Algebra für Ingenieure

Universität Hamburg

Reiner Lauterbach

SS 2000

Inhaltsverzeichnis

Kapitel 1

Einführung

1.1 Grundlegende Überlegungen

Die Algebra beschäftigt sich mit Strukturen, dies wiederum sind abstrakte Konzepte, die gemeinsame Eigenschaften vieler mathematischer Objekte herauskristallisieren. Schon die einfache Gleichung

$$1 + 1 = 2$$

stellt eine Abstraktion dar. Nur, wir haben uns auf diesem einfachen Niveau bereits derart an diese Abstraktion gewöhnt, daß wir diese kaum noch bemerken, ja es wird vielleicht manch einem von Ihnen so ergehen, daß er den Gedanken geradezu schwierig findet, obwohl es sehr einfach ist. Während man am Anfang der Menschheitsgeschichte nur zählte und feststellte, wenn ich ein Objekt habe und ein zweites dazulege, erhalte ich zwei Objekte (1 Objekt + 1 Objekt=2 Objekte). Nun, die Abstraktion beginnt damit, daß ich stattdessen schreibe

$$1 + 1 = 2,$$

also diese Gleichung unabhängig von konkreten Objekten betrachte. Wir erkennen sofort, die Abstraktion beginnt bereits eine Stufe früher: während im Satz „Ich habe zwei Äpfel“ zwei eine Eigenschaft einer Menge von Äpfeln darstellt, ist die Zahl 2 eine Abstraktion, sie bezeichnet eine gemeinsame Eigenschaft vieler Mengen, nämlich zwei Elemente zu haben.

Wir wollen hier aber nicht die Konstruktion der Zahlen und die zugrundeliegenden Abstraktionen behandeln, sondern die Zahlen als gegeben und uns vertraut voraussetzen. Was aber ist eine algebraische Struktur?

Wir beginnen mit einem Beispiel: auf der Menge der reellen (ganzen) Zahlen haben wir zwei Rechenoperationen, $+, \cdot$. Wir beschreiben markante Regeln:

Add1 $(x + y) + z = x + (y + z)$ (Assoziativgesetz).

Add2 $x + y = y + x$ (Kommutativgesetz)

Add3 Es gibt ein eindeutig bestimmtes Element, welches mit 0 bezeichnet wird, so daß

$$0 + x = x$$

für jedes x richtig ist.

Add4 Zu jedem Element x gibt es ein eindeutiges Negatives (additiv Inverses) mit

$$x + (-x) = 0.$$

Mul1 $(xy)z = x(yz)$ (Assoziativgesetz der Multiplikation)

Mul2 $xy = yx$ (Kommutativgesetz der Multiplikation)

Mul3 Es gibt ein Element, welches wir mit 1 bezeichnen wollen, so daß $1x = x$ für alle $x \in \mathbb{R}$ gilt.

Mul4 Für jedes $x \neq 0$ gibt es ein Element x^{-1} mit $xx^{-1} = 1$.

Dis $x(y + z) = xy + xz$

Ein typisches Beispiel mathematischen Schließens sind nun die beiden folgenden Aussagen.

Satz 1.1.1
Gelten die Regeln [Add1-4], [Mul1-3] und [Dis], so ist

$$0x = 0$$

und

$$(-a)b = -(ab).$$

Beweis.

$$\begin{aligned} 0x &= (0+0)x \text{ nach [Add3]} \\ &= 0x + 0x \text{ nach [Dis1]} \end{aligned}$$

Addieren wir nun $-x$ auf beiden Seiten, so ergibt sich

$$0 = 0x + 0,$$

und wegen [Add2] und [Add3] erhält man $0 = 0x$.

Die zweite Aussage beweist man ähnlich

$$0 = 0b = (a + (-a))b = (ab + (-a)b).$$

Daher ist $(-a)b$ das Inverse zu ab und dieses Element ist $-(ab)$. □

Bemerkenswert ist, daß diese Schlußfolgerung jetzt nicht nur für die Menge der reellen Zahlen gilt, sondern vielmehr auch für alle Strukturen in denen die Regeln [Add1-4], [Mul1-4] und [Dis1] gelten.

Was sind solche Strukturen?

Wir beginnen mit einem sehr einfachen Beispiel:

Beobachte: die Summe zweier

- gerader Zahlen ist gerade
- ungerader Zahlen ist gerade
- Zahlen von denen eine gerade, eine ungerade ist, ist ungerade.

Entsprechende Beobachtungen gelten für die Multiplikation.

Wie läßt sich dies in Formeln fassen?

Scheiben wir, und dies ist vielleicht im Moment etwas formal, 1 für eine ungerade Zahl, 0 für eine gerade, so erhalten wir die Rechenregeln

$$\begin{aligned} 0+0 &= 0 \\ 1+1 &= 0 \\ 0+1 = 1+0 &= 1 \\ 1 \cdot 1 &= 1 \\ 0 \cdot 1 = 1 \cdot 0 &= 0 \\ 0 \cdot 0 &= 0. \end{aligned}$$

Es ist eine einfache, wenn auch langwierige und vollkommen uninteressante Tätigkeit, die Richtigkeit der Regeln [Add1-Add4,Mul1-Mul4,Dis1] nachzuprüfen. Dieses Beispiel ist Prototyp einer Serie von Beispielen, die wir im folgenden näher betrachten wollen. Wir benötigen dazu einige, den meisten sicher wohlbekannte, Tatsachen, die wir in den nächsten Abschnitten zusammenstellen. Wir werden dann sehr schnell auch auf praktische und extrem wichtige Anwendungen zusteuern.

