Mathematik III
(für Informatiker)

Oliver Ernst

Professur Numerische Mathematik

Wintersemester 2014/15

TECHNISCHE UNIVERSITÄT
CHEMNITZ

Inhalt

Algebraische Strukturen

- Die bekanntesten algebraische Strukturen kennen wir für Zahlenmengen wie die natürlichen Zahlen $\mathbb{N}$, die ganzen Zahlen $\mathbb{Z}$, die rationalen Zahlen $\mathbb{Q}$, die reellen Zahlen $\mathbb{R}$ und die komplexen Zahlen $\mathbb{C}$.
- Weitere Strukturen, den Vektorraum bzw. Innenproduktraum oder auch Hilbert-Raum haben wir ebenfalls schon kennengelernt. Dabei haben wir festgestellt, dass mehrere konkrete Ausprägungen auf diese abstrakte Struktur passen.
- Sind mathematische Eigenschaften einer algebraischen Struktur einmal ermittelt, so gelten sie natürlich sofort für jedes konkrete Beispiel eines solchen Struktur.
- Nicht unähnlich: abstrakte Datentypen, abstrakte Objekte in der Informatik.

Definition 13.1

Eine binäre Operation auf einer nichtleeren Menge A ist eine Abbildung $\circ : A \times A \to A$. Das Bild eines Elementepaares $(a, b) \in A \times A$ wird mit $a \circ b$ bezeichnet. Das Paar $(A, \circ)$ heißt dann binäre algebraische Struktur oder auch Gruppoid.

Bekannte Zahlenmengen bilden mit den binären Operationen Addition und Multiplikation eine algebraische Struktur:

$$(\mathbb{N}, +), \quad (\mathbb{Z}, +), \quad (\mathbb{Q}, +), \quad (\mathbb{R}, +), \quad (\mathbb{C}, +),$$
$$(\mathbb{N}, \cdot), \quad (\mathbb{Z}, \cdot), \quad (\mathbb{Q}, \cdot), \quad (\mathbb{R}, \cdot), \quad (\mathbb{C}, \cdot).$$

Die Eigenschaft, dass das Ergebnis einer binären Operation auf einer Menge wieder in dieser Menge enthalten ist, nennt man Abgeschlossenheit. So ist etwa $\mathbb{N}$ nicht abgeschlossen bezüglich der Subtraktion.

Bildet $A = \mathbb{N}$ zusammen mit $a \circ b := a^b$ eine algebraische Struktur?

Wichtig sind folgende Eigenschaften algebraischer Strukturen (vgl. Kapitel 1).

Definition 13.2

Sei $(A, \circ)$ eine algebraische Struktur.

(a) Assoziativgesetz: für alle $a, b, c \in A$ gilt $(a \circ b) \circ c = a \circ (b \circ c)$.

(b) Kommutativgesetz: für alle $a, b \in A$ gilt $a \circ b = b \circ a$.

(c) Existenz eines neutralen Elements: Es gibt ein Element $e \in A$ mit der Eigenschaft

$$e \circ a = a \circ e = a \qquad \text{für alle } a \in A.$$

(d) Existenz inverser Elemente: Zu jedem $a \in A$ gibt es ein $a' \in A$ mit der Eigenschaft

$$a \circ a' = a' \circ a = e.$$

Wird speziell die binäre Operation als Addition $(+)$ oder Multiplikation $(\cdot)$ geschrieben, so bezeichnet man ein inverses Element zu a oft als $-a$ bzw. a^{-1}.

Beispiele:

(1) $(\mathbb{N}, +)$: assoziativ, kommutativ, neutrales Element $e = 0$; nur die Null besitzt ein inverses Element $e' = e$.

(2) $(\mathbb{Z}, +)$: alle Eigenschaften (a)-(d) gelten.

(3) $(\mathbb{Z}, \cdot)$: assoziativ, kommutativ, neutrales Element $e = 1$, inverse Elemente besitzen nur ± 1.

(4) $(\mathbb{Q}, \cdot)$: assoziativ, kommutativ, neutrales Element $e = 1$, inverse Elemente besitzen alle Elemente von $\mathbb{Q}$ außer 0.

