Kryptographie

Vorlesung von Dr. Norbert Hoffmann
LaTeX-Ausarbeitung von Sebastian Vollmer

Mathematisches Institut
Georg-August-Universität Göttingen
Sommersemester 2003

Inhaltsverzeichnis

0 Einleitendes

Thema In der Kryptographie geht es um Methoden zum Ver- und Entschlüsseln vertraulicher Nachrichten. Man unterscheidet zwei Typen von Ver- und Entschlüsselungsverfahren.

Symmetrische Verfahren Sender A und Empfänger B teilen ein Geheimnis, den *Schlüssel*. Dieser wird sowohl zum Verschlüsseln als auch zum Entschlüsseln gebraucht. Umgekehrt bedeutet das aber, dass B auch senden und A auch empfangen kann. Das Problem bei solchen Verfahrne ist der Austausch des Schlüssels, welcher geheim bleiben muss, damit das Verfahren sicher ist.

Asymmetrische Verfahren Wieder ist A Sender und B Empfänger, jedoch teilen die beiden diesmal nicht das Geheimnis eines gemeinsamen Schlüssels. In diesem Fall wird mit zwei Schlüssel gearbeitet. Einem zum Entschlüsseln, der nur B bekannt ist (private key), und einem zum Verschlüsseln, der zwar B "gehört" aber auch dem A bekannt ist, weil er veröffentlicht wurde (public key).
A verschlüsselt die Nachricht mit dem public key des B, und B entschlüsselt die Nachricht wieder mit seinem private key. Umgekehrt ist dies nicht möglich, A kann nicht entschlüsseln.

Wichtige Public-Key-Verfahren

- Rivest, Shamir und Adleman 1978: RSA-Verfahren
- Diffie und Hellman 1976, ElGamal 1985: ElGamal-Verfahren

Anwendungensbereiche Geheimdienst, e-commerce, Email-Verschlüsselung, ...

Literatur

(1) J. Buchmann: Einführung in die Kryptographie

(2) J. Wolfart: Einführung in die Zahlentheorie und Algebra

(3) N. Koblitz: A Course in Number Theory and Cryptography

(4) E. Kranakis: Primality and Cryptography

(5) A. Beutelspacher, J. Schwenk, K.-D. Wolfenstetter: Moderne Verfahren der Kryptographie

(6) K. Meyberg: Algebra

(7) A. Werner: Elliptische Kurven in der Kryptographie

1 Zahlentheorie und RSA-Verfahren

1.1 Restklassen und additive Chiffren

Problem Wie kann man geheime Nachrichten "sicher" über nicht abhörsichere Kanäle übertragen?

Beispiel Julius Cäsar schrieb in vertraulichen Briefen D statt A, E statt B, F statt C, usw. Die geheime Nachricht ERRARE HUMANUM EST (Klartext) hat er also übertragen als HUUDUH KXPDQXP HVW (Chiffretext). Das Klartextalphabet $\mathcal{P} = \{\text{A, B, C, D, }\ldots\text{, X, Y, Z}\}$ und das Chiffretextalphabet $\mathcal{C}$ sind hier gleich.
Das Verschlüsseln erfolgt durch eine injektive Abbildung $E : \mathcal{P} \to \mathcal{C}$.

$a \in \mathcal{P}$	A	B	C	D	$\ldots$	W	X	Y	Z
$E(a)$	D	E	F	G	$\ldots$	Z	A	B	C

Das Entschlüsseln erfolgt durch eine Abbildung $D : \mathcal{C} \to \mathcal{P}$ mit $D \circ E = \mathrm{id}_{\mathcal{P}}$, d.h. $D(E(a)) = a$ für alle $a \in \mathcal{P}$.

$a \in \mathcal{P}$	A	B	C	D	$\ldots$	W	X	Y	Z
$D(a)$	X	Y	Z	A	$\ldots$	T	U	V	W

Rechnen mit Restklassen

Erinnerung Seien $a, m \in \mathbb{Z}$. Dann sind gleichbedeutend:

i) $m|a$ (lies: m *teilt* a, m ist ein *Teiler* von a)

ii) a ist durch m *teilbar*

iii) a ist ein *Vielfaches* von m

iv) es gibt eine ganze Zahl k mit $a = k \cdot m$.

Konvention Sei $\mathbb{N} = \{1, 2, 3, \ldots\}$, also insbesondere $0 \notin \mathbb{N}$.

Definition 1.1.1 *Seien $a, b \in \mathbb{Z}$ und $m \in \mathbb{N}$. a heißt* kongruent *zu b* modulo *m, falls $b - a$ durch m teilbar ist. Wir schreiben dann*

$$a \equiv b \bmod m.$$

Beispiel Es ist $25 \equiv 4 \bmod 7$, denn $4 - 25 = -21 = (-3) \cdot 7$.

Lemma 1.1.2 *Sei $m \in \mathbb{N}$. Für alle ganzen Zahlen a, b, c gilt:*

i) $a \equiv a \bmod m$

ii) Wenn $a \equiv b \bmod m$, dann ist auch $b \equiv a \bmod m$.

iii) Wenn $a \equiv b \bmod m$ und $b \equiv c \bmod m$, dann ist auch $a \equiv c \bmod m$.

Beweis:

i) $a - a = 0 = 0 \cdot m$ ist durch m teilbar.

ii) Sei $a \equiv b \bmod m$, dann gibt es ein $k \in \mathbb{Z}$ mit $b - a = km$. Folglich ist $a - b = (-k)m$ durch m teilbar.

iii) Wegen $a \equiv b \bmod m$ gibt es ein $k \in \mathbb{Z}$ mit $b-a = km$, und wegen $b \equiv c \bmod m$ gibt es ein $l \in \mathbb{Z}$ mit $c-b = lm$. Folglich ist $c-a = (b-a)+(c-b) = km+lm = (k+l)m$ durch m teilbar.

□

Das Lemma besagt, dass Kongruenz modulo einem festen $m \in \mathbb{N}$ eine Äquivalenzrelation auf $\mathbb{Z}$ ist. Die Äquivalenzklassen heißen *Restklassen modulo m*.

Definition 1.1.3 *Für $m \in \mathbb{N}$ sei $\mathbb{Z}/m$ die Menge aller Restklassen modulo m.*

Notation Die Restklasse von $a \in \mathbb{Z}$ modulo m wird mit $[a]_m$ oder kurz $[a]$ bezeichnet. Es ist also

$$[a]_m = \{a + k \cdot m : k \in \mathbb{Z}\} \in \mathbb{Z}/m.$$

$[a]_m = [b]_m$ bedeutet dasselbe wie $a \equiv b \bmod m$. Die Elemente einer Restklasse nennt man ihre *Repräsentanten*. Zum Beispiel sind a und $a - 3m$ Repräsentanten von $[a] \in \mathbb{Z}/m$.

Notiz 1.1.4 *Sei $m \in \mathbb{N}$. Dann gilt*

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

Insbesondere hat $\mathbb{Z}/m$ genau m Elemente.

Beweis: Nach Division mit Rest ist jede ganze Zahl kongruent modulo m zu genau einer der Zahlen $0, 1, \ldots, m-1$. Jede Restklasse modulo m kommt also genau einmal vor in der Liste $[0], [1], \ldots, [m-1]$. □

Wir können unser Alphabet mit $\mathbb{Z}/26$ identifizieren:

$$A \leftrightarrow [1]_{26}, B \leftrightarrow [2]_{26}, C \leftrightarrow [3]_{26}, \ldots, Y \leftrightarrow [25]_{26}, Z \leftrightarrow [26]_{26} = [0]_{26}.$$

Lemma 1.1.5 *Sei $m \in \mathbb{N}$, und seien a, a', b, b' ganze Zahlen mit*

$$a \equiv a' \bmod m \qquad \textit{und} \qquad b \equiv b' \bmod m.$$

Dann gelten auch

i) $a + b \equiv a' + b' \bmod m$ *und*

ii) $a \cdot b \equiv a' \cdot b' \bmod m$.

Beweis: Nach Voraussetzung gibt es ganze Zahlen k, l mit

$$a' = a + k \cdot m \qquad \text{und} \qquad b' = b + l \cdot m.$$

Einsetzen ergibt

$$a' + b' = (a + b) + (k + l) \cdot m \equiv a + b \bmod m.$$

Das zeigt i). Ausmultiplizieren zeigt ii):

$$a'b' = ab + alm + bkm + klm^2 \equiv ab \bmod m.$$

□

Definition 1.1.6 *Die beiden Grundrechenarten*

$$+, \cdot : \mathbb{Z}/m \times \mathbb{Z}/m \to \mathbb{Z}/m$$

sind definiert durch

$$\begin{aligned} [a]_m + [b]_m &:= [a + b]_m \quad \textit{und} \\ [a]_m \cdot [b]_m &:= [a \cdot b]_m. \end{aligned}$$

Wir wählen dabei Repräsentanten a und b von $[a]_m$ bzw. $[b]_m$. Die Ergebnisse hängen laut Lemma 1.1.5 nicht von diesen Wahlen ab, d.h. sie sind *wohldefiniert*.

Lemma 1.1.7 *Sei $m \in \mathbb{N}$. Für alle $[a], [b], [c] \in \mathbb{Z}/m$ gilt:*

$$\begin{aligned} [a] + [b] &= [b] + [a], \\ [a] + ([b] + [c]) &= ([a] + [b]) + [c], \\ [a] + [0] &= [a], \\ [-a] + [a] &= [0], \\ [a] \cdot [b] &= [b] \cdot [a], \\ [a] \cdot ([b] \cdot [c]) &= ([a] \cdot [b]) \cdot [c], \\ [1] \cdot [a] &= [a] \quad \textit{und} \\ [a] \cdot ([b] + [c]) &= [a] \cdot [b] + [a] \cdot [c]. \end{aligned}$$

Beweis: Wähle Repräsentanten und benutze die Rechenregeln in $\mathbb{Z}$. □

Mathematische Beschreibung von Cäsars Verfahren:

Klartext- und Chiffretextalphabet werden dargestellt durch $\mathcal{P} = \mathcal{C} = \mathbb{Z}/26$. Verschlüsselt wird mit $E : \mathcal{P} \to \mathcal{C}$, $E([a]_{26}) = [a]_{26} + [3]_{26}$, und entschlüsselt wird mit $D : \mathcal{C} \to \mathcal{P}$, $D([b]_{26}) = [b]_{26} + [-3]_{26}$.

Ein Problem dabei ist, dass das Verfahren geheimgehalten werden muss, da der Chiffretext sonst von jedem entschlüsselt werden kann, der das Verfahren kennt. Wir führen deshalb zur Erschwerung einen Parameter $k \in \mathcal{K}$ ein. Wir nennen k *Schlüssel* und $\mathcal{K}$ *Schlüsselraum.*

Verschlüsselung $E_k : \mathcal{P} \to \mathcal{C}$ und Entschlüsselung $D_k : \mathcal{C} \to \mathcal{P}$ hängen nun von k ab.

Kerckhoffssches Prinzip (1883) Man muss sich darauf einstellen, dass ein Angreifer $\mathcal{P}$, $\mathcal{C}$, $\mathcal{K}$, $\{E_k : k \in \mathcal{K}\}$ und $\{D_k : k \in \mathcal{K}\}$ kennt, nur der Schlüssel k wird geheimgehalten.

Durch die begrenzte Zahl der Schlüssel (26) bietet dieses Verfahren allerdings nur begrenzte Sicherheit, zumal wenn Computer bei der Entschlüsselung zur Hilfe genommen werden.

Symmetrische Chiffren

Ein symmetrisches Verschlüsselungsverfahren besteht aus:

(1) Klartextalphabet $\mathcal{P}$, Chiffretextalphabet $\mathcal{C}$,

(2) Schlüsselraum $\mathcal{K}$,

(3) Abbildungen $E_k : \mathcal{P} \to \mathcal{C}$ und $D_k : \mathcal{C} \to \mathcal{P}$ mit $D_k \circ E_k = \mathrm{id}_{\mathcal{P}}$.

Beispiel: additive Chiffren Seien Klartext- und Chiffretextalphabet $\mathcal{P} = \mathcal{C} = \mathbb{Z}/m$ und der Schlüsselraum $\mathcal{K} = \mathbb{Z}/m$. Wir wählen einen Schlüssel $[k] \in \mathbb{Z}/m$. Verschlüsselt wird mit $E_{[k]} : \mathcal{P} \to \mathcal{C}$, $E([a]) = [a] + [k]$, und entschlüsselt mit $D_{[k]} : \mathcal{C} \to \mathcal{P}$, $D([b]) = [b] + [-k]$.

Im Spezialfall $m = 26$ und $[k] = [3]$ ist das Cäsars Verfahren.

1.2 Multiplikative Chiffren und Euklidischer Algorithmus

Seien wieder Klartext- und Chiffretextalphabet $\mathcal{P} = \mathcal{C} = \mathbb{Z}/m$ und der Schlüssel $[k] \in \mathbb{Z}/m$. Verschlüsselt werden soll mit $E_{[k]} : \mathcal{P} \to \mathcal{C}$, $E([a]) = [k] \cdot [a]$.

Problem Wie kann man Nachrichten entschlüsseln, die mit diesem $E_{[k]}$ verschlüsselt wurden?

Definition 1.2.1 *Der* größte gemeinsame Teiler $\mathrm{ggT}(a,b)$ *zweier ganzer Zahlen* a,b *ist die größte ganze Zahl* d*, für die* $d|a$ *und* $d|b$ *gilt.* a *und* b *heißen* teilerfremd*, falls* $\mathrm{ggT}(a,b)=1$.

Offenbar gelten $\mathrm{ggT}(a,b)=\mathrm{ggT}(b,a)$, $\mathrm{ggT}(a,b)=\mathrm{ggT}(-a,b)$ und $\mathrm{ggT}(a,0)=|a|$ für $a\neq 0$. Man setzt $\mathrm{ggT}(0,0)=0$.