1.2 Teilbarkeit

Wir setzen die Existenz und die wesentlichsten Eigenschaften der ganzen Zahlen $\mathbb{Z}$ als gegeben voraus. Mit $\mathbb{N}$ bezeichnen wir die Menge $1, 2, \ldots,$ der positiven ganzen Zahlen. Weiter sei $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ die Menge der nichtnegativen ganzen Zahlen.

Definition 1.2.1
Wir sagen, die Zahl $b \in \mathbb{Z}$ teilt die Zahl $a \in \mathbb{Z}$, wenn es eine Zahl $c \in \mathbb{Z}$ gibt, mit $a = bc$. In diesem Fall schreiben wir $b|a$. Gilt dies nicht, so schreiben wir $b \not| a$. Wir nennen b einen Teiler *von a. Einer ganzen Zahl a ordnen wir die Menge ihrer Teiler zu, die wir mit* **Teiler**(a) *bezeichnen wollen, und durch*

$$\mathbf{Teiler}(a) = \{b \in \mathbb{Z} \mid b|a\}$$

definiert werde.

Satz 1.2.2
Sind a, b ganze Zahlen, $b \neq 0$, so gibt es eine Zahl $r \in \mathbb{Z}$, $0 \leq r < b$ mit $b|(a - r)$.

Beweis. Wir nehmen an $b > 0$ und betrachten die Menge C der $c \in \mathbb{Z}$ $cb \leq a$. Sei d das maximale Element in dieser Menge C (ein solches Element existiert) Dann ist $bd + b > a \geq bd$ oder auch $0 \leq r = a - bd < b$. □

Definition 1.2.3
Die Zahl r, deren Existenz im Satz 1.2.2 gezeigt wurde, heißt der Rest *von a* modulo *b. Wir schreiben auch*

$$a \cong r \bmod b.$$

(Zu lesen ist dies: a ist kongruent r modulo b.)

Definition 1.2.4
Sind $a, b \in \mathbb{Z}$ *und* $q \in \mathbb{N} = \mathbb{N} \setminus \{0\}$, *so heißt* q *ein* gemeinsamer Teiler *von* a, b, *falls* $q|a$ *und* $q|b$ *gilt. Der maximale gemeinsame Teiler von* a, b *heißt* größter gemeinsamer Teiler *und wird mit* $\mathbf{ggT}(a, b)$ *bezeichnet.*

Lemma 1.2.5
$a|b$ *und* $a|c$ *implizieren, daß* $a|(b + c)$.

Beweis. $a|b$ bedeutet, daß $b = pa$, $a|c$, daß $c = qa$ gilt, und damit ist

$$b + c = pa + qa = (p + q)a.$$

□

Eine Methode zur Berechnung des größten gemeinsamen Teilers geht auf **Euklid**[1] zurück.

Satz 1.2.6
Algorithmus I: *Gegeben seien die Zahlen* $a, b \in \mathbb{Z}$. *Ist eine der Zahlen negativ, so betrachten wir das Negative der Zahl und gehen damit ohne Beschränkung der Allgemeinheit von zwei positiven Zahlen aus. Wir setzen*

$$a = q_0 b + r_0,\ 0 \le r < b, q_0 \in \mathbb{N}_0.$$

Setze $r_{-1} = b$ *und betrachte*

$$b = q_1 r_0 + r_1,\ 0 \le r_1 < r_0.$$

Dies fortsetzend erhalten wir

$$r_0 = q_2 r_1 + r_2,\ 0 \le r_2 < r_1,$$

und weiter

$$r_n = q_{n+2} r_{n+1} + r_{n+2}, 0 \le r_{n+2} < r_{n+1}.$$

Die Zahlenfolge $r_0, r_1, \ldots, r_n \ldots$ *besteht aus nichtnegativen Zahlen und ist streng monoton fallend. Daher gibt es das* **Abbruchkriterium**

$$r_j = 0.$$

Tritt also zum ersten Mal der Rest null in dieser Folge von Rechnungen auf, so beenden wir die Rechnung. Dann ist

$$r_{j-1} = \mathbf{ggT}(a, b).$$

---

[1] Euklid lebte um 300vC und gilt als Begründer der Mathematikerschule von Alexandria. Er verfaßte das einflußreichste Mathematikbuch aller Zeiten, die berühmten Elemente. Darin wird die Grundlage der Geometrie, wie sie noch heute gelehrt wird, gelegt.

Beispiel 1.2.7
Wir betrachten vier Beispiele:

1. *Sei* $a = 49, b = 35$. *Also ist* $q_0 = 1, r_0 = 14$. $35 = 2 \cdot 14 + 7$, *also* $q_1 = 2$ *und* $r_1 = 7$. *Dies fortsetzend ist*
$$14 = 2 \cdot 7 + 0$$
also $q_2 = 2$, $r_2 = 0$ *und damit* $\mathbf{ggT}(49, 35) = r_1 = 7$.

2. $a = 3628800$, $b = 243$. *Es ist* $3628800 = 14933 \cdot 243 + 81$, *also* $q_0 = 14933, r_0 = 81$. *Im nächsten Schritt finden wir*
$$b = 243 = 3 \cdot 81$$
und damit ist $r_1 = 0$ *und* $r_0 = 81$ *ist der größte gemeinsame Teiler von* $a = 3628800$ *und* $b = 243$.

