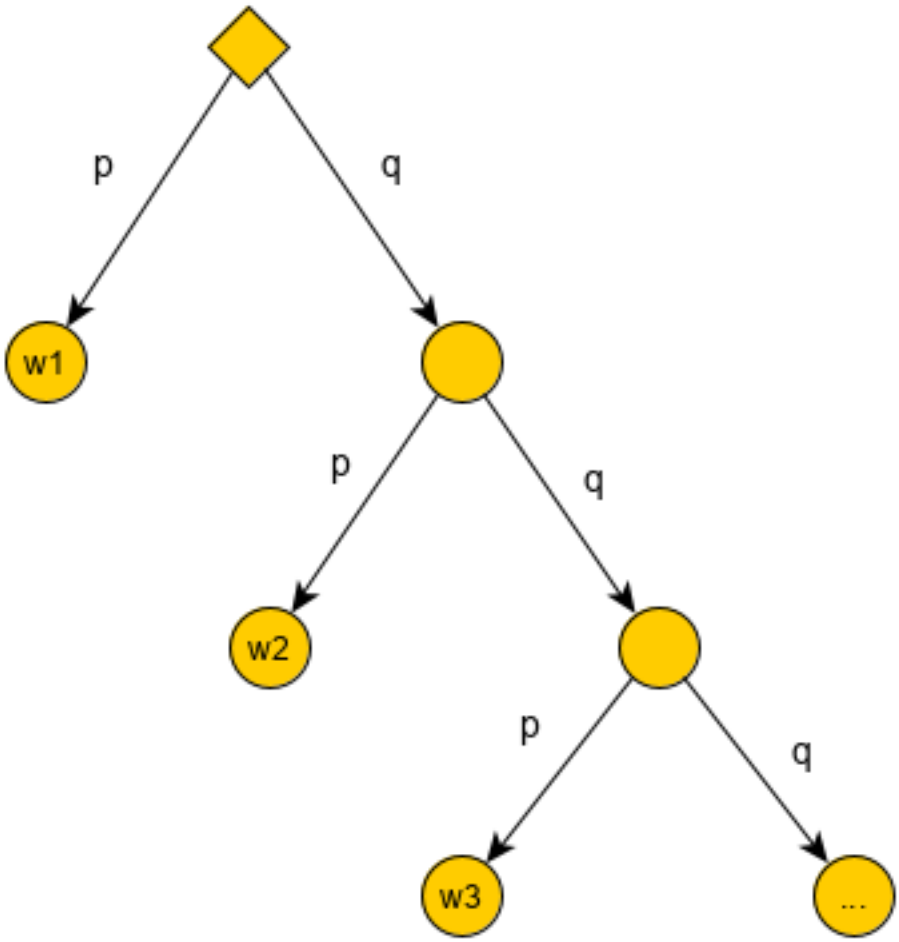


Abb. 2: Baumdiagramm: zur Signalübertragung

*Anmerkung:* $q^k$ geht exponentiell gegen 0. Also geht $1-(1-p)^k$ exponentiell gegen 1.

### 2.1.6 Eigenschaften

Seien $A, B \subseteq \Omega$ Ereignisse.

1. $Pr[\emptyset] = 0$, (da $0 \leq Pr[\emptyset] \leq 1 - Pr[\Omega] = 0$) und $Pr[\Omega] = 1$ (nach Definition)
2. $Pr[\bar{A}] = 1 - Pr[A]$

   $A \cup \bar{A} = \Omega \Rightarrow Pr[\bar{A}] + Pr[A] = Pr[\Omega] = 1$
3. $A \subseteq B \Rightarrow Pr[A] \leq Pr[B]$

   $Pr[B] = \sum_{\omega \in B} Pr[\omega] = \sum_{\omega \in A} Pr[\omega] + \sum_{\omega \in B-A} Pr[\omega] \geq \sum_{\omega \in A} Pr[\omega] = Pr[A]$
4. $A \cap B = \emptyset \Rightarrow Pr[A \cup B] = Pr[A] + Pr[B]$

   Additionssatz: $\sum_{\omega \in A \cup B} Pr[\omega] = \sum_{\omega \in A} Pr[\omega] + \sum_{\omega \in B} Pr[\omega]$

   Allgemeiner für $A_1, A_2, ...$ paarweise disjunkt gilt:

   $$Pr[\bigcup_{i \geq 1} A_i] = \sum_{i \geq 1} Pr[A_i]$$
5. $Pr[A \cup B] = Pr[A] + Pr[B] - Pr[A \cap B]$

   Siebformel:

$$|A \cup B \cup C| = |A| + |B| + |C| - (|A \cap B| + |A \cap C| + |B \cap C|) + |A \cap B \cap C|$$

$$|A_1 \cup A_2 \cup ... \cup A_n| =$$
$$= \sum_{i=1}^{n} |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| + \sum_{1 \leq i < j < k \leq n} |A_i \cap A_j \cap A_k| - + ... + (-1)^{n+1} |A_1 \cap ... \cap A_n|$$

#### Beweis: Allgemeine Siebformel

Sei $a \in A_1 \cup A_2 \cup ... \cup A_n$ beliebig.

Zeige: $a$ wird durch die Formel auf der rechten Seite genau einmal gezählt.