Lemma 1.2.2 *Sei* $m\in\mathbb{N}$*, und seien* $a,b\in\mathbb{Z}$ *kongruent modulo* m*. Dann gilt*

$$\mathrm{ggT}(a,m)=\mathrm{ggT}(b,m).$$

Beweis: Nach Voraussetzung gilt $b=a+km$ mit einem $k\in\mathbb{Z}$. Jeder Teiler d von a und m teilt also auch b. Damit folgt $ggT(a,m)\leq\mathrm{ggT}(b,m)$ und analog $\mathrm{ggT}(b,m)\leq\mathrm{ggT}(a,m)$. □

Definition 1.2.3 *Eine* prime Restklasse *modulo* $m\in\mathbb{N}$ *ist eine Restklasse* $[a]\in\mathbb{Z}/m$*, bei der* a *und* m *teilerfremd sind.* $(\mathbb{Z}/m)^*\subseteq\mathbb{Z}/m$ *bezeichnet die Menge aller primen Restklassen modulo* m*.*

Die Wohldefiniertheit folgt aus Lemma 1.2.2.

Wir hatten einen Schlüssel $[k]\in\mathbb{Z}/m$ und eine Verschlüsselung

$$E_{[k]}:\mathbb{Z}/m\to\mathbb{Z}/m, E_{[k]}([a])=[k]\cdot[a].$$

gewählt. Wenn k und m einen gemeinsamen Teiler $d>1$ haben, ist $E_{[k]}$ nicht injektiv. Denn es ist zwar $[m/d]_m\neq[0]_m$, aber

$$E_{[k]}([m/d]_m)=[k]_m[m/d]_m=[(k/d)\cdot m]_m=[0]_m=E_{[k]}([0]_m).$$

Daher sind nur prime Restklassen $[k]$ als Schlüssel geeignet, ein geeigneter Schlüsselraum ist $\mathcal{K}=(\mathbb{Z}/m)^*$.

Euklidischer Algorithmus

Der Euklidische Algorithmus ist ein Verfahren zur Berechnung vom ggT zweier ganzer Zahlen a und b:

- 0-ter Schritt: Setze $a_1=|a|$ und $b_1=|b|$.
- n-ter Schritt: Wenn $b_n=0$ ist, dann Abbruch mit Ergebnis a_n.
  Sonst dividiere a_n durch b_n mit Rest. Das liefert $q_n,r_n\in\mathbb{Z}$ mit

  $$a_n=q_n\cdot b_n+r_n \quad\text{und}\quad -b_n/2<r_n\leq b_n/2.$$

  Setze $a_{n+1}:=b_n$ und $b_{n+1}:=|r_n|$.

Satz 1.2.4 *Seien $a, b \in \mathbb{Z}$ und $|b| < 2^l$.*

i) Dieser Algorithmus bricht ab, und zwar im N-ten Schritt mit $N \leq l + 1$.

ii) Der Algorithmus liefert tatsächlich den ggT*, d.h. es gilt $a_N = \mathrm{ggT}(a, b)$.*

Beweis: Es ist $a_n, b_n \geq 0$ für alle n.

i) Per Konstruktion gilt $b_{n+1} = |r_n| \leq b_n/2$. Es ist also

$$b_n < 2^{l+1-n} \quad \text{für alle } n.$$

Falls nicht schon vorher abgebrochen wurde, folgt damit $b_{l+1} < 1$. Also ist dann $b_{l+1} = 0$ und der Abbruch erfolgt im $(l + 1)$-ten Schritt.

ii) Nach Wahl von r_n gilt

$$a_n \equiv r_n \bmod b_n.$$

Mit Lemma 1.2.2 folgt

$$\mathrm{ggT}(a_n, b_n) = \mathrm{ggT}(r_n, b_n) = \mathrm{ggT}(a_{n+1}, b_{n+1}).$$

Iteration liefert

$$\mathrm{ggT}(a, b) = \mathrm{ggT}(a_1, b_1) = \mathrm{ggT}(a_N, b_N) = a_N$$

wegen $b_N = 0$. □

Eine wichtige Folgerung aus dem Euklidischen Algorithmus:

Satz 1.2.5 (Bézout) *Seien $a, b \in \mathbb{Z}$ teilerfremd. Dann gibt es $x, y \in \mathbb{Z}$ mit*

$$x \cdot a + y \cdot b = 1.$$

Beweis: Seien a_n, b_n, q_n, r_n, N wie eben im Euklidischen Algorithmus. Wir konstruieren der Reihe nach (mit absteigender Induktion) ganze Zahlen

$$x_N, y_N, x_{N-1}, y_{N-1}, \ldots, x_1, y_1$$

mit der Eigenschaft

$$x_n \cdot a_n + y_n \cdot b_n = 1 \quad \text{für alle } n.$$

Wir wissen, dass $b_N = 0$ und $a_N = \mathrm{ggT}(a, b) = 1$ ist. Also sind

$$x_N := 1 \quad \text{und} \quad y_N := 0$$

geeignet. Seien x_{n+1} und y_{n+1} schon konstruiert. Dann gilt

$$\begin{aligned} 1 &= x_{n+1} \cdot a_{n+1} + y_{n+1} \cdot b_{n+1} \\ &= x_{n+1} \cdot b_n \pm y_{n+1} \cdot r_n \\ &= x_{n+1} \cdot b_n \pm y_{n+1}(a_n - q_n b_n) \\ &= \pm y_{n+1} \cdot a_n + (x_{n+1} \mp q_n y_{n+1}) \cdot b_n. \end{aligned}$$

Also sind

$$x_n := \pm y_{n+1} \quad \text{und} \quad y_n := x_{n+1} \mp q_n y_{n+1}$$

geeignet. Schließlich finden wir auf diese Weise $x_1, y_1 \in \mathbb{Z}$ mit

$$x_1 \cdot |a| + y_1 \cdot |b| = 1.$$

Also gilt der Satz mit $x := \pm x_1$ und $y := \pm y_1$. □

Dieses Verfahren zur Berechnung von x, y mit $xa + yb = 1$ heißt *erweiterter Euklidischer Algorithmus.*

Korollar 1.2.6 *Sei $m \in \mathbb{N}$, und sei $[a] \in (\mathbb{Z}/m)^*$ eine prime Restklasse modulo m. Dann gibt es eine Restklasse $[x] \in \mathbb{Z}/m$ mit $[x] \cdot [a] = [1]$.*

Beweis: Wähle einen Repräsentanten $a \in \mathbb{Z}$ von $[a]_m$. Dann sind a und m teilerfremd. Finde mit Satz 1.2.5 ganze Zahlen x und y, für die

$$xa + ym = 1$$

gilt. Die Restklasse $[x]_m$ von x erfüllt $[x]_m \cdot [a]_m = [1]_m$. □

Berechnet werden kann dieses x mit dem erweiterten Euklididschen Algorithmus.

Die Umkehrung der obigen Aussage gilt auch:

Lemma 1.2.7 *Wenn es zu $[a] \in \mathbb{Z}/m$ ein $[x] \in \mathbb{Z}/m$ gibt mit*

$$[x] \cdot [a] = [1],$$

dann ist $[a] \in (\mathbb{Z}/m)^*$ eine prime Restklasse.

Beweis: Wähle Repräsentanten $a, x \in \mathbb{Z}$ von $[a]_m$ und $[x]_m$. Laut Voraussetzung gilt

$$x \cdot a = k \cdot m + 1$$

für ein $k \in \mathbb{Z}$. Sei d gemeinsamer Teiler von a und m, dann folgt

$$d | x \cdot a - k \cdot m = 1.$$

Also ist $d = \pm 1$. Daher sind a und m teilerfremd. □

Wir hatten eine multiplikative Chiffre gewählt mit Klartext- und Chiffretextalphabet $\mathcal{P} = \mathcal{C} = \mathbb{Z}/m$, Schlüsselraum $\mathcal{K} = (\mathbb{Z}/m)^*$ und Verschlüsselung

$$E_{[k]} : \mathbb{Z}/m \to \mathbb{Z}/m, E_{[k]}([a]_m) = [k]_m \cdot [a]_m,$$

wobei $[k] \in \mathcal{K} = (\mathbb{Z}/m)^*$ der Schlüssel ist.

Mit dem Korollar 1.2.6 finden wir nun ein $[x] \in \mathbb{Z}/m$ mit

$$[x]_m \cdot [k]_m = [1]_m.$$

Damit können wir Nachrichten entschlüsseln, die mit $E_{[k]}$ verschlüsselt wurden. Nämlich durch

$$D_{[k]} : \mathbb{Z}/m \to \mathbb{Z}/m, D_{[k]}([a]_m) = [x]_m \cdot [a]_m.$$

Denn es ist $D_{[k]} \circ E_{[k]} = \mathrm{id}_{\mathcal{P}}$, da

$$\begin{aligned} D_{[k]}(E_{[k]}([a]_m)) &= [x]_m \cdot [k]_m \cdot [a]_m \\ &= [1]_m \cdot [a]_m \\ &= [a]_m \end{aligned}$$

für alle $[a]_m \in \mathcal{P} = \mathbb{Z}/m$ gilt.

Beispiel Seien $\mathcal{P} = \mathcal{C} = \mathbb{Z}/251$ und $[k] = [35]_{251}$. Als erstes ist zu zeigen, dass der Schlüssel geeignet gewählt wurde, also $[35]_{251} \in (\mathbb{Z}/251)^*$ ist, d. h. $\mathrm{ggT}(251, 35) = 1$.

Hierzu benutzen wir den Euklidischen Algorithmus:

$$\begin{array}{llrcll} a_1 = 251, & b_1 = 35. & 251 &=& 7 \cdot 35 + 6 & \Rightarrow \quad q_1 = 7, \quad r_1 = 6. \\ a_2 = 35, & b_2 = 6. & 35 &=& 6 \cdot 6 - 1 & \Rightarrow \quad q_2 = 6, \quad r_2 = -1. \\ a_3 = 6, & b_3 = 1. & 6 &=& 6 \cdot 1 + 0 & \Rightarrow \quad q_3 = 6, \quad r_3 = 0. \\ a_4 = 1, & b_4 = 0. & & & & \end{array}$$

Es ist also tatsächlich $\mathrm{ggT}(251, 35) = 1$.

Wir brauchen zum Entschlüsseln ein

$$[x] \in \mathbb{Z}/251 \quad \text{mit} \quad [x]_{251} \cdot [35]_{251} = [1]_{251}.$$

Dazu suchen wir $x, y \in \mathbb{Z}$ mit $x \cdot 35 + y \cdot 251 = 1$ und benutzen dafür den erweiterten Euklidischen Algorithmus:

$$\begin{aligned} 1 &= a_4 = b_3 \\ &= -r_2 = -(a_2 - q_2 b_2) = -a_2 + 6b_2 \\ &= -b_1 + 6r_1 = -b_1 + 6(a_1 - q_1 b_1) = 6a_1 - 43b_1 \\ &= 6 \cdot 251 - 43 \cdot 35. \end{aligned}$$

$x = -43$ und $y = 6$ sind folglich geeignet. Also ist $[-43] \cdot [k] = [1]$ in $\mathbb{Z}/251$.

Wir können also mit

$$D_{[k]} : \mathbb{Z}/251 \to \mathbb{Z}/251, D_{[k]}([b]) = [-43] \cdot [b]$$

Nachrichten entschlüsseln, die mit dem obigen Verschlüsselungsverfahren verschlüsselt wurden.

Problem Sender und Empfänger müssen einen Schlüssel $k \in \mathcal{K}$ vereinbaren, der keiner dritten Person bekannt sein darf, da diese Person sonst Nachrichten problemlos entschlüsseln könnte. Die Schwierigkeit bei diesem Verfahren ist es also, den Schlüssel so auszutauschen, dass er geheim bleibt. Ansätze zur Lösung dieses Problems:

Diffie und Hellman (1976) Verfahren zur sicheren Schlüsselvereinbarung , das nur einen öffentlichen Kanal und öffentlich bekannte Verfahren benutzt.

Rivest, Shamir und Adleman (1978) Verschlüsselung mit öffentlichem Schlüssel (public key) .

1.3 Abelsche Gruppen

Definition 1.3.1 *Eine* abelsche Gruppe $(A, +)$ *besteht aus einer Menge* A *und einer Abbildung*

$$+ : A \times A \to A \qquad (a, b) \mapsto a + b$$

mit folgenden Eigenschaften:

(1) Assoziativität: Für alle $a, b, c \in A$ *gilt*

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

(2) Kommutativität: Für alle $a, b \in A$ *gilt*

$$a + b = b + a.$$

(3) neutrales Element: Es gibt ein Element $0 \in A$*, so dass*

$$a + 0 = a \quad \textit{für alle } a \in A$$

gilt. 0 *heißt* neutrales Element *in* A*.*

(4) inverse Elemente: Zu jedem $a \in A$ *gibt es ein* $b \in A$*, so dass gilt:*

$$a + b = 0$$

b *heißt* invers zu a*.*

Lemma 1.3.2 *In jeder abelschen Gruppe* A *sind das neutrale und die inversen Elemente eindeutig bestimmt.*

Beweis: Seien $0, 0' \in A$ neutrale Elemente. Dann folgt

$$0' = 0' + 0 = 0 + 0' = 0.$$

Seien $b, b' \in A$ beide invers zu $a \in A$. Dann gilt

$$b' = b' + 0 = b' + (a + b) = (b' + a) + b = 0 + b = b.$$

□

Beispiele für abelsche Gruppen:

(1) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$.

(2) $(\mathbb{Z}/m, +)$ für jede natürliche Zahl m. Assoziativität und Kommutativät folgen aus Lemma 1.1.7, das neutrale Element ist $[0]_m$, und invers zu $[a]_m$ ist $[-a]_m$.

(3) $(V, +)$ für jeden Vektorraum V.

