

# **Mathematik 1**

## **im Studiengang Regenerative Energiesysteme und Energiemanagement**

**Prof. Dr.-Ing. Karin Landenfeld**



## **Vorlesung 1 - Grundlagen 1**

**Donnerstag 22.09.2022 1.+2. Viertel**

### **Inhalt:**

- **Organisatorisches MA1**
- **Vorlesungsinhalte MA1**
- **Zeitplan**
- **Grundlagen 1**
  - Motivation: RSA-Algorithmus
  - Teiler, Vielfache, modulo
  - ggt/ kgV
  - Primzahlenfaktorzerlegung
  - Euklidischer Algorithmus

## Wer ist da?

... Anwesenheitsliste

... ein paar Fragen zum Kennenlernen

### Frage 1: Haben Sie am Mathematik-Vorkurs teilgenommen?

- Ja, komplett
- Ja, teilweise
- Nein, ich hatte keine Zeit
- Nein, ich habe davon nichts gewusst
- Nein, ich habe ausreichende Vorkenntnisse
- Nein, sonstige Gründe

### Frage 2: Mit welchem Schulabschluss kommen Sie zu uns?

- Fachoberschule Technik
- Ein anderer Fachoberschulabschluss
- Allgemeines Gymnasium
- Technisches Gymnasium
- Master
- etwas anderes

### Frage 3: Haben Sie vor dem Studium eine Ausbildung oder ein anderes Studium absolviert oder kommen Sie direkt von der Schule?

- Ich komme direkt von der Schule
- Ich habe eine technische Ausbildung absolviert.
- Ich habe eine nicht technische Ausbildung absolviert.
- Ich habe ein freiwilliges ... Jahr gemacht.
- etwas anderes

### Frage 4: Wo wohnen Sie?

- In Hamburg
- In Niedersachsen
- In Schleswig-Holstein
- In Mecklenburg-Vorpommern
- woanders

## Organisatorisches MA1

### Kursraum für die Vorlesung Mathematik 1

(1) Link zur Lernumgebung <https://e-assessment.haw-hamburg.de/course/view.php?id=359>

<https://e-assessment.haw-hamburg.de/>

The screenshot shows the navigation bar of the HAW Hamburg e-assessment platform. It includes a menu icon, the HAW HAMBURG logo, and links for Mathematik, Informatik, and Naturwissenschaften. A downward arrow points to the course list. The course 'Mathe 1 REE (LND) WiSe 2022/23' is listed with a blue circular icon. To the right, the enrollment key 'Einschreibeschlüssel: LNDdnl\_WS22' is displayed. Below the course name is a fractal image, and at the bottom, it says 'Trainer/in: Karin Landenfeld'.

(2) Bereitstellung der Vorlesungsunterlagen (Skript, Vorlesungsmitschrift,...)

Mathe 1 REE (LND) WiSe 2022/23

Schreibtisch / Meine Module / MA1 REE (LND) WS22

This is a screenshot of the course page for 'Mathe 1 REE (LND) WiSe 2022/23'. It shows a navigation bar with 'Ankündigungen' (Announcements), 'Organisatorisches', and 'Grundlagen'. Under 'Grundlagen', there are three items: 'Skript - Kapitel 1: Grundlagen' (script), 'Vorlesungsaufgaben Grundlagen' (lecture assignments), and 'Übungsaufgaben Grundlagen 1 (ggT, kgV, Primfaktoren)' (exercise assignments). Each item has a small icon next to it.

(3) Übungsaufgaben passend zu den Vorlesungsinhalten

- > Onlineaufgaben mit sofortigem individuellem Feedback
- > mehrfach durchführbar, Musterlösung

(4) Lernumgebung für die Zwischentests und Prüfung

## **Klausur/ Prüfung in Mathematik 1**

Klausur als elektronische Prüfung

- in der Prüfungsperiode am Ende des Semesters
- Dauer: 120 Minuten
- in Präsenz im PC-Pool, 13.Stock, BT7

Anmeldung notwendig, Abmeldung bis 1 Woche vor der Prüfungsperiode möglich

Prüfungsvorleistung für Teilnahme an der Prüfung erforderlich

## **Prüfungsvorleistung**

3 PVL-Tests über das Semester verteilt, Dauer 60 Minuten

- Mittwoch 5.Viertel (16:00 – 17:30), genaue zeitliche Lage siehe Zeitplan
- elektronische Prüfungen in Präsenz im PC-Pool, 13.Stock, BT7
- Bestehen aller 3 Tests mit mindestens 50% erforderlich
- Bestehen mit mehr als 80%, dann Bonuspunkt für Klausur

Erfolgreiche Teilnahme an den Übungen

- Aktive Mitarbeit

## **MSTeams-Raum**

**falls Vorlesung oder Übungen digital stattfinden**



Mathematik 1 - WS22/23

Link zum MSTeams-Raum

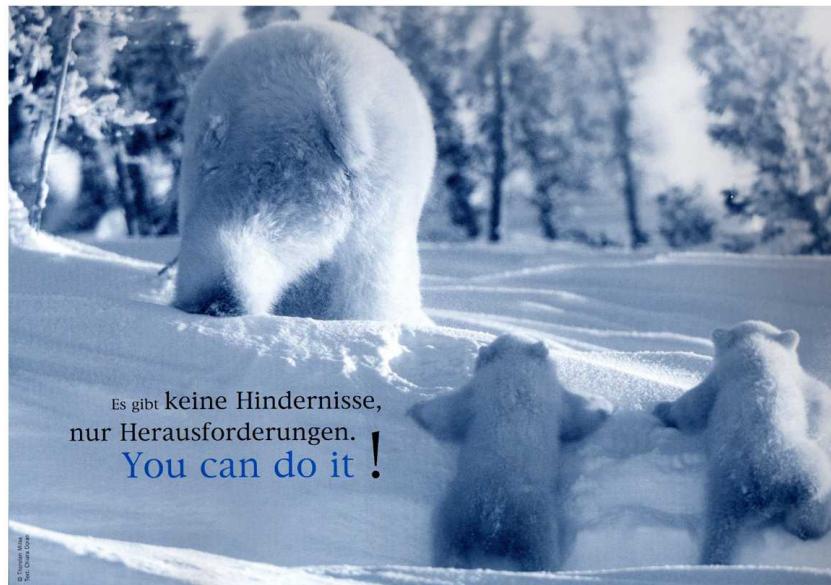
<https://teams.microsoft.com/l/team/>

19%3a4tls8WjRomArdTM0GzM9iNZ5xgGYoEOdAsjIQ\_To6c1%40thread.tacv2  
/conversations?groupId=77ebc417-8964-4323-b12a-  
b8e9c3a84338&tenantId=38d63075-6a27-4ec4-95f9-473f5ef2f1b5

## SEMESTERBEGLEITENDE ONLINE-AUFGABEN

auf e-assessment.haw-hamburg.de

- Online-Aufgaben passend zu den Vorlesungsinhalten zum Üben zu Hause
- Überprüfen des Verständnisses
- Sofortiges individuelles Feedback
- Verschiedene Aufgabentypen
- Randomisierte Aufgaben für ein mehrfaches Lösen
- Lernumgebung Moodle mit Erweiterung durch STACK und das Computer-Algebrasystem MAXIMA
- Individuelle Bearbeitung durch den Studierenden in Menge, Zeit und Ort
- Geräteunabhängig auf PC, Laptop, Smartphone
- Lernen mit Musterlösungen



## Digitale Übungsaufgaben und Tests

Schreibtisch > viaMINT ausprobieren > Kurzer Mathe-Test für Einsteiger

**Test-Navigation**

1	2	3	4	5
---	---	---	---	---

[Versuch beenden](#)

**Hinweise zur Formeleingabe**

Für den Ausdruck:	Geben Sie ein:
4,2	4.2
3x	3*x
$\pi$	pi
$\frac{2}{5}$	2/5
$\frac{1}{x+2}$	1/(x+2)
$x^n$	x^n
$\sqrt{x}, \sqrt[3]{x}$	sqrt(x)
$\sqrt[5]{y}$	y^(1/5)

**Frage 4**  
Unvollständig  
Erreichte Punkte 0,75 von 1,00  
 Frage markieren

Bestimmen Sie die Nullstelle der folgenden Funktionen:

a)  $f(x) = 2x + 42 \quad : \quad x_0 = -21$

Ihre letzte Antwort wurde folgendermaßen interpretiert:  
-21

b)  $f(x) = -4x - 12 \quad : \quad x_0 = 3$

Ihre letzte Antwort wurde folgendermaßen interpretiert:  
3

**Prüfen**

Nicht alle Ihre Antworten sind richtig.  
Bewertung für diese Einreichung: 0,50/0,50.  
zu b): Ihr Ergebnis ist betragsmäßig richtig, das Vorzeichen ist jedoch falsch.  
Bewertung für diese Einreichung: 0,25/0,50. Für diese Beantwortung erhielten Sie einen Punktabzug in Höhe von 0,05.