3. $a = 4409$, $b = 31$, *dann ist*
$$\begin{aligned} 4409 &= 142 \cdot 31 + 7 \\ 31 &= 4 \cdot 7 + 3 \\ 7 &= 2 \cdot 3 + 1 \\ 3 &= 3 \cdot 1, \end{aligned}$$
also $r_3 = 0$ *und* $\mathbf{ggT}(4409, 31) = r_2 = 1$.

4. *Sei* $a = 57317$, $b = 2197$, *dann ist*
$$\begin{aligned} 57317 &= 26 \cdot 2197 + 195 \\ 2197 &= 11 \cdot 195 + 52 \\ 195 &= 3 \cdot 52 + 39 \\ 52 &= 1 \cdot 39 + 13 \\ 39 &= 3 \cdot 13, \end{aligned}$$
damit ist $r_4 = 0$ *und* $\mathbf{ggT}(57317, 2197) = r_3 = 13$.

Darstellung des Euklidischen Algorithmus als Computerprogramm, in der Syntax der Sprache QBASIC: (Eingabe zweier Zahlen ungleich null, dies sollte vom Programm abgefragt werden, wir sparen uns dies. Ebenso sollte die erste Zahl größer gleich der zweiten sein, im anderen Fall sollte man die Zahlen vertauschen, diesen Schritt sparen wir uns ebenso.)

```
INPUT a\\
INPUT b\\
q=0\\
r=b\\
WHILE r>0
b=r\\
WHILE a-(q+1)*b>=0\\
q=q+1\\
WEND \\
q=0\\
r=a-q*b\\
a=b\\
WEND\\
PRINT "ggT",b
```

Aufgabe 1.2.8
Man realisiere den oben angegebenen Algorithmus in einem Computerprogramm und berechne damit den größten gemeinsamen Teiler einer Reihe von Zahlenpaaren.

Beweis von Satz 1.2.6. Erstens $r_{j-1}|a$, denn in der allgemeinen Zeile

$$r_n = q_{n+2}r_{n+1} + r_{n+2}$$

ist klar, daß ein gemeinsamer Teiler von r_{n+1} und r_{n+2} ein Teiler von r_n ist. Da aber $r_{j-1}|r_{j-2}$, teilt r_{j-1} alle vorhergehenden Reste.

Für die Gegenrichtung betrachten wir einen beliebigen gemeinsamen Teiler von a, b. Dieser teilt dann auch r_0. Dies gilt insbesondere auch für den größten gemeinsamen Teiler.

Wir haben damit gesehen, daß erstens r_{j-1} ein gemeinsamer Teiler von a, b ist, und daß jeder gemeinsamer Teiler r_{j-1} teilt. Damit ist r_{j-1} der größte gemeinsame Teiler. □

Aufgabe 1.2.9
Man versuche ein Zahlenpaar $(a, b) \in \mathbb{N}^2$ *zu finden, so daß der Euklidische Algorithmus möglichst vieler Schritte bedarf. Was ist das maximale* j*, wenn man* a, b *maximal* 100 *wählt?*

Einen zum Begriff des Teilers eng verwandten Begriff stellt das *Vielfache* dar.

Definition 1.2.10

1. *$a \in \mathbb{Z}$ heißt das* Vielfache *einer Zahl $b \in \mathbb{Z}$, wenn b Teiler von a ist.*

2. *a nennt man* gemeinsames Vielfaches *von $b, c \in \mathbb{Z}$, falls beide Zahlen b, c die Zahl a teilen.*

3. *Unter den positiven gemeinsamen Vielfachen von a, b gibt es ein kleinstes, dies wollen wir als* kleinstes gemeinsames Vielfache *von a, b bezeichnen und dafür die Schreibweise $\mathbf{kgV}(a, b)$ einführen.*

Aufgabe 1.2.11
Für eine Reihe von Zahlenpaaren (a, b) bestimme man $\mathbf{ggT}(a, b)$ und $\mathbf{kgV}(a, b)$ und überprüfe die Gleichung

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

Wir benötigen noch eine alternative Charakterisierung des größten gemeinsamen Teilers.

Satz 1.2.12
Die folgenden drei Aussagen sind äquivalent:

1. $\mathbf{ggT}(a, b) = d$.

2. *d ist ein positiver Teiler von a und b, so daß jeder andere gemeinsamer Teiler auch Teiler von d ist.*

3. *d ist die kleinste positive ganze Zahl, die in der Form*

$$d = xa + yb$$

mit $x, y \in \mathbb{Z}$ ausgedrückt werden kann.

Beweis. Wir beweisen dies nach dem Schema (1) $\iff$ (3)$\Rightarrow$ (2), (1) $\iff$ (2).

Zunächst zeigen wir (1) impliziert (3). Dies besteht aus zwei Teilen, nämlich erstens dem Beweis, daß eine entsprechende Darstellung existiert und zweitens der Aussage, daß es die kleinste Zahl mit einer solchen Darstellung ist. Daß eine solche Darstellung existiert folgt aus dem Euklidischen Algorithmus und führt zur grundsätzlichen **Berechenbarkeit** dieser Darstellung. Dazu betrachten wir nochmals den Euklidischen Algorithmus genauer.