**Komme *a* in *m* der Mengen $A_1, A_2, ..., A_n$ vor. ($1 \leq m \leq n$)**

- $a$ wird in $S_1$ m-mal gezählt
- - " - $S_2$ $\binom{m}{2}$-mal gezählt (=Anzahl Paare aus m Elementen)
- - " - $S_k$ $\binom{m}{k}$-mal gezählt
- - " - $S_m$ $\binom{m}{m}$-mal gezählt
- - " - $S_n$ 0-mal gezählt

$\Rightarrow a$ wird $\binom{m}{1} - \binom{m}{2} + \binom{m}{3} - + ... + (-1)^{m+1}\binom{m}{m}$ - mal gezählt.

Binomialtheorem: $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$

Setze $x = -1,\ y = 1,\ n \geq 1$

$\Rightarrow a$ wird 1-mal gezählt. (*n* wird durch *m* ersetzt und $(-1)(-1)^n = (-1)^{m+1}$)

### 2.1.7 Folgerung:

$$Pr[A_1 \cup A_2 \cup ... \cup A_n] =$$

$$\sum_{i=1}^{n} Pr[A_i] - \sum_{1 \leq i < j \leq n} Pr[A_i \cap A_j] + \sum_{1 \leq i < j < k \leq n} Pr[A_i \cap A_j \cap A_k] - + ... + (-1)^{n+1} Pr[A_1 \cap ... \cap A_n]$$

#### Beispiel:

*n* Seeleute kehren betrunken auf ihr Schiff zurück. Jeder fällt zufällig in eine Koje. Mit welcher Wk. liegt keiner in seiner eigenen Koje? (Komplementär: Min. ein Seemann liegt in seiner Koje)

Seemann *i* gehört Koje *i*, $i = 1, 2, ..., n$. Jede Verteilung der Seeleute auf die Kojen ist eine Permutation $\pi \in S_n$, d.h. $\pi : [n] \to [n]$.

Ereignis $A_i$ = Seemann *i* liegt in seiner Koje *i*, d.h. $A_i = \{\pi \in S_n \mid \pi(i) = i\}$

$|S_n| = n!$

$|A_i| = (n-1)!$, da *n-1* Seeleute beliebig auf *n-1* Kojen verteilt werden.

$Pr[\pi] = \frac{1}{|S_n|} = \frac{1}{n!}$ (Laplace-prinzip)

$Pr[A_i] = \frac{|A_i|}{|S_n|} = \frac{(n-1)!}{n!} = \frac{1}{n}$

$A = A_1 \cup A_2 \cup ... \cup A_n =$ min ein Seemann liegt in der richtigen Koje.

$\Rightarrow |A_1 \cup A_2 \cup ... \cup A_n| = \sum_{i=1}^{n} |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| + \sum_{1 \leq i < j < k \leq n} |A_i \cap A_j \cap A_k| - + ... + (-1)^{n+1} |A_1 \cap ... \cap A_n|$
$= \sum_{k=1}^{n} (-1)^{k+1} \binom{n}{k} (n-k)!$
$= \sum_{k=1}^{n} (-1)^{k+1} \frac{n!}{k!(n-k)!} * (n-k)!$
$= n! * \sum_{k=1}^{n} \frac{(-1)^{k+1}}{k!}$
$\Rightarrow Pr[A] = \frac{|A|}{|S_n|} = \frac{n! * \sum_{k=1}^{n} \frac{(-1)^{k+1}}{k!}}{n!} = \sum_{k=1}^{n} \frac{(-1)^{k+1}}{k!}$

Pr[]=1-Pr[A]=1-$\sum_{k=1}^{n} \frac{(-1)^{k+1}}{k!} = \sum_{k=0}^{n} \frac{(-1)^k}{k!} \xrightarrow{n \to \infty} \frac{1}{e} \approx 0.36788$

**Hinweis:** $\sum_{0}^{\infty} \frac{1}{k!} = e$ und $\sum_{0}^{\infty} \frac{x^k}{k!} = e^x$

$Pr[\bar{A}]$ ist die Wk., dass keiner in seiner Koje liegt.

### 2.1.8 Zusammenfassung: Wahrscheinlichkeitsräume

**Wahrscheinlichkeitsraum:** $\Omega = \{\omega_1, \omega_2, \omega_3, ...\}$

**Elementarereignisse:** $\omega_1, \omega_2, \omega_3, ...$

**Summe aller Elementarergeinissen:** $\sum_{\omega_i \in \Omega} Pr[\omega_i] = 1$

**Ereignis** $E \subseteq \Omega$: $Pr[E] = \sum_{\omega \in E} Pr[\omega]$

$E$ tritt ein, sobald ein Elementarereigniss eintritt.

**komplementär Ereignis:** $\bar{E} = \Omega - E$

**Laplace Experiment:** $Pr[E] = \frac{|E|}{|\Omega|}$

**Eigenschaften:** Seien $A, B \subseteq \Omega$ Ereignisse.

- $Pr[\emptyset] = 0$
- $Pr[\Omega] = 1$
- $Pr[\bar{A}] = 1 - Pr[A]$
- $A \subseteq B \Rightarrow Pr[A] \leq Pr[B]$

**Additionssatz:** $A_1, A_2, ...$ paarweise disjunkt gilt: $Pr[\bigcup_{i \geq 1} A_i] = \sum_{i \geq 1} Pr[A_i]$

**Allgemeine Siebformel:**

$$
\begin{aligned}
|A_1 \cup A_2 \cup ... \cup A_n| = & \sum_{i=1}^{n} |A_i| \\
& - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| \\
& + \sum_{1 \leq i < j < k \leq n} |A_i \cap A_j \cap A_k| \\
& - + ... \\
& + (-1)^{n+1} |A_1 \cap ... \cap A_n|
\end{aligned}
$$