[Vorherige Seite](#) [Nächste Seite](#)

## Digitale Übungsaufgaben und Tests

Schreibtisch > viaMINT ausprobieren > Kurzer Mathe-Test für Fortgeschrittene

**Test-Navigation**

1	2	3	4	5	6
7	8	9	10	11	

[Seiten einzeln anzeigen](#) [Überprüfung beenden](#)

**viaMINT**

- [Profil](#)
- [Lernen mit viaMINT](#)
- [Info](#)
- [Impressum](#)
- [Datenschutzerklärung](#)
- [Feedback](#)
- [Logout](#)

**Frage 1**  
Nicht beantwortet  
Erreichte Punkte 0,00 von 1,00  
 Frage markieren

Ordnen Sie die folgenden Brüche durch Drag-and-Drop in aufsteigender Reihenfolge an:

$\boxed{\phantom{0}} < \boxed{\phantom{0}} < \boxed{\phantom{0}} < \boxed{\phantom{0}} < \boxed{\phantom{0}}$

$\boxed{\frac{2}{9}}, \boxed{\frac{11}{12}}, \boxed{\frac{3}{4}}, \boxed{\frac{3}{8}}, \boxed{\frac{7}{18}}$

Ihre Antwort ist leider falsch.  
Zum Vergleich der Brüche werden alle Brüche auf den kleinsten gemeinsamen Nenner, in diesem Fall 72, erweitert:  

$$\frac{2}{9} = \frac{2 \cdot 8}{9 \cdot 8} = \frac{16}{72}, \frac{3}{8} = \frac{3 \cdot 9}{8 \cdot 9} = \frac{27}{72}, \frac{7}{18} = \frac{7 \cdot 4}{18 \cdot 4} = \frac{28}{72}, \frac{3}{4} = \frac{3 \cdot 18}{4 \cdot 18} = \frac{54}{72}, \frac{11}{12} = \frac{11 \cdot 6}{12 \cdot 6} = \frac{66}{72}$$
Anschließend müssen nur noch die Zähler verglichen werden.

Die richtige Antwort lautet:  
Ordnen Sie die folgenden Brüche durch Drag-and-Drop in aufsteigender Reihenfolge an:

$\boxed{\frac{2}{9}} < \boxed{\frac{3}{8}} < \boxed{\frac{7}{18}} < \boxed{\frac{3}{4}} < \boxed{\frac{11}{12}}$

## Inhalte der Vorlesung Mathematik 1

Grundlagen

Crashkurse Differential -und Integralrechnung

Vektoren, Matrizen, Lineare Gleichungssysteme

Logik

Folgen

Komplexe Zahlen

Funktionen

Differentialrechnung

siehe

[Ablaufplan\\_Mathematik1-REE1\\_WS2223\\_21092022.pdf](#)

### 1.1.3 Literaturhinweise

Beiliegend eine Liste der für dieses Skript verwendeten Literatur in Form von Büchern oder Internetquellen. Diese Bücher und Online-Quellen können für Vertiefung der Inhalte zum Selbststudium verwendet werden.

- **Koch, Jürgen und Stämpfle, Martin**  
**Mathematik für das Ingenieurstudium**

Hanser-Verlag, 3.Auflage, September 2015 (36,00 €)

*Bemerkung: sehr übersichtlich*

- **Rießinger, Thomas**  
**Mathematik für Ingenieure**

Springer Verlag, 10.Auflage 2017 (44,99 €)

*Bemerkung: umfangreicher Stoff, netter Schreibstil, sehr kleine Schrift, ergänzendes Übungsbuch*

- **Papula, Lothar**  
**Mathematik für Ingenieure und Naturwissenschaftler - Band 1 und 2** (Ein Lehr- und Arbeitsbuch für das Grundstudium)

Verlag Vieweg, Band 1, 15.Auflage 2018 (29,99 €)

Band 2, 14.Auflage 2015 (34,99 €)

*Bemerkung: sehr ausführlich beschriebene Inhalte, Beispiele und Lösungen im Buch, Standardwerk für Ingenieure*

- **Westermann, Thomas**  
**Mathematik für Ingenieure**

Springer Verlag, 8.Auflage 2020 (44,99 €)

*Bemerkung: übersichtlich, viele Anwendungsbeispiele*

#### Online-Links:

- [www.mathe-online.at](http://www.mathe-online.at)
- [mo.mathematik.uni-stuttgart.de](http://mo.mathematik.uni-stuttgart.de)
- [www.matheprisma.de](http://www.matheprisma.de)
- <http://www-hm.ma.tum.de/integration/branch.htm>

## Literatur als freie Online-Exemplare zum Download in der Bibliothek (katalog.haw-hamburg.de)

 <b>Mathematik für Ingenieure : ein anwendungsorientiertes Lehrbuch</b> 8. Auflage	☆	<i>aus dem HAW – Netz oder über einen VPN-Zugang von zu Hause</i>
von Westermann, Thomas		
Veröffentlicht: Berlin, Springer Vieweg, [2020]	<b>Volltextzugang</b>	

 <b>Mathematik für Ingenieure : Eine Einführung mit Anwendungs- und Alltagsbeispielen</b> 2., überarb. u. erw. Aufl. 2012	☆	
von Dürrschnabel, Klaus	<b>Volltextzugang</b>	

Veröffentlicht: Wiesbaden, Imprint Vieweg+Teubner Verlag, 2012

 <b>Mathematik für Ingenieure : Eine anschauliche Einführung für das praxisorientierte Studium</b>	☆	
10., ergänzte Auflage	<b>Volltextzugang</b>	

von Rießinger, Thomas

Veröffentlicht: Berlin, Heidelberg, Springer Vieweg, [2017]

<https://katalog.haw-hamburg.de/vufind/Search/Results?lookfor=mathematik+f%C3%BCr+Ingenieure&type=AllFields&limit=20>

 <b>Mathematik für Ingenieure und Naturwissenschaftler Band 1 : Ein Lehr- und Arbeitsbuch für das Grundstudium</b> 15., überarbeitete Auflage	☆	
von Papula, Lothar	<b>Volltextzugang</b>	

Veröffentlicht: Wiesbaden, Springer Vieweg, [2018]

 <b>Mathematik für Ingenieure und Naturwissenschaftler, Band 2 : ein Lehr- und Arbeitsbuch für das Grundstudium</b> 14., überarb. und erw. Aufl.	☆	
von Papula, Lothar	<b>Volltextzugang</b>	

Veröffentlicht: Wiesbaden, Springer Vieweg, 2015

 <b>Mathematische Formelsammlung : Für Ingenieure und Naturwissenschaftler</b> 12., überarbeitete Auflage	☆	
von Papula, Lothar	<b>Volltextzugang</b>	

Veröffentlicht: Wiesbaden, Springer Vieweg, [2017]

## Vorlesung: Materialien und Didaktik



- Skript - für jedes einzelne Kapitel als pdf
- Vorbereitete Unterlagen als Lückentext für jede Vorlesung im Moodle-Raum verfügbar ....für das eigene Mitschreiben
- Vorlesungsmitschrift nach der Vorlesung als pdf im Moodle-Raum verfügbar
- Passende digitale Übungsaufgaben werden nach der Vorlesung freigeschaltet
- Links auf weitere Materialien
- Forum für Fragen