Der erste Schritt besteht darin den Rest $a = cb + r_0$ zu berechnen. Dann hat r_0 die Darstellung

$$r_0 = a - cb.$$

Aus der allgemeinen Zeile

$$r_n = q_{n+2}r_{n+1} + r_{n+2}, 0 \leq r_{n+2} < r_{n+1}$$

schließen wir

$$r_{n+2} = r_n - q_{n+2}r_{n+1}.$$

Damit haben wir r_0 in der behaupteten Form dargestellt. Machen wir die Induktionsannahme, daß $r_n = x_n a + y_n b$ und $r_{n+1} = x_{n+1}a + y_{n+1}b$ sich in der gewünschten Form schreiben lassen, so erhalten wir daraus auch die Darstellung

$$\begin{aligned} r_{n+2} &= x_n a + y_n b - (q_{n+2}x_{n+1}a + q_{n+2}y_{n+1}b) \\ &= (x_n - q_{n+2}x_{n+1})a + (y_n - q_{n+2}y_{n+1})b. \end{aligned}$$

Jede Zahl mit der Darstellung

$$c = xa + yb$$

wird von jedem gemeinsamen Teiler von a, b geteilt, insbesondere vom größten gemeinsamen Teiler. Daher ist d die kleinste positive Zahl mit einer solchen Darstellung.

Nun kommen wir zu (3) $\Rightarrow$ (2). Sei d die kleinste positive Zahl mit einer solchen Darstellung. Dann ist jeder gemeinsame Teiler von a, b auch ein Teiler von d.

Wir kommen nun zu (3) $\Rightarrow$ (1) Aus dem ersten Beweisschritt wissen wir, daß $\mathbf{ggT}(a, b)$ eine Darstellung der Form

$$\mathbf{ggT}(a, b) = x'a + y'b$$

hat, also gilt für die Zahl d, die in (3) angegeben ist $d \leq \mathbf{ggT}(a, b)$, aber $\mathbf{ggT}(a, b)$ teilt d und daher ist $\mathbf{ggT}(a, b) = d$ und damit d ein Teiler von a und b. Damit haben wir neben gezeigt (3) $\Rightarrow$ (1) und (1) $\Rightarrow$ (2).

Bleibt als letzter Teil (2) $\Rightarrow$ (1). Dabei ist aber nichts zu zeigen. Nun haben wir auch die Äquivalenz von (1) und (2). $\square$

Eine wichtige Klasse von Zahlen stellen die sogenannten Primzahlen dar, die, wie wir bald sehen werden, auch bei Verschlüsselungen eine entscheidende Rolle spielen.

1.3 Primzahlen

Definition 1.3.1
Eine Zahl $p \in \mathbb{N}, p > 1$ wird als Primzahl *bezeichnet, falls p keine anderen positiven Teiler als 1 und p hat. Man sagt auch p ist* prim. *Ein Teiler einer Zahl, der zugleich Primzahl ist wird als* Primteiler *bezeichnet.*

Beispiel 1.3.2
$2, 3, 5, 7, 11, 13, 17, \ldots, 59, \ldots, 5914343, \ldots, 591434353, \ldots, 573171343, \ldots$ *sind Primzahlen.*

Satz 1.3.3
Jede Zahl $q \in \mathbb{N}, q > 1$, hat mindestens einen Primteiler.

Beweis. Dieser Beweis ist das Muster eines Beweises durch vollständige Induktion. Die Aussage ist richtig für $q = 2$.

Wir nehmen nun an, daß diese Aussage für alle $q = 2, \ldots, n$ bewiesen sei, und wollen daraus ableiten, daß diese Aussage auch für die $q = n + 1$ gilt. Nun gibt es zwei Fälle, entweder hat q keinen Teiler ungleich $1, q$, dann ist es prim und die Aussage wahr. Hat q aber einen solchen (echten) Teiler, sagen wir $1 < a < q$ teilt q, so ist $q = ab$ und beide Zahlen a, b sind echt zwischen 1 und q. Dann gilt aber, daß a einen Primteiler hat, und dieser ist auch ein Primteiler von q. □

Schon im alten Griechenland hat man sich die Frage gestellt, ob es unendlich viele Primzahlen gibt, und Euklid kannte bereits die Antwort.

Satz 1.3.4
Es gibt unendlich viele Primzahlen.

Beweis. Dies ist das Musterbeispiel eines Beweises durch Widerspruch. Wir nehmen an: es gebe nur **endlich viele Primzahlen**. Dann kann man diese aufschreiben, da wir sie nicht kennen, geben wir diesen die Namen $p_1, p_2, \ldots, p_n$. Jedenfalls denken wir uns, daß dies die vollständige Liste **aller Primzahlen** ist. Dann betrachten wir das Produkt

$$Q = p_1 \cdot p_2 \cdot \ldots \cdot p_n = \prod_{j=1}^{n} p_j$$

und dessen Nachfolger

$$P = Q + 1.$$

Dann teilt keine der Zahlen $p_1, \ldots, p_n$ die Zahl P (da ja alle diese Zahlen die Zahl $Q = P - 1$ teilen). Da aber P mindestens einen Primteiler haben muß, kann die Liste nicht vollständig gewesen sein. Dies ist ein Widerspruch. $\square$

Satz 1.3.5
Sind $a, b \in \mathbb{Z}$ und ist p eine Primzahl, welche das Produkt ab teilt, so teilt p entweder as oder b in Zeichen: $p|a$ oder $p|b$.

Andererseits, gilt für eine Zahl $p \in \mathbb{N}$ und alle Zahlen $a, b \in \mathbb{Z}$ der Schluß $p|(ab) \Rightarrow p|a$ oder $p|b$, so ist p prim.

Beweis. Angenommen, $p \not| a$ und $p|(ab)$. Dann ist $\mathbf{ggT}(a,p) = 1$ und nach Satz 1.2.12 gibt es $x, y \in \mathbb{Z}$ mit $xa + yp = 1$, also $xab + ybp = b$. Nun teilt $p|xab$ und ybp, also die gesamte linke Seite und damit auch b.