(5) $(\mathbb{Q}, \cdot)$: alle Eigenschaften (a)-(d) gelten.

Satz 13.3

(a) In einer algebraischen Struktur gibt es höchstens ein neutrales Element.

(b) In einer assoziativen algebraischen Struktur gibt es zu jedem Element höchstens ein inverses Element.

Inhalt

Definition 13.4

Eine algebraische Struktur heißt

(a) Halbgruppe, wenn sie assoziativ ist,

(b) Monoid, wenn wenn sie assoziativ ist und ein neutrales Element besitzt,

(c) Gruppe, wenn sie assoziativ ist, ein neutrales Element besitzt und jedes Element ein inverses Element besitzt.

Gilt in einer Halbgruppe, einem Monoid oder einer Gruppe zusätzlich das Kommutativgesetz, so heißt die entsprechende algebraische Struktur kommutative Halpbgruppe, Monoid oder Gruppe. Kommutative Gruppen werden auch abelsche Gruppen genannt.

Beispiele:

(1) $(\mathbb{Z}\setminus\{0\},+)$ ist eine Halbgruppe; $(\mathbb{N}\cup\{0\},+)$ und $(\mathbb{N},\cdot)$ sind Monoide, aber keine Gruppen.

(2) Sei $\mathscr{A}$ eine endliche Menge von Zeichen (Alphabet) sowie $A=\mathscr{A}^*$ die Menge aller endlichen Wörter über $\mathscr{A}$, d.h. alle endlichen Folgen $(x_1x_2\cdots x_k)$, $x_j\in\mathscr{A}$, sowie das leere Wort e. Als binäre Operation auf A sei die Konkatenation zweier Wörter $w_1=x_1\cdots x_k$ und $y_1\cdots y_\ell$ definiert durch $w_1\circ w_2=x_1\ldots x_k y_1\ldots y_\ell$. Dann ist $(A,\circ)$ ein Monoid.

(3) $(\mathbb{Z},+)$,$(\mathbb{Q},+)$,$(\mathbb{Q}\setminus\{0\},\cdot)$,$(\mathbb{R},+)$,$(\mathbb{R}\setminus\{0\},\cdot)$ sind abelsche Gruppen.

(4) $A=\mathbb{R}^{n\times n}$, $n\in\mathbb{N}$ bildet zusammen mit der Matrizenaddition eine abelsche Gruppe. Die invertierbaren Matrizen aus $\mathbb{R}^{n\times n}$ bilden bezüglich der Matrizenmultiplikation eine Gruppe, die jedoch nicht abelsch ist.

Satz 13.5

Sei $(A, \circ)$ eine Gruppe sowie $a, b \in A$ sowie a' das inverse Element von a. Dann ist $a' \circ b$ die eindeutig bestimmte Lösung der Gleichung $a \circ x = b$.

Inhalt

- Die ganzen Zahlen $\mathbb{Z}$ bilden sowohl mit der Addition als auch der Multiplikation eine algebraische Struktur (abelsche Gruppe bzw. Monoid).
- Ein Ring ist eine algebraische Struktur mit zwei binären Operationen, welche mit $+$ und $\cdot$ bezeichnet werden (aber nicht unbedingt mit Addition und Multiplikation übereinstimmen müssen).
- Das Distributivgesetz verbindet die beiden Operationen.
- Das neutrale Element der Addition wird, falls es existiert, mit 0 (Null), das der Multiplikation mit 1 (Eins) bezeichnet.
- Das additive inverse Element zu a wird mit $-a$, das multiplikative mit a^{-1} bezeichnet.

Definition 13.6

Eine algebraische Struktur $(R, +, \cdot)$ mit zwei binären Operationen heißt Ring, wenn folgende drei Eigenschaften gegeben sind

(i) $(R, +)$ ist eine kommutative Gruppe (mit neutralem Element 0),

(ii) $(R, \cdot)$ ist eine Halbgruppe, und

(iii) es gelten die Distributivgesetze

$$\text{für alle } a, b, c \in R \text{ gilt} \qquad a \cdot (b + c) = a \cdot b + a \cdot c$$
$$\text{sowie} \qquad (a + b) \cdot c = a \cdot c + b \cdot c.$$

Besitzt R ein neutrales Element bezüglich $\cdot$, so nennt man R Ring mit Eins, und ist R kommutativ bezüglich $\cdot$, so nennt man R einen kommutativen Ring.