(4) $(\mathbb{Q} \setminus \{0\}, \cdot)$. Das neutrale Element ist 1, und invers zu $q \in \mathbb{Q} \setminus \{0\}$ ist $1/q$.

(5) $(\mathbb{R} \setminus \{0\}, \cdot)$. Wie bei (4).

Proposition 1.3.3 *Für jedes $m \in \mathbb{N}$ ist $((\mathbb{Z}/m)^*, \cdot)$ eine abelsche Gruppe.*

Beweis: Offensichtlich ist nur $\cdot : (\mathbb{Z}/m)^* \times (\mathbb{Z}/m)^* \to \mathbb{Z}/m$. Es muss daher gezeigt werden, dass für $[a], [b] \in (\mathbb{Z}/m)^*$ auch $[a] \cdot [b] \in (\mathbb{Z}/m)^*$ ist. Laut Korollar 1.2.6 gibt es $[x], [y] \in \mathbb{Z}/m$ mit

$$[x]_m \cdot [a]_m = [1]_m \quad \text{und} \quad [y]_m \cdot [b]_m = [1]_m.$$

Daraus folgt

$$([x] \cdot [y])([a] \cdot [b]) = [1].$$

Laut Lemma 1.2.7 ist $[a] \cdot [b]$ also tatsächlich prim. Folglich haben wir

$$\cdot : (\mathbb{Z}/m)^* \times (\mathbb{Z}/m)^* \to (\mathbb{Z}/m)^*.$$

Assoziativität und Kommutativität folgen aus Lemma 1.1.7. $[1]_m$ ist das neutrale Element. Zu $[a] \in (\mathbb{Z}/m)^*$ gibt es ein Inverses $[x] \in \mathbb{Z}/m$ nach Korollar 1.2.6, dabei ist automatisch $[x] \in (\mathbb{Z}/m)^*$ nach Lemma 1.2.7. □

Definition 1.3.4 *Die* Ordnung *einer abelsche Gruppe $(A, +)$ ist die Anzahl $|A|$ der Elemente von A. $(A, +)$ heißt* endlich, *falls $|A| < \infty$.*

Beispiele

(1) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ und $(\mathbb{Q} \setminus \{0\}, \cdot)$ sind nicht endlich.

(2) $(\mathbb{Z}/m, +)$ ist endlich und hat die Ordnung m.

(3) $((\mathbb{Z}/m)^*, \cdot)$ ist endlich.

Definition 1.3.5 *Für $m \in \mathbb{N}$ bezeichnet $\varphi(m)$ die Ordnung der Gruppe $(\mathbb{Z}/m)^*$, d.h. die Anzahl der primen Restklassen modulo m.*

Beispiel Sei p Primzahl, d.h. $p > 1$ und $d|p$ nur für $d = \pm 1, \pm p$. Dann ist

$$(\mathbb{Z}/p)^* = \{[1], [2], \ldots, [p-1]\}$$

und somit $\varphi(p) = p - 1$.

Notation Sei $(A,+)$ eine abelsche Gruppe, $a,b \in A$ und $n \in \mathbb{N}$. Zur Vereinfachung vereinbaren wir folgende Schreibweisen:

$$\begin{array}{ccc} -a & \text{bedeutet} & \text{das Inverse zu } a. \\ b-a & \text{bedeutet} & b+(-a). \\ na & \text{bedeutet} & \underbrace{a+a+\cdots+a}_{n \text{ Summanden}}. \end{array}$$

Multiplikative Schreibweise:

$a \cdot b$ oder ab	statt	$a+b$	
1	statt	0	(neutrales Element)
a^{-1}	statt	$-a$	(Inverses zu a)
a^n	statt	na	mit $n \in \mathbb{N}$

Definition 1.3.6 *Sei $(A,+)$ eine abelsche Gruppe. Die* Ordnung *von $a \in A$ ist das kleinste $n \in \mathbb{N}$, für das $na = 0$ gilt (bzw. unendlich, falls $na \neq 0$ für alle $n \in \mathbb{N}$).*

Beispiele

(1) Die Ordnung von 1 in $(\mathbb{Z},+)$ ist unendlich.

(2) Die Ordnung von $[1]_m$ in $(\mathbb{Z}/m,+)$ ist m.

(3) Die Ordnung von $[9]_{12}$ in $(\mathbb{Z}/12,+)$ ist vier.

(4) Die Ordnung von $[2]_7$ in $((\mathbb{Z}/7)^*,\cdot)$ ist drei.

Lemma 1.3.7 *Jedes Element a einer endlichen abelschen Gruppe $(A,+)$ hat eine endliche Ordnung.*

Beweis: Für $k < l \in \mathbb{N}$ gilt $ka + (l-k)a = la$. Es folgt

$$(l-k)a = la - ka.$$

Wegen $|A| < \infty$ gibt es $k < l$ mit $ka = la$, d.h. es gilt

$$(l-k)a = 0.$$

Also hat a höchstens Ordnung $l - k < \infty$. □

Definition 1.3.8 *Eine* Untergruppe *einer abelschen Gruppe $(A,+)$ ist eine Teilmenge $U \subseteq A$ mit*

(1) $0 \in U$,

(2) $u + v \in U$ *für alle* $u, v \in U$,

(3) $-u \in U$ *für alle* $u \in U$.

Bemerkung $(U,+)$ ist dann selbst eine abelsche Gruppe.

Beispiele

(1) $\mathbb{Z}$ ist Untergruppe von $(\mathbb{Q},+)$.

(2) $\mathbb{Q}\setminus\{0\}$ ist Untergruppe von $(\mathbb{R}\setminus\{0\},\cdot)$.

(3) In jeder abelschen Gruppe $(A,+)$ sind A und $\{0\}$ Untergruppen.

(4) Die Menge der Vielfachen von $m\in\mathbb{N}$, also $\{km : k\in\mathbb{Z}\}$, ist Untergruppe von $(\mathbb{Z},+)$.

Lemma 1.3.9 *Sei $(A,+)$ abelsche Gruppe. Hat $a\in A$ die Ordnung $n<\infty$, so ist*

$$\langle a\rangle := \{0,a,2a,\ldots,(n-1)a\}\subseteq A$$

eine Untergruppe der Ordnung n.

Beweis: Das neutrale Element 0 von A liegt in $\langle a\rangle$.
Seien $ka, la\in\langle a\rangle$ mit $k,l\in\mathbb{N}$ und $k,l\leq n-1$. Es ist zu zeigen $ka+la\in\langle a\rangle$. Fallunterscheidung:
1. Fall: $k+l\leq n-1$. Dann ist $ka+la=(k+l)a\in\langle a\rangle$.
2. Fall: $n\leq k+l<2n-1$. Dann ist ebenfalls $ka+la=(k+l)a-na=(k+l-n)a\in\langle a\rangle$.
Sei $ka\in\langle a\rangle$ mit $1\leq k\leq n-1$. Dann ist auch $-ka=na-ka=(n-k)a\in\langle a\rangle$. Also ist $\langle a\rangle$ eine Untergruppe von A.
Es ist noch zu zeigen, dass $ka\neq la$ für $0\leq k<l\leq n-1$. Angenommen es ist $ka=la$. Dann steht $(l-k)a=la-ka=0$ wegen $l-k<n$ im Widerspruch dazu, dass a die Ordnung n hat. Also hat $\langle a\rangle$ die Ordnung n. □

Satz 1.3.10 (Lagrange) *Sei U eine Untergruppe einer endlichen abelschen Gruppe $(A,+)$. Dann ist $|U|$ ein Teiler von $|A|$. Insbesondere ist die Ordnung eines jeden $a\in A$ ein Teiler von $|A|$.*

Beweis: Wir nennen $a,b\in A$ *kongruent modulo* U, falls $b-a$ in U liegt. Wir zeigen, dass Kongruenz modulo U eine Äquivalenzrelation auf A ist:
Für alle a gilt $a\equiv a$, da $a-a=0\in U$. Wenn $a\equiv b$ gilt, dann liegt $b-a$ in U, also ist auch $a-b=-(b-a)$ in U, d. h. $b\equiv a$. Wenn $a\equiv b$ und $b\equiv c$ gelten, dann liegen $b-a$ und $c-b$ in U, also ist auch $c-a=(c-b)+(b-a)$ in U, d. h. $a\equiv c$. Kongruenz modulo U ist also tatsächlich eine Äquivalenzrelation. Daher ist A disjunkte Vereinigung der Äquivalenzklassen. Es reicht nun zu zeigen, dass jede dieser Äquivalenzklassen $|U|$ Elemente hat. Sei also $[a]$ die Äquivalenzklasse von $a\in A$. Laut Definition der Kongruenz ist

$$U\to[a],\quad u\mapsto a+u$$

eine surjektive Abbildung; tatsächlich ist sie auch injektiv: Wenn $u,v\in U$ dasselbe Bild haben, dann ist $a+u=a+v$, woraus durch Addition von $-a$ folgt, dass $u=v$ gilt. Also ist die Abbildung bijektiv, und $[a]$ hat genau $|U|$ Elemente. □

Korollar 1.3.11 (Fermat–Euler) *Sei $a \in (\mathbb{Z}/m)^*$ eine prime Restklasse modulo $m \in \mathbb{N}$. Dann gilt $a^{\varphi(m)} = 1$ in $(\mathbb{Z}/m)^*$.*

Beweis: Sei n die Ordnung von a in $((\mathbb{Z}/m)^*, \cdot)$. Nach Lagrange ist n Teiler von $\varphi(m)$. Damit folgt

$$a^{\varphi(m)} = a^n \cdot a^n \cdot \ldots \cdot a^n = 1 \cdot 1 \cdot \ldots \cdot 1 = 1.$$

□

Spezialfall (kleiner Fermatscher Satz) Ist p Primzahl und $a \in (\mathbb{Z}/p)^*$, so gilt $a^{p-1} = 1$.

1.4 Das RSA-Verfahren

Wir werden nun sehen, welche Bedeutung die Resultate des vorigen Abschnitts für die Kryptographie haben. Seien Klartext- und Chiffretextalphabet $\mathcal{P} = \mathcal{C} = (\mathbb{Z}/m)^*$. Alice möchte eine geheime Nachricht an Bob schicken. Bob hat $e, m \in \mathbb{N}$ festgelegt, so dass e teilerfremd zu $\varphi(m)$ ist. Das e heißt *öffentlicher Schlüssel* (public key) von Bob. Alice verschlüsselt ihre Nachricht mit

$$E_e : (\mathbb{Z}/m)^* \to (\mathbb{Z}/m)^*, a \mapsto a^e.$$

Bob berechnet ein $d \in \mathbb{N}$ mit $de \equiv 1 \bmod \varphi(m)$ (mit dem erweiterten Euklidischen Algorithmus). d ist der *geheime Schlüssel* (private key) von Bob, mit dem er die Nachricht von Alice entschlüsseln kann. Er entschlüsselt die Nachricht von Alice mit

$$D_d : (\mathbb{Z}/m)^* \to (\mathbb{Z}/m)^*, b \mapsto b^d.$$

Behauptung Es ist $D_d \circ E_e = \mathrm{id}_{\mathcal{P}}$.

Beweis: Sei $a \in \mathcal{P} = (\mathbb{Z}/m)^*$. Dann gilt

$$D_d(E_e(a)) = a^{e \cdot d} = a^{\varphi(m)} \cdot a^{\varphi(m)} \cdot \ldots \cdot a^{\varphi(m)} \cdot a = a,$$

denn es ist $a^{\varphi(m)} = 1$ nach Korollar 1.3.11. □

Die Sicherheit dieses Verfahrens beruht darauf, dass obwohl m allen bekannt ist, $\varphi(m)$ nur durch Bob problemlos berechnet werden kann. Dies kann von Bob durch eine geschickte Wahl des m gewährleistet werden. Genaueres hierzu werden wir noch sehen.
Man nennt dieses Verschlüsselungsverfahren ein *asymmetrisches Verfahren*. Das bedeutet: Alle können verschlüsseln, aber nur Bob kann entschlüsseln.

1.5 Der Chinesische Restsatz

Definition 1.5.1 *Seien A und B abelsche Gruppen.*

i) Eine Abbildung $f : A \to B$ heißt Homomorphismus, *falls*

$$f(a_1 + a_2) = f(a_1) + f(a_2)$$

für alle $a_1, a_2 \in A$ gilt.

ii) Ein Isomorphismus *$f : A \to B$ ist ein bijektiver Homomorphismus.*

iii) A und B heißen isomorph *($A \cong B$), falls es einen Isomorphismus $f : A \to B$ gibt.*

Ziel Wir wollen eine Formel für $\varphi(m)$ finden.

Notiz 1.5.2 *Sind $(A_1, +)$ und $(A_2, +)$ abelsche Gruppen, so ist auch $(A_1 \times A_2), +$ eine abelsche Gruppe, wenn man die Addition in $A_1 \times A_2$ definiert durch*

$$(a_1, a_2) + (b_1, b_2) := (a_1 + b_1, a_2 + b_2)$$

für alle $a_1, b_1 \in A_1$ und $a_2, b_2 \in A_2$.