Für die zweite Aussage kehren wir die Aussage um: p ist nicht prim, impliziert, daß die Aussage $p|(ab) \Rightarrow p|a$ oder $p|b$ nicht wahr ist. Dies ist einfach einzusehen. Ist $p = ab$, $1 < a, b < p$, so teilt $p|(ab)$, aber p teilt weder a noch b. $\square$

Korollar 1.3.6
Teilt eine Primzahl ein Produkt von n Zahlen $a_1 \cdot \ldots \cdot a_n$, so teilt sie mindestens einen der Faktoren.

Aufgabe 1.3.7
Man nennt zwei Zahlen $a, b \in \mathbb{Z}$ relativ prim, *wenn $\mathbf{ggT}(a,b) = 1$ ist. Man zeige:*

1. *Sind a, b relativ prim, so gibt es $x, y \in Z$ mit $xa + yb = 1$.*

2. *Sind a, b relativ prim, und gilt $a|bc$, so hat man $a|c$.*

Hinweis: man orientiere sich an dem Beweis von Satz 1.3.5.

Eine der wichtigsten Sätze zum Aufbau des Zahlensystems ist der folgende.

Satz 1.3.8
Jede Zahl $a \in Z, \neq -1, 0, 1$ hat eine Darstellung als Produkt von Primzahlen

$$a = p_1 \cdot p_2 \cdot \ldots \cdot p_j.$$

Diese Darstellung ist bis auf die Reihenfolge der Faktoren eindeutig.

Beweis. Wir wissen bereits, daß a mindestens einen Primteiler besitzt. Durch Induktion kann man nun vom anderen Teiler wieder einen Primteiler abspalten, bis man schließlich eine Zerlegung in Primzahlen vorliegen hat. Auch die Eindeutigkeit beruht auf einem Induktionsschluß. Angenommen, $a = 2$, so hat man (offenkundig) eine eindeutige Zerlegung in Primfaktoren.

Wir nehmen an, daß für alle Zahlen $1 < b \leq n$ gezeigt sei, daß eine bis auf die Reihenfolge der Faktoren eindeutige Zerlegung in Primfaktoren existiert. Sei $a = n + 1$ und

$$a = p_1 \cdot \ldots \cdot p_j.$$

Angenommen, diese Zerlegung ist nicht eindeutig. Dann gibt es eine zweite Zerlegung

$$a = q_1 \cdot \ldots \cdot q_k.$$

Nun teilt p_1 die Zahl a und somit

$$p_1 | q_1 \cdot \ldots \cdot q_k.$$

Nach Korollar 1.3.6 teilt p_1 eine der Zahlen $q_1, \ldots q_k$. Da diese alle prim sind, ist $p_1 = q_{l_1}$ für ein l_1. Für die Zahl $p_2 \cdot \ldots \cdot p_j = q_1 \cdot \ldots \cdot q_k / p_1$ ist die Eindeutigkeit der Zerlegung aber (induktiv) bereits gezeigt. □

1.4 Rechnen mit Resten

Wir beginnen mit einer einfachen Beobachtung:

Ist p eine Primzahl und sind $a, b \in \mathbb{Z}$, so ist der Rest von $(a + b) \bmod p$ gleich der Summe der Reste von $a \bmod p$ und $b \bmod p$, also

$$(a \bmod p + b \bmod p) \bmod p = (a + b) \bmod p.$$

Die Begründung ist genauso einfach wie instruktiv:
Ist $a = cp + r_a$ und $b = dp + r_b$, $0 \leq r_a + r_b$, so ist

$$a + b = (cp + r_a) + (dp + r_b) = (c + d)p + r_a + r_b$$

Ist $r_a + r_b < p$, so sind wir fertig, andernfalls folgt

$$a + b = (c + d + 1)p + (r_a + r_b - p)$$

und $0 \leq r_a + r_b - p < p$. Im ersten Fall ist

$$(a + b) \cong (r_a + r_b) \bmod p,$$

im zweiten Fall ist

$$(a+b) \cong (r_a + r_b - p) \bmod p \cong r_a + r_b \bmod p.$$

Anders ausgedrückt gilt

$$(a+b) \cong (a \bmod p + b \bmod p) \bmod p.$$

Ähnliches gilt für die Multiplikation

$$a \cdot b = (cp + r_a)(dp + r_b) = (cd)p^2 + (r_a d + r_b c)p + r_a r_b.$$

Wieder ist der erste Teil durch p teilbar und der Rest ist durch den Ausdruck $r_a r_b$ gegeben, solange dieser kleiner p ist. Jedenfalls ist der Rest der Teilung von ab durch p durch den Rest der Teilung $r_a r_b$ durch p gegeben. Insgesamt ergibt sich wieder

$$a \cdot b \cong r_a r_b \bmod p.$$

Wir wollen dies noch etwas formaler ausdrücken.

Definition 1.4.1
Sei p eine Primzahl, und $0 \leq k < p$. Wir nennen die Menge aller ganzen Zahlen, die bei Teilung durch p den Rest k haben, die Restklasse k modulo p *und schreiben dafür C_k^p. Anders ausgedrückt*

$$C_k^p = \{a \in \mathbb{Z} \mid a \cong k \bmod p\}.$$

Es gibt genau p solcher Restklassen. (Wir erinnern uns an die Klasse der geraden bzw. der ungeraden Zahlen?)

