

## Zahlen

I like primes!

*gym* | LERBERMATT  
*fms*



## Inhaltsverzeichnis

|  |           |
|--|-----------|
| <b>1. Natürliche Zahlen</b>                            | <b>5</b>  |
| 1.1. Historisches . . . . .                            | 5         |
| 1.2. Die Menge der natürlichen Zahlen . . . . .        | 5         |
| 1.3. Primzahlen . . . . .                              | 6         |
| 1.3.1. Etwas Zahlentheorie . . . . .                   | 8         |
| 1.3.2. Sieb von Eratosthenes . . . . .                 | 8         |
| 1.3.3. Dichte von Primzahlen . . . . .                 | 8         |
| 1.3.4. Der grosse Satz von Fermat . . . . .            | 9         |
| 1.3.5. Primzahlen im Internet . . . . .                | 10        |
| 1.4. Übungen zu $\mathbb{N}$ und Primzahlen . . . . .  | 11        |
| 1.5. ggT und kgV . . . . .                             | 12        |
| 1.5.1. Euklid'scher Algorithmus . . . . .              | 13        |
| 1.6. Notizen zu den Übungen . . . . .                  | 14        |
| <b>2. Die ganzen Zahlen</b>                            | <b>19</b> |
| 2.1. Die negativen Zahlen . . . . .                    | 19        |
| 2.1.1. Historisches . . . . .                          | 19        |
| 2.1.2. Die Geschichte der Null . . . . .               | 19        |
| 2.2. Notizen zu den Übungen . . . . .                  | 21        |
| <b>3. Rationale Zahlen</b>                             | <b>22</b> |
| 3.1. Normalbrüche . . . . .                            | 22        |
| 3.2. Dezimalbrüche . . . . .                           | 22        |
| 3.3. Gedanken zu rationalen Zahlen . . . . .           | 23        |
| 3.4. Notizen zu den Übungen . . . . .                  | 24        |
| <b>4. Reelle Zahlen</b>                                | <b>25</b> |
| 4.1. Die Entdeckung der irrationalen Zahlen . . . . .  | 25        |
| 4.2. Notizen zu den Übungen . . . . .                  | 27        |
| <b>5. Dies &amp; Das zu Zahlenmengen</b>               | <b>28</b> |
| 5.1. Notizen zu den Übungen . . . . .                  | 30        |
| <b>6. Zahlensysteme</b>                                | <b>32</b> |
| 6.1. Zahlen in Babylonien (ca. 2000 v. Chr.) . . . . . | 32        |
| 6.2. Zahlensysteme . . . . .                           | 33        |
| 6.2.1. Additionssysteme . . . . .                      | 33        |
| 6.2.2. Positionssysteme . . . . .                      | 33        |
| 6.3. Das Binärsystem . . . . .                         | 34        |
| 6.3.1. Einleitung . . . . .                            | 34        |
| 6.3.2. Rechnen im Binärsystem . . . . .                | 35        |
| 6.3.3. Negative Zahlen . . . . .                       | 35        |

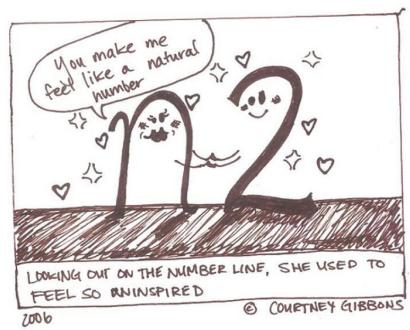
|   |           |
|---|-----------|
| 6.3.4. Multiplikation . . . . .                 | 36        |
| 6.4. Notizen zu den Übungen . . . . .           | 38        |
| <b>7. Modulo</b>                                | <b>41</b> |
| 7.1. Ein erstes Beispiel . . . . .              | 41        |
| 7.2. Motivation . . . . .                       | 41        |
| 7.3. Definition und weitere Beispiele . . . . . | 42        |
| 7.4. Die Uhr . . . . .                          | 43        |
| 7.5. Rechenregeln . . . . .                     | 43        |
| 7.6. Eigenschaften der Kongruenz . . . . .      | 45        |
| <b>8. Teilbarkeit</b>                           | <b>47</b> |
| 8.1. Teilbarkeit durch 3 . . . . .              | 47        |
| 8.2. Teilbarkeit durch 11 . . . . .             | 48        |
| 8.3. Teilbarkeit im Hexadezimalsystem . . . . . | 48        |
| 8.4. Notizen zu den Übungen . . . . .           | 49        |
| <b>9. Barcode</b>                               | <b>51</b> |
| <b>10. Die alte ISBN-Nummer</b>                 | <b>52</b> |
| 10.1. Prüfziffern . . . . .                     | 52        |
| 10.2. Ziffer fehlerhaft eingetippt . . . . .    | 52        |
| 10.3. Zahlendreher . . . . .                    | 55        |
| 10.4. Notizen zu den Übungen . . . . .          | 57        |
| <b>11. Rechnen Modulo 17</b>                    | <b>60</b> |
| 11.1. Potenzen . . . . .                        | 60        |
| 11.2. Kryptographie — eine erste Idee . . . . . | 61        |
| 11.3. Notizen zu den Übungen . . . . .          | 62        |
| <b>A. Die Osterformel von Gauss</b>             | <b>63</b> |
| <b>B. Gruppen</b>                               | <b>64</b> |
| B.1. Primitivwurzeln . . . . .                  | 65        |
| B.2. Notizen zu den Übungen . . . . .           | 67        |

# 1. Natürliche Zahlen

## 1.1. Historisches

Alles ist Zahl.

Diese Aussage stammt von PYTHAGORAS, dem berühmten griechischen Mathematiker und Philosophen, der um 550 v.u.Z. gelebt hat. In jungen Jahren soll er sich auf Anraten von THALES (624 – 546 v.u.Z.) auf eine langjährige Studienreise nach Ägypten begeben haben, um dort die vorhandenen Wissensschätze zu studieren. Nach PYTHAGORAS sollte das menschliche Leben geordnet und harmonisch sein, wie es die Zahlenverhältnisse in der Natur offenbarten. Dieses Zahlenverständnis kommt im Satz „Alles ist Zahl“ treffend zum Ausdruck und verdeutlicht, dass er die Zahlen als eine die gesamte Natur konstruierende Kraft betrachtete.



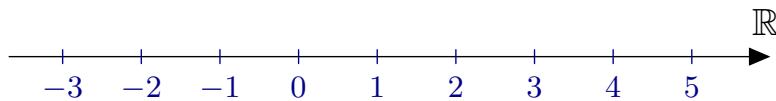
## 1.2. Die Menge der natürlichen Zahlen

Die natürlichen Zahlen  $\mathbb{N}$  sind die seit Alters her beim Zählen verwendeten Zahlen. Mit ihnen kann man eine Menge durchnummerieren. Die natürlichen Zahlen haben einen Anfang, die 1, aber kein Ende. Das Symbol für Unendlich ist eine  $\infty$ .

Auf  $\mathbb{N}$  können die Grundoperationen Addition und Multiplikation abgeschlossen durchgeführt werden. Das heisst, dass auch das Ergebnis einer solchen Operation wieder eine natürliche Zahl ist.

Die Null gehört für uns nicht zu den natürlichen Zahlen. Wird  $\mathbb{N}$  aber mit der Zahl Null erweitert, schreiben wir  $\mathbb{N}_0$ .

Zur Darstellung der natürlichen Zahlen eignet sich der **Zahlenstrahl**.



Eine saubere Fundierung der natürlichen Zahlen gelang im 19. Jahrhundert. Ein bedeutender Beitrag dazu stammte von GEORG CANTOR, dem die Einbindung des Unendlichen,  $\infty$ , gelang. Er schuf mit der Mengenlehre ein Fundament, in dem einerseits die



natürlichen Zahlen sicher eingebettet sind, aber auch der Begriff des Unendlichen nicht mit ihnen in Widerspruch gerät.

**Übung 1.1.**



JOHN VON NEUMANN definierte die natürlichen Zahlen  $\mathbb{N}_0$ , wobei wir hier die Null dazu zählen, auf mengentheoretischer Basis rekursiv wie folgt. Man beginnt mit der leeren Menge,  $\{\}$ . Die folgende Menge bestehe aus der Menge, die alle vorangegangenen Mengen als Elemente enthält. Formaler: Der Nachfolger der Menge  $M$  ist  $M' = M \cup \{M\}$ . Fährt man so immer fort, kriegt man eine Liste der natürlichen Zahlen  $\mathbb{N}_0$ . Nämlich, wenn man die Anzahl Elemente der entsprechenden Menge  $M$  zählt,  $\text{card}(M)$ .

- Sei also  $0 := \{\}$ . Wie schreibt sich dann die nächste natürliche Zahl 1?
- Notieren Sie in dieser Schreibweise die ersten 4 natürlichen Zahlen.

**Übung 1.2.**



Die Axiome der natürlichen Zahlenmenge von GIUSEPPE PEANO lauten wie folgt [?]:

- 1 ist eine natürliche Zahl.
- Jede natürliche Zahl  $n$  hat eine natürliche Zahl  $n'$  als Nachfolger.
- 1 ist kein Nachfolger einer natürlichen Zahl.
- Natürliche Zahlen mit gleichem Nachfolger sind gleich.
- Enthält eine Menge  $X$  die Zahl 1 und mit jeder natürlichen Zahl  $n$  auch stets deren Nachfolger  $n'$ , so enthält  $X$  bereits alle natürlichen Zahlen. (Ist  $X$  dabei selbst eine Teilmenge der natürlichen Zahlen, dann ist  $X$  gleich der Menge der natürlichen Zahlen.)

Überzeugen Sie sich davon, dass keines der fünf Axiome weggelassen werden darf. Lassen Sie dabei Axiom 5 unberührt. Was passiert, wenn man eines der ersten vier Axiome weg lässt? Geben Sie Gegenbeispiele an.

**1.3. Primzahlen**

Unter den natürlichen Zahlen gibt es solche, die jedem Divisionsversuch mit einem natürlichen Divisor, der zwischen 1 und der Zahl selbst liegt, widerstehen. Solche — in diesem Sinne teilerlose — Zahlen werden Primzahlen genannt.

**Definition 1.1: Primzahl**

Eine Zahl, die genau zwei verschiedene, natürliche Teiler hat, heisst Primzahl.

Somit gehören die Zahlen

$$2, 3, 5, 7, 11, 13, 17, 19, 23, \dots$$

zu den Primzahlen.

**Bemerkung 1.3.1.** Beachte, dass 1 per Definition keine Primzahl ist!

Primzahlen sind die Bausteine der natürlichen Zahlen. Dies besagt der folgende Satz, den ich gerne als Satz der DNA der natürlichen Zahlen bezeichne.

**Satz 1.1: DNA der natürlichen Zahlen**

Jede natürliche Zahl grösser 1 lässt sich eindeutig als Produkt von Primzahlen darstellen.

*Beweis.* Widerspruchsbeweis: Falls die Primfaktorzerlegung in  $\mathbb{N} \setminus \{1\}$  nicht eindeutig wäre, dann gäbe es eine kleinste Zahl  $n \in \mathbb{N} \setminus \{1\}$ , die auf mindestens 2 Arten darstellbar wäre:

$$n = p_1 \cdot \dots \cdot p_r = q_1 \cdot \dots \cdot q_s.$$

Da  $n$  das kleinste Beispiel ist, sind alle  $p_i \neq q_j$  für alle  $i, j$  in ihren Indexmengen. Ausserdem können wir OEdA annehmen, dass die Faktoren der Grösse nach sortiert seien (Wohlordnung von  $\mathbb{N}$ ) und  $p_1 \neq q_1$  mit  $p_1 + 1 \leq q_1 \leq \sqrt{n}$ . Betrachte nun  $m := n - p_1 q_1$  mit  $\sqrt{n} < m < n$ . Beachte, dass  $m < n$  eine eindeutige Primfaktorzerlegung hat. Aus

$$m = p_1 \cdot (p_2 \cdot \dots \cdot p_r - q_1) = q_1 \cdot (q_2 \cdot \dots \cdot q_s - p_1)$$

folgt  $p_1 | (q_2 \cdot \dots \cdot q_s - p_1)$ , also  $p_1 | (q_2 \cdot \dots \cdot q_s)$ . Weil aber für Zahlen kleiner  $n$  die Primfaktorzerlegung eindeutig ist, muss  $p_1 = q_j$  für ein  $j \neq 1$ . Widerspruch zu  $p_1 \neq q_j \forall j$ .  $\square$

**Übung 1.3.**

Zerlege die Zahlen 234600 und 7571 in ihre Primfaktoren.

### 1.3.1. Etwas Zahlentheorie

Als Bausteine der Zahlen scheinen die Primzahlen offensichtlich wichtig zu sein.

### 1.3.2. Sieb von Eratosthenes

Der alexandrinische Bibliothekar, Mathematiker und Geograph ERATOSTHENES (276 – 194 v.u.Z.), der als erster einen ausgezeichneten Wert für den Umfang der Erde ermittelt hat, konnte bereits ein einfaches Verfahren, um die Primzahlen schrittweise aus der Reihe der natürlichen Zahlen heraus zu filtern (das **Sieb des Eratosthenes**).

Betrachten wir die Primzahlen kleiner 100:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79,  
83, 89, 97

Auffallend ist, dass die Primzahlen scheinbar zufällig über  $\mathbb{N}$  verteilt sind. Zudem gibt es Primzahlen, die sich als Paar um eine einzige Zahl schmiegen, wie zum Beispiel 11 und 13, 17 und 19, 29 und 31 oder 59 und 61. Die von einem solchen **Primzahlzwilling** eingeschlossene Zahl besitzt immer viele Teiler, auf jeden Fall den Teiler 6.

#### Übung 1.4.



Beweise, dass die Zahl zwischen einem Primzahlzwilling,  $(p|p + 2)$  mit  $p, p + 2$  beide prim, durch 6 teilbar ist.

#### Übung 1.5.



Gibt es **Primzahldrillinge**, also Zahlentriple mit  $p, p + 2$  und  $p + 4$  alle prim?

Es ist übrigens nicht bekannt, ob es endlich oder unendlich viele Primzahlzwillinge gibt.

Die Lücken, das heisst die Anzahl der nichtprimen Zahlen zwischen zwei Primzahlen, sind in der Reihe der natürlichen Zahlen ganz verschieden gross. Je weiter in der Zahlenreihe fortgeschritten wird, um so grössere, derartige Lücken — nebst den kleinsten — treten auf.

### 1.3.3. Dichte von Primzahlen

Deutlich ist, dass die Primzahlen im allgemeinen mit wachsenden Zahlenwerten weniger häufig auftreten. Aber auch diese Gesetzmässigkeit wird durchbrochen. So finden wir in den ersten Hunderter-Blöcken die folgenden Anzahlen Primzahlen:

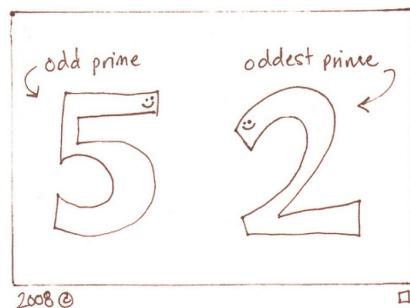


Abbildung 1: Seltsamste Primzahl

| 1 bis 100    | 101 bis 200 | 201 bis 300 |
|--------------|-------------|-------------|
| 25           | 21          | 16          |
| 301 bis 400  | 401 bis 500 | 501 bis 600 |
| 16           | 17          | 14          |
| 601 bis 700  | 701 bis 800 | 801 bis 900 |
| 16           | 14          | 15          |
| 901 bis 1000 |             |             |
| 14           |             |             |

Das erste Tausend weist also 168 Primzahlen auf, was etwa  $1/6$  aller natürlichen Zahlen dieses Intervalls entspricht. In den ersten 3000 finden sich etwa  $1/7$ , und unter den ersten 10 000 treffen wir auf rund  $1/8$ . Die Dichte nimmt also scheinbar ab. Ist die Menge der Primzahlen also endlich? Gibt es eine grösste Primzahl? Der *indirekte* Beweis der Antwort auf diese Frage, lieferte schon EUKLID<sup>1</sup>



### Übung 1.6.



Zeige, dass es unendlich viele Primzahlen gibt.