## 2.2 Bedingte Wahrscheinlichkeiten

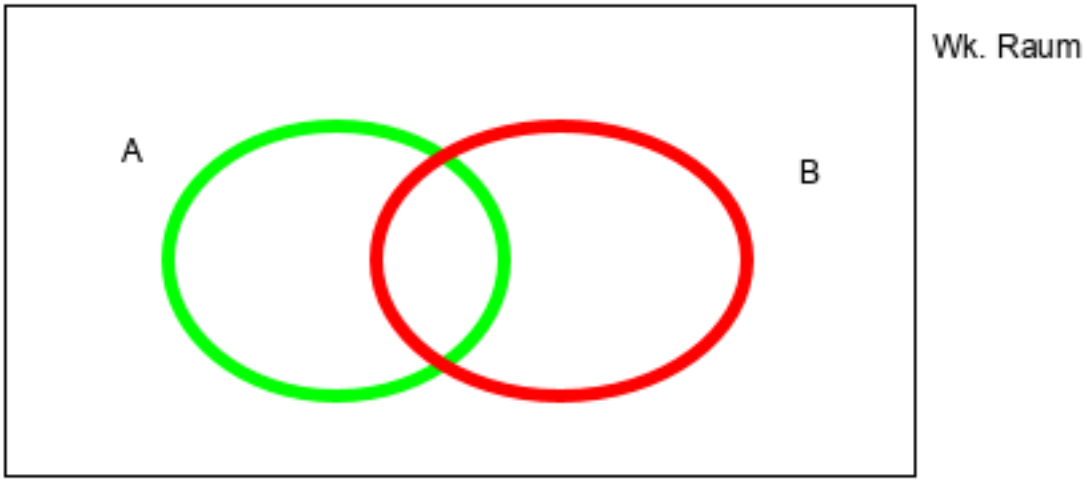


Abb. 3: Mengendiagramm mit den Mengen *A* und *B*

**Frage:** Wk. von *A*, wenn man bereits weiß, dass *B* eingetreten ist.

### 2.2.1 Definition 1: Bedingte Wahrscheinlichkeit

$\Omega$ Wk.raum, $B \subseteq \Omega$, $A \subseteq \Omega$ und $Pr[B] > 0$. Die bedingte Wahrscheinlichkeit A gegeben B ist definiert durch:

$$Pr[A \mid B] = \frac{Pr[A \cap B]}{Pr[B]}$$

Falls $Pr[B] = 0$, definiere: $Pr[A \mid B] = 0$

### 2.2.2 Eigenschaften: Bedingte Wahrscheinlichkeit

1. $A = B:\quad Pr[B \mid B] = \frac{Pr[B \cap B]}{Pr[B]} = 1$

2. $A \cap B = \emptyset: \quad Pr[A \mid B] = \frac{Pr[\emptyset]}{Pr[B]} = 0$
3. $B = \Omega: \quad Pr[A \mid \Omega] = \frac{Pr[A|\Omega]}{Pr[\Omega]} = Pr[A]$

#### Beispiele:

1. Würfel (Laplace Experiment)

   $p = Primzahl = \{2, 3, 5\}$, $u = ungerade = \{1, 3, 5\}$, $p \cap u = \{3, 5\}$

   $Pr[p] = Pr[u] = \frac{1}{2}$

   $Pr[p \mid u] = \frac{Pr[p \cap u]}{Pr[u]} = \frac{\frac{1}{3}}{\frac{1}{2}} = \frac{2}{3}$

2. 2 Kinder

   $\Omega = \{j, m\}^2 = \{jj, jm, mj, mm\}$

   $B = \{jm, mj, mm\}$, $A = \{mm\}$, $A \cap B = \{mm\}$

   $Pr[A \mid B] = \frac{Pr[A \cap B]}{Pr[B]} = \frac{\frac{1}{4}}{\frac{3}{4}} = \frac{1}{3}$

   C = 1. Kind ist $m = \{mj, mm\}$

   $Pr[A \mid C] = \frac{Pr[A \cap C]}{Pr[C]} = \frac{\frac{1}{4}}{\frac{1}{2}} = \frac{1}{2}$

### 2.2.3 Multiplikationssatz

Seien $A_1, A_2, ..., A_n \subseteq \Omega$ Ereignisse mit $Pr[A_1 \cap A_2 \cap ... \cap A_n] > 0$. Dann gilt:

$$Pr[A_1 \cap A_2 \cap ... \cap A_n] = Pr[A_1] * Pr[A_2 \mid A_1] * Pr[A_3 \mid A_1 \cap A_2] * Pr[A_n \mid A_1 \cap A_2 \cap ... \cap A_{n-1}]$$

#### Beweis:

Definition einsetzen: $Pr[A_1 \cap A_2 \cap ... \cap A_n] = Pr[A_1] * \frac{Pr[A_1 \cap A_2]}{Pr[A_1]} * \frac{Pr[A_1 \cap A_2 \cap A_3]}{Pr[A_1 \cap A_2]} * \frac{Pr[A_1 \cap A_2 \cap ... \cap A_n]}{Pr[A_1 \cap A_2 \cap ... \cap A_{n-1}]}$

Alle Nenner sich durch den vorherigen Zähler raus. Nur der Zähler vom letzten Term bleibt stehen. Somit stimmt die Gleichung.