Beweis: Wir überprüfen die Axiome aus Definition 1.3.1. Kommutativität und Assoziativität sind direkt aus der Definiton ersichtlich. Das neutrale Element ist $(0_1, 0_2) \in A_1 \times A_2$, wobei $0_1 \in A_1$ und $0_2 \in A_2$ die neutralen Elemente der jeweiligen Gruppen sind. Das inverse Element zu (a_1, a_2) mit $a_1 \in A_1$ und $a_2 \in A_2$ ist $(-a_1, -a_2)$. □

Satz 1.5.3 (Chinesischer Restsatz) *Seien $m_1, m_2 \in \mathbb{N}$ teilerfremd.*

i) Die Abbildung

$$\begin{aligned} f : \mathbb{Z}/m_1m_2 &\to \mathbb{Z}/m_1 \times \mathbb{Z}/m_2 \\ [a]_{m_1 m_2} &\mapsto ([a]_{m_1}, [a]_{m_2}) \end{aligned}$$

ist ein Isomorphismus abelscher Gruppen.

ii) Die Einschränkung von f ist ein Isomorphismus der multiplikativen abelschen Gruppen

$$(\mathbb{Z}/m_1m_2)^* \to (\mathbb{Z}/m_1)^* \times (\mathbb{Z}/m_2)^*.$$

Beweis:

i) Wohldefiniertheit: Sei a' ein weiterer Repräsentant von $[a]_{m_1 m_2}$. Dann folgt

$$m_1 m_2 | a' - a \quad \text{und daraus } m_1 | a' - a \text{ und } m_2 | a' - a,$$

also $[a]_{m_1} = [a']_{m_1}$ und $[a]_{m_2} = [a']_{m_2}$.

Homomorphie:

$$\begin{aligned} f([a] + [b]) &= ([a+b]_{m_1}, [a+b]_{m_2}) \\ &= ([a]_{m_1}, [a]_{m_2}) + ([b]_{m_1}, [b]_{m_2}) \\ &= f([a]) + f([b]). \end{aligned}$$

Surjektivität: Da m_1, m_2 teilerfremd sind, gibt es $x_1, x_2 \in \mathbb{Z}$ mit

$$x_1 m_1 + x_2 m_2 = 1$$

laut Satz 1.2.5.

Wir suchen ein Urbild von $([a_1], [a_2]) \in \mathbb{Z}/m_1 \times \mathbb{Z}/m_2$. Dazu wählen wir Repräsentanten $a_1, a_2 \in \mathbb{Z}$ und betrachten $a := a_1 x_2 m_2 + a_2 x_1 m_1$.

$$a_1 = a_1 x_1 m_1 + a_1 x_2 m_2 \equiv a \bmod m_1$$

und genauso $a_2 \equiv a \bmod m_2$. Also ist $[a]_{m_1 m_2}$ das gesuchte Urbild unter f.

Die Injektivität folgt aus der Surjektivität, da

$$|\mathbb{Z}/m_1 m_2| = m_1 m_2 = |\mathbb{Z}/m_1 \times \mathbb{Z}/m_2|.$$

ii) Es ist als erstes zu zeigen, dass diese Einschränkung von f tatsächlich nach $(\mathbb{Z}/m_1)^* \times (\mathbb{Z}/m_2)^*$ abbbildet. Sei also

$$[a] \in (\mathbb{Z}/m_1 m_2)^*,$$

d.h. $\mathrm{ggT}(a, m_1 m_2) = 1. \Rightarrow \mathrm{ggT}(a, m_1) = 1 = \mathrm{ggT}(a, m_2)$, d.h.

$$f([a]) \in (\mathbb{Z}/m_1)^* \times (\mathbb{Z}/m_2)^*.$$

Wir haben also eine Abbildung

$$f : (\mathbb{Z}/m_1 m_2)^* \to (\mathbb{Z}/m_1)^* \times (\mathbb{Z}/m_2)^*.$$

Diese ist ein Homomorphismus:

$$\begin{aligned} f([a] \cdot [b]) &= ([a \cdot b]_{m_1}, [a \cdot b]_{m_2}) \\ &= ([a]_{m_1}, [a]_{m_2}) \cdot ([b]_{m_1}, [b]_{m_2}) \\ &= f([a]) \cdot f([b]). \end{aligned}$$

Die Injektivität folgt aus i).

Surjektivität: Wegen der Surjektivität in i) reicht es, zu zeigen dass jedes $[a] \in \mathbb{Z}/m_1m_2$ mit $f([a]) \in (\mathbb{Z}/m_1)^* \times (\mathbb{Z}/m_2)^*$ eine prime Restklasse ist.
Wir wählen dazu einen Repräsentanten $a \in \mathbb{Z}$ und nehmen an, dass $\mathrm{ggT}(a, m_1) = 1 = \mathrm{ggT}(a, m_2)$ ist. Nach Satz 1.2.5 gibt es $x, y \in \mathbb{Z}$ mit $xa + ym_1 = 1$. Es folgt

$$xam_2 + ym_1m_2 = m_2.$$

Also teilt jeder gemeinsame Teiler d von a und m_1m_2 auch m_2. Es folgt $d = \pm 1$, da a und m_2 teilerfremd sind. Das zeigt $ggT(a, m_1m_2) = 1$, also ist $[a]_{m_1m_2}$ tatsächlich prim.

□

Korollar 1.5.4 *Sind $m_1, m_2 \in \mathbb{N}$ teilerfremd, so gilt $\varphi(m_1m_2) = \varphi(m_1) \cdot \varphi(m_2)$.*

1.6 Die Primfaktorzerlegung

Erinnerung $p \in \mathbb{Z}$ ist *prim*, wenn $p > 1$ und $d|p$ nur für $d = \pm 1, \pm p$.

Proposition 1.6.1 *Seien $a, b \in \mathbb{Z}$, und sei p eine Primzahl mit $p|ab$. Dann gilt*

$$p|a \quad \textit{oder} \quad p|b.$$

Beweis: Angenommen, $p \not| a$. Dann ist zu zeigen, dass $p|b$. Da p prim ist, folgt $\mathrm{ggT}(a, p) = 1$. Nach Satz 1.2.5 gibt es $x, y \in \mathbb{Z}$ mit $xa + yp = 1$, also

$$xab + ybp = b.$$

Mit $p|ab$ folgt daraus $p|b$. □

Korollar 1.6.2 *Teilt eine Primzahl p ein Produkt $a_1 \cdot \ldots \cdot a_n$ ganzer Zahlen, so teilt p einen der Faktoren.*

Satz 1.6.3 *Sei $n \in \mathbb{N}$.*

i) n besitzt eine Darstellung der Form

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_r^{e_r}$$

mit $r \in \mathbb{N} \cup \{0\}$, paarweise verschiedenen Primzahlen $p_1, p_2, \ldots, p_r$ und natürlichen Zahlen $e_1, \ldots, e_r$.

ii) Die Darstellung in i) ist eindeutig bestimmt bis auf die Reihenfolge der Faktoren.

Beweis:

i) Induktion über n. Induktionsanfang: Für $n = 1$ erfüllt $r = 0$ die Bedingung. Induktionsschritt: Sei $n > 1$. Wenn n prim ist, ist die Behauptung trivial. Sonst gibt es $a, b \in \mathbb{N}$ mit $a, b < n$ und $n = ab$. Laut Induktionsvoraussetzung sind a und b Produkt von Primpotenzen. Dasselbe gilt folglich auch für $n = ab$.

ii) Induktion über n. Induktionsanfang: Für $n = 1$ ist dies klar.
Induktionsschritt: Angenommen $n > 1$ habe die beiden Darstellungen

$$p_1^{e_1} \cdot \ldots \cdot p_r^{e_r} = n = q_1^{f_1} \cdot \ldots \cdot q_s^{f_s}.$$

Dann teilt p_1 das Produkt rechts. Mit Korollar 1.6.2 folgt $p_1 | q_i$ für ein i. Also ist $p_1 = q_i$, da q_i prim ist. Wir erhalten zwei Darstellungen von n/p_1:

$$p_1^{e_1 - 1} \cdot p_2^{e_2} \cdot \ldots \cdot p_r^{e_r} = n/p_1 = q_1^{f_1} \cdot \ldots \cdot q_i^{f_i - 1} \cdot \ldots \cdot q_s^{f_s}$$

Laut Induktionsvoraussetzung stimmen diese (bis auf Reihenfolge) überein. Also stimmen auch die beiden Darstellungen von n überein.

□

Faktorisierungsproblem Das Problem zu gegebenem $n \in \mathbb{N}$ die Primfaktorzerlegung

$$n = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$$

zu bestimmen, ist für große n sehr aufwendig. (Zumindest mit den heute bekannten Verfahren.) Die Faktorisierung ist leichter, wenn n kleinere Primfaktoren hat. Bei fester Größe von n ist die Faktorisierung dann am aufwendigsten, wenn $n = p_1 \cdot p_2$ mit etwa gleich großen Primzahlen p_1 und p_2 ist.

Wie wir noch sehen werden ist dieses Problem die Grundlage dafür, dass unser Bob aus dem vorigen Abschnitt sein m so wählen kann, dass nur er das $\varphi(m)$ problemlos berechnen kann.

Einige Faktorisierungsrekorde

- April 1994: 129 Dezimalstellen (Atkins, Graff, Lenstra, Leyland und > 600 weitere)
- März 2003: 160 Dezimalstellen (Bahr, Franke, Kleinjung, Lochter, Böhm)

Für die Faktorisierung einer Zahl mit 174 Dezimalstellen ist sogar ein Preis von \$10000 ausgesetzt.

Die Multiplikation zweier genügend großer Primzahlen ist also eine sogenannte *Einwegfunktion*, d. h. sie ist praktisch nicht umkehrbar.

Korollar 1.6.4 *Sei $n \in \mathbb{N}$, und sei*

$$n = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$$

die Primfaktorzerlegung von n. Dann ist jeder Teiler d von n von der Form

$$d = \pm p_1^{f_1} \cdot \ldots \cdot p_r^{f_r}$$

mit $0 \leq f_i \leq e_i$ für alle i.

Beweis: Wegen $d|n$ gibt es eine ganze Zahl k mit $n = k \cdot d$. Es folgt

$$n = |k| \cdot |d|.$$

Also ist n das Produkt der Primfaktoren von $|k|$ und $|d|$. Da die Primfaktorzerlegung von n eindeutig ist, folgt

$$|d| = p_1^{f_1} \cdot \ldots \cdot p_r^{f_r} \quad \text{und} \quad |k| = p_1^{e_1 - f_1} \cdot \ldots \cdot p_r^{e_r - f_r}$$

für geeignete $f_1, \ldots, f_r$. □

Korollar 1.6.5

i) Die einzigen Teiler einer Primpotenz p^e sind $\pm 1, \pm p, \pm p^2, \ldots, \pm p^e$.

ii) Wenn n eine natürliche Zahl ist, in deren Primfaktorzerlegung

$$n = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$$

die Primzahl p nicht vorkommt, dann sind n und p^e teilerfremd.

Satz 1.6.6 *Ist m eine natürliche Zahl mit Primfaktorzerlegung*

$$m = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r},$$

mit paarweise verschiedenen Primzahlen $p_1, \ldots, p_r$ und $e_1, \ldots, e_r \in \mathbb{N}$, so gilt

$$\varphi(m) = (p_1 - 1)p_1^{e_1 - 1} \cdot (p_2 - 1)p_2^{e_2 - 1} \cdot \ldots \cdot (p_r - 1)p_r^{e_r - 1}.$$

Beweis: Induktion nach r. Induktionsanfang: Für $r = 1$ ist $m = p^e$ Primpotenz. Nach Korollar 1.6.5.i) ist eine Restklasse $[a]$ modulo m genau dann prim, wenn a nicht durch p teilbar ist. Es folgt

$$(\mathbb{Z}/m)^* = \mathbb{Z}/m \setminus \{[0], [p], [2p], [3p], \ldots, [m - p]\},$$

und somit $\varphi(m) = m - m/p = p^e - p^{e-1} = (p - 1)p^{e-1}$.
Induktionsschritt: Sei $r \geq 2$. Dann gilt $m = m_1 \cdot m_2$ mit

$$m_1 := p_1^{e_1} \quad \text{und} \quad m_2 := p_2^{e_2} \cdot \ldots \cdot p_r^{e_r}.$$

Nach Korollar 1.6.5.ii) sind m_1 und m_2 teilerfremd. Wegen des Korollars 1.5.4 zum Chinesischen Restsatz gilt also

$$\varphi(m) = \varphi(m_1) \cdot \varphi(m_2).$$

Mit den Induktionsvoraussetzungen

$$\begin{aligned} \varphi(m_1) &= (p_1 - 1)p_1^{e_1 - 1} \quad \text{und} \\ \varphi(m_2) &= (p_2 - 1)p_2^{e_2 - 1} \cdot \ldots \cdot (p_r - 1)p_r^{e_r - 1} \end{aligned}$$

folgt die Formel für $\varphi(m)$. □

1.7 Parameter für RSA

Bob will verschlüsselte Nachrichten empfangen können. Dazu geht er wie folgt vor:

Er erzeugt zwei große Primzahlen p und q (z.B. $p \approx 2^{500} \approx q$), berechnet $m := pq$ und $\varphi(m) = (p-1)(q-1)$. (Beide haben im Beispiel etwa 300 Dezimalstellen.) Er wählt ein $e \in \mathbb{N}$, welches teilerfremd zu $\varphi(m)$ ist, (z.B. $e = 2^{16} + 1 = 65537$) und berechnet $d \in \mathbb{N}, d < \varphi(m)$ mit $de \equiv 1 \bmod \varphi(m)$. Die Berechnung erfolgt mit dem erweiterter Euklidischen Algorithmus. (Dieser braucht im Beispiel höchstens 17 Schritte.)
Bob veröffentlicht nun m, e und hält $\varphi(m)$ und d geheim. m nennt man RSA-Modul, e öffentlichen und d privaten Schlüssel von Bob.

Wenn Alice eine Nachricht an Bob senden möchte, kann sie diese mit Bobs öffentlichem Schlüssel verschlüsseln. Sie verwendet dazu die Verschlüsselungsfunktion

$$E_e : (\mathbb{Z}/m)^* \to (\mathbb{Z}/m)^*, \quad a \mapsto a^e.$$

(Dies geschieht rechnerisch mit schneller Exponentiation, welche im Beispiel höchstens $2 \cdot 16$ Multiplikationen modulo m pro Klartextbuchstaben benötigt.)