#### 1.3.4. Der grosse Satz von Fermat

Ein um die Jahrtausendwende gelöstes zahlentheoretisches Problem, das sogar in der Presse seinen Niederschlag fand, ist der grosse Satz von Fermat.

<sup>1</sup>griechischer Mathematiker um 350 v.u.Z..

**Satz 1.2: Grosser Fermat'scher Satz**

Für  $x, y, z, n \in \mathbb{N}$  mit  $n > 2$ ,  $y, z$  und  $n > 2$  ist Gleichung

$$x^n + y^n = z^n$$

nicht erfüllbar.

FERMAT<sup>2</sup> selbst hinterliess auf dem Blattrand einer Manuskriptseite die Notiz:

Wenn  $n$  eine Zahl grösser als 2 bedeutet, so gibt es keine positiven ganzen Zahlen  $a, b$  und  $c$ , so dass  $a^n + b^n = c^n$  wäre. Ich habe dafür einen wahrhaft wundervollen Beweis gefunden, der aber auf diesem Rande keinen Platz findet!

Für  $n = 2$  entspricht die oben genannte Gleichung dem Satz des Pythagoras, und der hat natürlich Lösungen. Man spricht in diesem Zusammenhang von [pythagoräischen Zahlentripeln](#).

### 1.3.5. Primzahlen im Internet

Die Suche nach schnellen Verfahren zum Auffinden von Primzahlen dauert bis zum heutigen Tag an; und das nicht nur aufgrund des Reizes, den sie seit jeher auf die Menschen ausgeübt haben. Über zweitausend Jahre lang wusste man keinen praktischen Nutzen aus dem Wissen über die Primzahlen zu ziehen. Dies änderte sich allerdings schlagartig mit dem Aufkommen des elektronischen Datenverkehrs, als Primzahlen zum Verschlüsseln von Informationen eine zentrale Rolle zu spielen begannen.

Die Güte einer Geheimsprache besteht einerseits darin, Botschaften ohne grossen Aufwand in Geheimschrift umschreiben (chiffrieren) zu können, andererseits darin, die Schwierigkeit für Uneingeweihte eine geheime Botschaft zu knacken (dechiffrieren), ins Unermessliche zu steigern. Solch asymmetrische Eigenschaften trifft man beim Rechnen mit Primzahlen an:

Es ist relativ einfach, das Produkt von zwei grossen Primzahlen zu berechnen, aber nahezu unmöglich, dieses Produkt wieder in seine Faktoren zu zerlegen.

Das Verschlüsseln einer Botschaft läuft heute tatsächlich auf die Multiplikation zweier sehr grosser Primzahlen hinaus, während das Entschlüsseln im Wesentlichen aus dem Faktorisieren dieses Produkts besteht (ausprobieren). Bis dato (2025) hat man noch

---

<sup>2</sup>französischer Mathematiker (1601–1665)

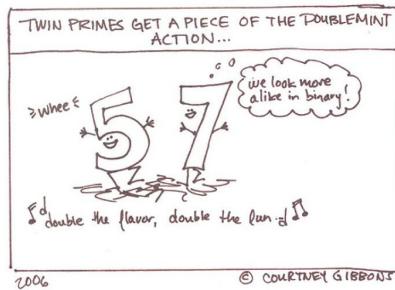


Abbildung 2: Primzahlzwillinge

keinen schnellen Algorithmus zur Faktorisierung eines Produkts zweier grosser Zahlen gefunden. Ja, man weiss sogar nicht einmal, ob ein solcher überhaupt existiert.

## 1.4. Übungen zu $\mathbb{N}$ und Primzahlen

### Übung 1.7.

Was taugen die folgenden Formeln als Primzahlerzeuger? Dabei steht stets  $p$  für eine Primzahl und  $n$  für eine natürliche Zahl.

- a)  $z_a = 2^p - 1$
- b)  $z_b = 2^p + 1$
- c)  $z_c = n^2 - n + 41$
- d)  $z_d = n^2 - 79n + 1601$

### Übung 1.8.

Wähle 5 gerade Zahlen zwischen 3 und 1000. Versuche jeder dieser Zahlen als Summe von zwei Primzahlen darzustellen (Stichwort Goldbach'sche Vermutung).

### Übung 1.9.

Es gibt „Primzahllücken“ beliebiger Grösse. Man definiert für  $n \in \mathbb{N}$  den Ausdruck  $n! := 1 \cdot 2 \cdot 3 \cdots \cdot n$  und sagt „ $n$  Fakultät“.

- a) Sind unter den Zahlen  $5! + 1, 5! + 2, 5! + 3, 5! + 4$  und  $5! + 5$  Primzahlen?
- b) Welche der Zahlen  $47! + 1, 47! + 2, 47! + 3, \dots, 47! + 47$  sind sicher nicht prim?

## 1. Natürliche Zahlen

---

- c) Formulieren Sie nun allgemein für  $n \in \mathbb{N}$  welche der Zahlen  $n! + 1, n! + 2, \dots, n! + n$  sicher nicht prim sind.

### Übung 1.10.



Nimm eine dreistellige Zahl und notiere sie zweimal hintereinander, so dass eine sechsstellige Zahl entsteht. Teile diese Zahl nacheinander durch 7, 11 und 13.

- Was fällt auf?
- Kannst du deine Vermutung begründen?

### Übung 1.11.



Zeige, dass die Summe von vier aufeinander folgenden natürlichen Zahlen niemals ein Vielfaches von 4 sein kann.

### Übung 1.12.



Vier aufeinanderfolgende natürliche Zahlen werden miteinander multipliziert und zum Produkt 1 addiert.

- Stelle einige konkrete Berechnungen an.
- Stelle eine Vermutung auf und versuche, diese zu beweisen.

### Übung 1.13.



Suche Quadratzahlen, welche bei der Division durch 3 den Rest 2 lassen. Solltest du keine derartige Zahl finden, so versuche zu beweisen, dass es keine Quadratzahl gibt, die bei der Division durch 3 den Rest 2 lässt.

## 1.5. ggT und kgV

Primfaktorzerlegungen spielen auch beim Bestimmen des **ggT** (grösster gemeinsamer Teiler) und des **kgV** (kleinstes gemeinsames Vielfaches) zweier natürlicher Zahlen  $a$  und  $b$  eine wichtige Rolle.

### Übung 1.14.



Bestimme das kgV und den ggT der Zahlen 153900 und 180600.

### 1.5.1. Euklid'scher Algorithmus

Um den ggT zweier Zahlen  $a$  und  $b$  zu finden, gelangt man häufig mit dem Euklid'schen Algorithmus am schnellsten zum Ziel. Als Beispiel betrachten wir nochmals die beiden Zahlen 153900 und 180600, dividieren zuerst die grössere durch die kleinere und bestimmen danach den Rest, der entsteht. In einem zweiten Schritt wird die kleinere Zahl durch den erhaltenen Rest geteilt und der dadurch resultierende neue Rest bestimmt, etc....

Zwischen dem ggT und dem kgV besteht der folgende Zusammenhang.



#### Satz 1.3: Produktsatz

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

*Beweis.* Für das kgV nimmt man jeweils die maximal vorkommende Anzahl der Primfaktoren aus beiden Zahlen, für den ggT jeweils die minimale Anzahl der gemeinsamen Primfaktoren. Kommt also ein Primfaktor nur in einer der Zahlen vor, so wird er wegen des kgVs verwendet und taucht im ggT nicht auf. Kommt ein Faktor in beiden Zerlegungen vor, so wird er in seiner maximalen Anzahl wegen des kgVs genommen und wegen seiner minimalen Anzahl für den ggT.  $\square$

#### Übung 1.15.



Zeige, dass der Euklid'sche Algorithmus stets den ggT der beiden Zahlen liefert.

#### Übung 1.16.



Bestimme den ggT und das kgV der Zahlen 5544 und 4410 mit dem euklidschen Algorithmus und dem letzten Satz.

## 1.6. Notizen zu den Übungen

### Notizen zu Übung 1.16



- a) Die 1 ist dann die Menge mit der  $0 = \{ \}$ , also  $1 = \{\{ \} \}$ . Beachten Sie, dass die leere Menge kein Element enthält, jedoch die 1 die leere Menge enthält, also ein Element.
- b) Die ersten vier natürlichen Zahlen lauten:  $1 = \{\{ \} \}$ ,  $2 = \{\{ \}, \{\{ \} \} \}$ ,  $3 = \{\{ \}, \{\{ \} \}, \{\{ \}, \{\{ \} \} \} \}$ ,  $4 = \{\{ \}, \{\{ \} \}, \{\{ \}, \{\{ \} \} \}, \{\{ \}, \{\{ \}, \{\{ \} \} \} \} \}$

### Notizen zu Übung 1.16



Lässt man beispielsweise 1 weg, so fehlt das Charakteristikum „natürliche Zahl sein“ und kann nicht weiter vererbt werden. Fehlt Axiom 2, so hätte nicht jede natürliche Zahl einen Nachfolger. Damit wäre es nicht möglich, alle (unendlich viele) natürlichen Zahlen zu erzeugen. Beispielsweise wäre  $\mathbb{N} = \{1, 2, 3\}$  möglich. Fehlt Axiom 3, so könnte man einen Zirkelschluss bilden, indem man beispielsweise 1 als Nachfolger der 2 nimmt:  $1, 2, 1, 2, 1, 2, 1, \dots$ . Verzichtet man auf Axiom 4, dann wäre es denkbar, dass zwei verschiedene natürliche Zahlen  $n \neq m$  den gleichen Nachfolger hätten. Zum Beispiel:  $1, 3, 2, 3, 2, \dots$ .

### Notizen zu Übung 1.16



$$234600 = 2^3 \cdot 3 \cdot 5^2 \cdot 17 \cdot 23, \quad 7571 = 67 \cdot 113$$

### Notizen zu Übung 1.16



Für  $(3 \bmod 5)$  stimmt die Aussage nicht. Lassen wir also diesen Fall ausser betracht.

Da 2 die einzige gerade Primzahl ist, muss die Zahl zwischen einem Primzahlzwillinge gerade sein. Betrachte für  $k \in \mathbb{N}$  grösser als 3 die Kette

$$k-2 \quad k-1 \quad k \quad k+1 \quad k+2 \quad k+3.$$

Damit werden für  $k \in \mathbb{N}$  alle natürlichen Zahlen durchlaufen.  $k-2$  und  $k$ , sowie  $k$  und  $k+2$  und  $k+1$ ,  $k+3$  können keine Primzahlzwillinge sein. Denn gälte  $k \bmod 3 \equiv 1$  dann  $k-2 \bmod 3 \equiv 2$ , also einer von beiden gerade bzw.  $k+2 \bmod 3 \equiv 0$ , also durch 3 teilbar. Analog für  $k \bmod 3 \equiv 2$ . Also kommt als Primzahlzwilling in dieser Kette nur  $(k-1 \mid p+1)$  in Frage.  $k-1 \bmod 3 \equiv 1$  kann nicht sein, da dann  $k+1 \bmod 3 \equiv 0$  wäre. Also muss  $k-1 \bmod 3 \equiv 2$  und damit  $k \bmod 3 \equiv 0$ . Also ist  $k$  durch 2 und durch 3 teilbar, also durch  $6 = 2 \cdot 3$ .

### Notizen zu Übung 1.16



Es gibt nur das Tripel  $(3|5|7)$ . Denn jedes weitere Tripel würde ungerade Zahlen enthalten, wobei sicher eine davon durch 3 teilbar wäre, da jede dritte ungerade Zahl durch 3

teilbar ist.

Man kann dies auch formal einsehen:

*Beweis.* Wäre  $(p|p+2|p+4)$  mit  $p > 3$  ein weiteres Tripel, so dürfte  $p$  nicht durch 3 teilbar sein. Es gälte also  $p \bmod 3 \equiv 1$  oder  $p \bmod 3 \equiv 2$ . Sei  $p \bmod 3 \equiv 1$ , dann ist aber  $p+2 \bmod 3 \equiv 0$  durch 3 teilbar, also keine Primzahl. Gälte  $p \bmod 3 \equiv 2$ , so wäre  $p+4 \bmod 3 \equiv 0$  durch 3 teilbar. Somit ist  $(3|5|7)$  der einzige Primzahldrilling.  $\square$

### Notizen zu Übung 1.16



*Beweis.* Gegenannahme: Es gebe endlich viele Primzahlen und daher gebe es eine grösste, die wir  $p$  nennen. Wir betrachten die Menge dieser endlich vielen Primzahlen

$$\{2, 3, 5, 7, 11, \dots, p\}.$$

Wir basteln daraus die Zahl

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdots \cdot p + 1 =: z.$$

Diese Zahl  $z \in \mathbb{N}$  ist sicher grösser als  $p$  und sie ist auch prim. Denn beispielsweise hat man  $z \div 7 = 2 \cdot 3 \cdot 5 \cdot 11 \cdots \cdot p + 1$ , d.h.  $z = 7 \cdot 2 \cdot 3 \cdot 5 \cdot 11 \cdots \cdot p + 1$  hat bei Division mit 7 Rest 1. Und dies gilt analog für alle Primzahlen in unserer Menge

$$\{2, 3, 5, 7, 11, \dots, p\}.$$

Dies widerspricht der Annahme, dass  $p$  die grösste Primzahl sei, denn  $z > p$  ist prim. Also muss das Gegenteil unserer Annahme gelten: Es gibt unendlich viele Primzahlen.  $\square$

### Notizen zu Übung 1.16



- a)  $p = 3$  liefert 4.
- b)  $p = 2$  liefert 8.
- c)  $n = 41$  liefert sicher keine Primzahl, weil  $z_c(41) = 41^2$ .
- d) Für  $n = 80$  ist  $z_d(80) = 41^2$

### Notizen zu Übung 1.16



Beispiele sind  $4 = 2 + 2$ ,  $6 = 3 + 3$ ,  $8 = 3 + 5$ ,  $10 = 3 + 7$ . Beachte, dass die Zerlegung nicht eindeutig sein muss. Beispielsweise ist  $10 = 3 + 7 = 5 + 5$  oder  $20 = 3 + 17 = 7 + 13$ .

Bis dato (2025) konnte die Goldbach-Vermutung nicht bewiesen werden.

Sidenote: Dem Russen VINOGRADOV gelang mittels statistischer Methoden über die Primzahlen um die Jahrhundertwende der Beweis, dass sich jede „genügend“ grosse, ungerade Zahl als Summe von drei Primzahlen schreiben lässt.

**Notizen zu Übung 1.16**



- a)  $5! + 1 = 121 = 11^2$ ,  $5! + 2 = 122$  ist gerade,  $5! + 3 = 123 = 3 \cdot 41$ ,  $5! + 4$  ist gerade,  $5! + 5 = 125 = 5^3$  sind alle nicht prim.
- b) Für  $47! + 1$  ist ohne Hilfsmittel aufwändig zu beurteilen, ob sie prim ist oder nicht. Hingegen  $47! + 2 = 1 \cdot 2 \cdot 3 \cdots \cdot 47 + 2 = 2 \cdot (1 \cdot 3 \cdots \cdot 47 + 1)$ . Analog  $47! + 3 = 1 \cdot 2 \cdot 3 \cdots \cdot 47 + 3 = 3 \cdot (1 \cdot 2 \cdot 4 \cdots \cdot 47 + 1)$ . Das heisst, alle Zahlen  $47! + 2$ ,  $47! + 3$ ,  $\dots$ ,  $47! + 47$  sind sicher nicht prim.
- c) Für  $n \in \mathbb{N}$  kann man im Allgemeinen wie oben nicht eruieren, ob  $n! + 1$  prim ist oder nicht. Andererseits sind  $n! + 2 = 2 \cdot (3 \cdot 4 \cdots \cdot n + 1)$  bis  $n! + n = n \cdot (2 \cdot 3 \cdots \cdot (n - 1) + 1)$  wegen der hier gezeigten Faktorisierung sicher nicht prim. Also gibt es Primzahllücken beliebiger Grösse.