**Beachte:** $A_1 \supseteq A_1 \cap A_2 \supseteq ... \supseteq A_1 \cap ... \cap A_n$

$\Rightarrow Pr[A_1] \geq Pr[A_1 \cap A_2] \geq ... \geq Pr[A_1 \cap ... \cap A_n] \geq 0$

#### Beispiel: Geburtstagsproblem

$\Omega = \{1, 2, ..., n = 365\}$, $m$ Personen zufällig.

A = alle *m* Personen haben an unterschiedlichen Tagen Geburtstag.

Personen $1, 2, ..., m$

$A_i$ = Person *i* hat an einem anderen Tag Geburtstag als die Personen $1, 2, .., i-1$. D.h. $A = A_1 \cap A_2 \cap ... \cap A_m$

$Pr[A_1] = 1$

$Pr[A_2 \mid A_1] = \frac{n-1}{n}$

$Pr[A_3 \mid A_1 \cap A_2] = \frac{n-2}{n}$

$Pr[A_j \mid A_1 \cap A_2 \cap ... \cap A_{j-1}] = \frac{n-(j-1)}{n}$

Nach *Multiplikationssatz*:

**Zu tun:** Check formula end

**Hinweis:** $1 - x \leq e^{-x}$

### 2.2.4 Satz: Totale Wahrscheinlichkeit

Seien $A_1, A_2, ..., A_n \subseteq \Omega$ paarweise disjunkt[1]. Sei $B \subseteq \Omega$ mit $B \subseteq A_1 \cup A_2 \cup ... \cup A_n$, dann gilt:

$$Pr[B] = \sum_{i=1}^{n} Pr[B \mid A_i] * Pr[A_i]$$

#### Beweis:

$B = (B \cap A_1) \cup (B \cap A_2) \cup ... \cup (B \cap A_n)$

$\Rightarrow Pr[B] = \sum_{i=1}^{n} Pr[B \cap A_i] = \sum_{i=1}^{n} Pr[B \mid A_i] * Pr[A_i]$, da $B \cap A_i$ paarweise disjunkt sind mit $i = 1, ..., n$.

**Hinweis**: $Pr[A \mid B] = \frac{Pr[A \cap B]}{Pr[B]} \Leftrightarrow Pr[A \cap B] = Pr[A|B] * Pr[B]$

### 2.2.5 Satz von Bayes:

Seien $A_1, A_2, ..., A_n \subseteq \Omega$ paarweise disjunkt[1], $B \subseteq A_1 \cup A_2 \cup ... \cup A_n$ und $Pr[B] > 0$, dann gilt:

$$Pr[A_i|B] = \frac{\Pr[A_i \cap B]}{Pr[B]} = \frac{Pr[B|A_i] * Pr[A_i]}{\sum_{i=1}^{n} Pr[B \cap A_i] * Pr[A_j]}$$

**Hinweise:** Dadurch wird es möglich aus $Pr[A|B]$, $Pr[B|A]$ zu berechnen. Dies ist möglich, da das UND kommutativ ist.

#### Beispiel: Datenübertragung über Kanal mit Fehlern (noisy)

Übertragen wird Bit 0 oder 1.

Ereignisse: für $i = 0, 1$

$S_i =$ Bit *i* wird gesendet.

$R_i =$ Bit *i* wird empfangen.

Es gelte: $Pr[S_0] = 0,3 \;\; , Pr[S_1] = 0,7$

Fehler: $Pr[R_1|S_0] = 0,3 \;\; , Pr[R_0|S_1] = 0,1$

[1] Werden zwi beliebige Mengen geschnitten, ist der Schnitt immer leer

Frage: Wk. für Übertragungsfehler?

$$\begin{aligned} Pr[-Fehler] &= Pr[(S_1 \cap R_0) \cup (S_0 \cap R_1)] \\ &= Pr[S_1 \cap R_0] + Pr[S_1 \cap R_1] \\ &= Pr[R_0|S_1] * Pr[S_1] + Pr[R_1|S_0] * Pr[S_0] \\ &= 0,1 * 0,7 + 0,3 * 0,3 = 0,16 \end{aligned}$$

Andere WK.'s:

$$\begin{aligned} Pr[R_1] &= Pr[R_1|S_0] * Pr[S_0] + Pr[R_1|S_1] * Pr[S_1] \qquad NR: Pr[R_1|S_1] = 1 - Pr[R_0 \mid S_1] \\ &= 0,3 * 0,3 + 0,9 * 0,7 = 0,72 \\ Analog: Pr[R_0] &= 0,28 \;\; oder \;\; 1 - 0,72 = 0,28 \\ Pr[S_1 \mid R_1] &= \frac{Pr[R_1 \mid S_1] * Pr[S_1]}{Pr[R_1]} = \frac{0,9 * 0,7}{0,72} = 0,875 \\ Analog: Pr[S_0 \mid R_0] &= 0,75 \end{aligned}$$

### Beispiel: 3 Münzen

Gegeben sind 3 Münzen von denen 2 fair sind und eine gefälscht ist. Für die Gefälschte gilt: $Pr[K] = \frac{2}{3}$.

Wähle die Reihenfolge und werfe jede zufällig.