Beispiele:

(1) $(\mathbb{Z}, +, \cdot)$ ist kommutativer Ring mit Eins.

(2) Die Menge $M \in R^{n\times n}$ aller $n \times n$-Matrizen mit Einträgen $m_{i,j}$ aus einem Ring R bilden bezüglich Matrizenaddition und -multiplikation wieder einen Ring.

(3) Polynome in der Variablen x über einem Ring R sind formale Summen

$$p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_k x^k.$$

mit Koeffizienten $a_0, \ldots, a_k \in R$. Für zwei Polynome $p(x) = \sum_{j=0}^{k} a_j x^j$ und $q(x) = \sum_{j=0}^{\ell} b_j x^j$ definieren wir

$$p(x)+q(x) = \sum_{j=0}^{\max\{k,\ell\}} (a_j+b_j)x^j, \quad p(x)\cdot q(x) = \sum_{j=0}^{k+\ell} \left(\sum_{i=\max\{0,j-\ell\}}^{\min\{j,k\}} a_i b_{j-i} \right) x^j.$$

Die Menge $R[x]$ aller solcher Polynome bildet mit dieser Addition und Multiplikation den Polynomring über R: $(R[x], +, \cdot)$.

- In jedem Ring gilt die Rechenregel $a \cdot 0 = 0 \cdot a = 0$.
- In einem Ring kann ein Produkt jedoch durchaus Null sein, obwohl beide Faktoren von Null verschieden sind (Beispiel später).
- Man nennt ein Element $a \neq 0$ eines Ringes R einen Nullteiler, wenn es ein $b \neq 0$ aus R gibt mit der Eigenschaft $a \cdot b = 0$ oder $b \cdot a = 0$. (In diesem Fall ist natürlich b ebenfalls ein Nullteiler.)

Definition 13.7

Ein kommutativer Ring mit Eins ohne Nullteiler heißt Integritätsbereich (oder auch Integritätsring).

In einem Integritätsbereich kann man kürzen: Ist $a \neq 0$ und $a \cdot b = a \cdot c$, so folgt $a \cdot (b - c) = 0$, also $b - c = 0$ und somit $b = c$.

In einem beliebigen Ring R kann man stets durch Elemente $a \in R$ kürzen, die ein multiplikatives Inverses a^{-1} besitzen. Solche Elemente heißen auch Einheiten. Es ist direkt nachzurechnen, dass die Menge aller Einheiten R^* von R eine (multiplikative) Gruppe bildet, die so genannte Einheitengruppe von R. Beispielsweise ist $\mathbb{Z}^* = \{-1, 1\}$.

Definition 13.8

Ein kommutativer Ring $(K, +, \cdot)$ mit Einselement $1 \neq 0$, in dem jedes Element $a \neq 0$ eine Einheit ist, also ein multiplikatives Inverses besitzt, heißt ein Körper.

Eine algebraische Struktur $(K, +, .)$ ist also genau dann ein Körper, wenn $(K, +)$ und $(K \setminus \{0\}, \cdot)$ kommutative Gruppen sind und die Distributivgesetze gelten.

Beispiele: $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$.

Satz 13.9

Jeder Körper ist ein Integritätsbereich, und jeder endliche Integritätsbereich ist ein Körper.

Inhalt

Definition 13.10 (Teilbarkeit, ggT, kgV)

Seien $a, b \in \mathbb{Z}$.

(a) Man sagt b teilt a, in Zeichen $b|a$, wenn es eine ganze Zahl c gibt mit $a = bc$.

(b) Eine Zahl $g \in \mathbb{Z}$ heißt größter gemeinsamer Teiler von a und b, geschrieben $g = \mathrm{ggT}(a, b)$, wenn folgende zwei Bedingungen erfullt sind:
   (i) g teilt sowohl a als auch b, d.h. $g|a$ und $g|b$.
   (ii) Für jeden weiteren Teiler t von a und b gilt $t|g$.