**Notizen zu Übung 1.16**



- a) Man kriegt wieder diejenige dreistellige Zahl, die man sich ausgedacht hat.
- b) Wenn man durch die Werte 7, 11 und 13 in Folge teilt, so entspricht dies einer Division mit  $7 \cdot 11 \cdot 13 = 1001$ . Eine dreistellige Zahl multipliziert mit  $1001 = 1000 + 1$  erzeugt den Effekt von zweimal hintereinander schreiben; zum Beispiel  $123 \cdot 1001 = 123123$ .

**Notizen zu Übung 1.16**



In der Tat ist für beliebig gewähltes  $n \in \mathbb{N}$  die Summe von vier aufeinander folgenden natürlichen Zahlen  $n + (n + 1) + (n + 2) + (n + 3) = 4n + 6 = 4 \cdot (n + 1) + 2$  immer  $(n + (n + 1) + (n + 2) + (n + 3)) \bmod 4 \equiv 2$ , hat also Rest 2 bei Division mit 4.

**Notizen zu Übung 1.16**



- a) Beispielsweise hat man  $1 \cdot 2 \cdot 3 \cdot 4 + 1 = 25 = 5^2$ ,  $2 \cdot 3 \cdot 4 \cdot 5 + 1 = 121 = 11^2$  oder  $10 \cdot 11 \cdot 12 \cdot 13 + 1 = 17161 = 131^2$ .

b) Für  $n \in \mathbb{N}$  beliebig berechnet man

$$\begin{aligned} n(n+1)(n+2)(n+3) + 1 &= (n^2 + n)(n^2 + 5n + 6) + 1 \\ &= n^4 + 6n^3 + 11n^2 + 6n + 1 \\ &= (n^2 + 3n + 1)(n^2 + 3n + 1) \\ &= (n^2 + 3n + 1)^2. \end{aligned}$$

Also ist dies immer eine Quadratzahl, da ja  $n^2 + 3n + 1 \in \mathbb{N}$ .

### Notizen zu Übung 1.16



Man kriegt bei der Division durch 3 nie den Rest 2. Einige Beispiele:  $1^2 \bmod 3 \equiv 1$ ,  $2^2 \bmod 3 \equiv 1$ ,  $3^2 \bmod 3 \equiv 0$  oder  $4^2 \bmod 3 \equiv 1$ .

In der Tat:

*Beweis.* Betrachten Sie für  $n \in \mathbb{N}$  die Kette

$$3n - 2, 3n - 1, 3n,$$

welche für  $n \in \mathbb{N}$  alle natürlichen Zahlen durchläuft. Die Quadrate  $(3n - 2)^2 = 9n^2 - 12n + 4 = 3 \cdot (3n^2 - 4n + 1) + 1$  und  $(3n - 1)^2 = 9n^2 - 6n + 1 = 3 \cdot (3n^2 - 2n) + 1$  haben offensichtlich Rest 1 bei Division mit 3. Das Quadrat  $9n^2 = 3 \cdot 3n^2$  hat Rest 0 bei Division durch 3. Daher kann keine Quadratzahl bei Division durch 3 Rest 2 haben.  $\square$

### Notizen zu Übung 1.16



Es ist

$$\begin{aligned} 153\,900 &= 2^2 \cdot 3^4 \cdot 5^2 \cdot 19 \\ 180\,600 &= 2^3 \cdot 3 \cdot 5^2 \cdot 7 \cdot 43 \end{aligned}$$

und daher  $\text{ggT}(180\,600, 153\,900) = 2^2 \cdot 3 \cdot 5^2$  und  $\text{kgV}(180\,600, 153\,900) = 2^3 \cdot 3^4 \cdot 5^2 \cdot 7 \cdot 19 \cdot 43$ .

### Notizen zu Übung 1.16



OEdA sei  $a \geq b$ . Wir zeigen zuerst, dass sich der ggT über eine „Algorithmusrunde“ nicht ändert. Der Algorithmus läuft so:

$$\begin{aligned} a &= q_1 \cdot b + r_1 \\ b &= q_2 \cdot r_1 + r_2 \\ r_1 &= q_3 \cdot r_2 + r_3 \\ &\vdots \\ r_{n-1} &= q_{n+1} \cdot r_n + 0 \end{aligned}$$

Es ist  $\text{ggT}(a, b) \leq \text{ggT}(b, r_1) = \text{ggT}(b, a - q_1 b)$ : Setze  $\text{ggT}(a, b) =: t$ . Klar  $t|a$  und  $t|b$ , d.h.  $\exists k, l \in \mathbb{Z}$  mit  $a = kt$  und  $b = lt$ . Es folgt  $a - q_1 b = kt - q_1 lt = t(k - q_1 l)$ , also teilt  $t$   $a - q_1 b$ . Somit gilt  $\text{ggT}(b, a - q_1 b) \leq \text{ggT}(a, b)$ . Sei umgekehrt  $\text{ggT}(b, a - q_1 b) =: u$ , also  $b = ku$  und  $a - q_1 b = lu$ . Es folgt  $a = lu - q_1 b = lu - q_1 ku = u(l - ku)$ , also ist  $u$  ein Teiler von  $\text{ggT}(a, b)$ , d.h.  $\text{ggT}(a, b) \leq \text{ggT}(b, a - q_1 b)$ . Insgesamt also  $\text{ggT}(a, b) = \text{ggT}(b, a - q_1 b)$ .

Weil im letzten Schritt  $\text{ggT}(r_{n-1}, r_n) = \text{ggT}(r_n, 0) = r_n$  ist  $\text{ggT}(a, b) = r_n$ , also gleich dem letzten, nichttrivialen Rest.

**Notizen zu Übung 1.16**



$$5544 = 4410 \cdot 1 + 134$$

$$4410 = 134 \cdot 32 + 122$$

$$134 = 122 \cdot 1 + 12$$

$$122 = 12 \cdot 10 + 2$$

$$12 = 2 \cdot 6 + 0$$

Der ggT ist also 2.

---

## 2. Die ganzen Zahlen

### 2.1. Die negativen Zahlen

#### 2.1.1. Historisches

Der indische Mathematiker und Astronom BRAHMAGUPTA (598-630) erkannte als einer der ersten das Wechselspiel von Zahlzeichen, indem er Regeln für das Teilen von Zahlen aufstellte: „Positiv geteilt durch positiv oder negativ geteilt durch negativ gibt positiv. Positiv geteilt durch negativ oder negativ geteilt durch positiv gibt negativ.“

In Europa erlaubte erst FIBONACCI (1180-1241) in seiner Finanzmathematik negative Zahlen und interpretierte sie korrekterweise als Schulden.



#### 2.1.2. Die Geschichte der Null

Ein ähnlich schwieriger Stand wie die negativen Zahlen hatte die Zahl Null, die in Europa auf Ablehnung und Unverständnis stiess: Null wurde mit nichts gleichgesetzt.

Im Anhang ?? ist ein Artikel von HERBERT CERUTTI abgedruckt, der im Februar 2002 im NZZ-Folio *Total Digital* erschienen ist.

#### Übung 2.1.



Hilberts Hotel ist ein Hotel mit unendlichen vielen, nummerierten Zimmern ( $1, 2, 3, \dots$ ). Der Portier ist mit allen Zimmern durch eine Gegensprechanlage verbunden. Aktuell sind alle unendlich vielen Zimmer besetzt.

- Es kommt ein Besucher an und möchte gerne ein Zimmer zum Übernachten buchen. Kann der Portier eines offerieren?
- Nun kommen unendlich viele Besucher an, die jeweile je ein Zimmer für sich buchen möchten. Kann der Portier helfen?

#### Übung 2.2.



Haben  $\mathbb{N}_0$  und  $\mathbb{Z}$  gleich viele Elemente? Anders: Finde eine bijektive Abbildung  $f : \mathbb{N}_0 \rightarrow \mathbb{Z}$ ?

## 2. Die ganzen Zahlen

---

Zwei Mengen  $\mathbb{A}$  und  $\mathbb{B}$  heissen **gleichmächtig** (haben gleich viele Elemente), falls es eine bijektive Abbildung  $f : \mathbb{A} \longrightarrow \mathbb{B}$  gibt.

## 2.2. Notizen zu den Übungen

### Notizen zu Übung 2.2



- a) Der Portier kann die unendlich vielen Gäste auffordern, ihr Zimmer zu verlassen und das Zimmer mit der um 1 grösseren Nummer zu belegen. Also  $1 \rightarrow 2, 2 \rightarrow 3, 3 \rightarrow 4$  etc. Nun ist Zimmer Nummer 1 frei. Als Funktion geschrieben:  $f : \mathbb{N} \rightarrow \mathbb{N}$ ,  $f(n) = n + 1$ .
- b) Ja! Beispielsweise kann der Portier beantragen, dass alle Gäste ins Zimmer mit der doppelten so grossen Nummer einziehen; also  $1 \rightarrow 2, 2 \rightarrow 4, 3 \rightarrow 6$  etc. Dadurch werden alle Zimmer mit ungeraden Nummern,  $1, 3, 5, \dots$ , frei, und das sind unendlich viele. Formal notiert:  $f : \mathbb{N} \rightarrow \mathbb{N}$ ,  $f(n) = 2n$ .

### Notizen zu Übung 2.2



Beispielsweise kann man alle geraden Zahlen auf die positiven Werte abbilden, 0 auf 0 und alle ungeraden Zahlen den negativen Werten zuordnen:

$$f : \mathbb{N}_0 \rightarrow \mathbb{Z}, f(n) = \begin{cases} \frac{n}{2} & \text{falls } n \text{ gerade} \\ -\frac{n+1}{2} & \text{falls } n \text{ ungerade} \end{cases}$$

### 3. Rationale Zahlen

#### 3.1. Normalbrüche

In der Menge der ganzen Zahlen  $\mathbb{Z}$  kann die Division nicht immer ausgeführt werden.

**Beispiel 3.1.1.** Die Rechnung  $8 \div 2$  liefert zwar wieder ein Element aus  $\mathbb{Z}$  als Lösung (nämlich 4), aber  $8 \div 3$  ist in  $\mathbb{Z}$  nicht mehr lösbar, denn  $\frac{8}{3} = 2.\overline{6} \notin \mathbb{Z}$ . Wir suchen deshalb eine möglichst einfache Menge, welche die ganzen Zahlen enthält und welche die Division uneingeschränkt zulässt (ausser der Division durch 0, natürlich!). Dies wird durch die Menge der rationalen Zahlen

$$\mathbb{Q} = \left\{ \frac{p}{q} \mid p \in \mathbb{Z}, q \in \mathbb{N} \right\}$$

gewährleistet.

| i,j | 1   | 2   | 3   | 4   | 5   |
|-----|-----|-----|-----|-----|-----|
| 1   | 1/1 | 1/2 | 1/3 | 1/4 | 1/5 |
| 2   | 2/1 | 2/2 | 2/3 | 2/4 | 2/5 |
| 3   | 3/1 | 3/2 | 3/3 | 3/4 | 3/5 |
| 4   | 4/1 | 4/2 | 4/3 | 4/4 | 4/5 |
| 5   | 5/1 | 5/2 | 5/3 | 5/4 | 5/5 |

#### 3.2. Dezimalbrüche

Dezimalbrüche können in zwei Kategorien eingeteilt werden: Dezimalbrüche

- mit periodischer Dezimalbruchentwicklung (z.B. 1.5 oder 3.512)
- ohne periodische Dezimalbruchentwicklung (z.B. 0.10100100010 ...)

Dezimalbrüche mit abbrechender Dezimalbruchentwicklung können unter der Menge Dezimalbrüche mit periodischer Dezimalbruchentwicklung subsummiert werden.



#### Satz 3.1: Dezimaldarstellung rationaler Zahlen

Jeder Normalbruch lässt sich in Form eines periodischen Dezimalbruchs schreiben, und umgekehrt.

Man muss zeigen, dass

- jeder Normalbruch in einen periodischen Dezimalbruch und
- jeder periodische Dezimalbruch in einen Normalbruch umgewandelt werden kann.

Im Folgenden soll das Verfahren zur Umwandlung an ein paar Beispielen erläutert werden.

### 3.3. Gedanken zu rationalen Zahlen

#### Übung 3.1.



Wie muss der Nenner eines Bruches beschaffen sein, damit die Dezimalbruchdarstellung abbrechend ist?

#### Übung 3.2.



Behauptung: Die Periodenlänge eines Bruches

$$\frac{1}{q}$$

wird nie länger als  $q - 1$ .

#### Übung 3.3.



- Verwandle den Bruch  $\frac{3}{11}$  in eine Dezimalzahl.
- Bestimme den Bruch zur rationalen Zahl  $0.\overline{132}$ .

### 3.4. Notizen zu den Übungen



#### Notizen zu Übung 3.3

Denken wir uns, wie man die Dezimaldarstellung mit schriftlicher Division erhält. Pro Divisionsschritt wird der jeweilige Rest ein Vielfaches von 10 mit Primfaktorzerlegung  $10 = 2 \cdot 5$  sein, weil wir ja im Dezimalsystem rechnen. Solch ein Rest wird somit genau dann ohne Divisionsrest teilbar sein, wenn in der Primfaktorzerlegung des Divisors (also dem Nenner) nur Primfaktoren 2 oder 5 vorkommen. Beispielsweise haben  $\frac{1}{8} = \frac{1}{2^3} = 0.125$ ,  $\frac{1}{10} = \frac{1}{2 \cdot 5} = 0.1$  oder  $\frac{1}{25} = \frac{1}{5^2} = 0.04$  abbrechende Dezimaldarstellung.



#### Notizen zu Übung 3.3

Sei  $q \in \mathbb{N}$  beliebig. Bei der schriftlichen Division von 1 mit  $q$  können sicherlich nur Reste kleiner  $q$  auftauchen; also die Reste  $0, 1, 2, 3, \dots, q - 1$ . Dies sind  $q$  Stück. Im Falle vom Rest 0 haben wir eine abbrechende Dezimaldarstellung. Also können alternierend höchstens die Reste  $1, 2, 3, \dots, q - 1$  vorkommen, und das sind  $q - 1$  Stück. Die Periodenlänge ist daher nie grösser als  $q - 1$ .



#### Notizen zu Übung 3.3

a)

$$\begin{aligned} 3 \div 11 &= 0.2\overline{72} && (\text{Rest } 3) \\ 30 \div 11 &= 2 && (\text{Rest } 8) \\ 80 \div 11 &= 7 && (\text{Rest } 3) \end{aligned}$$

b)

$$\begin{aligned} 0.\overline{132} &= x \\ 13.\overline{232} &= 100x \\ 99x &= 13.1 \\ x &= \frac{13.1}{99} = \frac{131}{990} \end{aligned}$$

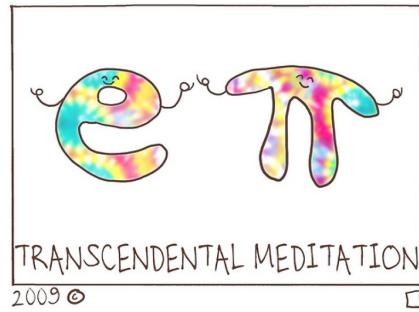
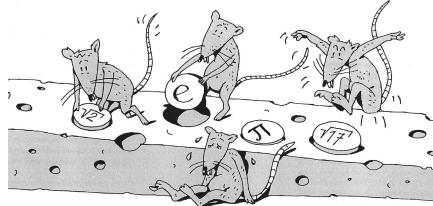


Abbildung 3: irrats and transcendentals

## 4. Reelle Zahlen

Es scheint, als sei die Zahlengerade durch die „überall dicht“ liegenden rationalen Zahlen lückenlos besetzt, da sich zwischen zwei noch so nahe beieinander liegenden rationalen Zahlen immer noch unendlich viele andere rationale Zahlen befinden. Diese Ansicht ist falsch! Es gibt noch Lücken.

### 4.1. Die Entdeckung der irrationalen Zahlen

In der goldenen Ära Griechenlands (bis ca. 400 v.u.Z.) galten unter den Gelehrten die natürlichen Zahlen und die Lehre ihrer Verhältnisse als das Mass aller Dinge. Die Entdeckung von inkommensurablen Längen riss eine grosse Kluft zwischen die Arithmetik, die diese irrationalen Zahlen erschaffen konnte, und die Geometrie, die sie nicht messen konnte. Ein Beispiel einer Zahl, die nicht durch ein Verhältnis zweier ganzer Zahlen ausgedrückt werden kann, ist  $\sqrt{2}$ .