$E_i =$ Münze *i* ist gefälscht, $i = 1, 2, 3$

$Pr[E_i] = \frac{1}{3}$, $\Omega = \{K, Z\}^3$

**Ergebnis sei:**

| 1 | 2 | 3 |
|---|---|---|
| K | K | Z |

Frage: Wie groß ist die Wk., dass Münze 1 die gefälschte Münze ist?

$B = \{(K, K, Z)\}$

$Pr[E_1 \mid B] =?$

$Pr[B \mid E_1] = \frac{2}{3} * \frac{1}{2} * \frac{1}{2} = \frac{1}{6}$

$Pr[B \mid E_2] = \frac{1}{2} * \frac{2}{3} * \frac{1}{2} = \frac{1}{6}$

$Pr[B \mid E_3] = \frac{1}{2} * \frac{1}{2} * \frac{1}{3} = \frac{1}{12}$

$Pr[E_1 \mid B] = \frac{Pr[B|E_1] * Pr[E_1]}{\sum_{i=1}^{3} Pr[B|E_i] * Pr[E_i]} = \frac{2}{5}$

## 2.2.6 Definition: Unabhängigkeit

*A* und *B* sind voneinander unabhängig, falls das Zutreffen von Ereignis *B*, die Wk. von *A* nicht ändert. D.h. es gilt: $Pr[A \mid B] = Pr[A]$ Folglich: $\frac{Pr[A \cap B}{Pr[B]} = Pr[A]$

$$\Rightarrow Pr[A \cap B] = Pr[A] * Pr[B]$$

Ist $Pr[A] > 0$, dann folgt $Pr[B] = \frac{Pr[A \cap B]}{Pr[A]} = Pr[B \mid A]$

#### Beispiel: 2 Würfel, geordnet

A = 1. Würfel ist gerade

B = 2. Würfel ist gerade

C = Summe ist 7

$\Omega = [6]^2$

Definiere: $G = \{2, 4, 6\}$

$A = G \times [6]$, $|A| = 3 * 6 = 18$, $Pr[A] = \frac{18}{36} = \frac{1}{2}$

$B = [6] \times G$, $|B| = 6 * 3 = 18$, $Pr[A] = \frac{18}{36} = \frac{1}{2}$

$C = \{(1,6), (2,5), (3,4), (4,3), (5,2), (6,1)\}$, $Pr[C] = \frac{1}{6}$

$Pr[A \cap B] = Pr[G \times G] = \frac{9}{36} = \frac{1}{4} = Pr[A] * Pr[B] \Rightarrow$ *A* und *B* sind unabhängig.

$Pr[A \cap C] = Pr[\{(2,5), (4,3), (6,1)\}] = \frac{3}{36} = \frac{1}{12} = Pr[A] * Pr[C] \Rightarrow$ *A* und *C* sind unabhängig. Analog: $B \cap C \Rightarrow$ A/B sind unabhängig von C.

$Pr[A \cap B \cap C] = Pr[\emptyset] = 0 \neq Pr[A] * Pr[B] * Pr[C] \Rightarrow$ Nicht alle drei sind unabhängig.

### 2.2.7 Definition: Unabhängigkeit von n Ereignissen

$A_1, A_2, ..., A_n$ heißen unabhängig, falls:

$$\forall I \subseteq [n] : Pr[\bigcap_{i \in I} A_i] = \prod_{i \in I} Pr[A_i]$$

**Erklärung:** Alle möglichen Kombinationen werden betrachtet und müssen unabhängig sein.

### 2.2.8 Satz:

**Sind *A* und *B* unabhängig, dann sind auch unabhängig:**

- $\bar{A}$ und $B$
- $A$ und $\bar{B}$
- $\bar{A}$ und $\bar{B}$

#### Beweis: zu $\bar{A},\ B$

$\bar{A} \cap B = B - A = B - (A \cap B) \Rightarrow (\bar{A} \cap B) \cup (A \cap B) = B$[2]

$\Rightarrow Pr[(\bar{A} \cap B) \cup (A \cap B)] = Pr[\bar{A} \cap B] + Pr[A \cap B] = Pr[\bar{A} \cap B] + Pr[A] * Pr[B] = Pr[B]$

$$\begin{aligned} Pr[\bar{A} \cap B] &= Pr[B] - Pr[A] * Pr[B] \\ &= (1 - Pr[A]) * Pr[B] \qquad\qquad = Pr[\bar{A}] * Pr[B] \end{aligned}$$

Analog für $A,\ \bar{B}$. Damit folgt auch, dass $\bar{A}$ und $\bar{B}$ unabhängig sind.

[2] $\bar{A} \cap B$ sind disjunkt

#### Beweis: für $\bar{A}, \bar{B}$

A, B unabhängig $\Rightarrow \bar{A},\ B$ unabhängig. Def: $\bar{A} = C. \Rightarrow C,\ \bar{B}$ unabhängig $\Rightarrow \bar{A},\ \bar{B}$ unabhängig.

**Def:**

Für $A \subseteq \Omega$, $A^1 = A$ und $A^0 = \bar{A}$

### 2.2.9 Satz:

Seien $A_1, A_2, ..., A_n \subseteq \Omega$, dann gilt:

$A_1, A_2, ..., A_n$ sind unabhängig $\Rightarrow$

$\forall s_1, s_2, ..., s_n \in \{0,1\} Pr[A_1^{s_1} \cap A_2^{s_2} \cap, ..., A_n^{s_n}] = Pr[A_1^{s_1}] * Pr[A_2^{s_2}] * Pr[A_2^{s_2}] * ... * Pr[A_n^{s_n}]$

---

**Zu tun:** Beweis

---

### 2.2.10 Folgerungen:

A, B unabhängig:

$\Leftrightarrow \bar{A}, B$ unabh.