(c) a und b heißen teilerfremd, wenn $\mathrm{ggT}(a, b) = 1$.

(d) Eine Zahl $k \in \mathbb{Z}$ heißt kleinstes gemeinsames Vielfaches von a und b, geschrieben $k = \mathrm{kgV}(a, b)$, wenn folgende zwei Bedingungen erfüllt sind:
   (i) k ist ein Vielfaches von sowohl a als auch b, d.h. $a|k$ und $b|k$.
   (ii) Für jedes weitere Vielfache v von a und b gilt $k|v$.

Bemerkung: Mit g ist auch $-g$ größter gemeinsamer Teiler zweier Zahlen. Mit der Festlegung, dass dieser stets positiv ist, wird der größte gemeinsame Teiler eindeutig bestimmt. Analog verfährt man beim kleinsten gemeinsamen Vielfachen.

Satz 13.11 (Division mit Rest)

Es seien $a, b \in \mathbb{Z}$ und $b > 0$. Dann gibt es Zahlen $q, r \in \mathbb{Z}$ mit

$$a = bq + r \quad \text{und} \quad 0 \leq r < b.$$

Satz 13.12 (Euklidscher Algorithmus)

Führt man zu $a, b \in \mathbb{Z}$ die folgende Kette von Divisionen mit Rest durch,

$$\begin{aligned}
a &= bq_0 + r_0, & 0 < r_0 < b,\\
b &= r_0 q_1 + r_1, & 0 < r_1 < r_0,\\
r_0 &= r_1 q_2 + r_2, & 0 < r_2 < r_1,\\
&\vdots\\
r_{k-2} &= r_{k-1} q_k + r_k, & 0 < r_k < r_{k-1},\\
r_{k-1} &= r_k q_{k+1} + 0,
\end{aligned}$$

so muss diese wegen $b > r_0 > r_1 > \cdots \geq 0$ nach endlich vielen Schritten mit einem verschwindenden Rest abbrechen. Für den zuletzten berechneten Rest gilt $r_k = \mathrm{ggT}(a, b)$.

Bemerkung: Die Anzahl der Divisionsschritte ist (auf den ersten Blick) durch b beschränkt. Tatsächlich ist der Algorithmus viel schneller. Aus $r_{k-2} \geq r_k + r_{k-1} \geq 2r_k$ folgt

$$r_k \leq \frac{1}{2} r_{k-2}.$$

Der Euklidische Algorithmus terminiert also nach wenigen Schritten. Genauer gilt: $r_k \leq b2^{-\lfloor k/2 \rfloor}$. Der Algorithmus bricht also spätestens nach $2(\log b/\log 2) + 1$ Schritten ab.

Satz 13.13

Ist $d = \mathrm{ggT}(a,b)$, $a, b \in \mathbb{Z} \setminus \{0\}$, so gibt es ganze Zahlen e, f mit

$$d = ae + fb.$$

Diese können mit dem Euklidischen Algorithmus berechnet werden.

Definition 13.14

Eine natürliche Zahl $p > 1$ heißt Primzahl, wenn die einzigen Teiler von p die Zahlen ± 1 und $\pm p$ sind. Die Menge der Primzahlen wird mit $\mathbb{P}$ bezeichnet.

Satz 13.15

Teilt eine Primzahl p ein Produkt ganzer Zahlen $a_1, \ldots, a_r$, also $p | a_1 a_1 \cdots a_r$, dann teilt sie wenigstens einen der Faktoren, also $p | a_j$ für ein $j \in \{1, \ldots, r\}$.

Satz 13.16 (Fundamentalsatz der Zahlentheorie)

Jede natürliche Zahl $a \geq 2$ lässt sich als Produkt von Primzahlen darstellen:

$$a = p_1 \cdot p_2 \cdots p_r \qquad \text{mit} \quad p_1, \ldots, p_r \in \mathbb{P}$$

wobei die Darstellung bis auf die Reihenfolge eindeutig ist.

Satz 13.17

Es gibt unendlich viele Primzahlen.