*Beweis.* Indirekter Beweis hier über die Parität. Man könnte auch über die Eindeutigkeit der Primfaktorzerlegung argumentieren.

Sei  $\sqrt{2} \in \mathbb{Q}$ . Da  $\sqrt{2}$  positiv, gibt es  $a, b \in \mathbb{N}$  mit  $\sqrt{2} = \frac{a}{b}$  vollständig gekürzt. Es folgt

$$2 = \frac{a^2}{b^2}$$

$$2b^2 = a^2$$

und damit muss  $a^2$  gerade sein. Wenn  $a^2$  gerade ist, so muss auch  $a$  gerade sein, da in



$a^2$  mindestens zwei Faktoren 2 vorkommen müssten. Betrachte weiter

$$2b^2 = a^2$$

$$b^2 = \frac{a^2}{2} = \frac{a}{2} \cdot a,$$

was heisst, dass  $b^2$  und damit  $b$  gerade ist, denn das Produkt  $\frac{a}{2} \cdot a$  ist immer gerade. Dies ist ein Widerspruch zur vollständig gekürzten Darstellung  $\frac{a}{b}$ , da dieser Quotient sicher noch mit 2 gekürzt werden könnte!  $\square$

Die irrationalen Zahlen können nicht durch einen abbrechenden oder periodischen Dezimalbruch beschrieben werden. Sie bilden zusammen mit den rationalen Zahlen die Menge der reellen Zahlen,  $\mathbb{R}$ .

Neben den Wurzelzahlen  $\sqrt{2} = 1.41421\dots$ ,  $\sqrt{3} = 1.73205\dots$  etc. gehören Zahlen wie  $\Pi = 3.14159\dots$ , die Euler'sche Zahl  $e = 2.71828\dots$  und die Zahl des goldenen Schnitts  $\Phi = 1.61803\dots$  bzw.  $\varphi = 0.618\dots$  zu den berühmtesten irrationalen Zahlen.

**Bemerkung 4.1.1.** Die reellen Zahlen werden manchmal auch in zwei Mengen aufgeteilt: In die **algebraischen**, die als Nullstellen von Polynomen mit ganzzahligen Koeffizienten aufgefasst werden können, also im Wesentlichen Wurzelausdrücke, und in die **transzentenden Zahlen**, das sind alle anderen. Während zum Ersteren die Zahl  $\sqrt{2}$  und die des goldenen Schnitts  $\phi$  gehören, sind die Zahlen  $\pi$  und  $e$  transzendenten Zahlen.

### Übung 4.1.



Zeige, dass alle Primzahlwurzeln, das heisst  $\sqrt{p}$  mit  $p$  prim, irrational sind.

### Übung 4.2.



Zeige, dass jede Primzahlwurzel  $\sqrt{p}$  algebraisch ist.

## 4.2. Notizen zu den Übungen

### Notizen zu Übung 4.2



Sei  $p \in \mathbb{N}$ ,  $p$  prim. Gegenannahme  $\sqrt{p} \in \mathbb{Q}$ , das heisst  $\exists a \in \mathbb{Z}, b \in \mathbb{N}$  so, dass

$$\sqrt{p} = \frac{a}{b}.$$

Es folgt

$$\begin{aligned}\sqrt{p} &= \frac{a}{b} && ((\ )^2) \\ p &= \frac{a^2}{b^2} && (\cdot b^2) \\ b^2 \cdot p &= a^2\end{aligned}$$

In der Primfaktorzerlegung der Quadratzahlen  $a^2$  und  $b^2$  kommt jeder Primfaktor der Zerlegung sicher eine gerade Anzahl Mal vor. Der Primfaktor  $p$  jedoch kommt in der Zahl  $b^2 \cdot p$  eine ungerade Anzahl Mal vor. Widerspruch zur Gleichheit in  $((\ )^2)$ !

### Notizen zu Übung 4.2



Offensichtlich liefert  $x^2 - p = 0$  die Behauptung.

## 5. Dies & Das zu Zahlenmengen

### Übung 5.1.



Zu welcher kleinstmöglichen Zahlenmenge ( $\mathbb{N}$ ,  $\mathbb{Z}$ ,  $\mathbb{Q}$  und  $\mathbb{R}$ ) gehören die folgenden Zahlen?

- a)  $-5$
- b)  $4.\bar{7}$
- c)  $-\frac{5}{3}$
- d)  $5.15515551555\dots$
- e)  $\sqrt{121}$
- f)  $\frac{15}{5}$
- g)  $0$
- h)  $-0.38\bar{2}\bar{7}$

### Übung 5.2.



Sind diese Aussagen wahr oder falsch? Finde Beispiele oder Gegenbeispiele.

- a) Alle Differenzen von zwei natürlichen Zahlen sind natürliche Zahlen.
- b) Es gibt Quotienten von zwei natürlichen Zahlen, die irrational sind.
- c) Alle Quotienten von zwei rationalen Zahlen sind rationale Zahlen.
- d) Alle Wurzeln aus natürlichen Zahlen sind irrationale Zahlen.
- e) Das Quadrat einer irrationalen Zahl ist eine irrationale Zahl.

### Übung 5.3.



Sind diese Aussagen wahr oder falsch? Begründe.

- a) Es gibt unendlich viele Zahlen zwischen  $0.1$  und  $\frac{1}{9}$ .
- b)  $(1 + \sqrt{2})$  ist eine irrationale Zahl, deren Quadrat irrational bleibt.
- c) Es gibt unendlich viele Zahlen, deren Wurzel gleich der Zahl selbst ist.

- 
- d) Es gibt unendlich viele Zahlen, deren Wurzel grösser als die Zahl selbst ist.

**Übung 5.4.**



Ist die Zahl  $0.9999999\cdots = 0.\bar{9}$  gleich 1? Begründe deine Antwort.

**Übung 5.5.**



Eine Zahl geht auf Reisen...

- Ergänze die Tabelle. Berechne auch den Term und vereinfache jeweils.
- Wähle andere Ausgangszahlen. Überprüfe, ob die Reise immer durch die gleichen Zahlenmengen geht.
- Nimm die Reise mit einer beliebigen natürlichen Zahl in Angriff. Die Reise soll möglichst lange innerhalb der natürlichen Zahlen verlaufen.

| VORSCHRIFT                                | ZAHL      | ZAHLENMENGEN                                     | TERM          |
|---|-----------|--|---------------|
| Denk dir eine Primzahl                    | 7         | $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ | $x$           |
| Dividiere durch 4                         | 1.75      | $\mathbb{Q}, \mathbb{R}$                         | $\frac{x}{4}$ |
| Ziehe die Wurzel                          | 1.32...   | $\mathbb{R}$                                     |               |
| Addiere 1                                 | 2.32...   |  |               |
| Quadriere                                 |           |  |               |
| Subtrahiere die Wurzel deiner Anfangszahl |           |  |               |
| Verdopple                                 |           |  |               |
| Subtrahiere die Hälfte der Anfangszahl    |           |  |               |
| Ziehe die Wurzel                          | 1.4142... |  |               |

### 5.1. Notizen zu den Übungen

#### Notizen zu Übung 5.5



- a)  $\mathbb{Z}$
- b)  $\mathbb{Q}$ ,  $4.\overline{7}$  ist periodisch.
- c)  $\mathbb{Q}$
- d)  $\mathbb{R}$ , diese Zahl hat weder periodische noch abbrechende Nachkommastellen.
- e)  $\mathbb{N}$ , da  $\sqrt{121} = 11$ .
- f)  $\mathbb{N}$ , da  $\frac{15}{5} = 3$ .
- g)  $\mathbb{Z}$
- h)  $\mathbb{Q}$ , da die Nachkommastellen periodisch sind.

#### Notizen zu Übung 5.5



- a) Nein, zum Beispiel  $2 - 5 = -3 \notin \mathbb{N}$ .
- b) Nein. Für  $a, b \in \mathbb{N}$  ist  $\frac{a}{b}$  per Definition ( $\mathbb{Q} = \left\{ \frac{x}{y} \mid x \in \mathbb{Z}, y \in \mathbb{N} \right\}$ ) eine rationale Zahl.
- c) Ja, denn  $\frac{\frac{a}{c}}{\frac{d}{c}} = \frac{ad}{bc} \in \mathbb{Q}$ .
- d) Nein, beispielsweise  $\sqrt{4} = 2 \in \mathbb{N}$ .
- e) Nein, zum Beispiel  $(\sqrt{2})^2 = 2 \in \mathbb{N}$ .

#### Notizen zu Übung 5.5



- a) Ja, denn  $\frac{1}{9} = 0.\overline{1}$ . Also sind  $0.11, 0.101, 0.1001$  etc. bereits unendlich viele Zahlen dazwischen.
- b) Ja,  $(1 + \sqrt{2})^2 = 1 + 2\sqrt{2} + 2$  ist irrational.

c) Nein, denn es müsste

$$\begin{aligned}\sqrt{x} &= x && ((\ )^2) \\ x &= x^2 && (-x) \\ x^2 - x &= 0 \\ x(x - 1) &= 0\end{aligned}$$

Also sind  $x = 0$  und  $x = 1$  die einzigen Fixpunkte.

d) Ja, jeder Wert  $0 < x < 1$  ist kleiner als seine Wurzel  $\sqrt{x}$ .

### Notizen zu Übung 5.5



Betrachte  $0.\bar{9} =: x$ . Also  $10x = 9.\bar{9}$ , und es folgt:

$$\begin{aligned}10x - x &= 9.\bar{9} - 0.\bar{9} && (\text{TU}) \\ 9x &= 9 && (\div 9) \\ x &= 1\end{aligned}$$

Das heisst  $0.\bar{9} = 1$ .

### Notizen zu Übung 5.5



Für eine beliebige Zahl  $x$  geht die Reise so:

$$\begin{aligned}x \rightarrow \frac{x}{4} \rightarrow \sqrt{\frac{x}{4}} &= \frac{\sqrt{x}}{2} \rightarrow \frac{\sqrt{x} + 2}{2} \rightarrow \frac{x + 4\sqrt{x} + 4}{4} \rightarrow \frac{x + 4}{4} \\ &\rightarrow \frac{x + 4}{2} \rightarrow 2 \rightarrow \sqrt{2}\end{aligned}$$

Also landet man bei dieser Reise immer bei  $\sqrt{2}$ .

## 6. Zahlensysteme

### Übung 6.1.



In welchem Zahlensystem rechnest du? Welche Ziffern brauchst du dafür?

#### 6.1. Zahlen in Babylonien (ca. 2000 v. Chr.)



Abbildung 4: Babylonische Rechentafel und Sternkarte

Die Babylonier verwendeten als eines der ersten Völker ein „hybrides“ Positionssystem. Der Wert eines Zeichens hängt auch von dessen Position ab. Während wir heute in unserem Dezimalsystem (Basis 10) die Ziffern  $0, 1, 2, \dots, 9$  verwenden, brauchten die Babylonier in ihrem Sechzigersystem 59 Ziffern; ein Zeichen für die Null, gab es damals noch nicht.

Abschliessend noch ein Beispiel, wie diese Zeichen verwendet werden.

$$\begin{array}{ccc} \text{Symbol} & \text{Symbol} & \text{Symbol} \\ \begin{array}{c} \diagup \\ \diagdown \end{array} & \begin{array}{c} \nwarrow \\ \swarrow \end{array} & \begin{array}{c} \diagup \\ \diagdown \\ \diagup \end{array} \\ 4 \cdot 60 + & 4 \cdot 10 + & 5 \cdot 1 \\ 240 & 40 & 5 \end{array}$$

### Übung 6.2.



Welches Zahlensystem verwendeten die Babylonier?

## 6.2. Zahlensysteme

Man unterscheidet im Wesentlichen zwischen Additionssystemen und Positionssystemen.

### 6.2.1. Additionssysteme

In einem Additionssystem wird eine Zahl als Summe der Werte ihrer Ziffern dargestellt. Dabei spielt die Position der einzelnen Ziffern keine Rolle.

### 6.2.2. Positionssysteme

In einem Positionssystem bestimmt die Stelle (Position) den Wert der jeweiligen Ziffer. Die „niederwertigste“ Position steht dabei ganz rechts.

Ein Stellenwertsystem hat eine Basis  $b$ . Jede Zifferposition hat einen Wert, der einer Potenz der Basis entspricht. Für die  $k$ -te Position hat man einen Wert von  $b^{k-1}$ .

Die Berechnung des Zahlenwertes  $z_n z_{n-1} \dots z_0$  erfolgt durch Multiplikation der einzelnen Ziffern  $z_i$  mit den zugehörigen Stellenwerten  $b_i$  und Addition dieser Produkte:

$$\text{Zahlenwert} = z_n \cdot b^n + \dots + z_i \cdot b^i + \dots + z_0 \cdot b^0.$$

**Beispiel 6.2.1.** Unter der Zahl 1257 im üblichen Dezimalsystem (d.h. zur Basis 10) verstehen wir den Wert

$$1 \cdot 10^3 + 2 \cdot 10^2 + 5 \cdot 10^1 + 7 \cdot 10^0 = 1257.$$

Mit der Beschränkung des niedrigsten Exponenten auf 0 kann man nur ganze Zahlen darstellen. Lässt man auch negative Exponenten zu, kann man auch rationale Zahlen in einem Stellenwertsystem schreiben. Dabei wird der Übergang vom nichtnegativen zum negativen Exponenten durch ein Trennzeichen markiert, beispielsweise einem Punkt:

$$1 \cdot 10^2 + 2 \cdot 10^1 + 1 \cdot 10^0 + 4 \cdot 10^{-1} + 7 \cdot 10^{-2} = 121.47$$

### Übung 6.3.

Die Idee des Positionssystems mit einer bestimmten Basis wird auch beim Binärsystem (Basis 2) verwendet.

Die binäre Zahl 1011 entspricht der Dezimalzahl

$$1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 8 + 2 + 1 = 11.$$



Stelle die Dezimalzahlen von 1 bis 20 im Binärsystem dar. Beschreibe dein Vorgehen.

**Übung 6.4.**



Verwandle folgende Binärzahlen in Dezimalzahlen

1      11      111      1111      ...

und

10      100      1000      10000      ...

**Übung 6.5.**



Finde für die Dezimalzahl 34 die Binärschreibweise.

### 6.3. Das Binärsystem

#### 6.3.1. Einleitung

Wie könnte eine Codierung von Zeichen im Computer realisiert werden? Der Computer arbeitet mit elektrischem Strom. Das heisst er kann lediglich die beiden Zustände „Strom an“ und „Strom aus“ unterscheiden. Man codiert 1 für den ersten und 0 für den zweiten Zustand. Die Information, die durch den Strom in einer Leitung codiert ist, heisst **ein Bit** (binary digit). So lassen sich bloss zwei Zeichen codieren. Kombiniert man aber zwei Leitungen, lassen sich nun vier Zustände unterscheiden:

| Leitung 1 | Leitung 2 |
|-----------|-----------|
| 0         | 0         |
| 0         | 1         |
| 1         | 0         |
| 1         | 1         |

**Übung 6.6.**



Stelle eine Tabelle für drei Leitungen auf.

**Übung 6.7.**



Wie viele Leitungen braucht man, um alle Buchstaben des Alphabets codieren zu können?

In der Informatik ist es üblich, acht Leitungen zur Speicherung von Informationen zusammenzufassen. Insgesamt lassen sich damit  $2^8 = 256$  verschiedene Zeichen darstellen. Man spricht bei dieser Bündelung von acht Leitungen vom Informationsgehalt ein **Byte**.

**Bemerkung 6.3.1.** Früher rechnete man noch in Kilobyte, was ca. 1000 Bytes entspricht. Kilo wurde in diesem Zusammenhang nicht wie üblich für den Wert Tausend verwendet, sondern für  $2^{10} = 1024 \approx 1000$ . Deshalb ist zum Beispiel ein Megabyte = 1024 Kilobyte.

Wie rechnet der Computer mit diesen Binärzahlen?