## Kontaktmöglichkeiten

- Benachrichtigungen an die Semestergruppe über das Nachrichtenforum aus dem Moodle-Kurs "Mathematik 1" auf e-assessment.haw-hamburg.de
- Meine Erreichbarkeit:  
Email: karin.landefeld@haw-hamburg.de  
Tel.: 040 -42875-8393
- Büro: Berliner Tor 7, Raum 1280  
Sprechstunde: nach Vereinbarung

## **Kapitel 1**

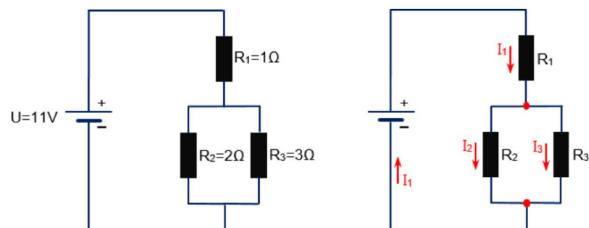
### **Einführung und Grundlagen**



Kapitel 1 Einführung und Grundlagen

## Anwendungen der Mathematik

### Elektrische Schaltungen - Bestimmung der Ströme



Mathematik:

- Vektoren und Matrizen
- Lineare Gleichungssysteme

### Transformatoren - Komplexe Wechselstromrechnung

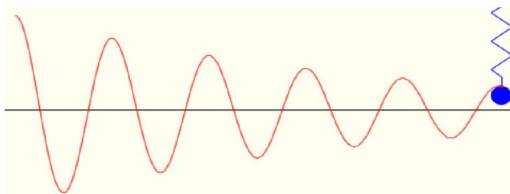


aus [https://de.wikipedia.org/wiki/Komplexe\\_Wechselstromrechnung#Anwendung\\_und\\_Verallgemeinerung](https://de.wikipedia.org/wiki/Komplexe_Wechselstromrechnung#Anwendung_und_Verallgemeinerung)

Mathematik:

- Komplexe Zahlen
- Trigonometrische Funktionen
- Rechnen mit Potenzen

### Federpendel

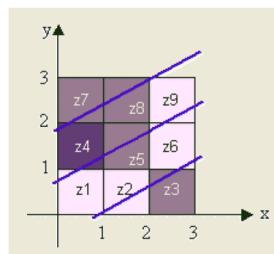
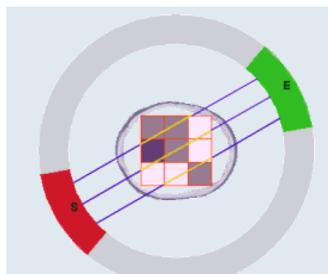


aus <http://www.matheprisma.de/Module/Schwingu/>

Mathematik:

- Harmonische Schwingungen
- Differentialgleichungen

### Computer-Tomographie



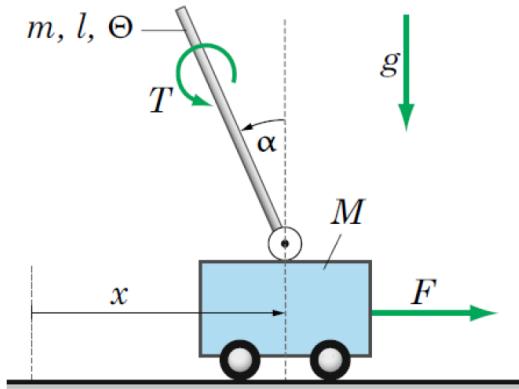
aus <http://www.matheprisma.de/Module/CT>

Mathematik:

- Lineare Gleichungssysteme
- Modellierung und numerische Lösungsverfahren

## Anwendungen der Mathematik

### Segway – Balancieren mit Differentialgleichungen

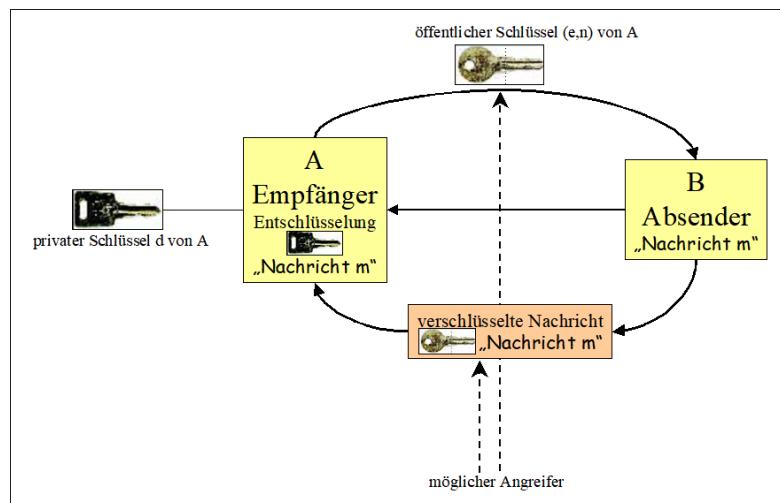


aus J. Härterich, A. Röoch, Das Mathe-Praxis-Buch, <https://www.springer.com/gp/book/9783642383052>

#### Mathematik:

- Matrizen und Lineare Gleichungssysteme
- Eigenwerte und Eigenvektoren
- Funktionen
- Differentialgleichungen
- Taylorreihen

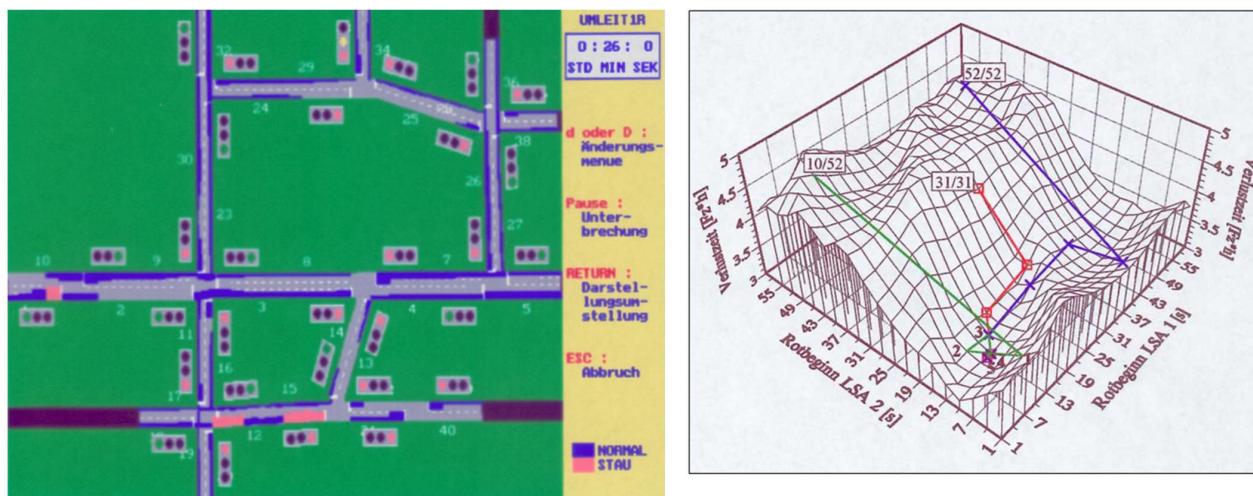
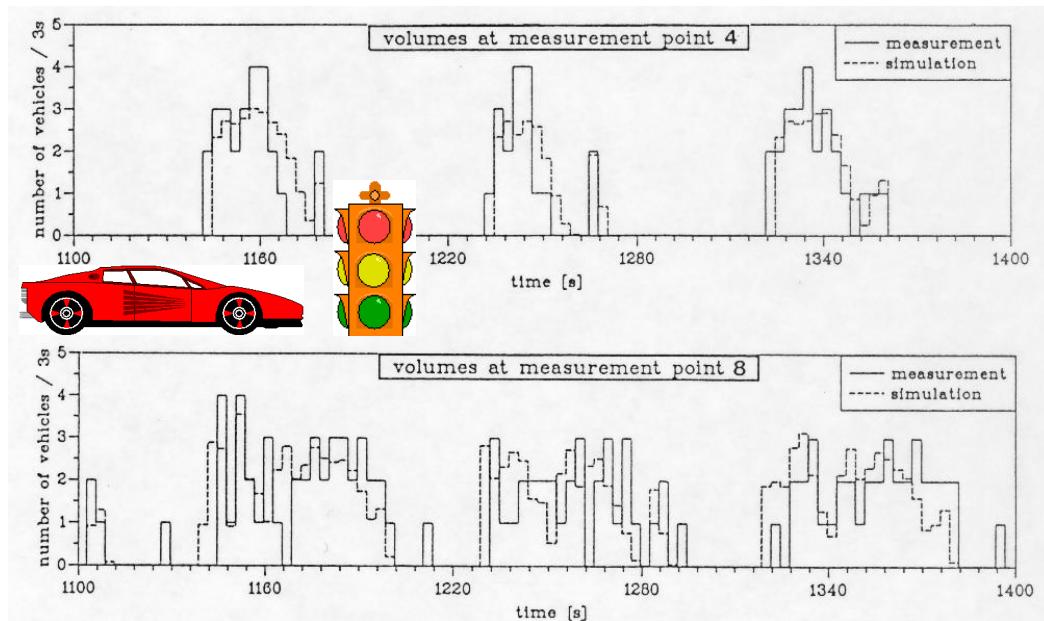
### Verschlüsselung mit dem RSA-Algorithmus



