

# Chinese Remainder Theorem

Timo Grautstück

18. Juni 2020

# Inhaltsverzeichnis

<b>1</b>	<b>Einleitung</b>	<b>3</b>
<b>2</b>	<b>Kongruenzen und Restklassen</b>	<b>4</b>
2.1	Kongruenzen . . . . .	4
2.2	Restklassen . . . . .	5
2.3	Veranschaulichung von Restklassen . . . . .	5
<b>3</b>	<b>Ringe und Körper</b>	<b>6</b>
3.1	Axiome . . . . .	6
3.2	algebraische Strukturen . . . . .	6
3.3	Ringe . . . . .	6
3.4	Körper . . . . .	7
3.5	Restklassenring . . . . .	7
3.5.1	Verknüpfungstabelle (Addition) . . . . .	7
3.5.2	Verknüpfungstabelle (Multiplikation) . . . . .	8
<b>4</b>	<b>Chinese Remainder Theorem</b>	<b>10</b>
4.1	großzahlige Modulooperationen . . . . .	10
<b>5</b>	<b>Euklidischer Algorithmus</b>	<b>11</b>
5.1	Algorithmus . . . . .	11
5.2	erweiterter Algorithmus . . . . .	11
<b>6</b>	<b>Permutation</b>	<b>12</b>
6.1	identische Abbildung . . . . .	12
6.2	Schreibweisen . . . . .	13
6.2.1	Zweizeilenform . . . . .	13
6.2.2	Tupelschreibweise . . . . .	13
6.2.3	Zyklenschreibweise . . . . .	13

# 1 Einleitung

Das “Chinese Remainder Theorem” im Deutschen unter anderem als chinesischer Restklassensatz bezeichnet, ist ein Theorem der abstrakten Algebra und Zahlentheorie. Die erste Schrift des Theorems stammt von dem chinesischen Mathematiker Sun Zi aus seinem damaligen Buch “Sun Zis Handbuch der Arithmetik” ca. 3. Jahrhundert. Man nutzt das Theorem unter anderem, um großzahlige Modularechnungen mittels mehrerer kleinzahliger Berechnungen zu bestimmen oder zur Berechnung simultaner Kongruenzen.

## 2 Kongruenzen und Restklassen

Der Chinesische Restklassensatz funktioniert, indem man eine Rechenoperation Namens Modulo nutzt (*Division mit Rest*). Um das ganze besser zu verstehen, sollte man einige grundlegende Begriffe klären, wie Kongruenz oder Restklassen.

### 2.1 Kongruenzen

**Definition 2.1.1.** Ist  $m \in \mathbb{N}$  und  $a, b \in \mathbb{Z}$  kann man sagen, dass  $a$  kongruent zu  $b$  modulo  $m$  ist, wenn  $m$  die Differenz  $b - a$  teilt.

$$a \equiv b \pmod{m}$$

Beispiel 2.1.2.

$$10 \equiv 0 \pmod{5}, \quad 12 \equiv 2 \pmod{5}$$

---

Teilt  $m$  jedoch  $b - a$  nicht, so bezeichnet man  $a$  inkongruent zu  $b$  modulo  $m$ . Um die Definition zu unterstützen, würde ich den Vorgang der modulo Operation wie folgt beschreiben:

Sei eine Zahl 22 gegeben und diese entspricht  $a$ . Soll nun  $a$  modulo 7 berechnet werden, entspricht  $m = 7$ . Nun ist die Frage welche Zahl entspricht  $b$  bzw. 22 ist kongruent welcher Zahl modulo 7.

$$22 \equiv b \pmod{7}$$

**Lemma 2.1.3.**

1. Wie oft passt  $m$  in  $a$  ?
2. Wenn  $m$ ,  $a$  nicht ganzzahlig teilt, welcher Rest bleibt über ?
3. Falls ein Rest existiert, ist dieser Rest  $b$ , existiert kein Rest entspricht  $b = 0$ .

Beispiel 2.1.4.