Für eine natürliche Zahl a und eine Primzahl p schreibt man $\nu_p(a) = k$, falls gilt $p^k | a$, aber $p^{k+1} \nmid b$. Aus dem Fundamentalsatz erhält man dann durch Zusammenfassung der entsprechenden Primzahlteiler zu Primzahlpotenzen die sogenannte Primfaktorenzerlegung von a als

$$a = 2^{\nu_2(a)} \cdot 3^{\nu_3(a)} \cdot 5^{\nu_5(a)} \cdots = \prod_{p \in \mathbb{P}} p^{\nu_p(a)}.$$

Satz 13.18

Es seien $\prod_{p\in\mathbb{P}} p^{\nu_p(a)}$ und $\prod_{p\in\mathbb{P}} p^{\nu_p(b)}$ die Primfaktorenzerlegungen von $a, b \in \mathbb{N}$. Dann gilt:

$$\mathrm{ggT}(a,b) = \prod_{p\in\mathbb{P}} p^{\min\{\nu_p(a),\nu_p(b)\}} \quad \text{und} \quad \mathrm{kgV}(a,b) = \prod_{p\in\mathbb{P}} p^{\max\{\nu_p(a),\nu_p(b)\}}.$$

Insbesondere gilt auch

$$\mathrm{ggT}(a,b) \cdot \mathrm{kgV}(a,b) = ab.$$

Inhalt

Erinnerung: In Kapitel 2 der Vorlesung hatten wir den Bergiff einer Relation R auf einer Menge M definiert als Teilmenge von $M \times M$, und eine Äquivalenzrelation als eine solche, welche die drei folgenden Eigenschaften besitzt:

(a) Reflexivität. $\forall x \in M : (x, x) \in R$.

(b) Symmetrie. $\forall x, y \in M : (x, y) \in R \Rightarrow (y, x) \in R$.

(c) Transitivität. $\forall x, y, z \in M : (x, y) \in R \wedge (y, z) \in R \Rightarrow (x, z) \in R$.

Anstelle von $(x, y) \in R$ schreiben wir im Folgenden einfacher $x \sim_R y$ oder, wenn die Relation R aus dem Kontext klar ist, $x \sim y$.

Definition 13.19

Sei R eine Äquivalenzrelation auf der Menge M. Für $x \in M$ heißt die Menge

$$[x] := \{y \in M : x \sim y\}$$

die von x erzeugte Äquivalenzklasse.

Beachte: Aufgrund der Reflexivitätseigenschaft ist $[x] \neq \emptyset$ für alle $x \in M$.

Satz 13.20

(a) Sei R eine Äquivalenzrelation auf der Menge M. Dann bilden die (verschiedenen) Äquivalenzklassen der Elemente von M eine Partition von M.

(b) Ist Umgekehrt $\mathscr{P} = \{M_j\}_{j\in J}$ eine Partition der Menge M und bezeichne $[x]$ jene Teilmenge aus $\mathscr{P}$, welche x enthält. Definiert man nun $x \sim y$ genau dann, wenn $[x] = [y]$, so ist hierdurch eine Äquivalenzrelation auf M definiert.

Korollar 13.21

Sei R eine Äquivalenzrelation auf der Menge M und $x \in M$. Gilt $y \in [x]$, so folgt $[x] = [y]$, d.h. die Äquivalenzklasse ist unabhängig von der Auswahl des Repräsentanten.

Definition 13.22

Sei R eine Äquivalenzrelation auf der Menge M. Sei ferner $\circ$ eine binäre Operation auf M. Wir sagen, die binäre Operation $\circ$ respektiert die Relation R, falls für alle $x, x', y, y' \in M$ gilt

$$x' \sim x \ \wedge \ y' \sim y \Rightarrow x' \circ y' \sim x \circ y.$$

Satz 13.23

Sei R eine Äquivalenzrelation auf der Menge M, sowie $\circ$ eine binäre Operation auf M, welche die Relation R respektiert. Dann wird durch die Vorschrift

$$[x] \circ [y] := [x \circ y]$$

eine binäre Operation auf der Menge M_R aller Äquivalenzklassen von R auf M erklärt.

Definition 13.24

Sei $m \in \mathbb{N}$ fest. Zwei Zahlen $a, b \in \mathbb{Z}$ heißen kongruent modulo m, falls m ein Teiler von $b - a$ ist. Man schreibt hierfür auch kurz $a \equiv b \mod m$.