Bob kann diese Nachricht von Alice entschlüsseln durch

$$D_d : (\mathbb{Z}/m)^* \to (\mathbb{Z}/m)^*, \quad b \mapsto b^d.$$

(Dies geschieht wieder durch schnelle Exponentiation, im Beispiel werden höchstens $\frac{2}{\log(2)} \log(d) \approx 2000$ Multiplikationen modulo m pro Buchstaben gebraucht.)

Dieses Verfahren ist offensichtlich ist viel langsamer als symmetrische Verfahren, aber mit guter Hardware ist es machbar. In der Praxis werden Daten oft mit einem symmetrischen Verfahren verschlüsselt, dessen Schlüssel zuvor mit RSA ausgetauscht wurde. Die Sicherheit des Verfahrens beruht darauf, dass ein Angreifer m nicht faktorisieren, und daher auch $\varphi(m)$ und d nicht berechnen kann. Und ohne $\varphi(m)$ und d kann er auch nicht entschlüsseln.

1.8 Digitale Signatur

Eine weitere wichtige Anwendung von RSA neben der Verschlüsselung ist die digitale Signatur. Eine *Unterschrift* von Bob unter einen Text sollte folgende Eigenschaften haben:

(1) Überprüfbarkeit: Jeder kann überprüfen, ob es tatsächlich Bobs Unterschrift ist.

(2) Echtheit: Der Text stimmt mit dem überein, den Bob unterschrieben hat.

(3) Identität und Fälschungssicherheit: Es war Bob, der unterschrieben hat. Niemand anderes kann Bobs Unterschrift leisten.

Ziel Bob unterschreibt digital. Dies nennt man dann digitale Signatur.

RSA-Signatur Sei weiterhin m Bobs veröffentlichter RSA-Modul, e Bobs öffentlicher und d Bobs privater Schlüssel. Der zu unterschreibende Text bestehe aus Buchstaben aus $(\mathbb{Z}/m)^*$. Bob unterschreibt $a \in (\mathbb{Z}/m)^*$ mit $a^d \in (\mathbb{Z}/m)^*$. Wir überprüfen nun, ob diese digitale Unterschrift die Eigenschaften erfüllt, die eine Unterschrift haben sollte:

(1) Überprüfbarkeit: $a, b \in (\mathbb{Z}/m)^*$ ist Text mit Bobs Unterschrift, falls $a = b^e$ ist.

(2) Echtheit: Ein Angreifer ändert den Text a in $a' \neq a$, also haben wir jetzt den Text mit Unterschrift a', a^d. Dies fliegt beim Überprüfen auf, denn es ist $(a^d)^e \neq a'$.

(3) Identität und Fälschungssicherheit:

$$\begin{array}{rcl} \text{Bobs Unterschrift} & = & \text{RSA-Entschlüsselung} \\ \text{unter } a & & \text{des Chiffretextbuchstaben } a \end{array}$$

Die Unterschrift ist also genauso schwer zu fälschen wie die RSA-Verschlüsselung zu brechen ist.

Die dignitale Signatur genügt also den Anforderungen, die an eine Unterschrift gestellt werden.

1.9 Erzeugung großer Primzahlen

Primzahltest Laut Definition ist $n \in \mathbb{N}$ nicht prim, wenn es ein $d|n$ mit $1 < d < n$ gibt. Bei großem n muss man auf diese Weise jedoch viel zu viele d's ausprobieren. Wir wissen, dass $n \in \mathbb{N}$ nicht prim ist, wenn $a^{n-1} \neq 1$ für ein $a \in (\mathbb{Z}/n)^*$ gilt (nach dem kleinen Fermatschen Satz). Das Problem hierbei ist, dass auch wenn n nicht prim ist, oft gilt $a^{n-1} = 1$ in $(\mathbb{Z}/n)^*$.

Lemma 1.9.1 *Ist p eine Primzahl, so hat die Kongruenz $x^2 \equiv 1 \bmod p$ nur die Lösungen $x \equiv 1$ und $x \equiv -1$.*

Beweis: Sei x eine ganze Zahl mit $x^2 \equiv 1 \bmod p$. Dann folgt

$$p|x^2 - 1 = (x-1)(x+1).$$

Mit Proposition 1.6.1 folgt

$$\begin{array}{rcl} p|(x-1) & \text{oder} & p|(x+1), \text{ also} \\ x \equiv 1 & \text{oder} & x \equiv -1 \bmod p. \end{array}$$

□

Mit anderen Worten: Wenn $a^2 \equiv 1 \bmod n$ für ein $a \not\equiv \pm 1 \bmod n$ gilt, so ist n nicht prim.

Bemerkung 1.9.2 *Kennt man ein $a \in \mathbb{Z}$ mit $a^2 \equiv 1$ und $a \not\equiv \pm 1$ modulo n, so kann man mit dem Euklidischen Algorithmus sogar einen echten Teiler von n finden, nämlich* $\mathrm{ggT}(a-1, n)$. *Echter Teiler bedeutet in diesem Fall* $1 < \mathrm{ggT}(a-1, n) < n$.

Beweis: Wegen $a \not\equiv 1 \bmod n$ ist $a-1$ nicht durch n teilbar, also ist $\mathrm{ggT}(a-1, n) < n$. Angenommen, $\mathrm{ggT}(a-1, n) = 1$. Dann gäbe es ein $x \in \mathbb{Z}$ mit $x(a-1) \equiv 1 \bmod n$. Dann folgt

$$a + 1 \equiv x(a-1)(a+1) \equiv x(a^2 - 1) \equiv x \cdot 0 \equiv 0 \bmod n.$$

Dies steht im Widerspruch zur Annahme $a \not\equiv -1 \bmod n$. □

Satz 1.9.3 *Sei n eine ungerade natürliche Zahl, $n \geq 3$. Zerlege $n-1$ in eine Zweierpotenz 2^e und eine ungerade Zahl u, d. h. $n - 1 = 2^e \cdot u$.*

i) Ist n prim, so haben alle $n-1$ Restklasse $[a] \neq 0$ modulo n die folgende Eigenschaft:

$$(*)\ a^u \equiv 1 \bmod n, \quad \textit{oder} \quad \textit{es gibt ein } f < e \textit{ mit } a^{2^f u} \equiv -1 \bmod n.$$

ii) Ist n nicht prim, so haben weniger als $n/2$ Restklassen $[a]$ modulo n die Eigenschaft (*).

Beweis: i) Wir betrachten die Restklassen modulo n von

$$a^u, a^{2u}, a^{4u}, a^{8u}, \ldots, a^{2^e u} = a^{n-1}.$$

Nach dem kleinen Fermatschen Satz ist die letzte gleich [1]. Also sind alle gleich [1], oder es gibt ein $f < e$ mit

$$a^{2^f u} \not\equiv 1 \quad \text{und} \quad a^{2^{f+1} u} \equiv 1 \bmod n.$$

Demnach ist $a^{2^f u} \equiv -1 \bmod n$ wegen Lemma 1.9.1.

ii) Alle $a \in \mathbb{Z}/n$, für die (*) gilt, erfüllen $a^{n-1} = 1$ und liegen daher in $(\mathbb{Z}/n)^*$. Wir betrachten die Menge M aller $f < e$, zu denen es ein $a \in (\mathbb{Z}/n)^*$ gibt mit $a^{2^f u} = -1$. Es ist $M \neq \emptyset$, da $0 \in M$, denn es gilt $(-1)^{2^0 u} = -1$. Sei F das größte Element von M, und sei

$$U := \{a \in \mathbb{Z}/n : a^{2^F u} = \pm 1\}.$$

Alle $a \in \mathbb{Z}/n$, für die (*) gilt, liegen in U. Daher reicht zu zeigen, dass

$$|U| < n/2.$$

Aber U ist *Untergruppe* von $((\mathbb{Z}/n)^*, \cdot)$. Wir sehen gleich, dass U sogar eine *echte* Untergruppe ist, d.h. $U \subsetneq (\mathbb{Z}/n)^*$. Mit dem Satz von Lagrange folgt dann

$$|U| \leq \varphi(n)/2 < n/2.$$

Wir müssen daher nur noch zeigen $U \subsetneq (\mathbb{Z}/n)^*$. Hierfür unterscheiden wir zwei Fälle.

1. Fall: n ist Primpotenz, also ist $n = p^g$ mit einer Primzahl p und $g \geq 2$. Wir betrachten $a := [p+1] \in (\mathbb{Z}/n)^*$. Nach der Binomischen Formel modulo p^2 ist

$$(1+p)^{n-1} \equiv 1 + (n-1)p \not\equiv 1 \bmod p^2,$$

also erst recht $(1+p)^{n-1} \not\equiv 1 \bmod n$, d.h.

$$a^{n-1} \neq 1.$$

Daraus folgt $a \notin U$, wie benötigt.

2. Fall: n ist keine Primpotenz. Folglich ist $n = n_1 n_2$ mit n_1, n_2 teilerfremd. Nach Wahl von F gibt es ein $a = [\alpha] \in (\mathbb{Z}/n)^*$ mit $a^{2^F u} = -1$. Nach dem Chinesischen Restsatz gibt es ein $b = [\beta] \in (\mathbb{Z}/n)^*$ mit

$$\begin{aligned} \beta &\equiv 1 \bmod n_1 \quad \text{und} \quad \beta \equiv \alpha \bmod n_2. \\ \Rightarrow \beta^{2^F u} &\equiv 1 \bmod n_1 \quad \text{und} \quad \beta^{2^F u} \equiv -1 \bmod n_2, \end{aligned}$$

also ist $\beta^{2^F u} \not\equiv \pm 1 \bmod n$ und damit $b \notin U$, wie benötigt. □

Bemerkung Eine Verfeinerung dieses Beweises zeigt, dass (*) im Fall ii) sogar nur für weniger als $n/4$ Restklassen gilt.

Primzahltest (Miller-Rabin) Gegegeben sei $n \in \mathbb{N}$, n ungerade. Um zu überprüfen, ob n prim ist, führen wir folgendes Verfahren durch:

(1) Wir wählen eine zufällige Restklasse $a \in \mathbb{Z}/n$ und überprüfen die Eigenschaft (*). Dies geschieht durch schnelles Potenzieren. Der Rechenaufwand dafür ist z.B. ≤ 1000 Multiplikationen modulo n, falls $n \approx 2^{500}$ ist.

(2) Falls (*) nicht erfüllt ist, ist n nicht prim. In dem Fall wird das Verfahren abgebrochen.

(3) Falls (*) erfüllt ist, wählen wir ein neues zufälliges a und wiederhole das Verfahren t mal, etwa $t = 30$.

Ergebnis

- War (*) einmal nicht erfüllt, so ist n nicht prim.
- War (*) immer erfüllt, so ist n *vermutlich* prim. Wäre n nicht prim, würde mit Wahrscheinlichkeit $\geq 1 - 1/2^t$ wenigstens eines der a nicht (*) erfüllen. (Im Bsp. mit Wahrscheinlichkeit $\geq 1 - 1/1000000000$.)

Der Primzahltest nach Miller-Rabin ist also ein *probabilistischer* Test.

Primzahlerzeugung Es ist keine Formel bekannt, die immer Primzahlen liefert. Allerdings brauchen wir für RSA unvorhersagbare Primzahlen, deshalb erzeugen wir große zufällige Primzahlen mit folgendem Verfahren:

(1) Wir erzeugen eine Zufallszahl n der gewünschten Größe.

(2) Wir überprüfen mit dem Miller-Rabin-Test, ob n vermutlich prim ist. Falls ja, so ist $p := n$ geeignet und das Verfahren kann abgebrochen werden.

(3) Sonst erzeugen wir eine neue Zufallszahl n und wiederhole das Verfahren so lange, bis für n der Miller-Rabin-Test positiv ausgeht.

Frage Wie viele n's werden getestet, bis eines als prim erkannt wird? Oder anders gefragt: Wie groß ist der "Anteil" der Primzahlen in $\mathbb{N}$?.

Definition 1.9.4 *Für $n \in \mathbb{N}$ bezeichne $\pi(n)$ die Anzahl der Primzahlen kleiner oder gleich n.*

Lemma 1.9.5 *Für alle $n \in \mathbb{N}$ gilt*

$$n^{\pi(2n)-\pi(n)} \leq \binom{2n}{n} \leq (2n)^{\pi(2n)}.$$

Beweis: Linke Ungleichung: Sei p prim und $n < p \leq 2n$. Dann gilt $p|(2n)!$, aber $p \not| n!$, also $p|\binom{2n}{n}$. D.h. all diese p kommen in der Primfaktorzerlegung von $\binom{2n}{n}$ vor. Es folgt

$$\binom{2n}{n} \geq \prod_{\substack{p \text{ prim} \\ n<p\leq 2n}} p \geq \prod_{\substack{p \text{ prim} \\ n<p\leq 2n}} n = n^{\pi(2n)-\pi(n)}.$$

Rechte Ungleichung: Wir haben die Primfaktorzerlegung

$$n! = \prod_{p\leq n \text{ prim}} p^{e_p} \quad \text{mit} \quad e_p = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \ldots.$$

Dabei bezeichnet $\lfloor x \rfloor$ die größte ganze Zahl $\leq x$ für $x \in \mathbb{R}$. Genauso erhalten wir

$$(2n)! = \prod_{p\leq 2n \text{ prim}} p^{f_p} \quad \text{mit} \quad f_p = \left\lfloor \frac{2n}{p} \right\rfloor + \left\lfloor \frac{2n}{p^2} \right\rfloor + \ldots + \left\lfloor \frac{2n}{p^{k_p}} \right\rfloor.$$

Dabei ist $k_p :=$ Exponent der größten Potenz von p, die $\leq 2n$ ist. Es folgt

$$\binom{2n}{n} = \prod_{p\leq 2n \text{ prim}} p^{f_p - 2e_p}.$$

Aber $\lfloor 2x \rfloor - 2\lfloor x \rfloor$ ist 0 oder 1 für alle $x \in \mathbb{R}$. Demnach ist $f_p - 2e_p \leq k_p$ für alle p, also

$$\binom{2n}{n} \leq \prod_{p\leq 2n \text{ prim}} p^{k_p} \leq \prod_{p\leq 2n \text{ prim}} (2n) = (2n)^{\pi(2n)}.$$

□

Satz 1.9.6 (Tschebyscheff 1852) *Für alle $n \in \mathbb{N}$ mit $n \geq 3$ gilt*

$$\frac{1}{2}\frac{n}{\log n} < \pi(n) < 2\frac{n}{\log n},$$

dabei ist log *der natürliche Logarithmus.*

Beweis: Wir beweisen diesen Satz mit Lemma 1.9.5. Zunächst beweisen wir folgende Behauptung:

i) Es ist $\binom{2n}{n} < 4^n$ für alle $n \in \mathbb{N}$.
ii) Es ist $3^n < \binom{2n}{n}$ für $n \geq 5$.

zu i): Mit der Binomischen Formel folgt

$$4^n = (1+1)^{2n} = \sum_{k=0}^{2n} \binom{2n}{k} \cdot 1^k \cdot 1^{n-k} > \binom{2n}{n}.$$

zu ii): Mit Induktion. Induktionsanfang für $n = 5$:

$$\binom{10}{5} = \frac{10 \cdot 9 \cdot 8 \cdot 7 \cdot 6}{5 \cdot 4 \cdot 3 \cdot 2 \cdot 1} = 9 \cdot 4 \cdot 7 > 9 \cdot 27 = 3^5.$$

Induktionsschritt von n auf $n+1$:

$$\binom{2(n+1)}{n+1} \Big/ \binom{2n}{n} = \frac{(2n+2)!(n!)^2}{(2n)!((n+1)!)^2} = \frac{(2n+2)(2n+1)}{(n+1)^2} = \frac{4n+2}{n+1} > 3.$$

Also ist $\binom{2(n+1)}{n+1} > 3\binom{2n}{n} > 3^{n+1}$ nach Induktionsvoraussetzung.