#### Mathematik:

- Primzahlen
- Grundlegende Eigenschaften natürlicher Zahlen

## Anwendungen der Mathematik



Mathematik:

- Simulation
- Differenzengleichungen
- Extremwertbestimmung

### 1.3.1 Griechische Buchstaben

	
Alpha	$\alpha$
Beta	$\beta$
Gamma	$\gamma$
Delta	$\delta$
Epsilon	$\varepsilon$
Zeta	$\zeta$
Eta	$\eta$
Theta	$\vartheta$
Kappa	$\kappa$
Iota	$\iota$
Lambda	$\lambda$
Mikron, My	$\mu$
Ny	$\nu$
Xi	$\xi$
Omekron	$\circ$
Pi	$\pi$
Rho	$\rho$
Sigma	$\sigma$
Tau	$\tau$
Ypsilon	$\upsilon$
Phi	$\phi$
Chi	$\chi$
Psi	$\psi$
Omega	$\omega$



Tabelle im Skript Kapitel Grundlagen

### 1.3.2 Zeichen und Begriffe

n-Fakultät	$n!$	$1 \cdot 2 \cdot 3 \cdot \dots \cdot n$	$4! = 1 \cdot 2 \cdot 3 \cdot 4 = 24$
n über k <i>Binomial-Koeffizient</i>	$\binom{n}{k}$	$\binom{n}{k} = \frac{n!}{(n-k)!k!}$ Anzahl k-elementiger Teilmengen einer n-elementigen Menge	$\binom{4}{2} = \frac{4!}{(4-2)!2!} = 6$
Modulo	$n \bmod m$ ( $n \% m$ )	Rest der ganzzahligen Division von n und m	$14 \bmod 4 = 2$
teilt	$n m$	n ist Teiler von m (bzw. m ist durch n ohne Rest teilbar)	$4 12$

#### Bemerkung: Rechnen mit Fakultäten

$$\frac{(n+1)!}{n!} = n+1 \text{ zum Beispiel } \frac{7!}{6!} = 7$$

$$\frac{(n+1)!}{(n-1)!} = n(n+1) \text{ zum Beispiel } \frac{10!}{8!} = 9 \cdot 10 = 90$$

#### Beispiele:

$$3! =$$

$$10! =$$

$$20! =$$

$$\frac{5!}{3!} =$$

$$\frac{123!}{122!} =$$

$$\frac{n!}{(n-2)!} =$$

**Bemerkung:** Kürzen von Fakultäten ist sehr leicht möglich.  
Es bleiben dort, wo die größere Zahl steht (Zähler oder Nenner), die höchsten Faktoren stehen und zwar so viele, wie die Differenz der beiden "Fakultätszahlen" ergibt.

### 1.3.2 Zeichen und Begriffe

Summenzeichen	$\sum$		Beispiel: Summe der Zahlen 1-4 $\sum_{i=1}^4 i = 1 + 2 + 3 + 4$
Produktzeichen	$\prod$		Beispiel: Produkt der Zahlen 1-4 $\prod_{i=1}^4 i = 1 \cdot 2 \cdot 3 \cdot 4$

#### Bemerkung: Rechenregeln mit Summen

(1) Zusammenfassen von Summen

$$\sum_{k=0}^n A(k) + \sum_{k=0}^n B(k) = \sum_{k=0}^n (A(k) + B(k))$$

(2) Multiplikation mit konstanten Elementen

$$c \cdot \sum_{k=0}^n A(k) = \sum_{k=0}^n (c \cdot A(k))$$

(3) Indexverschiebung

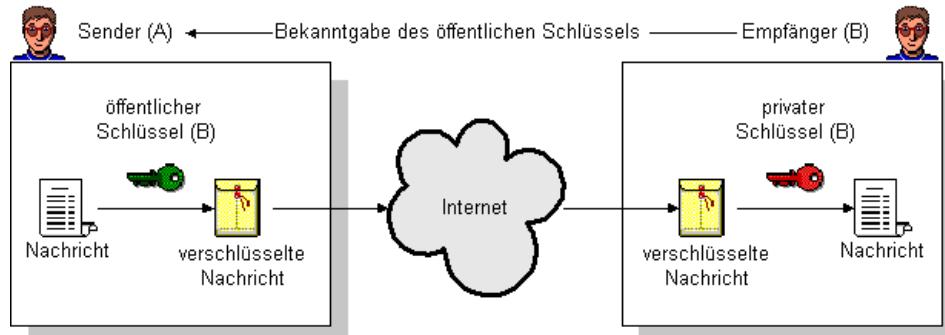
$$\sum_{k=0}^n A(k) = \sum_{k=1}^{n+1} A(k-1)$$

(4) Abspaltung des letzten Summanden

$$\sum_{k=1}^n A(k) = \left( \sum_{k=1}^{n-1} A(k) \right) + A(n)$$

## Sichere Nachrichtenübermittlung mit der Mathematik

### Verschlüsselungsalgorithmen in der Kryptographie Beispiel: RSA-Verfahren



aus ddi.cs.uni-potsdam.de

<http://www.matheprisma.de/Module/RSA/>

## Einfache Verschlüsselungen z.B. Caesar-Chiffren



<https://www.elektronik-kompendium.de/sites/net/1907041.htm>

### Aufgabe:

Wie lautet die Nachricht des verschlüsselten Textes?

x h e h u j d e h d f k w x k u j o h l v c z h l  
— e b e — a b e a c — e — e —

<http://www.matheprisma.de/Module/Caesar/index.htm>

## Einfache Verschlüsselungen z.B. Caesar-Chiffren

Mathematisches Konzept: Ein-eindeutige Zuordnung

**Aufgabe:**

Wieviel verschiedene Verschiebe-Cäsare gibt es?

- 26
- $26!$
- $26^{26}$
- sonstiges

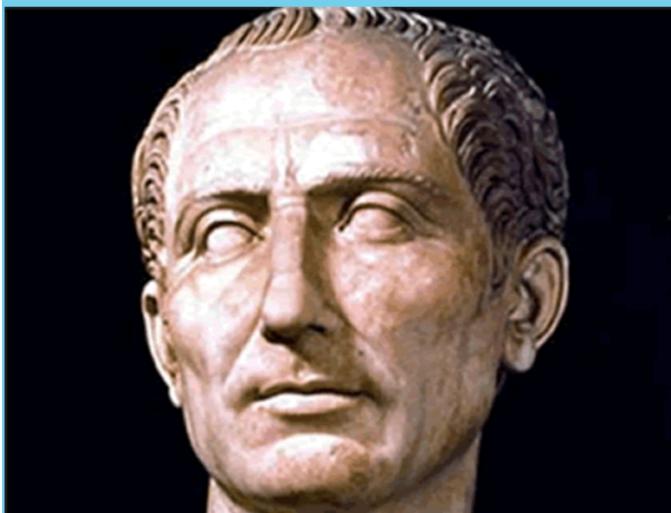
<http://www.matheprisma.de/Module/Caesar/index.htm>

### Weitere Informationen zum Caesar-Chiffren

<http://www.matheprisma.de/Module/Caesar/index.htm>

<https://www.informatik.uni-leipzig.de/~meiler/Schuelerseiten.dir/BLuebeck/caesar.html>

# Die Cäsar-Chiffrierung



Beim Cäsar-Chiffre handelt es sich um eine monoalphabetische Substitution (Vertauschung). Dabei wird jedem Buchstaben eines Textes ein anderer eindeutiger Buchstabe zugeordnet. Diese Zuordnung ist allerdings nicht willkürlich, sondern basiert auf der zyklischen Rotation (Drehung) des Alphabets um  $k$  Zeichen, dabei folgt auf Z wieder A. Das  $k$  ist dann der Schlüssel, mit dem ver- bzw. entschlüsselt wird.