Satz 13.25

Sei $m \in \mathbb{N}$ fest. Durch die Beziehung

$$a \sim b :\Leftrightarrow a \equiv b \mod m, \qquad a, b \in \mathbb{Z},$$

wird eine Äquivalenzrelation erklärt. Die Menge aller Äquivalenzklassen $[a] = [a]_m$ wird mit $\mathbb{Z}_m$ bezeichnet. Es gilt

$$\mathbb{Z}_m = \{[0], [1], \ldots, [m-1]\}.$$

Bemerkung: Die Äquivalenzklassen der Konruenz modulo m werden auch Restklassen genannt, da sie genau aus den ganzen Zahlen bestehen, welche bei der Division durch m denselben Rest ergeben.

Satz 13.26

Sei $m \in \mathbb{N}$ fest. Die binären Operationen Addition und Multiplikation auf der Menge $\mathbb{Z}$ respektieren die Kongruenzrelation modulo m. Diese sind somit auch binäre Operationen auf $\mathbb{Z}_m$.

Beispiel: Verknüpfungstafel der Addition in $\mathbb{Z}_5$:

$+$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[0]_5$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[1]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$	$[0]_5$
$[2]_5$	$[2]_5$	$[3]_5$	$[4]_5$	$[0]_5$	$[1]_5$
$[3]_5$	$[3]_5$	$[4]_5$	$[0]_5$	$[1]_5$	$[2]_5$
$[4]_5$	$[4]_5$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$

Beispiel: Verknüpfungstafel der Addition in $\mathbb{Z}_4$. (Wenn die Restklassenmenge klar ist, kann die Restklassenklammer auch weggelassen werden.)

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Satz 13.27

Eine Restklasse $[a] \in \mathbb{Z}_m$ besitzt genau dann eine multiplikativ inverse Restklasse, wenn $\mathrm{ggT}(a, m) = 1$ ist.

Man bestimme in $\mathbb{Z}_{17}$ die inverse Restklasse zu $[15]$.

Man zeige: ist die Quersumme einer Zahl $n \in \mathbb{N}$ ist genau dann durch 9 teilbar, wenn n es ist.

Satz 13.28

$(\mathbb{Z}_m, +, \cdot)$ ist ein kommutativer Ring mit Eins. $(\mathbb{Z}_m, +, \cdot)$ ist genau dann auch ein Integritätsbereich, wenn m eine Primzahl ist. In diesem Fall bildet $(\mathbb{Z}_m, +, \cdot)$ auch einen Körper.

Prüfziffern dienen der Erkennung von Übertragungsfehlern bei Artikelnummern, Sozialversicherungsnummern, Bankkontonummern usw. Ein Beispiel ist die Internationale Standard-Buchnummer (ISBN), mit Format

$$\text{ISBN } a_1\text{–}a_2a_3a_4\text{–}a_5a_6a_7a_8a_9\text{–}p$$

Ziffern a_1 bis a_9 beschreiben Gruppe, Verlag und Titel des Buches. Die letzte Ziffer p ist die Prüfziffer, mit der Eigenschaft

$$10a_1 + 9a_2 + 8a_3 + \cdots + 3a_8 + 2a_9 + p \equiv 0 \mod 11. \tag{13.1}$$

Damit besitzt p die Darstellung

$$p \equiv a_1 + 2a_2 + \cdots + 9a_9 \mod 11, \qquad p \in 0, 1, 2, \ldots, 9, X,$$

wobei X für die „Ziffer“ 10 steht.

Ist ISBN 3–211–82084–1 eine korrekte ISBN-Nummer?

Mit Hilfe des ISBN-Codes können sowohl Einzelfehler als auch Vertauschungsfehler an zwei beliebigen Stellen erkannt werden, eine Fehlerkorrektur ist allerdings i. Allg. nicht möglich.

Satz 13.29

Jeder Fehler in einer Ziffer sowie alle Vertauschungen zweier Ziffern werden vom ISBN-Code erkannt.