### 6.3.2. Rechnen im Binärsystem

Die Addition von Binärzahlen funktioniert prinzipiell genau so, wie die Addition von Dezimalzahlen.

#### Übung 6.8.

Addiere schriftlich die Binärzahlen 1001011 und 101011.

Werden mehrere Binärzahlen addiert, kann der Übertrag natürlich auch grösser als 1 werden.

#### Übung 6.9.

Addiere schriftlich die Binärzahlen 1001011, 101011 und 101010.

### 6.3.3. Negative Zahlen

Schauen wir vierstellige Binärzahlen, sogenannte **Nibbles**, an. Insgesamt können mit einem Nibble 16 verschiedene Zahlen dargestellt werden. Was passiert nun bei fortlaufender Addition von 1 ausgehend von der Zahl 0?

$$0 \xrightarrow{+1} 1 \xrightarrow{+1} 2 \xrightarrow{+1} \dots \xrightarrow{+1} 14 \xrightarrow{+1} 15 \xrightarrow{+1} ???$$

Wir können diese Additionskette als Zyklus auffassen, wenn wir die binäre Vierstelligkeit nicht verlassen wollen. Addieren wir nun zur Zahl  $1111_{(2)}$  die 1, so erhalten wir  $(1)0000_{(2)}$ , also die Zahl 0 mit einem Überlauf. Wenn Addieren gleichzusetzen mit um eins im Uhrzeigersinn verschieben ist, dann sollte man Subtrahieren mit der Umkehrung definieren.

#### Übung 6.10.

Welche Binärzahl repräsentiert  $-7_{(10)}$ ? Addiere  $-7_{(10)} + 7_{(10)}$ .

Die Frage, die bleibt, ist: Welcher Zahl entspricht die  $1000_{(2)}$ ? Es könnte  $-8$  oder  $+8$

bedeuten. Man löst dieses Dilemma, indem man einfach ein Vorzeichenbit einführt. Somit können wir also mit einem Nibble die Zahlen  $-8$  bis  $7$  darstellen.

Genau diesen Zusammenhang kann man zur Berechnung der Darstellung einer negativen Zahl im Binärsystem verwenden:

- Ist eine Zahl gegeben, so bildet man zuerst das sogenannte Einerkomplement, indem man einfach jedes der 8 Bit „kippt“.
- Danach addiert man noch 1 zum Einerkomplement.

**Beispiel 6.3.1.** Wir betrachten die Zahl  $23 = 00010111_{(2)}$ . Durch Kippen erhält man  $11101000$ . 1 addieren bringt  $11101001 = -23$ .

Wir sind nun in der Lage, die Subtraktion im Binärsystem zu lösen, indem wir sie auf die Addition zurückführen.

$$\begin{aligned} 127 - 19 &= 127 + (-19) \\ &= 0111\ 1111_{(2)} + 1110\ 1101_{(2)} \\ &= (1)0110\ 1100_{(2)} \\ &= 108 \end{aligned}$$

### Übung 6.11.



Prüfe durch Rechnung obiges Beispiel. Berechne danach im Binärsystem

- $115 - 48$
- $77 - 76$

### 6.3.4. Multiplikation

Neben der Addition und Subtraktion von Binärzahlen spielt die Multiplikation von Binärzahlen eine wesentliche Rolle. Wir kennen ein Verfahren in den Dezimalzahlen, welches wir direkt auf das Binärsystem anwenden können. Jedoch liegt dabei der Schwerpunkt auf dem Addieren, wie das folgende Beispiel zeigt.

**Beispiel 6.3.2.** Wir berechnen das Produkt von  $0000\ 1001_{(2)}$  und  $0010\ 0111_{(2)}$ . Dezimal erhalten wir  $9 \cdot 23 = 207$ . Binär

### Übung 6.12.



Berechne  $9 \cdot 23$  binär.

Bei der Multiplikation entstehen so bis zu acht Summanden, die anschliessend addiert werden müssen, dagegen ist die Multiplikation als solches sehr einfach. Ferner sieht man nun im Ergebnis zwei Bytes aneinander gereiht. Dabei haben wir Glück und das zweite Byte bleibt mit Nullen gefüllt, so dass unser Resultat wieder in ein Byte hinein passt. Es könnte ja auch sein, dass das vordere Byte benötigt wird, nämlich dann, wenn das Ergebnis grösser als 255 ist.

**Übung 6.13.**



Vergleiche das Binärsystem mit dem Hexadezimalsystem. Beschreibe, wie man ohne grossen Rechenaufwand Zahlen im Hexadezimalsystem ins Binärsystem umwandeln kann.

## 6.4. Notizen zu den Übungen

### Notizen zu Übung 6.13



Wir Schweizer rechnen im Dezimalsystem, 10-er System. Wie der Name sagt, brauchen wir in diesem Positionssystem 10 Ziffern: 0, 1, 2, …, 9.

### Notizen zu Übung 6.13



Die Babylonier verwendeten das 60-er System, auch Sexagesimalsystem genannt. Überbleibsel davon stecken beispielsweise in der Zeit- (Minuten, Sekunden) oder Winkelmessung (Grad, Minuten, Sekunden).

### Notizen zu Übung 6.13



| BIN  | DEC | BIN   | DEC |
|------|-----|-------|-----|
| 0001 | 1   | 1011  | 11  |
| 0010 | 2   | 1100  | 12  |
| 0011 | 3   | 1101  | 13  |
| 0100 | 4   | 1110  | 14  |
| 0101 | 5   | 1111  | 15  |
| 0110 | 6   | 10000 | 16  |
| 0111 | 7   | 10001 | 17  |
| 1000 | 8   | 10010 | 18  |
| 1001 | 9   | 10011 | 19  |
| 1010 | 10  | 10100 | 20  |

### Notizen zu Übung 6.13



a) 1, 3, 7, 15,  $2^k - 1$

b) 2, 4, 8, 16,  $2^k$

### Notizen zu Übung 6.13



Ich gucke, welche Zweierpotenz noch Platz hat und fahre dann mit dem Rest analog fort. Man kann auch stetig durch zwei Teilen und am Ende die Binärzahl rückwärts zusammensetzen.

a)  $34 = 2^5 + 2^1 = 100010_{(2)}$

b)  $34 \div 2 \equiv 0$ ,  $17 \div 2 \equiv 1$ ,  $8 \div 2 \equiv 0$ ,  $4 \div 2 \equiv 0$ ,  $2 \div 2 \equiv 0$ ,  $1 \div 2 \equiv 1$ . Wenn man die Reste nun rückwärts auflistet, hat man die Zweierpotenzen-Aufspaltung von 34, also  $34 = 100010_{(2)}$ .

### Notizen zu Übung 6.13



| Leitung 1 | Leitung 2 | Leitung 3 |
|-----------|-----------|-----------|
| 0         | 0         | 0         |
| 0         | 0         | 1         |
| 0         | 1         | 0         |
| 0         | 1         | 1         |
| 1         | 0         | 0         |
| 1         | 0         | 1         |
| 1         | 1         | 0         |
| 1         | 1         | 1         |

### Notizen zu Übung 6.13



Für das Alphabet mit 26 Buchstaben braucht man mindestens 5 Leitungen, da  $2^4 = 16$  und  $2^5 = 32$ . Als Standardgrösse hat sich ein **Byte**,  $2^8 = 256$  Zustände, etabliert.

### Notizen zu Übung 6.13



$$\begin{array}{r}
 1001001 \\
 + 101011 \\
 \hline
 1110100
 \end{array}$$

### Notizen zu Übung 6.13



$$\begin{array}{r}
 1001011 \\
 + 101011 \\
 + 101010 \\
 \hline
 10100000
 \end{array}$$

### Notizen zu Übung 6.13



$-7 = 1001_{(2)}$  und  $7 = 0111_{(2)}$ .

$$\begin{array}{r}
 1001 \\
 + 0111 \\
 \hline
 (1)0000
 \end{array}$$

## Notizen zu Übung 6.13

a)  $01110011 - 00110000 = 01110011 + 11010000 = (1)01000011$

$$b) 77 - 7601001101 - 01001100 = 01001101 + 10110100 = (1)00000001$$

## Notizen zu Übung 6.13

$$\begin{array}{ccccccccccccc}
 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & \cdot & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\
 & & & & & & & & & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\
 & & & & & & & & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\
 \hline
 & & & & & & & & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\
 & & & & & & & & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1
 \end{array}$$

## Notizen zu Übung 6.13

Es ist  $2^4 = 16$  und daher kann man immer einen Viererblock binär als Hexadezimalzahl notieren. Zum Beispiel ist  $1\ 0010_{(2)} = 12_{(16)}$  oder  $A2_{(16)} = 1010\ 0011$ .



## 7. Modulo

Modulare Arithmetik — rechnen mit Resten — ist ein nützliches Werkzeug der Zahlentheorie.

### 7.1. Ein erstes Beispiel

Wir wissen, dass die Menge  $\mathbb{Z}$  in zwei Klassen aufgespalten werden kann.

- die geraden Zahlen:

$$\dots, -6, -4, -2, 0, 2, 4, 6, \dots$$

- die ungeraden Zahlen:

$$\dots, -5, -3, -1, 1, 3, 5, \dots$$

Nun können wir gewisse Verallgemeinerungen über die Gesetzmäßigkeiten dieser Zahlen formulieren; in Abhängigkeit ihrer Zugehörigkeit zu einer der beiden Klassen. Beispielsweise ist die Summe zweier gerader Zahlen wieder gerade. Die Summe einer geraden und einer ungeraden Zahl ist ungerade. Die Summe zweier ungeraden Zahlen ist gerade. Das Produkt zweier gerader Zahlen ist gerade, usw.

### 7.2. Motivation

Im obigen Beispiel ist der sogenannte **Modulus** gleich 2. Der Modulus kann als Anzahl der Klassen betrachtet werden, in die unsere Zahlenmenge  $\mathbb{Z}$  aufgeteilt wird.

Jetzt legen wir für jede der beiden Klassen ein Symbol fest. Wir schreiben 0 für die Klasse aller geraden Zahlen und 1 für die Klasse aller ungeraden Zahlen<sup>3</sup>. Die Bezeichnung erfolgte willkürlich; wir hätten auch 2 und 1, oder  $-32$  und  $177$  wählen können. 0 und 1 sind aber die üblichen Bezeichnungen.

Die Aussage

Die Summe zweier gerader Zahlen ist eine gerade Zahl.

wird wie folgt schlank geschrieben:

$$0 + 0 \equiv 0 \pmod{2}$$

Hier bezeichnet das Symbol  $\equiv$  nicht Gleichheit, sondern **Kongruenz**.  $\pmod{2}$  bedeutet, dass unser Modulus 2 ist. Obige Aussage liest man: „Null plus Null ist kongruent Null Modulo Zwei“. Die Aussage, dass die Summe einer geraden und einer ungeraden Zahl ungerade ist, schreibt sich

$$0 + 1 \equiv 1 \pmod{2}.$$

Diese Beispiele sind trivial. Wie aber schreiben wir, dass die Summe zweier ungerader Zahlen gerade ist?

$$1 + 1 \equiv 0 \pmod{2}.$$

Analoge Aussagen erhält man für die Multiplikation:

$$0 \cdot 0 \equiv 0 \pmod{2}$$

$$0 \cdot 1 \equiv 0 \pmod{2}$$

$$1 \cdot 1 \equiv 1 \pmod{2}$$

### 7.3. Definition und weitere Beispiele

Selbverständlich kann man auch Modulo  $m$ ,  $m \in \mathbb{N}$ , rechnen. Wir definieren

#### Definition 7.1: Modulo

Sei  $m \in \mathbb{N}$ . Zwei Zahlen  $a, b \in \mathbb{Z}$  heißen kongruent Modulo  $m$ , falls ein  $k \in \mathbb{Z}$

---

<sup>3</sup>Präziser müsste man zum Beispiel  $\bar{0}$  für die Klasse der geraden Zahlen schreiben, weil 0 selber ja ein Element der Klasse der geraden Zahlen ist.

existiert, so dass  $a - b = k \cdot m$ . Man schreibt

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

**Beispiel 7.3.1.** 5 und 8 sind kongruent Modulo 3, denn es gilt  $5 - 8 = -1 \cdot 3$ .

Wir betrachten ganze Zahlen Modulo 3. Klar ist, dass alle Vielfachen von 3,  $3n$ , kongruent Modulo 3 sind, da jede Differenz zweier solcher Zahlen durch 3 teilbar ist. Analog sind alle Zahlen der Form  $3n + 1$  und alle Zahlen der Form  $3n + 2$  kongruent Modulo 3,  $n \in \mathbb{Z}$ .

$$\begin{aligned} \dots &\equiv -6 \equiv -3 \equiv 0 \equiv 3 \equiv 6 \equiv 9 \dots \pmod{3} \\ \dots &\equiv -7 \equiv -4 \equiv -1 \equiv 2 \equiv 5 \equiv 8 \dots \pmod{3} \\ \dots &\equiv -8 \equiv -5 \equiv -2 \equiv 1 \equiv 4 \equiv 7 \dots \pmod{3} \end{aligned}$$

## 7.4. Die Uhr

Ein alltäglicher Fall ist der Modulus 12. Man nennt den Fall  $m = 12$  auch die „Uhr-Arithmetik“.

**Beispiel 7.4.1.** Wenn es 07:00 Uhr ist, welche Zeit haben wir in 25 Stunden. Da  $25 \equiv 1 \pmod{12}$  können wir einfach 1 zu 7 addieren:

$$7 + 25 \equiv 7 + 1 \equiv 8 \pmod{12}.$$

Also 08:00 Uhr. Die Sekunden und Minuten auf der Uhr sind auch modular, nämlich Modulo 60.

## 7.5. Rechenregeln

Die Grundlage für folgende Rechenregeln ( $a, b \in \mathbb{Z}$  und  $m, n \in \mathbb{N}$ ) mit Moduln bildet

### Satz 7.1: Modulare Äquivalenz

$$a \equiv b \pmod{m} \Leftrightarrow a - b \equiv 0 \pmod{m} \Leftrightarrow m \mid (a - b)$$

Die restlichen Sätze, inklusive die Äquivalenzeigenschaften, folgen unmittelbar.

**Satz 7.2: Additon mod**

$$a \equiv b \pmod{m} \Rightarrow a + c \equiv b + c \pmod{m}$$

**Satz 7.3: Multiplikation mod**

$$a \equiv b \pmod{m} \Rightarrow ac \equiv bc \pmod{m}$$

**Satz 7.4: Potenz mod**

$$a \equiv b \pmod{m} \Rightarrow a^n \equiv b^n \pmod{m}$$

**Satz 7.5: Additivität mod**

$$a \equiv b \pmod{m} \text{ und } c \equiv d \pmod{m} \Rightarrow a + c \equiv b + d \pmod{m}$$

**Satz 7.6: Multiplikativität mod**

$$a \equiv b \pmod{m} \text{ und } c \equiv d \pmod{m} \Rightarrow ac \equiv bd \pmod{m}$$

**Satz 7.7: Chinese mod**

$$\gcd(m, n) = 1, a \equiv b \pmod{m} \text{ und } a \equiv b \pmod{n} \Rightarrow a \equiv b \pmod{mn}$$

**Satz 7.8: Primzahlprodukt**

Ist  $p$  eine Primzahl, so gilt

$$ab \equiv 0 \pmod{p} \Rightarrow a \equiv 0 \pmod{p} \text{ oder } b \equiv 0 \pmod{p}$$

*Beweis.* Sei  $p$  prim und  $ab \equiv 0 \pmod{p}$ .  $\exists k \in \mathbb{Z}$  mit  $ab - 0 = ab = kp$ , also teilt  $p$  das Produkt  $ab$ . Wegen der Eindeutigkeit der Primfaktorzerlegung muss  $p$  entweder in der Zerlegung von  $a$  oder von  $b$  vorkommen. Das heisst  $p|a$  oder  $p|b$ .  $\square$

**Satz 7.9: Kürzungssatz**

$$\gcd(a, m) = 1 \text{ und } ab \equiv ac \pmod{m} \Rightarrow b \equiv c \pmod{m}$$

*Beweis.* Sei  $\gcd(a, m) = 1$  und  $ab \equiv ac \pmod{m}$ . Es folgt  $ab - ac = a(b - c) \equiv 0 \pmod{m}$ . Da  $\gcd(a, m) = 1$  folgt  $m|(b - c)$  und nach Definition  $b \equiv c \pmod{m}$ .  $\square$

**Übung 7.1.**

Gib konkrete Beispiele zu den Sätzen und beweise sie.