$\Leftrightarrow A, \bar{B}$ unabh.

$\Leftrightarrow \bar{A}, \bar{B}$ unabh.

A, B, C unabh. $\Rightarrow A \cap B, C$ unabh. und $A \cup B, C$ unabh.

---

**Zu tun:** Beweise

---

---

**Zu tun:** Beispiele + Anwendungen

---

### 2.2.11 Zusammenfassung: Bedingte Wahrscheinlichkeit

$A, B \subseteq \Omega$

**Bedingte Wahrscheinlichkeit A gegeben B:**

$$Pr[A \mid B] = \frac{Pr[A \cap B]}{Pr[B]}$$

**Sonderfälle:**

1. $A = B: \quad Pr[B \mid B] = \frac{Pr[B \cap B]}{Pr[B]} = 1$
2. $A \cap B = \emptyset: \quad Pr[A \mid B] = \frac{Pr[\emptyset]}{Pr[B]} = 0$
3. $B = \Omega: \quad Pr[A \mid \Omega] = \frac{Pr[A \mid \Omega]}{Pr[\Omega]} = Pr[A]$

**Multiplikationssatz:**

Seien $A_1, A_2, ..., A_n \subseteq \Omega$ Ereignisse mit $Pr[A_1 \cap A_2 \cap ... \cap A_n] > 0$. Dann gilt:

$$Pr[A_1 \cap A_2 \cap ... \cap A_n] = Pr[A_1] * Pr[A_2 \mid A_1] * Pr[A_3 \mid A_1 \cap A_2] * Pr[A_n \mid A_1 \cap A_2 \cap ... \cap A_{n-1}]$$

**Totale Wahrscheinlichkeit:**

Seien $A_1, A_2, ..., A_n \subseteq \Omega$ paarweise disjunkt. Sei $B \subseteq \Omega$ mit $B \subseteq A_1 \cup A_2 \cup ... \cup A_n$, dann gilt:

$$Pr[B] = \sum_{i=1}^{n} Pr[B \mid A_i] * Pr[A_i]$$

**Satz von Bayes:**

Seien $A_1, A_2, ..., A_n \subseteq \Omega$ paarweise disjunkt[1], $B \subseteq A_1 \cup A_2 \cup ... \cup A_n$ und $Pr[B] > 0$, dann gilt:

$$Pr[A_i|B] = \frac{\Pr[A_i \cap B]}{Pr[B]} = \frac{Pr[B|A_i] * Pr[A_i]}{\sum_{i=1}^{n} Pr[B \cap A_i] * Pr[A_j]}$$

**Unabhängigkeit:**

2 Ereignisse:

$$Pr[A \cap B] = Pr[A] * Pr[B]$$

n Ereignisse:

$$\forall I \subseteq [n] : Pr[\bigcap_{i \in I} A_i] = \prod_{i \in I} Pr[A_i]$$

oder

$$\forall s_1, s_2, ..., s_n \in \{0, 1\} Pr[A_1^{s_1} \cap A_2^{s_2} \cap, ..., A_n^{s_n}] = Pr[A_1^{s_1}] * Pr[A_2^{s_2}] * Pr[A_2^{s_2}] * ... * Pr[A_n^{s_n}]$$

Erklärung: Alle möglichen Kombinationen werden betrachtet und müssen unabhängig sein.

KAPITEL 3

# Einführung in die IT-Sicherheit

## 3.1 Einführung

### 3.1.1 Datenschutz vs. Datensicherheit

**Datenschutz:**

Die Gewährleistung der Rechte von Betroffenen bei der Verarbeitung ihrer personenbezogener Daten. Also der Schutz der Personen. Bei Datenschutzverletzungen werden die Persönlichkeitsrechte und Grundrechte von Menschen verletzt.

**Datensicherheit/Security:**

*Schutz von Informationssystemen. Die Arte der daten spielt keine Rolle.* Die technische Sicherung, Erhaltung und Verfügbarkeit der Datenverarbeitungssysteme und der mit ihnen verarbeiteten Daten. Die Datensicherheit betrifft alle Daten im Unternehmen, unabhängig davon ob es sich um personenbezogene Daten handelt, oder um daten ohne Personenbezug. Probleme bei der Datensicherheit führen zum Verlust oder zur Verfälschung von Daten und zur unberechtigten Einsichtnahme durch Dritte in die Daten. Im schlimmsten Fall kann mangelnde Datensicherheit ein Unternehmen ruinieren, auch wenn keine personenbezogenen Daten betroffen sind. Die Sicherstellung der Datensicherheit personenbezogener Daten ist also ebenfalls eine wichtige Aufgabe im Datenschutz.

**Safety:**

Die physische Sicherheit, also die Verfügbarkeit von Daten und IT.

### 3.1.2 IT-Sicherheit in Unternehmen

Risiken: - Social engineering - veraltete Software - Cloudanbieter

Folgen von zu geringer IT-Sicherheit: - Finanzieller Schaden - Wirtschaftsspionage - Datenverlust - Image schaden - Produktionsausfall

### 3.1.3 OWASP Top 10:

Definiert die top 10 größten Sicherheitsrisiken in Software.