Wir beweisen nun die linke Ungleichung aus dem Satz durch Nachrechnen für $n \leq 11$. Mit dem Lemma 1.9.5 und der Abschätzung eben folgt, dass für gerade $n \geq 10$ gilt

$$\pi(n) \log n \geq \log \binom{n}{n/2} > \frac{n}{2} \log 3 > \frac{n}{2},$$

und für ungerade $n \geq 13$

$$\pi(n) \log n > \pi(n-1) \log(n-1) > \frac{n-1}{2} \log 3 > \frac{n}{2}$$

wegen $\log 3 > n/(n-1)$ für diese n. In beiden Fällen folgt die linke Ungleichung.

Wir betrachten nun die rechte Ungleichung. Beweis durch Induktion über n. Induktionsanfang für $n \leq 400$: Die Fälle $n \leq 8$ werden nachgerechnet. Jede Primzahl $p \neq 2$ ist ungerade, 1 und 9 sind nicht prim. Also folgt

$$\pi(n) < n/2 \quad \text{für} \quad n \geq 9.$$

Gilt außerdem $n \leq 50$, so ist $\log n < 4$ und damit

$$\pi(n) < n/2 < 2n/\log n.$$

Ein analoges Argument zeigt den Rest des Induktionsanfanges: Wenn p prim ist, gilt $p = 2, 3$ oder $p \equiv \pm 1 \bmod 6$, aber nicht $p = 1, 25, 35$. Es folgt

$$\pi(n) < n/3 \quad \text{für} \quad n \geq 35.$$

Wenn zusätzlich $n \leq 400$ ist, dann ist $\log n < 6$, also

$$\pi(n) < n/3 < 2n/\log n.$$

Induktionsschritt von n auf $2n-1$ und $2n$ mit $n \geq 60$: Wir wissen schon

$$\big(\pi(2n) - \pi(n)\big)\log(n) < \log \binom{2n}{n} < 2n \log 2$$

nach Lemma 1.9.5 und der Abschätzung eben. Also folgt

$$\begin{aligned}
\pi(2n) &< \pi(n) + \frac{2n}{\log n}\log 2. \quad \Big| \text{ Induktionsvoraussetzung} \\
&< \frac{2n}{\log n}(1 + \log 2) \\
&= \frac{2n-1}{\log(2n)}(1 + \frac{1}{2n-1})(1 + \frac{\log 2}{\log n})(1 + \log 2) \\
&< \frac{2n-1}{\log(2n)} \cdot 2 \quad \text{wegen } n \geq 60.
\end{aligned}$$

Daraus folgt sowohl

$$\pi(2n) < 2\frac{2n}{\log(2n)}$$

als auch

$$\pi(2n-1) \leq \pi(2n) < 2\frac{2n-1}{\log(2n-1)}.$$

□

Bemerkung Wir haben also eine Heuristik für den Anteil der Primzahlen nahe n. Wegen $\pi(n) \approx f(n)$ mit $f(x) := x/\log x$ erwartet man für $1 \ll d \ll n$

$$\frac{\pi(n+d) - \pi(n-d)}{2d} \approx \frac{f(n+d) - f(n-d)}{2d} \approx f'(n) \approx 1/\log n.$$

Wir wollten große (zufällige) Primzahlen erzeugen. Dabei sind wir so vorgegangen, dass wir große Zufallszahlen erzeugt und dann getestet haben, ob sie prim sind. Dies haben wir solange gemacht, bis eine Primzahl gefunden wurde.
Wir wissen jetzt, dass wir etwa $\log n$ Zufallszahlen nahe n testen müssen, um eine Primzahl zu finden. Im Beispiel $n \approx 2^{500}$ sind das etwa 350. (Alles bis auf einen Faktor zwischen $1/2$ und 2, da $1/2 f(n) < \pi(n) < 2f(n)$.)

Bemerkung Der Primzahlsatz (Hadamard, de la Vallée Poussin 1896) besagt

$$\lim_{n\to\infty} \pi(n) \Big/ \frac{n}{\log n} = 1.$$

Riemannsche Vermutung Es gibt eine Konstante C, so dass für alle $n \geq 2$ gilt

$$\left| \pi(n) - \int_2^n \frac{d\,x}{\log x} \right| < C\sqrt{n}\log n.$$

Aufgaben

(1) Löse die Kongruenz $x^3 + 4x^2 - 3x + 6 \equiv 0 \pmod{12}$.

(2) In $\mathbb{Z}/15$ suche die Lösungen der Gleichung $x^3 + [3]x^2 + [5]x + [4] = 0$.

(3) Entziffre den unten stehenden Chiffretext eines alphabetischen Cäsars. Dazu kann die folgende Häufigkeitstabelle der Buchstaben in deutschen Texten nützlich sein (Angaben in Prozent).

a	5,96	f	1,23	k	1,12	p	0,59	u	4.87	z	1,21
b	1,77	g	3,25	l	3,19	q	0,01	v	0,76		
c	3,17	h	4,61	m	2,47	r	6,42	w	2,03		
d	5.22	i	7,97	n	11,06	s	7,48	x	0,01		
e	17,98	j	0,06	o	2,00	t	5,55	y	0,01		

Chiffretext:

MNARC	JURNW	RBLQN	QDVJW	RBCUN	XWKJC
CRBCJ	JUKNA	CRNAO	JWMER	NAINQ	WQDWM
NACBR	NKIRP	MRNNA	BCNLQ	ROOAR	NADWM
MNLQR	OOARN	AVJBL	QRWNK	NBCNQ	NWMJD
BIFNR	TXWIN	WCARB	LQNWB	LQNRK	NWJWM
NANWA	JWMMR	NKDLQ	BCJKN	WMNBJ	UYQJK
NCBBC	JWMNW				

(4) Das Klartextalphabet $\mathcal{P}$ bestehe ebenso wie das Chiffretextalphabet $\mathcal{C}$ aus den 26 Buchstaben des Alphabets. Ferner sei der n-te Buchstabe des Alphabets (mit 0 beginnend) mit der Restklasse $[n]_{26}$ in $\mathbb{Z}/26$ identifiziert.

(a) Verschlüssle den folgenden Klartext mit Hilfe der Abbildung $E : \mathcal{P} \longrightarrow \mathcal{C}$, $x \mapsto x(13x + 2)$.

Klartext:

Der Abt Johannes Trithemius ist der Schutzpatron der Kryptologen.

(b) Der folgende Chiffretext wurde durch Verschlüsseln eines Klartextes mit der Abbildung E aus (a) gewonnen. Entschlüssle ihn!

Chiffretext:

PJAQK	ITIDQ	MINIV	IINZS	QEUIJ	ZIIQN
EBQXX	VQIVD	IVXAB	VINTA	KAOXI	QNIYK
EBJOI	KKIJS	CVZPI	VOBZ		

(5) (a) Beweise die 9-er Probe: Eine natürliche Zahl ist genau dann durch 9 teilbar, wenn ihre Quersumme durch 9 teilbar ist.

(b) Beweise die 11-er Probe: Eine natürliche Zahl ist genau dann durch 11 teilbar, wenn ihre alternierende Quersumme durch 11 teilbar ist.

(6) (a) Berechne den größten gemeinsamen Teiler der Zahlen 9503 und 2002.

(b) Finde ganze Zahlen x und y mit $803x + 174y = 1$.

(c) Berechne das Inverse von 720 in $(\mathbb{Z}/1001)^*$.

(7) Gib die Verknüpfungstabelle einer abelschen Gruppe der Ordnung 4 an, die kein Element der Ordnung 4 enthält. Findet man eine solche Gruppe unter den Gruppen der Form $(\mathbb{Z}/m)^*$?

(8) (a) Gib die Elemente von $(\mathbb{Z}/15)^*$ an und bestimme $\varphi(15)$.

(b) Erstelle die Verknüpfungstabelle der Gruppe $(\mathbb{Z}/15)^*$.

(c) Bestimme die Ordnung der Elemente der Gruppe $(\mathbb{Z}/15)^*$.

(9) (a) Es seien a und b zwei Elemente einer abelschen Gruppe mit teilerfremden, endlichen Ordnungen n_a und n_b. Dann gilt für die Ordnung n_{a+b} von $a + b$ die Formel $n_{a+b} = n_a \cdot n_b$.

(b) Zeige, dass es in jeder abelschen Gruppe der Ordnung 6 ein Element der Ordnung 6 gibt.

(10) (Schnelles Potenzieren) Es sei $m > 1$ eine natürliche Zahl, a eine Restklasse modulo m. Die natürliche Zahl e sei in der Binärdarstellung durch $e = (1e_1e_2...e_n)_{\text{bin}}$ gegeben, wobei also $e_k \in \{0, 1\}$ für $k \leq n$ gilt und $e = \sum_{k=0}^{n} e_k 2^{n-k}$ (mit $e_0 := 1$).

(a) Zur Berechnung von a^e definiere die Restklassen $a_0, a_1, ..., a_n$ durch die folgende rekursive Vorschrift:

$$\begin{aligned} a_0 &= a \\ a_{k+1} &= a_k^2, \text{ falls } e_{k+1} = 0 \\ a_{k+1} &= a_k^2 \cdot a, \text{ falls } e_{k+1} = 1 \end{aligned}$$

Beweise $a^e = a_n$.

(b) Führe das Verfahren mit $m = 119$, $a = [15]$ und $e = 29$ aus und berechne $[15]^{29}$.

(c) Zeige, dass das in (a) beschriebene Verfahren stets mit $\frac{2}{\log(2)} \log(e)$ Multiplikationen auskommt. (Zum Vergleich: Beim gewöhnlichen Potenzieren werden zur Berechnung von a^e genau $e-1$ Multiplikationen $\mod m$ benötigt.)

(11) Löse die simultane Kongruenz

$13x \equiv 7 \mod 11$
$19x \equiv 1 \mod 23$.

(12) (RSA-Verfahren) Es sei $m = 6499$. Dann ist $\varphi(m) = 6336$. Diese beiden Zahlen seien Bestandteile eines RSA-Verfahrens, wobei der öffentliche Schlüssel $e = 5$ zum Potenzieren benutzt wird.

(a) Berechne das multiplikative Inverse von e modulo $\varphi(m)$.

(b) Verschlüssle den folgenden Klartext:

$[1405]_m$ $[2107]_m$ $[0905]_m$ $[1809]_m$ $[0733]_m$

(c) Entschlüssle den folgenden Chiffretext:

$[4355]_m$ $[1442]_m$

(13) (Legendre-Symbol) Es sei p eine ungerade Primzahl.

(a) Es sei a eine zu p prime Zahl. Zeige, dass die Kongruenz $x^2 \equiv a \bmod p$ genau 2 modulo p inkongruente Lösungen besitzt oder gar keine Lösung. Ist die Kongruenz $x^2 \equiv a \bmod p$ lösbar, so heißt a *Quadratischer Rest (modulo p)*, ansonsten *Quadratischer Nichtrest (modulo p)*. Das *Legendresymbol* $\left(\frac{a}{p}\right)$ ist definiert als 1, falls a Quadratischer Rest ist, sonst als -1.

(b) Beweise, dass es genau $\frac{p-1}{2}$ prime Quadratische Reste modulo p gibt.

(c) Die Abbildung $a \mapsto \left(\frac{a}{p}\right)$ ist ein Gruppenhomomorphismus von $(\mathbb{Z}/p)^*$ nach $(\{\pm 1\}, \cdot)$.

(14) (a) Ist die Verschlüsselungsabbildung $E_e : (\mathbb{Z}/m)^* \longrightarrow (\mathbb{Z}/m)^*$ des RSA-Verfahrens ein Gruppenhomomorphismus? Wie beantwortet sich die Frage für die Entschlüsselungsabbildung D_d anstatt E_e?