1.  $3 \cdot 7 = 21$
2.  $22 - 21 = 1$
3.  $22 \equiv 1 \pmod{7}$

Man bezeichnet 22 als Representant der Restklasse  $\bar{1}$  auf  $\mathbb{Z}_7$ , genau wie  $\{\dots, -8, 1, 8, 14, \dots\}$

## 2.2 Restklassen

Da jetzt klar ist, dass man sich bei Modulo für Reste interessiert, kann man nun auf Restklassen schauen. Wenn man von dem vorherigen Beispiel ausgeht, dass  $m$  7 entspricht, dann sei die Menge von  $\mathbb{Z}_7 := \{0, 1, 2, 3, 4, 5, 6\}$ . Diese Menge entspricht auch den Restklassen von  $\mathbb{Z}_7$ . Um Restklassen darzustellen, wird in diesem Dokument folgende Notation  $\bar{b}$  genutzt. Restklassen enthalten unendlich viele Elemente, jedoch enthalten zwei unterschiedliche Restklassen von einem bestimmten Modul  $m$ , niemals die selben Elemente. Jedoch ihr eigenes Element.

**Definition 2.2.1.** Sei  $m \in \mathbb{N}$  und  $b \in \mathbb{Z}$ , dann bezeichnet man die folgende Menge  $\bar{b} := \{a \in \mathbb{Z} \mid a \equiv b \pmod{m}\}$  als Restklasse von  $\mathbb{Z}_m$  und  $\forall a \in \bar{b}$  als Representant von  $\bar{b}$ .

Beispiel 2.2.2.

$$\bar{0} := \{\dots, -21, -14, -7, 0, 7, 14, 21, \dots\}$$

## 2.3 Veranschaulichung von Restklassen

-21	-20	-19	-18	-17	-16	-15
-14	-13	-12	-11	-10	-9	-8
-7	-6	-5	-4	-3	-2	-1
$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27

Nun kann man vertikal die jeweilig enthaltenden Elemente *Representanten* der unterschiedlichen Restklassen erkennen. Wenn man das nun mit der vorherigen Definition 2.1.1 prüft, sollte gelten, dass  $\forall a \in \bar{b}$ ,  $m$  Teiler von  $b - a$  ist.

*Beweis.*  $a = -21$ ,  $b = 0$ ,  $m = 7$

$$-21 \equiv 0 \pmod{7} \quad (2.1)$$

$$= 0 - (-21) = 21 \quad (2.2)$$

$$= 21/7 = 3 \quad \square$$

Man kann 21 durch 7 ganzzahlig teilen, also gilt auch 2.1.1 und wie in 2.1.3 zu sehen, dass  $b = 0$  sein muss. Man nennt die Menge aller Restklassen von  $\mathbb{Z}_m \rightarrow R_m$ .

$R_m \neq \mathbb{Z}_m$ , da  $R_m$  die Mengen der Restklassen enthält und  $\mathbb{Z}_m$  die Vereinigung der Mengen der Restklassen.

## 3 Ringe und Körper

Ringe und Körper sind algebraische Strukturen. Mengen  $G$  bilden diese Strukturen durch Einhalten von verschiedenen Axiomen mit mathematischen Operationen  $\circ \rightarrow (\oplus, \otimes)$ .

$$(G, \circ)$$

### 3.1 Axiome

**Lemma 3.1.1.**

1. *Abgeschlossenheit:*  $[x \circ y \in G]$
2. *Assoziativität:*  $(x \circ y) \circ z = x \circ (y \circ z)$
3. *Neutrales Element:*  $[e \in G] : e \circ x = x$
4. *Inverses Element:*  $[\exists x^{-1} \in G] : \forall x \in G : x \circ x^{-1} = e$
5. *Kommutativität:*  $x \circ y = y \circ x$

### 3.2 algebraische Strukturen

- 1, 2  $\rightarrow$  Halbgruppe
- 1, 2, 3  $\rightarrow$  Monoid (Halbgruppe mit 1.)
- 1, 2, 3, 4  $\rightarrow$  Gruppe
- 1, 2, 3, 4, 5  $\rightarrow$  Kommutativegruppe