Inhalt

Satz 13.30

Ist p eine Primzahl, so gilt $p|\binom{p}{k}$ für alle $k = 1, 2, \ldots, p-1$.

Satz 13.31

Ist p eine Primzahl und $a, b \in \mathbb{Z}_p$, so gilt $(a+b)^p = a^p + b^p$.
Mit anderen Worten: für alle $a, b \in \mathbb{Z}$ gilt $(a+b)^p \equiv a^p + b^p \mod p$.

Korollar 13.32

Ist p eine Primzahl sowie $a_1, \ldots, a_n \in \mathbb{Z}_p$, so gilt $(a_1 + \cdots + a_n)^p = a_1^p + \cdots + a_n^p$.
Mit anderen Worten: für alle $a_1, \ldots, a_n \in \mathbb{Z}$ gilt

$$(a_1 + \cdots + a_n)^p \equiv a_1^p + \cdots + a_n^p \mod p.$$

Satz 13.33 (Kleiner Satz von Fermat)

Ist p eine Primzahl und $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a,p) = 1$, so gilt $a^{p-1} \equiv 1 \mod p$.

Definition 13.34

Die Eulersche φ-Funktion $\varphi : \mathbb{N} \to \mathbb{N}$ ist definiert durch

$$\varphi(m) = \{a \in \mathbb{Z} : 1 \leq a \leq m,\ \mathrm{ggT}(a, m) = 1\}.$$

Bemerkung: Für einen Ring R hatten wir mit R^* die multiplikative Gruppe derjenigen Elemente zon R bezeichnet, welche eine multiplikative Inverse besitzen. Nach Satz 13.28 bilden die Restklassen $\mathbb{Z}_m, m \in \mathbb{N}$, einen Ring (mit Eins).
Für $m > 1$ gibt, im Anbetracht von Satz 13.27, der Wert $\varphi(m)$ somit die Anzahl der invertierbaren Elemente der Resklassen modulo m an, d.h. $\varphi(m) = |\mathbb{Z}_m^*|$.

(1) Man bestimme $\varphi(m)$ für $m = 1, 2, \ldots, 12$.
(2) Man zeige: für Primzahlen p gilt $\varphi(p) = p - 1$.

Satz 13.35

Sei p eine Primzahl und $n \in \mathbb{N}$. Dann gilt $\varphi(p^n) = p^{n-1}(p-1)$.

Angesichts der Primfaktorenzerlegung beliebiger natürlicher Zahlen

$$n = \prod_{p \in \mathscr{P}} p^{\nu_n(n)}, \qquad n \in \mathbb{N},$$

können wir die φ-Funktion für beliebige n dann ausrechnen, wenn wir ihr Verhalten für das Produkt teilerfremder Zahlen kennen. Genauer gesagt: es gilt

$$m, n \in \mathbb{N}, \quad \mathrm{ggT}(m,n) = 1 \qquad \Rightarrow \qquad \varphi(mn) = \varphi(m)\varphi(n).$$

Hierzu benötigen wir einen einfache Spezialfall des Chinesischen Restsatzes:

Satz 13.36

Seien $m, n \in \mathbb{N}$ mit $\mathrm{ggT}(m,n) = 1$ sowie $a, b \in \mathbb{Z}$ beliebig. Dann besitzt das Gleichungssystem

$$x \equiv a \mod m, \qquad x \equiv b \mod n$$

genau eine Lösung modulo $m \cdot n$.

Für den Beweis der Multiplikativität der φ-Funktion genügt es zu zeigen, dass $|\mathbb{Z}_{mn}^*| = |\mathbb{Z}_m^* \times \mathbb{Z}_n^*|$. Dies kann durch Angabe einer Bijektion zwischen beiden Mengen gezeigt werden.

Satz 13.37

Seien $m, n \in \mathbb{N}$ mit $\mathrm{ggT}(m,n) = 1$. Dann gilt $\varphi(mn) = \varphi(m)\varphi(n)$.