(b) Um verschlüsselte Nachrichten empfangen und Signaturen durchführen zu können, verwendet *Bob* das RSA-Verfahren mit dem Modul $m = 5917$ und dem öffentlichen Schlüssel $e = 119$. *Bob* hat die Nachricht $[2521]_m$ unterschrieben mit $[4267]_m$ und die Nachricht $[4787]_m$ mit $[1992]_m$. Fälsche *Bob*s Unterschrift unter die Nachricht $[3264]_m$.

(15) (RSA-Verfahren, Low-Exponent-Attack) *Alice* sendet an ihre drei Freunde *Bob*, *Chris* und *Dave* dieselbe geheime Botschaft. Sie verwendet dazu das RSA-Verfahren und benutzt jeweils die öffentlichen Schlüssel der drei Freunde. *Bob*s Schlüssel lautet $(m_B, e_B) = (173, 3)$, *Chris*' Schlüssel lautet $(m_C, e_C) = (167, 3)$ und *Dave*s Schlüssel ist $(m_D, e_D) = (137, 3)$. *Bob* erhält die verschlüsselte Nachricht $[60]_{m_B}$, *Chris* erhält $[4]_{m_C}$ und *Dave* erhält $[37]_{m_D}$.

Mister X hat alle drei Übertragungen belauscht. Er freut sich, dass jeder der Freunde den kleinen Schlüssel 3 zum Potenzieren gewählt hat und entziffert die Nachricht ohne Mühe.

(a) Stelle ein System von drei Kongruenzen auf, dem der Klartext $P \in \mathbb{N}$ genügt. Zeige, dass m_B, m_C und m_D paarweise teilerfremd sind.

(b) Löse das System aus (a) und finde den Klartext P (vorausgesetzt, dass $P < \min\{m_B, m_C, m_D\}$).

(c) Wie hätte *Mister X* die Nachricht entziffert, wenn m_B, m_C, m_D nicht paarweise teilerfremd gewesen wären?

(16) (Carmichael-Zahlen) Zusammengesetzte Zahlen $n \in \mathbb{N}$, für die $a^{n-1} \equiv 1 \bmod n$ gilt, sobald $ggT(a, n) = 1$ ist, heißen *Carmichael-Zahlen*.

(a) Berechne die Primfaktorzerlegung von 561 und zeige, dass 561 eine Carmichael-Zahl ist.

(b) Zeige: Ist die natürliche Zahl l so gewählt, dass $p_1 = 6l+1$, $p_2 = 12l+1$ und $p_3 = 18l+1$ sämtlich Primzahlen sind, dann ist $n = p_1 p_2 p_3$ eine Carmichael-Zahl.

(c) Finde zwei von 561 verschiedene Carmichael-Zahlen.

(17) (a) Zeige, dass $\exp(2x) \geq 1 + 2x \geq \frac{1}{1-x}$ für $0 \leq x \leq \frac{1}{2}$ gilt.

(b) Zeige für jede natürliche Zahl n

$$\exp\Big(\ 2 \sum_{p \leq n,\ \text{prim}} \frac{1}{p}\ \Big) \quad \geq \prod_{p \leq n,\ \text{prim}} \frac{1}{1 - \frac{1}{p}} \quad \geq \quad \sum_{k \leq n} \frac{1}{k}.$$

(c) Folgere, dass $\sum\limits_{p\ \text{prim}} \frac{1}{p}$ divergiert.

(18) (a) Es sei S eine endliche Menge von Primzahlen und $N \in \mathbb{N}$ mit $p|N$ für jedes $p \in S$. Finde eine Formel für die Anzahl A der Zahlen $n \leq N$, die durch keine der Primzahlen $p \in S$ teilbar sind, d.h. für $A = \#\{n \leq N,\ \text{für alle } p \in S \text{ gilt } p \not| n\}$.

(b) Bob wählt zufällig eine Zahl zwischen 1 und 2310. Wie groß ist die Wahrscheinlichkeit, dass sie durch keine der Zahlen $2, 3, 5, 7$ oder 11 teilbar ist?

(19) (a) Schätze die Anzahl der Primzahlen im Intervall $[10^{100}, 10^{100} + 10^6]$ ab.

(b) Falls möglich, beweise mit den Mitteln der Vorlesung, dass im Intervall $[10^{100}, 1.9 \cdot 10^{100}]$ eine Primzahl liegt.

(c) Falls möglich, beweise mit den Mitteln der Vorlesung, dass im Intervall $[10^{100}, 4.04 \cdot 10^{100}]$ eine Primzahl liegt.

(20) (Miller-Rabin-Test) Wähle eine der beiden Zahlen 10249 und 10253 und bezeichne sie mit n. Wähle dann eine zufällige Zahl $a \leq n - 1$ und führe zur Untersuchung der Primalität von n den Miller-Rabin-Test mit a durch.

(21) In der abelschen Gruppe $(\mathbb{Q}, +)$ ist $\mathbb{Z}$ eine Untergruppe. Es sei $A = \mathbb{Q}/\mathbb{Z}$.

(a) Zeige: In A hat jedes Element endliche Ordnung. Zu jeder natürlichen Zahl m gibt es ein Element der Ordnung m in A.

(b) Zeige: Die abelsche Gruppe A ist nicht endlich erzeugt.

(22) (RSA-Verfahren, Angriff durch Iteration)

(a) Es sei (m, e) der öffentlichen Schlüssel eines RSA-Verfahrens. Es sei P ein Klartext und C der Chiffretext, also $C \equiv P^e \bmod m$. Kann eine natürliche Zahl $s > 1$ so gewählt werden, dass sich nach s-maligem Verschlüsseln des Chiffretextes C wieder C ergibt, so kann der Klartext entziffert werden. Es gilt dann, dass P gleich dem $(s-1)$-malig verschlüsselten Chiffretext C ist. Begründe dieses! Ein Angriff auf RSA, der hierauf beruht, heißt *Angriff durch Iteration*.

(b) *Bob* will mit Hilfe des RSA-Verfahrens geheime Botschaften empfangen. Er wählt zwei Primzahlen p und q und berechnet den öffentlichen Schlüssel $m = pq = 3403$. Zum Potenzieren entscheidet er sich für den öffentlichen Schlüssel $e = 9$, damit das Verschlüsseln recht schnell zu erledigen ist. Er veröffentlicht m und e auf seiner Homepage und fügt hinzu, dass das Klartext-Alphabet A,B,C,...,X,Y,Z,., ,, !, ? mit den Doppelziffern 01,02,...,25,26,27,30,31,32,33 zu identifizieren ist, so dass immer 2 Buchstaben bequem verschlüsselt werden können. *Alice* sendet *Bob* eine Botschaft. Sie beginnt mit den Worten: HEY, BOB!

Verschlüssle diesen Text!

(c) *Mister X* war schon immer neugierig. Er belauscht den zweiten Teil von *Alice'* Botschaft und versucht einen Angriff durch Iteration. Er hat Glück, denn *Bob* ist ein schwerwiegender Fehler unterlaufen. Der Chiffretext, den *Mister X* belauscht, lautet: 0670 1143 3092 0494 0098.

Entziffre den Chiffretext mit Hilfe eines Angriffs durch Iteration! Finde p, q, $\varphi(m)$ und das multiplikative Inverse von e modulo $\varphi(m)$.

2 Strukturtheorie abelscher Gruppen

Erinnerung $(A, + : A \times A \to A)$ heißt abelsche Gruppe, wenn $+$ kommutativ und assoziativ ist, es ein neutrales Element $0 \in A$ gibt und zu jedem $a \in A$ ein Inverses $-a \in A$ existiert.

Ziel Sinn und Zweck dieses Kapitels ist es, die abelschen Gruppen $(\mathbb{Z}/m)^*$ besser zu verstehen, da in ihnen das RSA-Verfahren stattfindet. Zudem wollen wir uns auf das ElGamal-Verfahren vorbereiten, bei dem auch in abelschen Gruppen gerechnet wird.

2.1 Faktorgruppen

Sei $(A, +)$ eine abelsche Gruppe und $U \subseteq A$ eine Untergruppe. (D. h.: $0 \in U$, $u + v \in U$ und $-u \in U$ für alle $u, v \in U$.)

Definition 2.1.1 *Zwei Elemente $a, b \in A$ heißen* kongruent modulo U, *falls $b - a \in U$ ist.*

Lemma 2.1.2 *Kongruenz modulo U ist eine Äquivalenzrelation auf A. Die Äquivalenzklasse $[a]$ von $a \in A$ ist die Menge*

$$a + U := \{a + u : u \in U\}.$$

Beweis: Wir rechnen zunächst die Axiome für eine Äquivalenzrelation nach.
Es ist $a \equiv a \mod U$ für alle $a \in A$, denn $a - a = 0 \in U$.
Sei $a \equiv b \mod U$. Dann ist $b - a \in U$ und folglich auch $a - b = -(b - a) \in U$. Also ist dann auch $b \equiv a \mod U$.
Seien $a \equiv b \mod U$ und $b \equiv c \mod U$. Dann sind $b - a, c - b \in U$, also ist auch $c - a = (b - a) + (c - b) \in U$. Daraus folgt $a \equiv c \mod U$.
Nun betrachten wir die Äquivalenzklassen. Es gilt

$$[a] = \{b \in A | a \equiv b \mod U\} = \{b \in A | b - a \in U\} = \{b \in A | b \in a + U\} = a + U.$$

□

Definition 2.1.3 *Sei $(A, +)$ eine abelsche Gruppe und $U \subseteq A$ eine Untergruppe.*

i) Sei $a \in A$. Die Äquivalenzklasse $[a] = a + U$ heißt Nebenklasse (von a) nach U *oder auch* Restklasse (von a) modulo U.

ii) A/U bezeichnet die Menge aller Nebenklassen nach U, also

$$A/U = \{a + U : a \in A\}.$$

Proposition 2.1.4 *Die Menge A/U zusammen mit der Verknüpfung*

$$\begin{aligned} A/U \times A/U &\to A/U \\ (a+U, b+U) &\mapsto (a+b)+U \end{aligned}$$

ist eine abelsche Gruppe.

Beweis: Zunächst ist die Wohldefiniertheit der Verknüpfung zu zeigen. Seien dazu a, a' Repräsentanten von $a+U$ und b, b' Repräsentanten von $b+U$. Dann gilt

$$(a+b)-(a'+b') = (a-a')+(b-b') \in U,$$

also $(a+b)+U = (a'+b')+U$. Daher ist die Verknüpfung wohldefiniert. Dass A/U mit dieser Verknüpfung den Gruppenaxiomen genügt, zeigt man, indem man Repräsentanten wählt und die Gruppenaxiome für A ausnutzt. □

Bemerkung Für die Wohldefiniertheit von $+ : A/U \times A/U \to A/U$ war wichtig, dass $+ : A \times A \to A$ kommutativ ist.

Definition 2.1.5 *Die eben konstruierte abelsche Gruppe $(A/U, +)$ heißt* Faktorgruppe von A nach U.

Beispiele

(1) Seien $(A, +) = (\mathbb{Z}, +)$, $U = m\mathbb{Z} := \{mk : k \in \mathbb{Z}\}$ die Menge der Vielfachen einer natürlichen Zahl m. Dann ist $(A/U, +)$ die abelsche Gruppe $(\mathbb{Z}/m, +)$ der Restklassen modulo m.

(2) Es ist $A/A \cong \{0\}$ für jede abelsche Gruppe A, und $A/\{0\} \cong A$.

(3) Seien A, B abelsche Gruppen. Dann ist $A \times \{0\} \subseteq A \times B$ Untergruppe, und

$$(A \times B)/(A \times \{0\}) \cong B.$$

Proposition 2.1.6 *Sei U eine Untergruppe einer* endlichen *abelschen Gruppe $(A, +)$. Dann sind auch U und A/U endlich, und es gilt*

$$|A| = |U| \cdot |A/U|.$$

Beweis: Im Beweis des Satzes von Lagrange 1.3.10 haben wir schon gesehen, dass jede Nebenklasse nach U genau $|U|$ Elemente hat. Da A die disjunkte Vereinigung aller Nebenklassen nach U ist und es genau $|A/U|$ solche Nebenklassen gibt, folgt daraus bereits die Behauptung. □

2.2 Der Homomorphiesatz

Wiederholung Seien $(A, +)$ und $(B, +)$ abelsche Gruppen. Eine Abbildung $f : A \to B$ heißt Homomorphismus, falls $f(a+a') = f(a)+f(a')$ für alle $a, a' \in A$ gilt.

Beispiele Bei folgenden Abbildungen handelt es sich um Homomorphismen:

(1) $\mathrm{id} : A \to A$, $a \mapsto a$, und $0 : A \to B$, $a \mapsto 0$.

(2) Die Inklusion einer Untergruppe $U \subseteq A$, d. h. die Abbildung $U \to A$, $u \mapsto u$.

(3) $\mathbb{Z} \to \mathbb{Z}/m$, $a \mapsto [a]$.

(4) $A \to A/U$, $a \mapsto a + U$.

(5) Wir hatten für $a \in A$, $n \in \mathbb{N}$ definiert $na := a + \cdots + a \in A$. Wir setzen jetzt $(-n)a := -(na)$ und $0a := 0 \in A$. Es ist dann $\mu_a : \mathbb{Z} \to A$, $n \mapsto na$ ein Homomorphismus, denn $na + n'a = (n + n')a$ gilt für alle $n, n' \in \mathbb{Z}$.

(6) Die Exponentialfunktion $\exp : \mathbb{R} \to \mathbb{R} \setminus \{0\}$ ist ein Homomorphismus, denn $\exp(x + y) = \exp(x) \cdot \exp(y)$ gilt für alle $x, y \in \mathbb{R}$.

Lemma 2.2.1 *Ist $f : A \to B$ ein Homomorphismus abelscher Gruppen, so gilt:*

i) $f(0) = 0$

ii) $f(-a) = -f(a)$ *für alle* $a \in A$

Beweis:

i) Es ist $f(0) = f(0 + 0) = f(0) + f(0)$. Zieht man $f(0)$ ab, folgt somit $f(0) = 0$.

ii) Es ist $0 = f(0) = f(a + (-a)) = f(a) + f(-a)$ für alle $a \in A$. Daraus folgt $-f(a) = f(-a)$.