Praktisch verschiebt man das Alphabet um k Zeichen (z.B. k=4):

Zur Verschlüsselung wird nun für jeden Buchstaben aus dem Klartext der darunter stehende Buchstabe aus dem Geheimtext eingesetzt. Beim Entschlüsseln geht man umgekehrt vor und schreibt für jeden Buchstaben des Geheimtextes den entsprechenden Buchstaben des Klartextes. (Satz-, Leer- und Sonderzeichen werden nicht berücksichtigt.)

Mathematisch entspricht diese Verschlüsselung einer buchstabenweisen "Addition" der Schlüssel-Zahl  $k$  zu jedem Buchstaben des Klartextes. Entsprechend muss für die Entschlüsselung die Schlüssel-Zahl vom Geheimtext abgezogen werden, um wieder den Klartext zu erhalten.

#### Vorabklärungen

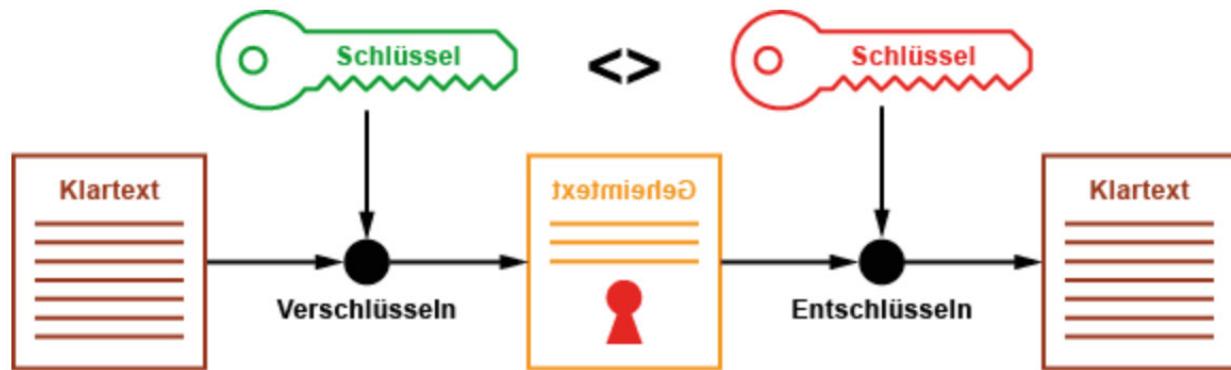
Verschluss  
KLARTEXT  
+ 44444444  
= OPEVXTBV

Um aus dem Geheimtext den Klartext zu erhalten, muss der Empfänger wissen, mit welchem Schlüssel k verschlüsselt wurde. Durch Umkehrung des Algorithmus - bei Benutzung des richtigen Schlüssels - ergibt sich dann wieder der Klartext.

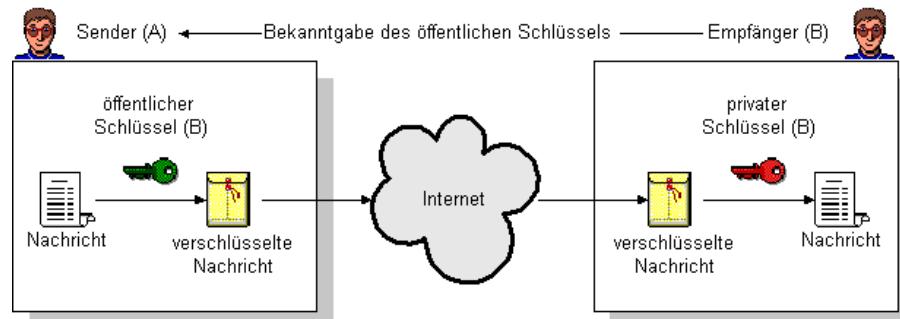
### **Entschlüsseln:**

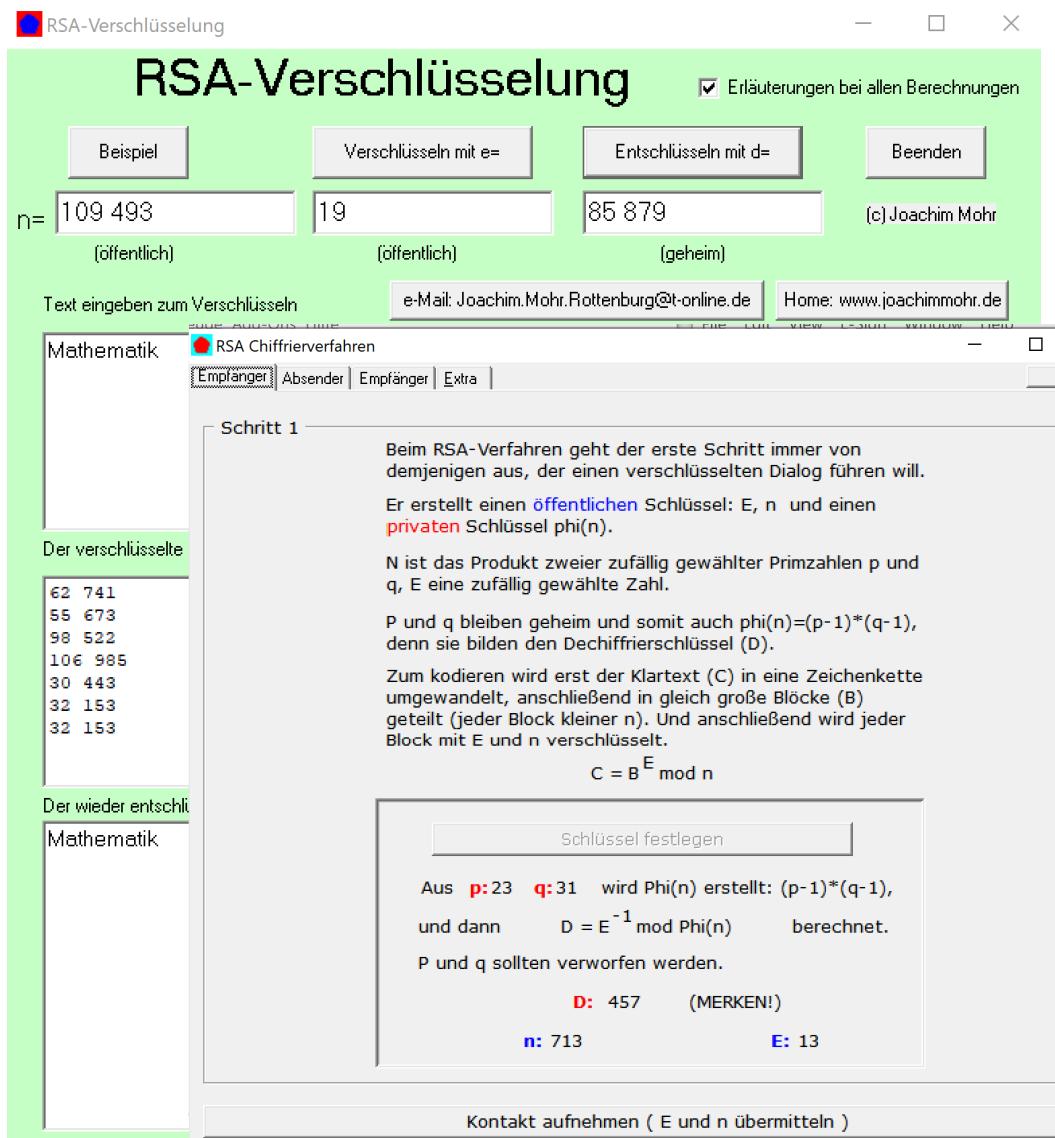
ENSCHEID  
OPEVXIBV  
- 44444444  
≡ KLARTEXT