Satz 13.38

Sei $n \in \mathbb{N}$ mit Primfaktorenzerlegung $n = p_1^{\nu_1} \cdot p_2^{\nu_2} \cdots p_r^{\nu_r}$. Dann gilt

$$\varphi(n) = \prod_{j=1}^{r} p_j^{\nu_j - 1}(p_j - 1) = n \prod_{j=1}^{r} \left(1 - \frac{1}{p_j}\right).$$

Satz 13.39 (Euler)

Sei $n \in \mathbb{N}$ beliebig sowie $k \in \mathbb{Z}$ mit $\mathrm{ggT}(k,n) = 1$. Dann gilt $k^{\varphi(n)} \equiv 1 \mod n$.

- Wir betrachten nun folgendes Beispiel zur Verschlüsselung mit öffentlichem Schlüssel (public-key cryptography).
- Eine zu versendende Nachricht bestehe aus Zahlen.
- Dem Empfänger der Nachricht seien zwei (öffentlich bekannte) Zahlen n und e zugeordnet.
- Jede zu versendende Zahl x wird verschlüsselt gemäß der Vorschrift

$$x \mapsto v(x) := x^e \mod n, \qquad 0 < v(x) < n.$$

Beispiel:

- Die zu versendende Nachricht laute `allekreterluegen`.
- Als Vorkehrung gegen statistische Textanalyse, bei welcher anhand von Häufigkeiten Rückschlüsse die Verschlüsselung einzelner Buchstaben gezogen werden könnte, wenden wir die Veschlüsselungsabbildung auf Buchstabengruppen (hier Paare) anstelle einzelner Buchstaben an.
- Wir ordnen jedem Buchstaben seine Ordnungszahl d_x zwischen 1 und 26 zu.
- Jedem Buchstabenpaar (x, y) ordnen wir die Zahl $(d_x - 1) \cdot 26 + d_y$ zu. Damit die Verschlüsselungs
- etwa $n = 5893$, als Exponent wählen wir $e = 17$.
- Für unsere Beispielnachricht erhalten wir zunächst

$$\begin{array}{llll} \texttt{al} \mapsto 12 & \texttt{le} \mapsto 291 & \texttt{kr} \mapsto 278 & \texttt{et} \mapsto 124 \\ \texttt{er} \mapsto 122 & \texttt{lu} \mapsto 307 & \texttt{eg} \mapsto 111 & \texttt{en} \mapsto 118 \end{array}$$

- Die zugehörigen Verschlüsselungen lauten

$$\begin{aligned} v(12) &= 4492 & v(291) &= 985 & v(278) &= 1618 & v(124) &= 5323 \\ v(122) &= 2579 & v(307) &= 1943 & v(111) &= 5542 & v(118) &= 738 \end{aligned}$$

- Die Umkehrabbildung ist gegeben durch

$$x = v(x)^d \mod n, \qquad 0 < v(x) < n \quad \text{mit } d = 1013.$$

Im Beispiel:

$$\begin{aligned} 4492^{1013} &\equiv 12 \mod 5893, & 985^{1013} &\equiv 291 \mod 5893, \\ 1618^{1013} &\equiv 278 \mod 5893, & 5323^{1013} &\equiv 124 \mod 5893, \\ 2579^{1013} &\equiv 122 \mod 5893, & 1943^{1013} &\equiv 307 \mod 5893, \\ 5542^{1013} &\equiv 111 \mod 5893, & 738^{1013} &\equiv 118 \mod 5893. \end{aligned}$$

- **Fazit:** Einziges geheim zu haltendes Datum ist der 'Schlüssel' d.
- Der Schlüssel d ist so zu wählen, dass $0 < d < \varphi(n)$ mit

$$[e]_{\varphi(n)} \cdot [d]_{\varphi(n)} = [1]_{\varphi(n)} \quad \text{d.h.} \quad e \cdot d \equiv 1 \mod \varphi(n),$$

d.h. d ist das mutiplikativ inverse Element von e in $\mathbb{Z}_{\varphi(n)}$.

Satz 13.40

Mit der oben angegebenen Vorschrift wird die Umkehrabbildung zur public-key Verschlüsselung realisiert.

- Die multiplikativ Inverse d zu e kann man mit dem Euklidschen Algorithmus bestimmen.
- Die Schwierigkeit bei der Entschlüsselung besteht in der Berechnung von $\varphi(n)$ ohne die Primfaktorenzerlegung von n zu kennen.