**7.6. Eigenschaften der Kongruenz**

Man zeigt einfach, dass für beliebige  $a, b, c$  und  $m \neq 0$  folgende Eigenschaften erfüllt sind:

- $a \equiv a \pmod{m}$  (Reflexivität)
- Falls  $a \equiv b \pmod{m}$ , dann gilt  $b \equiv a \pmod{m}$  (Symmetrie)
- Falls  $a \equiv b \pmod{m}$  und  $b \equiv c \pmod{m}$ , dann  $a \equiv c \pmod{m}$  (Transitivität)

**Definition 7.2: Äquivalenzrelation**

Eine Relation, die obige drei Bedingungen erfüllt, nennt man Äquivalenzrelation.  
Die Äquivalenzrelation  $\pmod{m}$  teilt  $\mathbb{Z}$  in  $m$  Äquivalenzklassen.

Man schreibt manchmal für die Äquivalenzklasse einer Zahl  $a$  etwa  $[a]$  oder auch  $\bar{a}$ , um zwischen Zahl und Klasse zu unterscheiden.

**Übung 7.2.**

Zeige, dass das Gleichungssystem

$$11x - 5y = 7 \tag{1}$$

$$9x + 10y = -3 \tag{2}$$

keine ganzzahlige Lösung besitzt.





Abbildung 5: The Mod Squad

**Übung 7.3.**

Zeige, dass für  $x, y, z \in \mathbb{Z}$  mit

$$x^2 + y^2 = z^2$$

mindestens eine der Zahlen durch 2, mindestens eine durch 3 und mindestens eine durch 5 teilbar ist.

---

## Teilbarkeitsregeln 1

- 2 letzte Ziffer durch 2 teilbar
- 3 Quersumme durch 3 teilbar
- 4 letzte 2 Ziffern durch 4 teilbar
- 5 letzte Ziffer = 0 oder 5
- 6 Zahl durch 2 UND 3 teilbar

## 8. Teilbarkeit

### 8.1. Teilbarkeit durch 3

Es gilt

#### Satz 8.1: Teilbarkeit durch 3

Eine Zahl ist genau dann durch 3 teilbar, wenn es ihre Quersumme ist.



*Beweis.* Sei  $n \in \mathbb{N}$  im Dezimalsystem als

$$n = a_r a_{r-1} \dots a_1 a_0$$

geschrieben, so ist explizit

$$n = a_0 + 10 \cdot a_1 + \dots + 10^r \cdot a_r.$$

Modulo 3 ist jetzt  $10 \equiv 1 \pmod{3}$ , also  $[10] = [1]$ . Damit ist

$$\begin{aligned}[n] &= [a_0 + 10 \cdot a_1 + \dots + 10^r \cdot a_r] \\ &= [a_0] + [10] \cdot [a_1] + \dots + [10]^r \cdot [a_r] \\ &= [a_0] + [a_1] + \dots + [a_r] \\ &= [a_0 + a_1 + \dots + a_r]\end{aligned}$$

das heisst, die Zahl  $n$  ist Modulo 3 gleich ihrer Quersumme. Insbesondere ist  $n$  genau dann durch 3 teilbar, wenn die Quersumme dies ist.  $\square$

#### Übung 8.1.



Vervollständigen und begründen Sie folgende Aussage:

Eine natürliche Zahl ist genau dann durch ... teilbar, wenn es ihre alternierende Quersumme ist.

Unter der *alternierenden Quersumme* verstehen wir die von rechts nach links gelesene „Quersumme“ mit abwechselnden Vorzeichen. Also beispielsweise wäre zur Zahl 123 die alternierende Quersumme  $3 - 2 + 1 = 2$ .

## 8.2. Teilbarkeit durch 11

Mit der Überlegung aus dem vorigen Beispiel lässt sich rasch eine Bedingung für die Teilbarkeit einer Zahl durch 11 herleiten. Es ist  $10 \equiv -1 \pmod{11}$ , also ist analog zur obigen Rechnung für eine Dezimalzahl

$$n \equiv a_0 - a_1 + a_2 - \cdots + (-1)^r a_r \pmod{11}.$$

Auf der rechten Seite steht hier die alternierende Quersumme. Eine Zahl ist also genau dann durch 11 teilbar, wenn es ihre alternierende Quersumme ist.

**Beispiel 8.2.1.** 12375 ist durch 11 teilbar, denn

$$5 - 7 + 3 - 2 + 1 = 0.$$

## 8.3. Teilbarkeit im Hexadezimalsystem

### Übung 8.2.



Überlege dir Teilbarkeitsregeln im Hexadezimalsystem. Betrachte dazu die Teilbarkeit einer Hexadezimalzahl durch 3, 5 und 17.

## 8.4. Notizen zu den Übungen

### Notizen zu Übung 8.2

Zum Beispiel zur Addition:



$$4 \equiv 10 \pmod{3} \Leftrightarrow 4 + 2 \equiv 10 + 2 \pmod{3}.$$

*Beweis.* Beweis über die Definition: Gelte  $a \equiv b \pmod{n}$  und sei  $c \in \mathbb{Z}$  beliebig. Das heisst  $\exists k \in \mathbb{Z}$  mit  $b - a = kn$  und daraus

$$kn = b - a = (b + c) - (a + c).$$

Das heisst  $a + c \equiv b + c \pmod{n}$ . □

Die übrigen Sätze zeigt man analog oder verwendet bereits bewiesene.

### Notizen zu Übung 8.2



Modulo 2 gilt:

$$x + y \equiv 1 \tag{3}$$

$$x \equiv 1 \tag{4}$$

Also ist  $x$  ungerade und  $y$  gerade. Modulo 5 gilt:

$$x \equiv 2 \tag{5}$$

$$4x \equiv 2 \tag{6}$$

Es folgt  $5x \equiv 4$ , Widerspruch, da  $5x \equiv 0 \pmod{5}$ !

### Notizen zu Übung 8.2



Modulo 2 betrachten wir die Fälle  $z^2 \equiv 0$  und  $z^2 \equiv 1$ . Im ersten Fall gälte dann  $x^2 \equiv 0$  und  $y^2 \equiv 0$  oder  $x^2 \equiv 1$  und  $y^2 \equiv 1$ . Für den zweiten Fall gilt oEdA  $x^2 \equiv 1$  woraus  $y^2 \equiv 0$  und damit  $y \equiv 0$  folgt. Also ist immer sicher mindestens eine Zahl durch 2 teilbar.

Modulo 3 gelte  $z^2 \equiv 1$ . Dann muss oEdA  $x^2 \equiv 1$  und  $y^2 \equiv 0$  gelten, also  $y \equiv 0 \pmod{3}$ . Oder es wäre  $x^2 \equiv 2$  und  $y^2 \equiv 2$ . Aber das kann wegen  $x \equiv \sqrt{2}$  nicht passieren. Aus dem gleichen Grund muss  $z^2 \equiv 2$  nicht betrachtet werden und für  $z^2 \equiv 0$  ist die Behauptung trivial. Somit ist mindestens eine Zahl durch 3 teilbar.

Modulo 5 äquivalent zu 0 ist wiederum trivial. Gelte noch Modulo 5  $z^2 \equiv 1$  oder  $z^2 \equiv 4$ . Im ersten Fall sind nur möglich  $x \equiv 1$  und  $y \equiv 0$  oder viceversa. Im zweiten Fall klappt nur  $x \equiv 4$  woraus  $y \equiv 0$  folgt. Also ist sicher mindestens eine Zahl durch 5 teilbar.

**Notizen zu Übung 8.2**

*Beweis.* Die Antwort ist 11. Denn für  $n \in \mathbb{N}_0$  gilt

$$10^n \equiv (-1)^n \pmod{11},$$

da ja  $10 \equiv -1 \pmod{11}$ . Daraus folgt

$$\begin{aligned} a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \cdots + a_1 \cdot 10^1 + a_0 \cdot 10^0 \\ \equiv a_k \cdot (-1)^k + a_{k-1} \cdot (-1)^{k-1} + \cdots + a_1 \cdot (-1)^1 + a_0 \cdot (-1)^0 \pmod{11} \\ \equiv (-1)^k a_k + (-1)^{k-1} a_{k-1} + \cdots - a_1 + a_0 \pmod{11} \end{aligned}$$

Das heisst man kann bequem von rechts nach links die alternierende Quersumme bilden und gucken, ob die durch 11 teilbar ist.  $\square$

**Notizen zu Übung 8.2**

Für das Hexadezimalsystem (16er System) könnte man eine Teilbarkeitsregel mit Quersumme für die Teilbarkeit mit 3 oder 5 formulieren, da für  $n \in \mathbb{N}_0$  gilt:  $16^n \equiv 1 \pmod{3}$  bzw.  $\pmod{5}$ . Für die alternierende Quersumme kann man sinngemäss eine Teilbarkeitsregel  $\pmod{17}$  formulieren, da  $16^n \equiv (-1)^n \pmod{17}$ .



Abbildung 6: Barcode EAN 13

## 9. Barcode

Ein ähnliches System und Prüfverfahren existiert für die wohlbekannten Barcodes zum Beispiel auf Verpackungen.

Bezahlt man in einem Geschäft seine Ware, so wird der Preis in aller Regel nicht per Hand eingegeben. Vielmehr wird der Strichcode, der sich auf jedem Artikel befindet, eingescannt; und selbst wenn dies aufgrund technischer Probleme nicht funktioniert, gibt der Kassierer nicht den Preis, sondern die zum Strichcode gehörende Ziffernfolge ein. Wie kommt es, dass ein Fehler beim Eingeben immer auffällt?

Man braucht also eine Idee, wie man Fehler bei der Eingabe mit hoher Wahrscheinlichkeit bemerken kann; und die Idee heisst Redundanz. Man hängt an den Teil des Codes, den man zur Identifikation des Produkts braucht, zusätzliche (redundante) Ziffern an, deren einziger Sinn es ist, den Code fehlerresistenter zu machen. Dabei sollten möglichst wenig zusätzliche Ziffern eine möglichst hohe Sicherheit bieten. Weshalb und wie man das mit nur einer Ziffer erreichen kann hat mit Modulo Arithmetik und Gruppen zu tun. Ähnliche Verfahren werden auch bei Kreditkarten, ISBN-Nummern, Seriennummer von Geldscheinen etc. verwendet.

## 10. Die alte ISBN-Nummer

### 10.1. Prüfziffern

Als ein kleines Beispiel beschreiben wir das alte ISBN-System. Dieses ist zwar nicht mehr ganz aktuell, aber für unsere Zwecke instruktiver als die inzwischen verwendete Variante.

Jedem Buch ist eine zehnstellige ISBN-Nummer zugeordnet, die zur eindeutigen Identifikation dient. Von diesen 10 Ziffern sind die ersten 9 die eigentliche Information, die zehnte ist eine Prüfziffer. Diese soll eine gewisse Sicherheit zur Vermeidung von Tipp- und Übertragungsfehlern gewährleisten. Bezeichne

$$Y = a_1 a_2 a_3 \dots a_9 a_{10}$$

eine ISBN Nummer. Dabei ist  $a_i \in \{0, 1, 2, \dots, 9\}$  und

$$a_{10} \equiv a_1 + 2a_2 + 3a_3 + \dots + 9a_9 = \sum_{i=1}^9 ia_i \pmod{11}.$$

Dies ergibt einen Wert zwischen 0 und 10. Falls man 10 erhält schreibt man ein X.

**Beispiel 10.1.1.** Wir nehmen als Beispiel das Buch

P. Hartmann, *Mathematik für Informatiker*, Vieweg, 2003.

mit der (alten) ISBN-Nummer 3-8348-0096-1.

Natürlich kann man nicht erwarten, dass so alle Fehler erkannt werden. Aber, wie wir gleich sehen werden, schützt das Modul 11 vor den alltäglichen.

### 10.2. Ziffer fehlerhaft eingetippt

Geschieht der Fehler in der Prüfziffer selbst, dann ist der Fall klar. Wir können also den Fehler zwischen 1 und 9 annehmen und müssen zeigen, dass die Prüfziffer falsch ist. Sei also

$$Y' = a_1 \dots a'_i \dots a_{10}$$

die fehlerhafte ISBN mit dem Fehler an der  $i$ -ten Stelle,  $1 \leq i \leq 9$ . Die Prüfziffer wäre so

$$a'_{10} = \sum_{j \neq i} ja_j + ia'_i \pmod{11}$$

Wir haben aber  $a_{10}$  und es gilt

$$a_{10} - a'_{10} = ia_i - ia'_i = i(a_i - a'_i) \mod 11$$

Wegen  $a_i \neq a'_i$  ist  $a_i - a'_i \neq 0$  und wegen  $1 \leq i \leq 9$  auch  $i \neq 0$ . Daraus folgt mit einer nicht ganz trivialen Überlegung, dass  $i(a_i - a'_i) \not\equiv 0 \mod 11$ . Dabei ist die Wahl des Moduls wichtig. Entscheidend für die letzte Folgerung ist, dass 11 eine Primzahl ist, denn für diese haben wir

### Satz 10.1: Primfaktorsatz

Sind  $p$  prim und  $a, b \in \mathbb{Z}$  mit  $p|ab$ , so gilt  $p|a$  oder  $p|b$ .

Wir brauchen die Negation des obigen Satzes: Teilt  $p$  weder  $a$  noch  $b$ , dann teilt  $p$  auch nicht  $ab$ .

*Beweis.* Wenn  $p$  weder  $a$  noch  $b$  teilt, dann kommt  $p$  nicht in der Primfaktorzerlegung von  $a$  und  $b$  vor, also auch nicht in der Primzahlzerlegung des Produkts  $ab$ . Das heisst  $p$  teilt  $ab$  nicht.  $\square$

Damit ist gezeigt, dass insbesondere für  $p = 11$  der letzte Schritt gilt und damit die Prüfziffer der ISBN eine fehlerhafte Ziffer erkennt.

### Übung 10.1.



Früher wurde für die Buchklassifikation anstelle der heute gebräuchlichen ISBN13- die **ISBN10**-Nummer verwendet. Diese beiden Nummern unterscheiden sich nur durch das Präfix 978 und die Prüfziffer, die restlichen 9 Ziffern stimmen überein. Ich habe mich in dieses Beispiel für die ISBN10 entschieden, da sie rechnerisch etwas handlicher ist.

Das Buch *Mathematik für Informatiker* hat die ISBN-10 Nummer 3 – 8348 – 0096 – 1



wobei die letzte Ziffer, 1, als Prüfziffer (Checksum) fungiert. Diese letzte Ziffer  $a_{10}$  wird in der ISBN10-Variante aus den vorangehenden Ziffern wie folgt berechnet:

$$a_{10} \equiv \sum_{k=1}^9 k \cdot a_k \mod 11.$$

- a) Überprüfe, ob die Checksum 1 korrekt ist.
- b) Wähle eine beliebige Position in der ISBN-Nummer aus und vertippe dich (absichtlich). Berechne nun die Prüfziffer der „vertippten“ Nummer.
- c) Angenommen, man vertippe sich an genau 2 Stellen, sagen wir Positionen 2 und 5. Registriert die Prüfziffer die Vertipper? Finde ein Beispiel für einen „Doppelvertipper“, der nicht erkannt wird.
- d) In wieviel Prozent der Fälle registriert die Prüfziffer den Vertipper an diesen Positionen nicht?

**Bemerkung 10.2.1.** All dies würde nicht funktionieren, wenn wir anstelle von 11 beispielsweise 10 als Modul verwendet hätten. Denn wegen  $10 = 2 \cdot 5$ , also  $2 \cdot 5 \equiv 0 \pmod{10}$  würde etwa ein Fehler an der  $i = 5$ -ten Stelle nicht erkannt, wenn die fehlerhafte Ziffer um 2 von der korrekten Ziffer abweicht. Die Prüfziffer Modulo 10 bliebe unverändert.