**Asymmetrische Verschlüsselung/ Public-Key-Verfahren  
z.B. RSA-Verfahren**



<https://www.elektronik-kompendium.de/sites/net/1907041.htm>





## Der RSA-Algorithmus

1. [Einleitung](#)
2. [Was ist RSA, was leistet RSA?](#)
3. [Wie funktioniert RSA?](#)
  - 3.1 [Grundlagen](#)
    - 3.1.1 [Satz von Euler](#)
    - 3.1.2 [Euklidischer Algorithmus](#)
  - 3.2 [Schlüsselerzeugung](#)
  - 3.3 [Verschlüsselung](#)
  - 3.4 [Entschlüsselung](#)
  - 3.5 [Signatur](#)
  - 3.6 [Erläuterndes Beispiel](#)
4. [Vor- und Nachteile](#)
5. [Anwendungsbereiche des RSA - Algorithmus](#)
6. [Beispielprogramm "RSA - Algorithmus"](#)
7. [Biographien der Entwickler](#)
8. [Literaturverzeichnis](#)

[https://www.zum.de/Faecher/Inf/RP/infschul/kr\\_rsa.html#programm](https://www.zum.de/Faecher/Inf/RP/infschul/kr_rsa.html#programm)

Person A	Person B
<p><b>1) Schlüsselbildung</b></p> <p><b>Wahl von Primzahlen</b></p> <p><math>p_A = 23</math>  <math>q_A = 13</math>  (in der Realität mindestens 100 Stellen)</p> <p><b>Berechnung</b></p> <p><math>n_A = p_A * q_A = 23 * 13 = 299</math>  <math>\varphi(n_A) = (p_A - 1) * (q_A - 1) = 22 * 12 = 264</math></p> <p><b>Wahl</b></p> <p><math>e_A = 5</math>  (<i>gewählt mit den Bedingungen:</i>  <math>1 &lt; e_A &lt; 264 \wedge \text{ggT}(e_A, 264) = 1</math>)</p> <p><b>Berechnung</b></p> <p><math>d_A</math> so, dass <math>e_A * d_A \text{ mod } \varphi(n_A) = 1</math>  <math>(5 * d_A) \text{ mod } 264 = 1 \Rightarrow d_A = 53</math></p> <p><b>Schlüssel</b></p> <p>öffentlicher Schlüssel: <math>(e_A, n_A) = (5, 299)</math>  privater Schlüssel : <math>d_A = 53</math></p>	
<p><b>2) Schlüsselverteilung</b></p> <p>öffentlicher Schlüssel: <math>(e_A, n_A) = (5, 299)</math> </p>	
	<p><b>3) Verschlüsselung</b></p> <p>Verschlüsselung der Nachricht  <i>Nachricht m = 99</i></p> <p>Formel: <math>c = m^{e_A} \text{ mod } n_A</math>  <math>c = 99^5 \text{ mod } 299 = 86</math>  <i>verschlüsselte Nachricht c = 86</i></p> <p> verschlüsselte Nachricht <math>c</math> wird an A übertragen</p>
<p><b>4) Entschlüsselung</b></p> <p>Verwendung des  privaten Schlüssel : <math>d_A = 53</math></p> <p>und des  öffentlichen Schlüssel: <math>(e_A, n_A) = (5, 299)</math></p> <p><math>m = c^{d_A} \text{ mod } n_A</math>  <math>m = 86^{53} \text{ mod } 299 = 99</math></p> <p>entschlüsselte Meldung ist: <math>m = 99</math></p>	

**Begriffe zur Klärung  
für den RSA-Algorithmus**

**Primzahlen**

**größter gemeinsamer Teiler**

**teilerfremd**

**modulo**

.

**Definition 1.1: Teiler und Vielfaches**

Eine Zahl  $a \in \mathbb{Z}$  heißt **durch**  $b \in \mathbb{Z}, b \neq 0$  **teilbar**,  
wenn es eine ganze Zahl  $q \in \mathbb{Z}$  gibt, so dass  $a = b \cdot q$  ist.

Diese Eigenschaft kann gesprochen über verschiedene Sätze ausgedrückt werden:

„in Zeichen  $b | a$ , gesprochen  $b$  teilt  $a$ “

„ $b$  ist ein **Teiler von**  $a$ .“

„ $a$  ist ein **Vielfaches von**  $b$ “

„Die Zahl  $b$  passt genau  $q$  - mal in die Zahl  $a$ .“

**Beispiel:**

$28$  ist durch  $7$  teilbar

$7$  teilt  $28$ , geschrieben  $7 | 28$

$28 = 7 \cdot 4$  "7 passt genau 4-mal in die 28"

**Satz 1.1: Teilbarkeitsregeln**

1. Gilt  $c | b$  und  $b | a$ , so gilt auch  $c | a$  :
2. Gilt  $b_1 | a_1$  und  $b_2 | a_2$ , so gilt auch  $b_1 b_2 | a_1 a_2$

**Beispiel:**

1.  $3 | 6$  und  $6 | 18 \Rightarrow 3 | 18$

2.  $3 | 6$  und  $4 | 8 \Rightarrow 12 | 48$

.

**Definition 1.2: Division mit Rest**

Für zwei ganze Zahlen  $a, b \in \mathbb{Z}$  mit  $b \neq 0$  gibt es genau eine Darstellung

$$a = b \cdot q + r \text{ mit } q, r \in \mathbb{Z} \text{ und } 0 \leq r < b, \text{ falls } b > 0 \\ \text{und } 0 \leq r < -b, \text{ falls } b < 0.$$

$a$  heißt Dividend,  $b$  Divisor  
und  $r$  Rest der ganzzahligen Division von  $a$  durch  $b$ .

**Definition 1.3: modulo, Rest der ganzzahligen Division**

$a \bmod b$  ist der Rest, den  $a$  bei der Division durch  $b$  lässt,

d.h. wenn  $a = b \cdot q + r$  mit  $q, r \in \mathbb{Z}$  und  $0 \leq r < b$

so ist  $a \bmod b = r$ .

**Beispiel:**

$$9 \bmod 2 = 1 \Leftrightarrow 9 = 2 \cdot 4 + 1$$

1 ist der Rest der ganzzahligen Division von 9 durch 2.

# Teilbarkeitsregeln

**Teilbar durch 2:**

<https://www.gut-erklaert.de/mathematik/teilbarkeitsregeln-mathematik.html>

Eine Zahl ist durch 2 teilbar wenn sie eine **gerade Zahl** ist.

**Teilbarkeit durch 3:**

Eine Zahl ist durch 3 teilbar, wenn ihre Quersumme durch 3 teilbar ist.

**Teilbar durch 4:**

Eine Zahl ist durch 4 teilbar, wenn die letzten beiden Stellen der Zahl durch 4 teilbar sind.

**Teilbar durch 5:**

Eine Zahl ist durch 5 teilbar, wenn die letzte Stelle eine 0 oder 5 ist.

**Teilbarkeit durch 6:**

Eine Zahl ist durch 6 teilbar wenn diese durch 2 und durch 3 teilbar sind.

**Teilen durch 7:**

Es gibt viele Teilbarkeitsregeln für die Zahl 7. Keine davon ist ganz einfach. Folgende Variante halte ich für am leichtesten und rechne dazu ein Beispiel vor

**Beispiel mit 2268:**

Wir teilen die Zahl immer in zwei Teile auf. Die letzte Ziffer (rot) und einfach alles was davor ist (blau).

- 161

Wir multiplizieren die letzte Stelle mit 2:

- $1 \cdot 2 = 2$

Von dem vorderen Teil der Zahl (16) ziehen wir dieses Ergebnis (2) ab.

- $16 - 2 = 14$

Ist dieses Ergebnis (14) durch 7 ohne Rest teilbar ist auch 161 ohne Rest durch 7 teilbar. Dies ist hier der Fall.