Lemma 1.4.2

1. *Jede ganze Zahl liegt in genau einer Restklasse* $\bmod p$.
2. *Sind x und y in der gleichen Restklasse, so ist p ein Teiler von $x - y$.*

Beweis. Die erste Aussage ist klar: jede Zahl liefert einen Rest bei der Teilung durch p und dieser ist eindeutig bestimmt. Ist $x = ap + r$, $y = bp + r$ (gleiche Rest, da sie in der gleichen Klasse liegen), so ist

$$x - y = (a - b)p.$$

□

Definition 1.4.3
Die nach ersten Aussage von Lemma 1.4.2 eindeutig bestimmte Restklasse, welche $x \in \mathbb{Z}$ enthält, wird mit $[x]_p$ bezeichnet.

Definition 1.4.4
Die Menge der Restklassen $\{[x]_p \mid x \in \mathbb{Z}\}$ wird mit $\mathbb{Z}/p\mathbb{Z}$ bezeichnet.

Lemma 1.4.5
Ist $y \in [x]_p$, so ist $x \in [y]_p$.

Beweis. $y \in [x]_p$ ist genau dann der Fall, wenn $x - y \cong 0 \bmod p$, und dies ist genau dann der Fall, wenn $x \in [y]_p$ ist. □

Wir wollen nun Rechenregeln für Restklassen einführen. Dazu folgende Lemmata.

Lemma 1.4.6
Sind $x \in [0]_p, y \in [0]_p$, so ist $x + y \in [0]_p$.

Beweis. $x = ap$, $y = bp$, daher $x + y = ap + bp = (a + b)p$. □

Lemma 1.4.7
Die Restklasse $[x' + y']_p$ ist unabhängig von der Wahl von $x' \in [x]_p$ und $y' \in [y]_p$.

Beweis. Seien $x', x'' \in [x]_p$ und $y', y'' \in [y]_p$. Zu zeigen ist

$$[x' + y']_p = [x'' + y'']_p.$$

Um dies nachzuweisen, müssen wir zeigen $x' + y' - x'' - y'' \cong 0 \bmod p$. Nun,

$$x' + y' - x'' - y'' = (x' - x'') + (y' - y'').$$

Beide Summanden sind in $[0]_p$, also ist auch die Summe wegen Lemma 1.4.6 in $[0]_p$. □

Damit können wir nun festlegen, was die Summe zweier Restklassen ist.

Definition 1.4.8

$$[x]_p + [y]_p = [x + y]_p.$$

Lemma 1.4.9
Diese Addition von Restklassen genügt den Bedingungen [Add1-4].

Beweis. Die Rolle der Null wird von $[0]_p$ übernommen, $[x]_p$ ist zu $[p-x]_p$ invers. □

Lemma 1.4.10
Sind $x \in [1]_p, y \in [k]_p$, so ist $x \cdot y \in [k]_p$.

Beweis. $x = ap + 1$, $y = bp + k$, daher $x \cdot y = (ap+1) \cdot (bp+k) = abp^2 + (ak+b)p + k$. Dies kongruent ist $k \bmod p$. □

Lemma 1.4.11
Die Restklasse $[x' \cdot y']_p$ ist unabhängig von der Wahl von $x' \in [x]_p$ und $y' \in [y]_p$.

Beweis. Seien $x', x'' \in [x]_p$ und $y', y'' \in [y]_p$. Zu zeigen ist

$$[x' \cdot y']_p = [x'' \cdot y'']_p.$$

Um dies nachzuweisen, müssen wir zeigen $x' \cdot y' - x'' \cdot y'' \cong 0 \bmod p$. Nun,

$$\begin{aligned} x' \cdot y' - x'' \cdot y'' &= x' \cdot y' - x' \cdot y'' + x' \cdot y'' - x'' \cdot y'') \\ &= x'(y' - y'') + y''(x' - x'') \end{aligned}$$

Nun teilt p sowohl $y' - y''$, wie auch $x' - x''$. Damit ist diese Summe in $[0]_p$. □

Damit können wir nun festlegen, was das Produkt zweier Restklassen ist.

Definition 1.4.12

$$[x]_p \cdot [y]_p = [x \cdot y]_p.$$

Satz 1.4.13
In der Menge der Restklassen mit der definierten Addition und Multiplikation sind die Regeln $[Add1-4], [Mul1-4], [Dis]$ erfüllt.

Beweis. Die einzige Regel, deren Nachweis etwas Mühe macht, ist die Existenz der multiplikativen Inverse. Sei p eine Primzahl, $1 < k < p$, dann ist $\mathbf{ggT}(k,p) = 1$, und nach dem Satz 1.2.12 gibt es $x, y \in \mathbb{Z}$ mit

$$xk + yp = 1$$

und $x > 0, y < 0$ oder $x < 0, y > 0$. $y < 0$ heißt aber

$$xk \cong 1 \bmod p$$

oder auch

$$[x]_p[k]_p = [1]_p.$$

Ist $y > 0$, so ist $xk = -1 \bmod p$ und $(xk)^2 = 1 \bmod p$, also $[x^2k]_p[k]_p = [1]_p$. □

Unser wichtigster Satz aus diesem Bereich stammt von FERMAT[2]

Bevor wir ihn beweisen können, brauchen wir noch zwei einfache Hilfsaussagen.

Lemma 1.4.14
Sei p eine Primzahl, dann ist das Produkt

$$\prod_{k=1}^{p-1}[k]_p = [p-1]_p.$$

Anders formuliert, nimmt man aus jeder Nebenklasse eine Zahl und multipliziert diese alle, so erhält man eine Zahl mit Rest $(p-1) \bmod p$.