### Übung 10.2.



Schreibe eine Python-Funktion, die zu gegebenem Input einer ISBN10-Nummer als Output angibt, ob die Nummer korrekt ist oder nicht.

Verwende anschliessend das Programm um zu testen, dass die Prüfziffer bemerkt, falls man zwei Ziffern vertauscht hat.

### Übung 10.3.



Zeige, dass die Checksum (siehe Aufgabe ?? auf Seite ??) einen Vertauscher bemerkt. Zeige dies für 2 Ziffern, die nicht zwingend aufeinander folgen.

### Übung 10.4.



Bei der ISBN13 berechnet sich die Prüfziffer  $z_{13}$  via

$$z_{13} \equiv 10 - \left( \sum_{k=1}^{12} z_k \cdot 3^{(k+1) \pmod{2}} \pmod{10} \right) \pmod{10}.$$

Überprüfen Sie die Korrektheit der ISBN13 Prüfziffer aus Aufgabe ?? auf Seite ??.

**Bemerkung 10.2.2.** Wie oben gesehen, ist also die Wahl des Moduls entscheidend. Bei 9 informationstragenden Ziffern braucht man also eine Primzahl grösser oder gleich 10, und 11 ist dafür die kleinstmögliche Wahl.

### 10.3. Zahlendreher

Die ISBN erkennt nicht nur einzelne fehlerhafte Ziffern, sondern auch den am häufigsten auftauchende Fehlertyp: das Vertauschen zweier aufeinanderfolgender Ziffern. In der Tat erkennt die Prüfziffer sogar Vertauschen von nicht unmittelbar aufeinanderfolgenden Ziffern, was zwar weniger vorkommt, aber für den folgenden Beweis ohne Mehraufwand mit einbezogen werden kann.



Sei

$$Y' = a_0 \dots a_{i-1} a_j a_{i+1} \dots a_{j-1} a_i a_{j+1} \dots a_{10}$$

eine falsche ISBN, die durch Vertauschen der  $i$ -ten mit der  $j$ -ten Ziffer entstand,  $1 \leq i < j \leq 9$ . Zwei Fälle lassen wir aussen vor. Erstens, dass die Prüfziffer eine der vertauschten Ziffern ist (diesen Fall könnte man separat behandeln), und zweitens, dass die vertauschten Ziffern identisch sind, dann hätte ja der Verdreher keine Wirkung. Als Prüfziffer für  $Y'$  erhält man so

$$a'_{10} \equiv \sum_{k \neq i,j} k a_k + i a_j + j a_i \pmod{11},$$

also

$$\begin{aligned} a_{10} - a'_{10} &= ia_i + ja_j - ia_j - ja_i \\ &= i(a_i - a_j) - j(a_i - a_j) \\ &= (i - j)(a_i - a_j). \end{aligned}$$

Wegen  $-8 \leq i - j < 0$  und  $0 < |a_i - a_j| \leq 9$  gilt wiederum  $i - j \not\equiv 0 \pmod{11}$  und  $a_i - a_j \not\equiv 0 \pmod{11}$ . Daraus folgt analog zur fehlerhaften Ziffer  $a_{10} - a'_{10} \not\equiv 0$ . Die Prüfziffer ist also fehlerhaft, und der Zahlendreher wird erkannt.

#### Übung 10.5.



Teste einen Zahlendreher anhand von 3-8348-0069-0.

#### Übung 10.6.



Zeige, dass die Checksum (siehe Aufgabe ?? auf Seite ??) einen Vertauscher bemerkt. Zeige dies für 2 Ziffern, die nicht zwingend aufeinander folgen.

#### Notizen zu Übung 10.6



*Beweis.* Seien  $i, j \in \{1, 2, \dots, 9\}$  mit  $i \neq j$  die vertauschten Positionen. Die involvierten Ziffern unterschieden sich natürlich auch,  $a_i \neq a_j$ , da sonst der Vertauscher gar nicht bemerkt würde. Betrachten Sie die korrekte,  $a_{10}$ , versus die inkorrekte,  $\tilde{a}_{10}$ , Checksum.

Die Differenz ist

$$\begin{aligned}a_{10} - \tilde{a}_{10} &= i \cdot a_i + j \cdot a_j - (i \cdot a_j + j \cdot a_i) \\&= i \cdot (a_i - a_j) + j \cdot (a_j - a_i) \\&= i \cdot (a_i - a_j) - j \cdot (a_i - a_j) \\&= (i - j) \cdot (a_i - a_j) \\&\not\equiv 0 \pmod{11}\end{aligned}$$

wobei man beim letzten Schritt gleich argumentiert wie im vorangegangenen Beweis: teilt die Primzahl 11 weder den einen noch den andern Faktor, dann sicher auch nicht das Produkt. Also teilt 11 nicht  $a_{10} - \tilde{a}_{10}$  und damit unterscheiden sich die Prüfziffern Modulo 11.  $\square$

## 10.4. Notizen zu den Übungen

### Notizen zu Übung 10.6



- a) Es ist  $1 \cdot 3 + 2 \cdot 8 + 3 \cdot 3 + 4 \cdot 4 + 5 \cdot 8 + 6 \cdot 0 + 7 \cdot 0 + 8 \cdot 9 + 9 \cdot 6 = 210 \equiv 1 \pmod{11}$ .
- b) Wenn ich mich zum Beispiel an der Stelle 5 vertippe, 3834900961, dann kriege ich als Checksum 6  $\not\equiv 1$ .
- c) Wenn man sich an den Stellen 2 und 5 vertippt, dann hat man als Differenz der Checksums

$$a_{10} - \tilde{a}_{10} = 2(a_i - \tilde{a}_i) + 5(a_j - \tilde{a}_j).$$

Nun probiert man für  $a_i, a_j, \tilde{a}_i, \tilde{a}_j \in \{0, 1, \dots, 9\}$  alle Kombinationen aus, die  $\pmod{11} \equiv 0$  ergeben. Denn in diesem Fall werden die Vertipper nicht bemerkt. Das ist im Allgemeine aufwändig und von den konkreten Ziffern abhängig. Für die vorliegende Nummer klappt dies beispielsweise für 3734400961, da  $2 \cdot (8 - 7) + 5 \cdot (8 - 4) = 22 \equiv 0 \pmod{11}$ .

- d) Man hat konkret

$$a_{10} - \tilde{a}_{10} = 2(8 - \tilde{a}_i) + 5(8 - \tilde{a}_j),$$

da sowohl an Position 2 als auch an Position 5 eine 8 steht. Als mögliche Differenz durch Vertipper ergibt sich eine Zahl aus der Menge

$$\{8, 7, 6, 5, 4, 3, 2, 1, -1\}.$$

Diese gewichtet man mit der Position 2 bzw. 5 und prüft, welche Summen Modulo 11 äquivalent 0 sind. In der Illustration 7 auf Seite 58 sind links die möglichen Differenzen  $8 - \tilde{a}_i$  und  $8 - \tilde{a}_j$  und rechts diese mit 2 bzw. 5 multipliziert abzulesen. Eine Kante wurde dann eingezeichnet, wenn die Summe der beiden Spaltenwerte  $\pmod{11}$  äquivalent 0 ist, der Vertipper also nicht bemerkt wird. Beispielsweise bedeutet die Kante von 16 zu  $-5$  folglich  $16 + (-5) = 11 \equiv 0 \pmod{11}$ . Dies geschieht durch den Vertipper 0 an der Stelle 2 und 9 an der Stelle 5.

Das sind  $\frac{9}{81} = \frac{1}{9} \approx 11\%$  der Fälle, in denen ein Vertipper an den zwei Positionen 2 und 5 nicht erkannt wird.

### Notizen zu Übung 10.6



Ein Beispiel ist

```
# Funktion zur Kontrolle einer ISBN10
def isbncheck(isbnr):
    # Einzelne Ziffern aus der Nummer listen
    isbnls = [int(num) for num in str(isbnr)]
```

|    |    |
|----|----|
| 8  | 8  |
| 7  | 7  |
| 6  | 6  |
| 5  | 5  |
| 4  | 4  |
| 3  | 3  |
| 2  | 2  |
| 1  | 1  |
| -1 | -1 |

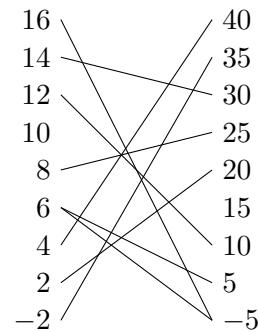


Abbildung 7: Mögliche Differenzen (ungewichtet und gewichtet) der Vertipper

```

summod = 0
# Ziffern gewichten, zusammenzaehlen und mod 11 rechnen
for k in range(1,10):
    summod = (summod + (k)*isbnls[k-1]) % 11
# Checksum vergleichen mit Pruefziffer
if summod == isbnls[9]:
    return print("ok")
else:
    return print("tatataaa")

```

### Notizen zu Übung 10.6



*Beweis.* Seien  $i, j \in \{1, 2, \dots, 9\}$  mit  $i \neq j$  die vertauschten Positionen. Die involvierten Ziffern unterschieden sich natürlich auch,  $a_i \neq a_j$ , da sonst der Vertauscher gar nicht bemerkt würde. Betrachten Sie die korrekte,  $a_{10}$ , versus die inkorrekte,  $\tilde{a}_{10}$ , Checksum. Die Differenz ist

$$\begin{aligned}
 a_{10} - \tilde{a}_{10} &= i \cdot a_i + j \cdot a_j - (i \cdot a_j + j \cdot a_i) \\
 &= i \cdot (a_i - a_j) + j \cdot (a_j - a_i) \\
 &= i \cdot (a_i - a_j) - j \cdot (a_i - a_j) \\
 &= (i - j) \cdot (a_i - a_j) \\
 &\not\equiv 0 \pmod{11}
 \end{aligned}$$

wobei man beim letzten Schritt gleich argumentiert wie im vorangegangenen Beweis: teilt die Primzahl 11 weder den einen noch den andern Faktor, dann sicher auch nicht das Produkt. Also teilt 11 nicht  $a_{10} - \tilde{a}_{10}$  und damit unterscheiden sich die Prüfziffern Modulo 11.  $\square$

### Notizen zu Übung 10.6



Wir setzen die ISBN13-Nummer  $978 - 3 - 8348 - 0096 - 1$  ein, rechnen etappenweise, zuerst die Summe  $\sum_{k=1}^{12} z_k \cdot 3^{(k+1) \bmod 2} \bmod 10$

$$\begin{aligned} &= 9 \cdot 1 + 7 \cdot 3 + 8 \cdot 1 + 3 \cdot 3 + 8 \cdot 1 + 3 \cdot 3 + 4 \cdot 1 + 8 \cdot 3 + 0 + 0 + 9 \cdot 1 + 6 \cdot 3 \\ &= 119 \equiv 9 \pmod{10} \end{aligned}$$

Also ist insgesamt  $z_{13} = 10 - 9 \equiv 1 \pmod{10} = 1$ .

**Notizen zu Übung 10.6**



Brauche dein Python-Programm von oben.



## 11. Rechnen Modulo 17

Nimmt man für das Modul eine Primzahl, so hat man eine Reihe von interessanten Besonderheiten. So ist beispielsweise Modulo 17  $13 + 8 = 21 \equiv 4 \pmod{17}$  oder  $4 - 9 = -5 \equiv 12 \pmod{17}$ . Ferner  $5 \cdot 4 = 20 \equiv 3 \pmod{17}$  und  $9 \cdot 2 = 18 \equiv 1 \pmod{17}$ . Die letzte Kongruenz besagt, dass 9 dasselbe ist wie  $\frac{1}{2}$  (Modulo 17).

### 11.1. Potenzen

Wir berechnen illustrativ alle Potenzen von 3 Modulo 17.

#### Übung 11.1.



Vervollständige folgende Tabelle

|       |   |   |    |    |    |    |    |    |
|-------|---|---|----|----|----|----|----|----|
| n     | 0 | 1 | 2  | 3  | 4  | 5  | 6  | 7  |
| $3^n$ | 1 | 3 | 9  | 10 |    |    |    |    |
| n     | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| $3^n$ |   |   |    |    |    |    |    |    |

Es fällt auf, dass jede Zahl ungleich 0 eine Potenz von 3 ist, also jeder mögliche, nicht-triviale Rest taucht genau einmal auf. Ausserdem stellt man fest, dass

$$3^{16} \equiv 3 \cdot 6 = 18 \equiv 1 \pmod{17}.$$

Die Tatsache, dass alle Zahlen ausser 0 eine Potenz von 3 sind und ausserdem  $3^{16} \equiv 1 \pmod{17}$ , hat zur Folge, dass jede Zahl  $a \not\equiv 0 \pmod{17}$  als 16-te Potenz den Wert 1 hat. Denn  $a$  ist eine Potenz von 3, also  $a = 3^n$  und daher

$$a^{16} = (3^n)^{16} = (3^{16})^n \equiv 1^n = 1 \pmod{17}$$

Das bedeutet, es gilt auch

$$a^{17} = a, a^{33} = a, a^{49} = a, \dots$$

und daraus erhält man

$$a = a^{33} = a^{3 \cdot 11} = (a^3)^{11}.$$

**Bemerkung 11.1.1.** Man zieht die dritte Wurzel, indem man mit 11 potenziert.

**Übung 11.2.**

Ziehe durch Potenzieren

- a) die siebte Wurzel aus  $a^7 \pmod{17}$
- b) die fünfte Wurzel aus  $a^5 \pmod{17}$

## 11.2. Kryptographie — eine erste Idee

Diese letztgenannten Beziehungen enthalten eine der Grundideen zur Verschlüsselung mittels Zahlentheorie. Benutzt man die 16 Zahlen von 1 bis 16 als (verkürztes) Alphabet, so kann man die Potenzierung mit 3 als Verschlüsselung und die Potenzierung mit 11 als Entschlüsselung benutzen.

**Beispiel 11.2.1.** Es gilt  $a^{33} \equiv a \pmod{17}$ . Wir wählen den Buchstaben c, den dritten im Alphabet, und verschlüsseln ihn durch  $3^3 \equiv 10 \pmod{17}$ , was einem K Ciphertext entspricht. Wir entschlüsseln durch  $10^{11} \equiv 3 \pmod{17}$  und haben wieder den Klartext c.

Ein besonders angenehmer Aspekt dieses Verfahrens ist, dass man zur Ver- und Entschlüsselung dasselbe Verfahren benutzen (Potenzierung) und dass die Reihenfolge von Ver- und Entschlüsselung vertauscht werden kann. Dies eröffnet interessante Möglichkeiten in der Kryptographie. Die Anwendbarkeit des Verfahrens hängt nun entscheidend davon ab, ob und wie leicht man zum Verschlüsselungsexponenten 3 den Entschlüsselungsexponenten 11 ermitteln kann.

**11.3. Notizen zu den Übungen****Notizen zu Übung 11.2**

|       |    |    |    |    |    |    |    |    |
|-------|----|----|----|----|----|----|----|----|
| n     | 0  | 1  | 2  | 3  | 4  | 5  | 6  | 7  |
| $3^n$ | 1  | 3  | 9  | 10 | 13 | 5  | 15 | 11 |
| n     | 8  | 9  | 10 | 11 | 12 | 13 | 14 | 15 |
| $3^n$ | 16 | 14 | 8  | 7  | 4  | 12 | 2  | 6  |

**Notizen zu Übung 11.2**

Es gilt für ein beliebiges Element  $a \in \mathbb{Z}_{17}^*$ , dass  $a^{16} \equiv 1 \pmod{17}$ . Also ist  $a^{17} \equiv a$  und somit für  $k \in \mathbb{N}_0$ :  $a^{33} \equiv a^{49} \equiv a^{65} \equiv a^{17+16k} \equiv a$ . Somit ist  $(a^7)^7 \equiv a$  und  $(a^5)^{13} \equiv a$ .

---

## A. Die Osterformel von Gauss

Die Gauss'sche Osterformel erlaubt die Berechnung des Osterdatums für ein gegebenes Jahr. Das Verfahren gilt allgemein für den Gregorianischen Kalender.