### 3.3 Ringe

**Definition 3.3.1.** Eine Menge  $(G, \circ)$  nennt man *Ring*, wenn die folgenden Axiome mittels Multiplikation und Addition erfüllt werden:

1.  $(G, \oplus)$  ist kommutative Gruppe mit neutralem Element 0.
2.  $(G, \otimes)$  ist Halbgruppe.
3. *Distributivität:*  $x \cdot (y + z) = x \cdot y + x \cdot z$

### 3.4 Körper

**Definition 3.4.1.** Ein Körper ist ein kommutativer Ring mit Einselement, in dem jedes von Null verschiedene Element invertierbar ist. Es müssen folgende Axiome erfüllt werden:

1.  $(G, \oplus)$  ist kommutative Gruppe mit neutralem Element 0.
  2.  $(G \setminus \{0\}, \otimes)$  ist kommutative Gruppe mit neutralem Element 1.
  3. Distributivität:  $x \cdot (y + z) = x \cdot y + x \cdot z$
- 

### 3.5 Restklassenring

Ein Restklassenring ist ein Faktoring, der aus Restklassen besteht.

#### 3.5.1 Verknüpfungstabelle (Addition)

Durch Verknüpfungstabellen, kann man sehr gut veranschaulichen, welche Restklassen existieren und was es für neutrale bzw. inverse Elemente gibt.

$(\mathbb{Z}_4, \oplus)$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$(\mathbb{Z}_5, \oplus)$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Nun erkennt man, dass das Neutrale Element, wie im Unterpunkt 3. (Axiome 3.1) beschrieben, für die Addition auf dem Modul  $\mathbb{Z}_4$  die Null ist.

*Beweis.*

$$\begin{aligned} 0 \in \mathbb{Z}_4 : 0 + 1 &\equiv 1 \pmod{4} \\ 0 \in \mathbb{Z}_5 : 0 + 2 &\equiv 2 \pmod{5} \end{aligned}$$

□

Da ein neutrales Element besteht, könnte man prüfen ob auch ein inverses Element besteht. Um ein inverses Element von einer bestimmten Zahl oder auch Repräsentanten zu bestimmen, sollte diese Zahl mit ihrem inversen Element durch die jeweiligen Rechen-*voschrift Addition, Multiplikation* wieder das neutrale Element ergeben. Auch dafür kann der “Chinesische Restklassensatz” angewendet werden. Jedoch kann man dies auch gut in der *Verknüpfungstabelle 3.5.1* ablesen.

*Beweis.*

$$\begin{aligned} [3 \in \mathbb{Z}_4] : 1 \in \mathbb{Z}_4 : 1 + 3 &\equiv 0 \pmod{4} \\ [2 \in \mathbb{Z}_5] : 3 \in \mathbb{Z}_5 : 3 + 2 &\equiv 0 \pmod{5} \end{aligned}$$

□

Man hat durch die Verknüpfungstabelle herausgefunden, dass die in 3.1 Axiome 3. & 4. für  $(\mathbb{Z}_4, \oplus)$  sowie  $(\mathbb{Z}_5, \oplus)$  zustimmen. Auch (1.; 2.; 5.) erfüllen diese beiden Strukturen. Daher kann man laut 3.2 *algebraische Strukturen* davon ausgehen, dass es sich hier um eine Kommutativegruppen handelt.

### 3.5.2 Verknüpfungstabelle (Multiplikation)

$(\mathbb{Z}_4, \otimes)$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$(\mathbb{Z}_5, \otimes)$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Es fällt bei der Verknüpfungstabelle der Multiplikation eine Besonderheit auf. Auch hier gibt es ein inverses Element, das wäre in diesem Fall auf der Struktur  $(\mathbb{Z}_n, \otimes)$  die 1.