**Teilbarkeit durch 8:**

Eine Zahl ist durch 8 teilbar, wenn die letzten drei Stellen durch 8 teilbar sind.

**Teilbar durch 9:**

Eine Zahl ist durch 9 teilbar, wenn die Quersumme durch 9 teilbar ist.

**Teilbar durch 10, 100, 1000:**

Eine Zahl ist durch 10 teilbar, wenn diese auf 0 endet.

## Modulo - Berechnung

$a \bmod b$  (oder in C-Syntax `%`) gibt den Rest der ganzzahligen Division von  $a$  geteilt durch  $b$  an.

### Anwendung: modulo bei der Quersummenberechnung

- Algorithmus zur Berechnung der Quersumme
- spaltet von hinten die einzelnen Ziffern mit Hilfe der modulo-Berechnung ( $\bmod 10$ ) ab.
- Algorithmus: Quersumme der Zahl  $x$  berechnen  
solange bis  $x = 0$   
 $\text{rest} = x \bmod 10$   
 $\text{summe} = \text{summe} + \text{rest}$   
 $x = x / 10$  (ganzzahlige Division)

### Beispiel:

$x=123$

$123 \% 10 \Rightarrow$  Ziffer 3    rest=3    summe =3

$123 / 10$  (ganzzahlig)     $\Rightarrow$      $x=12$

$12 \% 10 \Rightarrow$  Ziffer 2    rest=2    summe =3+2=5

$12 / 10$  (ganzzahlig)     $\Rightarrow$      $x=1$

$1 \% 10 \Rightarrow$  Ziffer 1    rest=1    summe =3+2+1=6

$1 / 10$  (ganzzahlig)     $\Rightarrow$      $x=0$

*Ende*

**Aufgabe:**

Wenn der 45. Tag eines Jahres ein Sonntag ist,  
welcher Wochentag ist dann der 210. Tag desselben Jahres?

## Größter gemeinsamer Teiler

Der **größte gemeinsamer Teiler**, kurz **ggT**, ist die größte natürliche Zahl, die zwei oder mehrere ganze Zahlen ohne Rest teilt. Nachfolgend sind einige Definitionen dargestellt, die diese Eigenschaft formal beschreiben.

### Definition 1.4: größter gemeinsamer Teiler ggT

Sind  $a, b, d \in \mathbb{Z}$  und gilt  $d | a$  und  $d | b$ ,  
so heißt  $d$  **gemeinsamer Teiler** von  $a$  und  $b$ .

Wenn für jeden anderen gemeinsamen Teiler  $c$  von  $a$  und  $b$  gilt:  $c | d$ ,  
so heißt  $d$  **größter gemeinsamer Teiler** von  $a$  und  $b$   
und wird mit  $d = \text{ggt}(a, b)$  bezeichnet.



### Beispiele:

(1)  $\text{ggT}(12, 18) = 6$ , denn  $6 | 12$  und  $6 | 18$

2 und 3 sind weitere Teiler von 12 und 18, aber beides sind kleinere Zahlen und  
sind als Faktor in der 6 enthalten, denn  $2 | 6$  und  $3 | 6$ .

Es gibt keine größere Zahl als 6, die sowohl 12 als auch 18 teilt.

(2)  $\text{ggT}(100, 20) = 20$ ,

(3)  $\text{ggT}(-4, 14) = 2$

(4)  $\text{ggT}(3, 8) = 1$

### Bemerkung:

- Ist der  $\text{ggT}(a, b) = 1$ , so heißen die Zahlen teilerfremd.
- Ist der  $\text{ggT}(a, b) = b$ , so ist  $a$  ein Vielfaches von  $b$

## Euklidischer Algorithmus

**Satz 1.2:**

Seien  $a$  und  $b$  ganze Zahlen mit  $a \neq 0$ . Seien  $q$  und  $r$  Zahlen, für die gilt:  $b = q \cdot a + r$ .

Dann gilt  $\text{ggT}(b,a) = \text{ggT}(a,r)$ .

**Euklidischer Algorithmus zur Berechnung des ggT:**

Der ggT kann mittels des Euklidischen Algorithmus berechnet werden.

Eingangsgrößen sind zwei natürliche Zahlen  $a$  und  $b$ . Bei der Berechnung verfährt man nach Euklid wie folgt:

1. setze  $m = a; n = b$
2. ist  $m < n$ , so vertausche  $m$  und  $n$
3. berechne  $r$  mit  $m = q \cdot n + r$  (d.h.  $r$  ist Rest der ganzzahligen Division)
4. setze  $m = n, n = r$
5. ist  $r \neq 0$  fahre fort mit Schritt 2, ist  $r=0$ , dann ist  $m$  der gesuchte ggT

Nach Ablauf des Verfahrens hat man **mit  $m$  den ggT von  $a$  und  $b$  gefunden**.


**Beispiel des Euklidischen Algorithmus:**

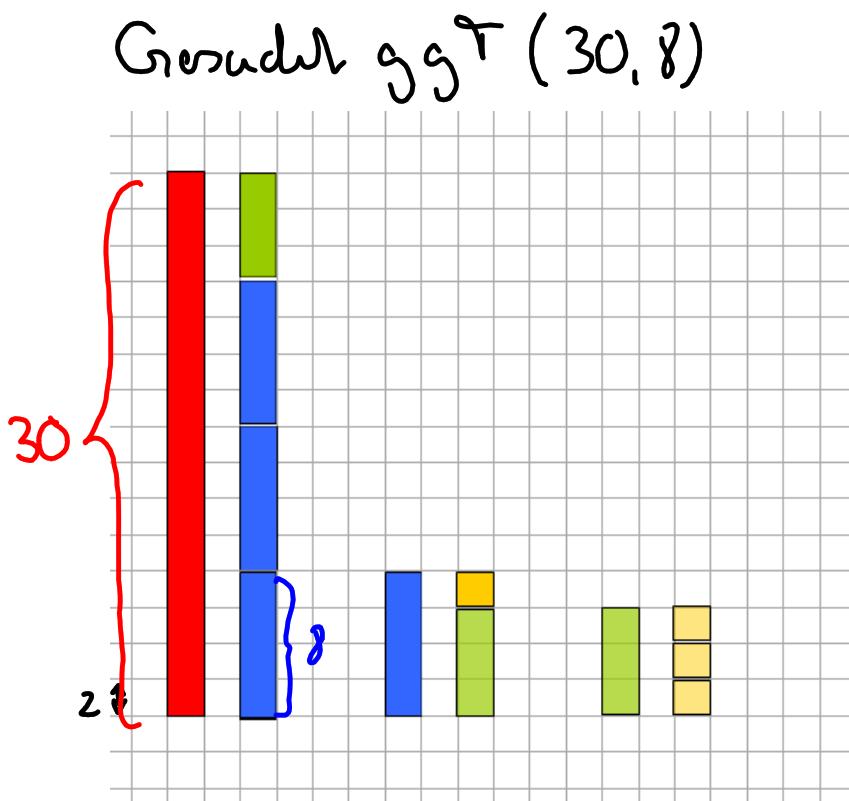
*Bestimmung des ggT von  $a = 105$  und  $b = 63$*

$m$	$n$	$q$	$r$
105	63		
105	63	1	42
63	42	1	21
42	21	2	0
<span style="border: 1px solid black; padding: 2px;">21</span>			

21 ist der ggT von 63 und 105

## Erläuterungen zum Euklidischen Algorithmus

Warum funktioniert das so?



## Algorithmus zur Berechnung des größten gemeinsamen Teilers(ggT) zweier Zahlen

### 6.8.5 Der ggT - erweiterter Euklidsche Algorithmus

Der Algorithmus

$$\begin{aligned}
 792 &= 10 \cdot 75 + 42 \\
 75 &= 1 \cdot 42 + 33 \\
 42 &= 1 \cdot 33 + 9 \\
 33 &= 3 \cdot 9 + 6 \\
 9 &= 1 \cdot 6 + 3 \\
 6 &= 2 \cdot 3 + 0
 \end{aligned}$$

Das Beispiel zeigt, wie man mit Hilfe des Euklidschen Algorithmus' den ggT(792,75) bestimmt.