Beweis. Ist $p = 2$, so besteht das Produkt nur aus einem Faktor $1 = p-1$ und es ist nichts zu zeigen. Für eine ungerade Primzahl hat dieses Produkt $p-2$ nichttriviale Faktoren. (Der Faktor 1 spielt keine Rolle und kann weggelassen werden.) Wir streichen nun aus dem Produkt immer eine Klasse und die Inverse weg. Da $p-2$ ungerade ist, bleibt am Ende mindestens eine Klasse übrig, die zu sich selbst invers ist. Eine solche Klasse ist $[p-1]_p$, denn es gilt

$$(p-1)^2 = p^2 - 2p + 1 \cong 1 \bmod p.$$

Wenn dies die einzige Klasse mit dieser Eigenschaft ist, sind wir fertig. Sei $[q]_p$ eine zu sich selbst inverse Klasse, dann ist $q^2 \cong 1 \bmod p$, also $q^2 = 1 + mp$ für ein $m \in \mathbb{Z}$. Das bedeutet aber $(q+1)(q-1) = mp$ und $p|(q+1)(q-1)$. Daher teilt p entweder $q-1$ oder $q+1$, und da $1 \leq q < p$ ist, bleiben die Fälle $q = 1$ und $q = p-1$ übrig. Damit ist die Behauptung gezeigt. □

[2]Pierre de Fermat (20.8.1601–12.1.1665) französischer Jurist und Mathematiker. Er verfaßte Arbeiten zur Geometrie und Zahlentheorie. Bekannt ist vor allem der nach ihm benannte Satz, der vor kurzem von Andrew Wiles bewiesen wurde.

Lemma 1.4.15
Ist p eine Primzahl und $1 \leq a < p$ eine ganze Zahl, so definiert

$$h_a : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} : [x]_p \mapsto [ax]_p$$

eine Abbildung mit folgenden Eigenschaften:

1. h_a *ist* injektiv, *d.h. ist* $h_a([x]_p) = h_a([y]_p)$, *so ist* $[x]_p = [y]_p$.
2. h_a *ist* surjektiv, *d.h. zu jeder Klasse* $[y]_p$ *existiert eine Klasse* $[x]_p$ *mit* $h_a([x]_p) = [y]_p$.

Beide Eigenschaften bleiben erhalten, wenn wir die Abbildung

$$h_a : \mathbb{Z}/p\mathbb{Z} \setminus \{[0]_p\} \to \mathbb{Z}/p\mathbb{Z} \setminus \{[0]_p\}$$

betrachten.

Beweis. Wir zeigen zunächst die Injektivität. Angenommen

$$h_a([x]_p) = h_a([y]_p).$$

Dann gibt es ein $x' \in [x]_p$ und ein $y' \in [y]_p$ mit

$$p|(ax' - ay').$$

Schreiben wir $x' = \alpha p + r_x$ und $y' = \beta p + r_y$, so teilt p den Ausdruck $(a(\alpha p + r_x) - a(\beta p + r_y)$, also

$$p|(a(\alpha p + r_x) - a(\beta p + r_y)).$$

Es gilt aber

$$(a(\alpha p + r_x) - a(\beta p + r_y)) = p(a\alpha - b\beta) + a(r_x - r_y).$$

Dies wird aber genau dann von p geteilt, wenn

$$p|a(r_x - r_y).$$

Nun teilt eine Primzahl ein Produkt genau dann, wenn sie einen der Faktoren teilt. Da $p \not| a$ teilt p die Zahl $r_x - r_y$. Dann ist aber

$$x - y \cong 0 \bmod p,$$

also $[x]_p = [y]_p$. Wir kommen zur Surjektivität. Für jedes a ist $h_a : \mathbb{Z}/p\mathbb{Z}$ in sich, verschiedene Urbilder haben verschiedene Bilder. Als ist die Anzahl der Elemente im Bild gleich der Anzahl der Elemente im Urbildraum. Daher ist die Abbildung surjektiv. Beachte: dieses Argument funktioniert nur bei **endlichen** Mengen. □

Satz 1.4.16 (Kleiner Fermat'scher Satz)
Gegeben sei eine Primzahl p. Für $1 \leq a < p$ gilt

$$a^{p-1} \cong 1 \bmod p.$$

Beweis. Wir betrachten das Produkt aller von null verschiedenen Klassen

$$\begin{aligned}
[p-1]_p &= \prod_{k=1}^{p-1} [k]_p \\
&= \prod_{k=1}^{p-1} h_a([k]_p) \\
&= a^{p-1} \prod_{k=1}^{p-1} [k]_p \\
&= a^{p-1} [p-1]_p.
\end{aligned}$$

Multiplikation mit der Klasse $[p-1]_p$ liefert

$$[1]_p = a^{p-1}[1]_p.$$

Dies bedeutet natürlich $[a^{p-1}]_p = [1]_p$ oder auch $a^{p-1} \cong 1 \bmod p$. □

Beispiel 1.4.17

1. $p = 3$, $a = 2$ *liefert* $2^2 \cong 1 \bmod 3$.
2. $p = 7$, $a = 5$ *ergibt* $5^6 \cong 1 \bmod 7$.
3. $13^{573171342} \cong 1 \bmod 573171343$.

1.5 Eine Anwendung in der Kryptographie

Die Verschlüsselung einer Nachricht besteht aus zwei Komponenten, eine Übertragung in ein System von Zahlen und daran anschließend die Anwendung einer Verschlüsselung. Wir interessieren uns dabei vornehmlich für Systeme mit einem öffentlichen Schlüssel, was dies genau bedeutet, werden wir in Kürze sehen. Gegeben sei also eine Zahl $x \in \mathbb{Z}$. Die Verschlüsselung soll diese Zahl in eine Zahl $y \in \mathbb{Z}$ verwandeln, aus der man mit dem Entschlüsselungscode wieder die Zahl x zurückgewinnen kann.