**Bemerkung A.0.1.** In seltenen Fällen kann der Algorithmus im Gregorianischen Kalender den 26. April als spätesten Ostersonntag liefern. Die bei der Kalenderreform aufgestellte Zusatzbestimmung, dass der letzte mögliche Ostersonntag der 25. April ist, muss zusätzlich beachtet werden.

Nun zum Verfahren ( $\div$  steht für eine ganzzahlige Division ohne Nachkommastellen):

$$\begin{aligned}a &= \text{Jahr} \mod 19 \\b &= \text{Jahr} \mod 4 \\c &= \text{Jahr} \mod 7 \\k &= \text{Jahr} \div 100 \\p &= (8k + 13) \div 25 \\q &= k \div 4 \\M &= (15 + k - p - q) \mod 30 \\N &= (4 + k - q) \mod 7 \\d &= (19a + M) \mod 30 \\e &= (2b + 4c + 6d + N) \mod 7\end{aligned}$$

Mit den so bestimmten Variablen kann man nun das Osterdatum berechnen:

$$\text{Ostern} = (22 + d + e)\text{ter März},$$

wobei der 32. März der 1. April ist etc.

### Übung A.1.



Berechne das Datum der nächsten Ostern.

### Notizen zu Übung A.1



Selbstkontrolle ;)

## B. Gruppen

### Definition 2.1: Gruppe

Eine Gruppe  $\langle \mathbb{G}, * \rangle$  ist eine nichtleere Menge  $\mathbb{G}$  zusammen mit einer inneren Verknüpfung  $* : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}$  (Abgeschlossenheit), so dass

- $\forall a, b, c \in \mathbb{G}: a * (b * c) = (a * b) * c$  (Assoziativität)
- $\exists e \in \mathbb{G}$  so, dass  $\forall a \in \mathbb{G}: e * a = a * e = a$  (Neutrales)
- $\forall a \in \mathbb{G} \exists \tilde{a} \in \mathbb{G}$  so, dass  $a * \tilde{a} = \tilde{a} * a = e$  (Inverse)

### Übung B.1.



Bei welchen Strukturen handelt es sich um Gruppen?

a)  $\langle \mathbb{N}, + \rangle$

b)  $\langle \mathbb{Z}, + \rangle$

c)  $\langle \mathbb{Q}, \cdot \rangle$

d)  $\langle \mathbb{Z}_6^*, \cdot \rangle$

e)  $\langle \mathbb{N}, - \rangle$

f)  $\langle \mathbb{Z}, \cdot \rangle$

g)  $\langle \mathbb{R}, \cdot \rangle$

h)  $\langle \mathbb{Z}_{100}^*, + \rangle$

i)  $\langle \mathbb{N}_0, + \rangle$

j)  $\langle \mathbb{Q}, + \rangle$

k)  $\langle \mathbb{Z}_{11}^*, \cdot \rangle$

l)  $\langle \mathbb{Z}_{32}^*, \cdot \rangle$

Falls es sich um eine Gruppe handelt, gib das neutrale Element an und beschreibe, wie man zu einem gegebenen Element  $a \in \mathbb{G}$  sein inverses  $\tilde{a} \in \mathbb{G}$  findet. Falls es keine Gruppe ist, gib ein Argument an, an dem die Struktur scheitert.

**Übung B.2.**

Zeige, dass das neutrale Element einer Gruppe eindeutig bestimmt ist.

**Übung B.3.**

Zeige, dass das inverse Element  $\tilde{a} \in \mathbb{G}$  jedes Elements  $a \in \mathbb{G}$  eindeutig bestimmt ist.

**B.1. Primitivwurzeln****Definition 2.2: Primitivwurzel**

Ein Element  $a \in \mathbb{Z}_n^*$  mit Multiplikation nennen wir Primitivwurzel Modulo  $n$ , falls  $a^k$  mit  $k \in \mathbb{N}$  alle Reste erzeugt.

**Beispiel B.1.1.**  $2 \in \mathbb{Z}_7^*$  ist keine Primitivwurzel, da  $2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 1, 2^4 \equiv 2, \dots$ .

Hingegen ist  $3 \in \mathbb{Z}_7^*$  Primitivwurzel:  $3^1 \equiv 3, 3^2 \equiv 2, 3^3 \equiv 6, 3^4 \equiv 4, 3^5 \equiv 5, 3^6 \equiv 1$ .

**Übung B.4.**

Bestimme für  $k \in \mathbb{N}$  in der Gruppe  $\langle \mathbb{Z}_{17}^*, \cdot \rangle$  die Werte der Potenzen  $2^k$  und  $3^k$ .

**Übung B.5.**

Zeige: Sei  $a \in \mathbb{Z}_{17}^*$  beliebig. Dann gilt  $a^{16} \equiv 1 \pmod{17}$ .

**Definition 2.3: Euler'sche  $\varphi$ -Funktion**

Für  $n \in \mathbb{N}$  ist die Euler'sche  $\varphi$ -Funktion definiert durch

$$\varphi(n) := \text{card}(\{a \in \mathbb{N} \mid 1 \leq a \leq n, \gcd(a, n) = 1\}).$$

**Übung B.6.**

Bestimmen Sie die Funktionswerte der Euler'schen  $\varphi$ -Funktion für die Argumente

- a) 6
- b) 10
- c) 11

- d) 51
- e)  $p$  für  $p \in \mathbb{N}$  prim
- f)  $p \cdot q$  für  $p, q \in \mathbb{N}$  prim

**Übung B.7.**



Welche Elemente  $a \in \mathbb{Z}_{12}^*$  haben inverse Elemente in der Struktur  $\langle \mathbb{Z}_{12}^*, \cdot \rangle$ ?

**Übung B.8.**



Wie viele Primitivwurzeln hat die multiplikative Restklassengruppe  $\langle \mathbb{Z}_{73}^*, \cdot \rangle$ ?

**Übung B.9.**



Bestimme alle Primitivwurzeln der Gruppe  $\langle \mathbb{Z}_{13}^*, \cdot \rangle$ .

**Übung B.10.**



Bestimmen Sie alle Primitivwurzeln der Gruppe  $\langle \mathbb{Z}_{17}^*, \cdot \rangle$ .

**Übung B.11.**



Bestimmen Sie alle Primitivwurzeln der Gruppe  $\langle \mathbb{Z}_{31}^*, \cdot \rangle$ .

## B.2. Notizen zu den Übungen

### Notizen zu Übung B.11



Es gibt teilweise mehrere Begründungen pro Teilaufgabe. Ich habe mich jeweils mit einer begnügt.

- a) Das neutrale Element der Addition, die 0, fehlt.
- b) Dies ist eine Gruppe mit neutralem Element 0. Das Inverse zu  $a \in \mathbb{Z}$  ist  $\tilde{a} = -a$ .
- c) Dies ist keine Gruppe, denn 0 hat kein inverses Element. Jedoch ist  $\langle \mathbb{Q}^*, \cdot \rangle$  eine Gruppe mit neutralem Element 1, und zu  $a \in \mathbb{Q}^*$  ist  $\tilde{a} = \frac{1}{a}$  invers.
- d) Dies ist keine Gruppe. Wegen  $2 \cdot 3 \equiv 0$  ist die Verknüpfung nicht abgeschlossen.
- e) Auch diese Struktur ist nicht abgeschlossen. Beispielsweise ist  $5 - 7 = -2 \notin \mathbb{N}$ .
- f) 0 hat in dieser Struktur kein inverses Element, also handelt es sich nicht um eine Gruppe.
- g) Wiederum ist die 0 Spielverderber, da sie kein inverses Element bezüglich der Multiplikation besitzt. Jedoch ist  $\langle \mathbb{R}^*, \cdot \rangle$  eine Gruppe mit neutralem Element 1 und zu  $a \in \mathbb{R}^*$  ist  $\tilde{a} = \frac{1}{a}$  invers.
- h) Dies ist keine Gruppe, da das neutrale Element 0 fehlt. Jedoch wäre  $\langle \mathbb{Z}_{100}, + \rangle$  eine Gruppe mit neutralem Element 0 und inversen Elementen  $\tilde{a} = 100 - a \pmod{100}$ .

### Notizen zu Übung B.11



*Beweis.* Widerspruchsbeweis: Sei ein neutrales Element  $e$  nicht eindeutig. Es gebe also zwei verschiedene neutrale Elemente  $e_1, e_2 \in \mathbb{G}$ ,  $e_1 \neq e_2$ , beide  $*$ -neutral. Es ist

$$e_1 = e_1 * e_2 = e_2,$$

wobei der erste Schritt gilt, da  $e_2$   $*$ -neutral ist und Schritt zwei, da  $e_1$   $*$ -neutral ist. Also insgesamt  $e_1 = e_2$ . Widerspruch zur Annahme!  $\square$

### Notizen zu Übung B.11



*Beweis.* Widerspruchsbeweis mit Gegenannahme: Seien  $\tilde{a}_1 \neq \tilde{a}_2$  in  $\mathbb{G}$  beide  $*$ -invers zu  $a \in \mathbb{G}$ . Betrachte

$$\tilde{a}_1 = \tilde{a}_1 * e = \tilde{a}_1 * (a * \tilde{a}_2) = (\tilde{a}_1 * a) * \tilde{a}_2 = e * \tilde{a}_2 = \tilde{a}_2$$

Widerspruch zur Annahme  $\tilde{a}_1 \neq \tilde{a}_2$ !  $\square$

### Notizen zu Übung B.11



Sei  $k \in \mathbb{N}$ . Betrachte die Tabelle 1 auf Seite 68.

| $k$   | 1 | 2 | 3  | 4  | 5  | 6  | 7  | 8  | 9  | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|-------|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| $2^k$ | 2 | 4 | 8  | 16 | 15 | 13 | 9  | 1  | 2  | 4  | 8  | 16 | 15 | 13 | 9  | 1  |
| $3^k$ | 3 | 9 | 10 | 13 | 5  | 15 | 11 | 16 | 14 | 8  | 7  | 4  | 12 | 2  | 6  | 1  |

Tabelle 1: 2er- und 3er-Potenzen in  $\langle \mathbb{Z}_{17}^*, \cdot \rangle$

### Notizen zu Übung B.11



*Beweis.* Aus Tabelle 1 auf Seite 68 wissen wir, dass für  $a \in \langle \mathbb{Z}_{17}^*, \cdot \rangle$  beliebig es ein  $k \in \mathbb{Z}$  gibt, so dass  $3^k \equiv a$ . Es folgt

$$a^{16} \equiv (3^k)^{16} \equiv (3^{16})^k \equiv 1^k \equiv 1.$$

□

### Notizen zu Übung B.11



Die Euler'sche  $\varphi$ -Funktion einer natürlichen Zahl  $n \in \mathbb{N}$  zählt die Anzahl teilerfremden Zahlen zwischen und inklusive 1 und  $n$ . Im Folgenden werden also für  $\varphi(n)$  immer natürliche Zahlen  $k \in \mathbb{N}$  mit  $1 \leq k \leq n$  betrachtet.

- a)  $\varphi(6) = 2$ , da 1 und 5 teilerfremd zu 6 sind.
- b) Wegen  $10 = 2 \cdot 5$  sind 1, 3, 7 und 9 teilerfremd zu 10, also  $\varphi(10) = 4$ .
- c) Primzahlen haben als grössten gemeinsamen Teiler ungleich 1 nur sich selbst, d.h.  $\varphi(11) = 10$ .
- d)  $51 = 3 \cdot 17$  und man kann die Multiplikativität  $\varphi(3 \cdot 17) = \varphi(3) \cdot \varphi(17)$  der Euler'schen  $\varphi$ -Funktion brauchen:

$$\varphi(3 \cdot 17) = \varphi(3) \cdot \varphi(17) = 2 \cdot 16 = 32.$$

- e) *Beweis.* Ist  $p$  prim, so hat  $p$  per Definition nur die Teiler 1 und sich selbst. Also ist für  $k \in \mathbb{N}$ ,  $1 \leq l \leq p$ , nur im Falle  $l = p$  der  $\gcd(l, p) = p$ , sonst immer 1. Das heisst es gilt  $\varphi(p) = p - 1$ . □

- f) *Beweis.* Betrachten wir für  $p, q \in \mathbb{N}$  prim die natürlichen Zahlen von 1 bis  $pq$ . Das sind natürlich  $pq$  Stück, wovon  $p, 2p, 3p, \dots, qp$  und  $q, 2q, 3q, \dots, pq$  mit  $pq$  nicht den grössten gemeinsamen Teiler 1 haben. Die Anzahl Zahlen, welche mit  $pq$  den grössten

gemeinsamen Teiler 1 haben beträgt also  $pq - p - q + 1$  (+1, da wir  $pq$  bzw.  $qp$  doppelt gezählt haben.). Es ist

$$\varphi(p \cdot q) = pq - p - q + 1 = (p - 1)(q - 1) = \varphi(p) \cdot \varphi(q).$$

□

### Notizen zu Übung B.11



Erwischt man einen Teiler, ausser 1, von 12, dann wird der Rest nie 1, das multiplikativ neutrale Element, betragen. Das heisst alle Elemente mit grösstem gemeinsamen Teiler 1 zu 12 werden ein inverses Element haben. Nämlich sind 1, 5, 7 und 11 alle zu sich selbst invers.

### Notizen zu Übung B.11



Nach Gauss gibt es  $\varphi(\varphi(73))$  Primitivwurzeln. Das sind

$$\varphi(\varphi(73)) = \varphi(72) = \varphi(2) \cdot \varphi(31) = 1 \cdot 30 = 30.$$

### Notizen zu Übung B.11



Nach Carl F. Gauss gibt es  $\varphi(\varphi(13)) = \varphi(12) = 4$  Primitivwurzeln (gcd 1 haben die Werte 1, 5, 7 und 11.). Nun suchen wir eine Primitivwurzel durch Ausprobieren:  $2^1 \equiv 2$ ,  $2^2 \equiv 4$ ,  $2^3 \equiv 8$ ,  $2^4 \equiv 3$ ,  $2^5 \equiv 6$ ,  $2^6 \equiv 12$ ,  $2^7 \equiv 11$ ,  $2^8 \equiv 9$ ,  $2^9 \equiv 5$ ,  $2^{10} \equiv 10$ ,  $2^{11} \equiv 7$ ,  $2^{12} \equiv 1$  ist also eine Primitivwurzel. Damit sind die Primitivwurzeln  $2^1 \equiv 2$ ,  $2^5 \equiv 6$ ,  $2^7 \equiv 11$  und  $2^{11} \equiv 7$ .

### Notizen zu Übung B.11



Es gibt  $\varphi(\varphi(17)) = \varphi(16) = 8$  Primitivwurzeln (gcd 1 haben die Werte 1, 3, 5, 7, 9, 11, 13 und 15.). Aus Tabelle 1 auf Seite 68 entnehmen wir, dass 2 keine, dafür aber 3 eine Primitivwurzel ist. Also sind die Primitivwurzeln von  $\mathbb{Z}_{17}^*$ :  $3^1 \equiv 3$ ,  $3^3 \equiv 10$ ,  $3^5 \equiv 5$ ,  $3^7 \equiv 11$ ,  $3^9 \equiv 14$ ,  $3^{11} \equiv 7$ ,  $3^{13} \equiv 12$  und  $3^{15} \equiv 6$ .

### Notizen zu Übung B.11



Hier haben wir  $\varphi(\varphi(31)) = \varphi(30) = 8$  (1, 7, 11, 13, 17, 19, 23, 29). 2 ist wegen  $2^5 \equiv 1$  keine Primitivwurzel. 3 entpuppt sich als Primitivwurzel, und wir haben somit 3, 11, 12, 13, 17, 21, 22, 24 als solche in  $\mathbb{Z}_{31}^*$ .

## **Abbildungsverzeichnis**

|    |  |    |
|----|--|----|
| 1. | Seltsamste Primzahl . . . . .  | 9  |
| 2. | Primzahlzwillinge . . . . .  | 11 |
| 3. | irrats and transcendents . . . . .                                       | 25 |
| 4. | Babylonische Rechentafel und Sternkarte . . . . .                        | 32 |
| 5. | The Mod Squad . . . . .  | 46 |
| 6. | Barcode EAN 13 . . . . .   | 51 |
| 7. | Mögliche Differenzen (ungewichtet und gewichtet) der Vertipper . . . . . | 58 |