Im ersten Schritt fragen wir, wie häufig die zweite Zahl, also 75 ganzzahlig in der ersten, nämlich 792 enthalten ist. Diese Ganzzahldivision liefert 10 und den Rest 42. Im weiteren Verlauf werden wir sehen, dass die Zahl 10 für den weiteren Verlauf unwichtig ist, also getrost vergessen werden kann. Wesentlich ist, wir berechnen 792 mod 75 und das ist 42. Im zweiten Schritt fragen wir: Wie groß ist der Rest, wenn wir 75 ganzzahlig durch 42 teilen. Wir bestimmen also 75 mod 42. Diese Schritte wiederholen sich.

Somit berechnen wir nacheinander:

$$\begin{aligned}
 792 \bmod 75 &= 42 \\
 75 \bmod 42 &= 33 \\
 42 \bmod 33 &= 9 \\
 33 \bmod 9 &= 6 \\
 9 \bmod 6 &= 3 \\
 6 \bmod 3 &= 0
 \end{aligned}$$

Ist der Rest 0, ist der Algorithmus zu Ende. 3 ist der gesuchte größte gemeinsame Teiler. Da garantiert werden kann, dass der Rest irgendwann 0 ist, sagen wir, der Algorithmus terminiert.

allgemeine  
Darstellung

Zu bestimmen ist ggT(a,b)

Wir setzen  $r_0 = a$  und  $r_1 = b$ ; und bestimmen

1. Schritt

$$r_0 \bmod r_1 =: r_2$$

2. Schritt

$$r_1 \bmod r_2 =: r_3$$

3. Schritt

$$r_2 \bmod r_3 =: r_4$$

i-ter Schritt

$$r_{i-1} \bmod r_i =: r_{i+1}$$

n-ter und letzter Schritt. Er ist dadurch gekennzeichnet, dass der Rest 0 ist.

$$r_{n-1} \bmod r_n = 0$$

$r_n$  ist der gesuchte ggT(a,b)

## Euklidischer Algorithmus

### Weiteres Beispiel

Beispiel:

gesucht sei ggT(969, 627)

$$969 = 1 \cdot 627 + 342$$

$$627 = 1 \cdot 342 + 285$$

$$342 = 1 \cdot 285 + 57$$

$$285 = 5 \cdot 57 + 0$$

Damit ist man fertig:  $\text{ggT}(969, 627) = 57$

<http://www.zum.de/Faecher/Materialien/dorner/manuskripthtml/diogl1/euklidalg.html>

## Kleinstes gemeinsames Vielfaches

Das **kleinste gemeinsame Vielfache**, kurz **kgV**, ist die kleinste natürliche Zahl, die zwei oder mehrere ganze Zahlen ohne Rest teilt. Nachfolgend sind einige Definitionen dargestellt, die diese Eigenschaft formal beschreiben.

### Definition 1.5: kleinste gemeinsames Vielfaches kgV

Sind  $a, b, d \in \mathbb{Z}$

Ein Zahl  $d \in \mathbb{Z}$  heißt **kleinstes gemeinsames Vielfaches** von  $a$  und  $b$ , bezeichnet  $kgV(a, b)$  wenn folgende Bedingungen erfüllt sind:

- (1) Sowohl  $a$  als auch von  $b$  sind Teiler von  $d$  :  $a | d$  und  $b | d$
- (2) Es gibt keine kleinere Zahl, für die die Eigenschaft (1) erfüllt ist.

### 1.4.3 Primzahlen und Primfaktorzerlegung

#### Definition 1.6: Primzahl

Eine natürliche Zahl  $p$  wird eine Primzahl genannt, falls  $p > 1$  ist und 1 und  $p$  die einzigen natürlichen Zahlen sind, die  $p$  teilen.

#### Definition 1.7: Primfaktorzerlegung

Unter der **Primfaktorzerlegung**, auch als **Zerlegung in Primfaktoren** bezeichnet, versteht man die Darstellung einer natürlichen Zahl  $a \in \mathbb{N}$  als Produkt von Primzahlen

$$a = p_1 \cdot p_2 \cdot p_3 \cdot \dots \cdot p_n \quad \text{mit Primzahlen } p_1, p_2, p_3, \dots, p_n, n \in \mathbb{N}$$

Die in der Primfaktorzerlegung einer Zahl auftretenden Primzahlen  $p_1, p_2, p_3, \dots, p_n$  nennt man die **Primfaktoren** dieser Zahl.

#### → Beispiele:

$$1200 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5 = 2^4 \cdot 3 \cdot 5^2 \quad \text{mit Primfaktoren 2, 3, 5}$$

$$6936 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 17 \cdot 17 = 2^3 \cdot 3 \cdot 17^2 \quad \text{mit Primfaktoren 2, 3, 17}$$

#### Satz 1.3: Fundamentalsatz der Arithmetik

Der **Fundamentalsatz der Arithmetik** besagt, dass jede natürliche Zahl eine Primfaktorzerlegung besitzt und dass diese, bis auf die Reihenfolge der Faktoren, eindeutig ist.

**Satz 1.4: Primfaktzerlegung zur Berechnung des ggT und des kgV**

Den größten gemeinsamen Teiler ggT und auch das kleinste gemeinsame Vielfache kgV kann man auch aus der Primfaktzerlegung von  $a$  und  $b$  bestimmen.

Für den **ggT(a,b)** verwendet man **alle Primfaktoren, die  $a$  und  $b$  gemeinsam haben**, und multipliziert diese. („Schnittmenge der Primfaktoren“)

Kommen Faktoren mit einem Exponenten vor, wird jeweils der kleinste Exponent genommen.

Für das **kgV(a,b)** wird **jeder Primfaktor mit dem jeweils höchsten Exponenten** verwendet, und anschließend multipliziert. („Obermenge der Primfaktoren“)

Kommen Faktoren mit einem Exponenten vor, wird jeweils der **größte Exponent** genommen.

→ **Beispiel:**

$$a = 63 = 3 \cdot 3 \cdot 7$$

$$b = 105 = 3 \cdot 5 \cdot 7$$

$$\text{ggT} (63, 105) = 3 \cdot 7 = 21$$

$$\text{kgV} (63, 105) = 3 \cdot 3 \cdot 5 \cdot 7 = 315$$

**Satz 1.5: ggT und kgV**

Für zwei Zahlen  $a, b \in \mathbb{N}$  gilt der folgende Zusammenhang für den größten gemeinsamen Teiler ggT(a,b) und kgV(a,b):

$$\text{kgV}(a, b) = \frac{a \cdot b}{\text{ggT}(a, b)}$$

→ **Beispiel:**

$$a = 63 = 3 \cdot 3 \cdot 7$$

$$b = 105 = 3 \cdot 5 \cdot 7$$

$$\text{ggT} (63, 105) = 3 \cdot 7 = 21$$

$$\text{kgV} (63, 105) = \frac{63 \cdot 105}{21} = \frac{3 \cdot 3 \cdot 7 \cdot 3 \cdot 5 \cdot 7}{3 \cdot 7} = 315$$

**Weiteres Beispiel**

$$1200 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5 = 2^4 \cdot 3 \cdot 5^2$$

$$6936 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 17 \cdot 17 = 2^3 \cdot 3 \cdot 17^2$$

**Aufgaben**

**Frage : "Thema Prímfaktoren"**

**Auf wie viele Nullen endet das Produkt der Zahlen 1 bis 100?**

- a) 2
- b) 10
- c) 15
- d) 20
- e) 24
- f) 100

Frage: Die Schatzkiste ("Thema Teilbarkeit")



**Sensationsfund am Strand von Honolulu!**

Es wurde eine Kiste angespült, in der sich laut Zeugenaussagen zahllose Goldmünzen befanden. Darüber, wie groß der Schatz tatsächlich ist, herrscht zur Stunde noch Verwirrung.

"In die Kiste passen allerhöchstens 400 Münzen", sagte einer der glücklichen Finder, "wir haben sie abgezählt. Erst paarweise, dabei blieb ein Goldstück übrig. Dann in Dreiergruppen, wobei wieder eines übrig war. Ebenso in Vierer-, Fünfer- und Sechsergruppen. Erst als wir jeweils Siebener-Stapel bildeten ging es auf."

Wie viele Münzen können es demnach nur sein?

.