1. **Injection**: e.g. SQL-injection
2. **Broken Authentication**: Fehlerhafte implementierte Funktionen für Authentisierung oder Session Management
3. **Sensitive Data Exposure**: WEB API schützt sensible Daten nicht richtig. z.B. keine Verschlüsselung
4. **XML External Entities (XXE)**: XML-Verarbeitungsanwendungen werten auch Referenzen auf externe XML Dokumente aus
5. **Broken Access Control**: Einschränkungen für authentisierte Benutzer werden nicht hinreichend umgesetzt
6. **Security Misconfiguration**: Unsichere Konfiguration von Diensten, die extern erreichbar sind. (z.B. Standardeinstellung)
7. **Cross-Site Scripting (XSS)**: Einbetten nicht vertrauenswürdiger Daten in eine Website ohne Überprüfung
8. **Insecure Deserialization**: Unzureichende Überprüfung von vom Nutzer eingegebener Daten, vor dem Deserialisieren
9. **Using Components with Known Vulnerabilities**: Einsatz von Software mit bekannten Sicherheitslücken
10. **Insufficient Logging & Monitoring**

### 3.1.4 5 Säulen der IT-Sicherheit

Die 5 Säulen geben vor auf was im Bezug auf IT-Sicherheit geachtet werden, wenn es um Daten geht. Also um das speichern aber insbesondere auch beim Übertragen von Daten.

1. **Confidentiality (Vertraulichkeit)**: Nur autorisierte Personen können die Daten verstehen. z.B. Verschlüsselung
2. **Authenticity (Authentizität)**: Daten wurden wirklich vom angegebenen Urheber erstellt und nicht von jemand anderem
3. **Non-/Repudiation (Verbindlichkeit):**
    - Non-Repudiation: Es kann sicher festgestellt werden, wer die Daten abgesendet hat
    - Repudiation: Ein Absender soll abstreiten können etwas gesandt zu haben. z.B. Anonymisierung
4. **Integrity (Integrität)**: Daten können nicht unbemerkt verfälscht werden
5. **Availability (verfügbarkeit)**: Daten sind immer dann verfügbar wenn sie benötigt werden

### 3.1.5 3 wichtigsten Ziele der IT-Sicherheit: CIA Triad

Von diesen 5 Säulen, werden 3 als die wichtigsten angesehen. Es können jedoch nie alle 3 erreicht werden, da sie teilweise widersprüchlich sind.

- Availability
- Confidentiality
- Integrity

**Availability vs. Confidentiality:** Information öffentlich im Internet verfügbar, dann kann sie nicht geheim gehalten werden. Durch (sicheres) Löschen einerInformation kann garantiert werden, dass niemand Zugriff darauf bekommt. Dann ist die Information aber auch nicht mehr verfügbar.

**Availability vs. Integrity:** Je mehr (unabhangige) Systeme eine Information enthalten, desto vefügbarer ist sie. Je mehr und unabhängiger die Systeme sind, desto schwerer ist es die Integrität der Information zu gewährleisten. Die Integrität einer Information ist garantiert wenn niemand diese ändern kann.

**Confidentiality vs. Integrity:** Je geheimer einer Information ist,desto weniger "Kopien" sollte es geben. Um Integrität zu garantieren müsste aber irgendwo eine "Kopie" der Information vorhanden sein. Je mehr die Integrität einerInformation geschützt ist, desto mehr muss zusätzlich über die Information gespeichert werden (bis hin zur vollständigen Kopie)

## 3.2 Staatliche Überwachung

### 3.2.1 Staatliche Behörden

- BND - Deutschland
- NSA - USA
- FBI - USA

### 3.2.2 Mögliche Informationen über Einzelpersonen

- Potenziell bedrohliche Telefongespräche ins Ausland können aufgezeichnet werden
- Luftfahrt Daten
- Post Daten
- Telekommunikations Daten
- Banken Daten

### 3.2.3 Zweck der Staatlichen Überwachung

- Terrorismusbekämpfung

### 3.2.4 Argumente gegen staatliche Überwachung

- Nur weil man selber das Recht auf Privatsphäre nicht in Anspruch nimmt, gibt es trotzdem Personen die dieses Recht brauchen
- Gespeicherte Daten können durchsickern
- Kriminelle und unschuldige werden in einen Topf geworfen
- Die Daten können in Zukunft böswillig verwendet werden

### 3.2.5 Schutzmaßnahmen gegen Überwachung

- Sorgfältige Auswahl von Anbietern
- Verschlüsseln von Emails und Daten
- Anonymisierung z.B TOR
- Sichere Passwörter

- Regelmäßige Updates

## 3.3 Wirtschaftsspionage

### 3.3.1 Folgen von Informationsverlust in einer Firma

- Abwanderung von Kunden
- Image schaden
- Umsatz Verluste

### 3.3.2 Wirtschaftsspionage in kleineren Unternehmen

- Oft geringere Schutzmaßnamen -> leichter anzugreifen
- Können helfen in größere Unternehmen zu gelangen
- Kann ein Unternehmen ruinieren
- Auch kleine Unternehmen haben sensible Daten

### 3.3.3 Malware

Schadsoftware die meist Schwachstellen nutzt um auf ein System zu gelangen.