Definition 1.5.1
Ein RSA-Verschlüsselungsverfahren besteht aus

1. *zwei Primzahlen* p, q*;*

2. *einer Kodierzahl* v *und einer Dekodierzahl* w*, wobei*

$$vw \cong 1 \bmod (p-1)(q-1)$$

   gilt. Dabei sind p, q, w *geheim,* v *und* $m = qp$ *bekannt.*

Einer Zahl x *wird die Zahl*

$$y = C(x) = x^v \bmod m$$

zugeordnet.

Nun stellt sich die Frage, wie man aus y den Wert x zurückgewinnen kann. Wir betrachten die Abbildung

$$y \mapsto D(y) = y^w \bmod m.$$

Dann ist

$$\begin{aligned} DC(x) &= x^{vw} \bmod m \\ &= x^{a(p-1)(q-1)+1} \bmod m \\ &= x \cdot (x^{a(p-1)})^{q-1} \bmod m. \end{aligned}$$

Betrachten wir den letzten Ausdruck $\bmod q$, so erhalten wir

$$[x]_q \cdot [x^{a(p-1)}]_q = [x]_q,$$

entsprechend können wir den Ausdruck auch $\bmod p$ betrachten und erhalten als Ergebnis $[x]_p$. Eine Zahl $DC(x)$, deren Rest $\bmod p$ $[x]_p$ und $\bmod q$ $[x]_q$ ist Restklasse $\bmod m$ betrachtet $[x]_m$.

Beispiel 1.5.2
$p = 3$, $q = 7$, $x = 4$. *Dann ist* $(p-1)(q-1) = 12$ *und* $vw \cong 1 \bmod 12$. *Setze* $v = 5$, $w = 17$. *Dann ist*

$$y = 4^5 \bmod 21 = 1024 \bmod 21 = 16 \bmod 21.$$

Nun ergibt sich (durch scharfes hinsehen oder eine kurze Rechnung)

$$y^{17} \bmod 21 = (y^5)^3 \cdot y^2 \bmod 21 = 4^3 \cdot 16^2 \bmod 21 = 1\dot{2}56 \bmod 21 = 4 \bmod 21.$$

Wir sehen hier, sind $m = 21$ und $v = 5$ bekannt, so muß zum Knacken des Codes die Zahl m in Primfaktoren zerlegt werden, daraus erhält man p, q und damit kann ein gültiger Wert von w errechnet werden. Die Sicherheit des Codes ergibt sich aus der Komplexität, die Zahl m zu faktorisieren.

Beispiel 1.5.3
In Algebra Interactive! von Cohen, Cuypers & Sterk *wird als Aufgabe 20 auf Seite 19 folgender Code vorgeschlagen: zuerst wird eine Umsetzung von Text in Zahlen nach folgender Tabelle vorgeschlagen*

$$\begin{array}{ccc} A & = & 01 \\ B & = & 02 \\ C & = & 03 \\ D & = & 04 \\ \vdots & = & \vdots \\ X & = & 24 \\ Y & = & 25 \\ Z & = & 26. \end{array}$$

Ein Leerraum entspreche 00. *Für deutsche Texte wollen wir folgeden Erweiterung verwenden:*

$$\begin{array}{ccc} \text{Ä} & = & 27 \\ \text{Ö} & = & 28 \\ \text{Ü} & = & 29 \\ \text{ß} & = & 30. \end{array}$$

Nun wird dort der Text codiert indem man zwei benachbarte Buchstaben zu einer vierstelligen Zahl zusammenfaßt. Dort werden die Primzahlen $p = 43, q = 61$ mit Produkt $m = 2623$ gewählt. Nun ist $42 \cdot 60 = 2520$ und wir müssen bei einer Verschlüsselungszahl $v = 37$ die Kongruenz

$$vm \cong 1 \bmod 2520$$

lösen. Wir tun dies mit der Verallgemeinerung des Euklidischen Algorithmus

$$1 = \mathbf{ggT}(2520, 37)$$

und erhalten

$$1 = -9 * 2520 + 613 * 37.$$

Der Text **DECODING SUCCEEDED** *nimmt mit der vorgeschlagenen Umsetzung die Form*

0405 0315 0409 1407 0019 2103 0305 0504 0504

an. Durchläuft a *die Liste der Zahlen und berechnet man* $a^{37} \bmod 2623$*, so erhält man die im dem Buch angegebene Folge*

0249 1133 1279 1744 0248 1188 1220 1357 1357.

Bekannt ist dabei i.a. die Zahl $v = 37$ *und* $m = 2623$*. Daraus müssen* p, q*,* $(p-1)(q-1)$ *und* $w = 613$ *berechnet werden. Durch* $b^w \bmod 2623$ *wird die zweite Folge decodiert.*

Beispiel 1.5.4

Preisaufgabe! *Nach den obigen Umsetzungsregeln wurde ein deutscher Satz in Zahlen umgewandelt. Codiert wurde mit* $m = 16637$ *und* $v = 179$*. Dabei entstand folgende Zahlenfolge, die zu decodieren und in den ursprünglichen Text zurückzuverwandeln ist.*

7330 14285 16606 13133 3208 12033 785 3227 15539

12116 8887 11532 13452 13061 14316 16346 15777 15539