*Beweis.*

$$\begin{aligned} 1 \in \mathbb{Z}_4 : 1 \cdot 3 &\equiv 3 \pmod{4} \\ 1 \in \mathbb{Z}_5 : 1 \cdot 2 &\equiv 2 \pmod{5} \end{aligned}$$

□

Jedoch existiert nicht für jedes Element eine multiplikative Inverse. Denn solange man auf die Struktur  $(\mathbb{Z}_m, \otimes)$  schaut und  $m$  keine Primzahl ist. Dann existiert für jedes Element das den selben größten gemeinsamen Teiler ( $[gcd(a,b)]$  siehe. *Euclid's algorithm*) wie  $m$  hat, keine multiplikative Inverse. (Verknüpfungstabelle  $\mathbb{Z}_4$  [2,2])

*Beweis.*

$$\begin{aligned} 2 &\equiv 2 \pmod{4} \\ 4 &\equiv 0 \pmod{4} \\ 10 &\equiv 2 \pmod{4} \end{aligned}$$

□

Daraus kann man schließen, wenn  $n$  keine Primzahl ist. Wird auf der Struktur  $(\mathbb{Z}_n, \otimes)$ , das 4. Axiom nicht erfüllt, jedoch (1.; 2.; 3.; 5.). Also erhält man für die Struktur  $(\mathbb{Z}_n, \otimes)$  einen Monoid.

Damit ist  $(\mathbb{Z}_n, \oplus, \otimes)$  ein Ring (3.3 Ringe), da ein Monoid die Kriterien einer Halbgruppe erfüllt und 3. die Distributivität gegeben ist. So erhält man für die Restklassen einen



Restklassenring.

Wenn  $m$  jedoch eine Primzahl ist, dann finden man eine multiplikative Inverse für jedes Element, außer dem Nullelement. *Siehe 3.5.2*  $(\mathbb{Z}_5, \otimes)$ .

Das heißt diesmal wird das *3. Axiom* erfüllt und wir erhalten für die Struktur  $(\mathbb{Z}_m, \oplus, \otimes)$  einen Körper. Somit bezeichnet man die Restklassen als Restklassenkörper.

## 4 Chinese Remainder Theorem

### 4.1 großzahlige Moduloberechnungen

Wenn  $x \equiv 14 \pmod{84}$  gegeben ist und  $x$  gesucht wird, kann man dies mithilfe des Chinesischen Restsatzes.

$$\sum_i [M_i]_m \cdot [M_i]_{m_i}^{-1} \cdot x_i \pmod{m}$$

Man geht wie folgt vor:

**Lemma 4.1.1.**

1. Zerlege  $m = 84$  in  $m_i$  Faktoren.
2. Zerlege  $x$  in  $x_i$  durch  $x \equiv x_i \pmod{m_i}$
3. Berechne  $M_i \pmod{m_i}$  durch z.B.  $m_2 \cdot m_3 \equiv [M_1] \pmod{m_1}$
4. Ermittle die multiplikative Inverse  $M_i^{-1}$  durch  $M_i \cdot M_i^{-1} \equiv e \pmod{m_i}$
5. Berechne  $x$  durch  $[M_i \cdot M_i^{-1} \cdot x_i]$ .

*Beispiel 4.1.2.*

1.  $84 = 3 \cdot 4 \cdot 7 = m_1 \cdot m_2 \cdot m_3$
2.
  - $14 \equiv 2 \pmod{3} \rightarrow [2 = x_1]$
  - $14 \equiv 2 \pmod{4} \rightarrow [2 = x_2]$
  - $14 \equiv 0 \pmod{7} \rightarrow [0 = x_3]$
3.
  - $4 \cdot 7 \equiv 1 \pmod{3} \rightarrow [M_1 \pmod{m_1}]$
  - $3 \cdot 7 \equiv 1 \pmod{4} \rightarrow [M_2 \pmod{m_2}]$
  - $3 \cdot 4 \equiv 5 \pmod{7} \rightarrow [M_3 \pmod{m_3}]$
4.
  - $1 \cdot 1 \equiv 1 \pmod{3} \rightarrow [M_1^{-1} = 1]$
  - $1 \cdot 1 \equiv 1 \pmod{4} \rightarrow [M_2^{-1} = 1]$
  - $5 \cdot 3 \equiv 1 \pmod{7} \rightarrow [M_3^{-1} = 3]$
5.  $(4 \cdot 7 \cdot 1 \cdot 2) + (1 \cdot 3 \cdot 7 \cdot 2) + (3 \cdot 4 \cdot 3 \cdot 0) = \boxed{98 \equiv 14 \pmod{84}}$