**Virus**

Hängt sich an bestehendes Programm. Der Virus wird ausgeführt, wenn das Programm ausgeführt wird. Viren können sich verändern, um die Erkennung zu erschweren.

**Wurm**

Schadsoftware, die sich selbst verbreitet. Sucht nach weiteren Zielen. Würmer können meist ferngesteuert werden.

**Trojaner**

Programme, die neben erwünschten Funktionen auch unerwünschte Funktionen ausführen. Programme müssen aktiv installiert werden.

**Rootkit**

An sich nicht schädlich. Kann aber andere Schadsoftware unterstützen.

**Backdoor**

Ermöglicht Angreifer einfaches eindringen in System

**Ransomware**

Erpresst Nutzer, indem die Daten verschlüsselt werden.

**Spyware**

Spioniert den infizierten Rechner aus.

**Scareware**

Versucht Nutzer zu verängstigen. Für Behebung von Sicherheitslücke soll bezahlt werden.

**Adware**

Zeigt regelmäßige nervige Werbung

### 3.3.4 Social Engineering

Eigenschaften des Menschen werden ausgenutzt um den Mensch dazu zu bringen unzulässig zu Handeln. z.B. Daten herausgeben. Angreifer kann sich als andere Person ausgeben und zum Beispiel Passörter verlangen.

### 3.3.5 Schutzmaßnahmen gegen Social Engineering

- Schulungen der Mitarbeiter
- Zugriffsrechte Begrenzen

### 3.3.6 Einfallstore für Wirtschaftsspionage

- Unsichere Computer und Smartphones
- Innentäter
- Malware
- Social Engineering
- Geschäftsreisen

### 3.3.7 Schutzmaßnahmen gegen Wirtschaftsspionage

- Klarer Umgang mit Schützenswerten Daten
- Geheimhaltungspflicht
- Regelungen für den Gebrauch von Hardware
- Sicherheitsverantwortlichen ernennen
- Clean-Desk-Policy
- Absicherung des internen Netzes
- Passwortschutz
- Zugangsbeschränkungen
- Verschlüsselung der Daten
- Verbote für USB-sticks, ...
- Verschlüsselte Emails
- Schulungen
- Bauliche Sicherungen

## 3.4 IT-Sicherheits-Management

### 3.4.1 Was sollte eine Leitlinie zur Informationssicherheit enthalten

### 3.4.2 Welche Aufgaben haben üblicherweise IT-Sicherheitsbeauftragte

### 3.4.3 Wie wird zweckmäßig ein IS-Management-Team gebildet?

### 3.4.4 Wer ist für die Bekanntgabe der Leitlinie zur Informationssicherheit verantwortlich?

### 3.4.5 Welche Aufgabe obliegt dem Informationssicherheitsmanagement?

### 3.4.6 Überlegen Sie sich ein Szenario aus dem betrieblichen Alltag und finden Sie den am besten geeigneten Baustein

## 3.5 Kryptographie - Symmetrische Verschlüsselung

### 3.5.1 Warum ist Kryptographie für IT-Sicherheit so wichtig? Erklärung anhand der 5 Säulen der ITS

- **Vertraulichkeit:** nur befugte verstehen die Daten. (Verschlüsselung)
- **Authenzität:** Daten stammen von angegebenen Urheber. (Digitale Signatur)
- **Verbindlichkeit:** Nachverfolgbar, dass Daten gesendet wurden, und wie oft. (Zeitstempel)
- **Integrität:** Daten wurden nicht im Nachhinein manipuliert. (Message Digests)

### 3.5.2 Was erzeugt ein pRNG im Gegensatz zu einem RNG?

Ein pRNG (pseudo random number generator) erzeugt keine wirklichen Zufallszahlen. Es sieht nur zufällig aus. Ein RNG generiert richtige Zufallszahlen.

### 3.5.3 Was haben One-Time-Pads mit absoluter Sicherheit zu tun?

Jede Information, wird mit einem anderem Schlüssel verschlüsselt.

Absolute/informationstheoretische Sicherheit: Chiffretext gibt keine Hinweise auf Plaintext. Anzahl möglicher Schlüssel > Anzahl möglicher Plaintexte.

### 3.5.4 Wieso ist security by obscurity schlecht? Welches Prinzip (mit Erklärung) sollte stattdessen verwendet werden?

Sobald der Quellcode in die öffentlichkeit gelangt, ist der Algorithmus nicht mehr sicher. **Das einzige Geheimnis sollte der Schlüssel sein, während die Algorithmen öffentlich bekannt sind. Es gibt genügend Kryptosysteme, die diese Anforderung erfüllen.

### 3.5.5 Was unterscheidet eine Blockchiffre von einer Stromchiffre?

- Eine Stromchiffre kann unendlich lang sein.
- Eine Blockchifre hingegen hat immer eine feste Größe. Längere Daten werden in mehrere Blöcke zerlegt

### 3.5.6 Nenne Sie jeweils einen Vor- und einen Nachteil von Selbstsynchronisierenden Stromchiffren.

Vorteile: - Selbst bei identischen Schlüsseln, unterscheiden sich die Geheimtexte, wenn sich die plaintexte unterscheiden. - Wenn Bits verloren gehen, synchronisiert sich das System selbst

Nachteile: - Replay attacks sind möglich - Keine Berechnung der Schlüsselbits im Voraus

### 3.5.7 Wie funktioniert DES? (Zeichnung)

**Zu tun:** Zeichnung einfügen