## 5 Euklidischer Algorithmus

Der Euklidische Algorithmus kann dafür genutzt werden, um den größten gemeinsamen Teiler zu bestimmen  $ggT(a, b)$ . Jedoch kann der erweiterte Euklidische Algorithmus auch dafür genutzt werden, um die Multiplikative Inverse von  $e \equiv a^{-1} \cdot a \pmod{b}$  zu bestimmen. Jedoch kann diese nur gefunden werden, wenn der  $ggT(a, b) = 1$  ist.

### 5.1 Algorithmus

Um den größten gemeinsamen Teiler von  $ggT(a, b)$  zu bestimmen, gehe man wie folgt vor, schreibe untereinander:

1. Wie oft passt  $a$  ganzzahlig in  $b \rightarrow b = x \cdot a$
2. entsteht ein Rest  $m$ , dann Addiere  $\rightarrow b = x \cdot a + r$
3. Ist der Rest  $= 0$ , dann ist der  $ggT(a, b)$  der vorherige Rest.

### 5.2 erweiterter Algorithmus

## 6 Permutation

Unter einer Permutation versteht man eine Anordnung von Objekten in einer bestimmten Reihenfolge. Man unterscheidet zwischen einer Permutation mit und ohne Wiederholung. Wobei die Permutation mit Wiederholung bestimmte Elemente mehrmals enthalten kann und die Permutation ohne Wiederholung Elemente nur einmalig enthält.

Betrachtet man eine Klasse  $G$  mit  $(a_1, \dots, a_n)$  Plätzen und  $(1, \dots, n)$  Schüler. Ordnet man jedem Schüler dieser Klasse einen Platz zu, dann wäre z.B eine Permutation  $\pi$ , wenn jeder Schüler mit seinem dazugehörigen Nachbarn die Plätze tauscht. (*Natürlich gehe man dann in diesem Szenario davon aus, dass jeder Schüler einen dazu gehörigen Nachbarn besitzt, bzw. die Klasse eine gerade Anzahl an Schüler besitzt*).

Selbst wenn das nicht gegeben wäre und einer Person auf ihren vorherigen Platz sitzen bliebe, würden wir diesen Vorgang als eine Permutation bezeichnen denn.

**Definition 6.0.1.** Eine Permutation ist eine bijektive Abbildung einer  $n$ -elementigen Menge  $G$  auf sich selbst man schreibt

$$\begin{array}{l} \pi: G \rightarrow G \\ \pi: = (a_1, a_2, \dots, a_n) \end{array}$$

### 6.1 identische Abbildung

Nun iteriert man Schüler und Plätze eindeutig, sitzt Schüler 1 auf Platz 1, Schüler 2 auf Platz 2 usw. bis Schüler  $n$  auf Platz  $n$  sitzt.

$$\begin{array}{l} \pi: \quad 1 \rightarrow a_1 \\ \quad \quad 2 \rightarrow a_2 \\ \quad \quad \vdots \\ \quad \quad n \rightarrow a_n \end{array}$$

Dies bezeichnet man als *identische Abbildung* einer Permutation und nutzt die verkürzte Schreibweise  $id(\pi): = (1, 2, 3, \dots, n)$ . Auch bekannt als Neutrales Element aus  $\pi$ .

Auch das inverse zum Neutralen Element besitzt eine bestimmte Permutation die *inverse Permutation* mit  $\bar{\pi}: = (n, n-1, \dots, 1)$ .

## 6.2 Schreibweisen

### 6.2.1 Zweilzeilenform

### 6.2.2 Tupelschreibweise

### 6.2.3 Zyklenschreibweise

### 6.2.4 Permutationsmatrix