□

Definition 2.2.2 *Sei $f : A \to B$ ein Homomorphismus abelscher Gruppen.*

i) $\ker(f) := f^{-1}(0) = \{a \in A : f(a) = 0\}$ *heißt der* Kern *von* f.

ii) $\mathrm{im}(f) := f(A) = \{f(a) : a \in A\}$ *heißt das* Bild *von* f.

Proposition 2.2.3 *Sei $f : A \to B$ ein Homomorphismus abelscher Gruppen.*

i) $\mathrm{im}(f)$ *ist eine Untergruppe von* B.

ii) $\ker(f)$ *ist eine Untergruppe von* A.

iii) f *ist genau dann injektiv, wenn* $\ker(f) = \{0\}$ *ist.*

Beweis:

i) Es ist $f(0) = 0 \in B$, also $0 \in \mathrm{im}(f)$.
Seien $b, b' \in \mathrm{im}(f)$, also $b = f(a)$ und $b' = f(a')$ mit $a, a' \in A$. Dann ist $b + b' = f(a) + f(a') = f(a + a') \in \mathrm{im}(f)$.
Sei $b \in \mathrm{im}(f)$, also $b = f(a)$ für ein $a \in A$. Dann ist $-b = f(-a) \in \mathrm{im}(f)$.

ii) Es ist $0 \in \ker(f)$ wegen $f(0) = 0$.
Seien $a, a' \in \ker(f)$. Dann gilt $f(a + a') = f(a) + f(a') = 0 + 0 = 0$, also $a + a' \in \ker(f)$.
Sei $a \in \ker(f)$. Dann gilt $f(-a) = -f(a) = -0 = 0$, also $-a \in \ker(f)$.

iii) Sei f injektiv. Es ist $0 \in \ker(f)$, da $f(0) = 0$ ist. Sei $a \in \ker(f)$, dann gilt $f(a) = 0 = f(0)$. Wegen der Injektivität von f folgt daraus $a = 0$, also $\ker(f) = \{0\}$.
Sei $\ker(f) = \{0\}$. Seien $a, a' \in A$ mit $f(a) = f(a')$. Dann gilt $f(a - a') = f(a) - f(a') = 0$, also $a - a' \in \ker(f) = \{0\}$. D.h. $a = a'$, f ist also injektiv.

□

Bemerkung $f : A \to B$ ist genau dann surjektiv, wenn $\mathrm{im}(f) = B$ ist. Daher ist der Homomorphismus f genau dann ein Isomorphismus, wenn $\ker(f) = \{0\}$ und $\mathrm{im}(f) = B$ ist.

Satz 2.2.4 (Homomorphiesatz) *Ist $f : A \to B$ ein Homomorphismus abelscher Gruppen, so gilt*

$$A/\ker(f) \cong \mathrm{im}(f).$$

Beweis: Wir zeigen, dass $g : A/\ker(f) \to \mathrm{im}(f) \subseteq B$, $[a] \mapsto f(a)$ ein Isomorphismus ist. Daraus folgt die Behauptung dann sofort.
Wohldefiniert: Seien $a, a' \in A$ mit $[a] = [a']$. Dann ist $a' - a \in \ker(f)$, d.h. $f(a' - a) = 0$. Daher gilt $f(a') - f(a) = f(a' - a) = 0$, woraus $f(a') = f(a)$ folgt.
Homomorphie: Es gilt

$$g([a] + [a']) = g([a + a']) = f(a + a') = f(a) + f(a') = g([a]) + g([a']).$$

Injektivität: Sei $[a] \in \ker(g)$, d.h. $0 = g([a]) = f(a)$, also $a \in \ker(f)$. Daraus folgt $[a] = 0$ in $A/\ker(f)$, was zeigt $\ker(g) = \{0\}$.
Surjektivität: Sei $b \in \mathrm{im}(f)$. Dann gibt es ein $a \in A$ mit $b = f(a)$. Wegen $f(a) = g([a])$ folgt $b = f(a) \in \mathrm{im}(g)$. □

Beispiel Seien $m_1, m_2 \in \mathbb{N}$ teilerfremd. $f : \mathbb{Z} \to \mathbb{Z}/m_1 \times \mathbb{Z}/m_2$, $a \mapsto ([a]_{m_1}, [a]_{m_2})$ ist ein Homomorphismus. Nach dem Homomorphiesatz gilt

$$\mathbb{Z}/\ker(f) \cong \mathrm{im}(f) \subseteq \mathbb{Z}/m_1 \times \mathbb{Z}/m_2.$$

Außerdem ist $\ker(f) = m_1\mathbb{Z} \cap m_2\mathbb{Z} = m_1 m_2 \mathbb{Z}$, da m_1 und m_2 teilerfremd sind. Es folgt also

$$\mathbb{Z}/\ker(f) = \mathbb{Z}/m_1 m_2 \cong \mathrm{im}(f),$$

insbesondere hat es $m_1 m_2$ Elemente. Wegen $|\mathbb{Z}/m_1 \times \mathbb{Z}/m_2| = m_1 m_2$ folgt sogar $\mathrm{im}(f) = \mathbb{Z}/m_1 \times \mathbb{Z}/m_2$ und insgesamt

$$\mathbb{Z}/m_1 m_2 \cong \mathbb{Z}/m_1 \times \mathbb{Z}/m_2.$$

Beispiel Angewandt auf den Homomorphismus

$$\mathbb{R} \to \mathbb{C}^*, x \mapsto \exp(2\pi i x) = \cos(2\pi x) + i \sin(2\pi x)$$

liefert der Homomorphiesatz 2.2.4, dass $R/Z \cong S^1$ ist. Dabei ist S^1 die multiplikative Gruppe der komplexen Zahlen vom Betrag eins.

2.3 Endlich erzeugte abelsche Gruppen

Definition 2.3.1 *Sei $(A, +)$ eine abelsche Gruppe, $a_1, \ldots, a_k \in A$. Die Untergruppe*

$$\langle a_1, \ldots, a_k \rangle := \{n_1 a_1 + \ldots + n_k a_k : n_1, \ldots, n_k \in \mathbb{Z}\} \subseteq A$$

heißt die von $a_1, \ldots, a_k$ erzeugte *Untergruppe von A.*

Lemma 2.3.2 *Für jede Untergruppe $U \subseteq A$, die $a_1, \ldots, a_k$ enthält, gilt*

$$\langle a_1, \ldots, a_k \rangle \subseteq U.$$

Beweis: Aus $a_1, \ldots, a_k \in U$ folgt $n_1 a_1, \ldots, n_k a_k \in U$ für alle $n_i \in \mathbb{Z}$, also liegen auch alle Summen $n_1 a_1 + \ldots + n_k a_k$ in U. D.h. $\langle a_1, \ldots, a_k \rangle \subseteq U$. □

Definition 2.3.3 *Eine abelsche Gruppe $(A, +)$ heißt* zyklisch, *wenn es ein $a \in A$ gibt mit $\langle a \rangle = A$.*

Beispiele

(1) $\mathbb{Z}$ ist zyklisch, 1 ist ein Erzeuger, -1 ist auch Erzeuger.

(2) $\mathbb{Z}/m$ ist zyklisch, $[1]$ ist ein Erzeuger.

(3) $(\mathbb{Z}/5)^*$ ist zyklisch mit Erzeuger $[2]_5$, wie man nachrechnet.

Lemma 2.3.4 *Jede Untergruppe $U \subseteq \mathbb{Z}$ ist zyklisch.*

Beweis: Die Behauptung ist klar, falls $U = \{0\}$ ist. Sonst enthält U positive ganze Zahlen, sei m die kleinste dieser Zahlen. Wir zeigen nun, dass U von m erzeugt wird: Sei $k \in U$. Division mit Rest liefert $k = qm + r$ mit $q \in \mathbb{Z}$ und $0 \leq r < m$. Da k und m in U sind, folgt $r \in U$. Wegen der Minimalität von m ergibt sich $r = 0$, also $k = qm \in \langle m \rangle$ und damit $U = \langle m \rangle$. □

Proposition 2.3.5 *Sei $(A, +)$ eine zyklische Gruppe mit Erzeuger $a \in A$.*

(1) Hat a unendliche Ordnung, so gilt $A \cong \mathbb{Z}$.

(2) Hat a endliche Ordnung m, so gilt $A \cong \mathbb{Z}/m$.

Beweis: Wir haben einen Homomorphismus $\mu_a : \mathbb{Z} \to A$, $n \mapsto na$. Nach dem Homomorphiesatz gilt

$$\mathbb{Z}/\ker(\mu_a) \cong \mathrm{im}(\mu_a) = \langle a \rangle = A.$$

Nach dem vorigen Lemma kann die Untergruppe $U := \ker(\mu_a)$ von $\mathbb{Z}$ nur $\{0\}$ oder $m\mathbb{Z}$ sein. Daraus folgt die Behauptung. □

Definition 2.3.6 *Sei A eine abelsche Gruppe. A heißt* endlich erzeugt, *wenn es (endlich viele) Elemente $a_1, \ldots, a_k \in A$ gibt, die zusammen A erzeugen, d.h. für die gilt*

$$\langle a_1, \ldots, a_k \rangle = A.$$

Beispiele

(1) Jede endliche abelsche Gruppe A ist endlich erzeugt.

(2) $\mathbb{Z}^r := \underbrace{\mathbb{Z} \times \mathbb{Z} \times \ldots \mathbb{Z}}_{r \text{ Faktoren}}$ ist endlich erzeugt, nämlich von den r Einheitsvektoren in $\mathbb{Z}^r$.

(3) $\mathbb{Q}$ und $\mathbb{Q}/\mathbb{Z}$ sind nicht endlich erzeugt.

(4) $A_1 \times \ldots \times A_k$ ist endlich erzeugt, wenn $A_1, \ldots, A_k$ zyklische Gruppen sind.

Satz 2.3.7 *Sei A eine endlich erzeugte abelsche Gruppe. Dann gibt es (endlich viele) zyklische Gruppen $A_1, \ldots, A_k$ mit*

$$A \cong A_1 \times \ldots \times A_k.$$

Beweis: Sei k die kleinste natürliche Zahl, für die es $a_1, \ldots, a_k \in A$ gibt, die zusammen A erzeugen. Wir betrachten alle Relationen der Form

$$n_1 a_1 + \ldots + n_k a_k = 0,$$

wobei die $n_1, \ldots, n_k$ ganze Zahlen sind und die $a_1, \ldots, a_k$ zusammen A erzeugen. Wir unterscheiden zwei Fälle:

1. Fall: Tritt dabei kein $n_i > 0$ auf, dann auch nie ein $n_i < 0$. Also ist

$$\mathbb{Z}^k \to A, \quad (n_1, \ldots, n_k) \mapsto n_1 a_1 + \ldots + n_k a_k$$

ein injektiver Homomorphismus für alle $a_1, \ldots, a_k$, die A erzeugen. Da der Homomorphismus auch surjektiv ist, folgt $A \cong \mathbb{Z}^k$.

2. Fall: Ansonsten sei n^* die kleinste positive Zahl, die dabei unter den $n_1, \ldots, n_k$ vorkommt, und seien $a_1, \ldots, a_k$ die zugehörigen Erzeuger. Wir nummerieren so, dass $n^* = n_1$ ist, also

$$n^* a_1 + n_2 a_2 + \ldots + n_k a_k = 0.$$

Wir zeigen nun, dass $n^* | n_i$ für alle $i > 1$ gilt:

Angenommen, $n^* \not| n_2$, also $n_2 = qn^* + r$ mit $q \in \mathbb{Z}$ und $0 < r < n^*$. Dann erzeugen auch $a_1' := a_1 + qa_2, a_2, a_3, \ldots, a_k$ zusammen A, und es gilt die Relation

$$n^* a_1' + ra_2 + n_3 a_3 + \ldots + n_k a_k = 0$$

wegen $n^* a_1' + ra_2 = n^* a_1 + n^* q a_2 + ra_2 = n^* a_1 + n_2 a_2$. Dies ist ein Widerspruch zur Minimalität von n^*. Das zeigt $n^* | n_2$. Genauso zeigen wir $n^* | n_3, \ldots, n_k$.

Wir ersetzen jetzt a_1 durch

$$a_1^* := a_1 + \frac{n_2}{n^*} a_2 + \frac{n_3}{n^*} a_3 + \ldots + \frac{n_k}{n^*} a_k.$$

Nach Konstruktion gilt $n^* a_1^* = 0$. Außerdem gilt

$$n a_1^* \notin \langle a_2, \ldots, a_k \rangle$$

für alle n mit $0 < n < n^*$ (wegen der Minimalität von n^*). Daraus folgt

$$\langle a_1^* \rangle \cap \langle a_2, \ldots, a_k \rangle = \{0\}.$$

Deswegen ist der Homomorphismus

$$\begin{aligned} \langle a_1^* \rangle \times \langle a_2, \ldots, a_k \rangle &\to A \\ (na_1, a) &\mapsto na_1 + a \end{aligned}$$

injektiv. Er ist auch surjektiv, da $a_1^*, a_2, \ldots, a_k$ zusammen A erzeugen. Es folgt

$$A \cong \langle a_1^* \rangle \times \langle a_2, \ldots, a_k \rangle.$$

Wir beweisen die Behauptung nun durch Induktion über k. Induktionsanfang: Für $k = 1$ ist A selbst zyklisch. Induktionsschritt von $k-1$ nach k. Nach Induktionsvoraussetzung ist $\langle a_2, \ldots, a_k \rangle$ Produkt zyklischer Gruppen, also ist auch $A \cong \langle a_1^* \rangle \times \langle a_2, \ldots, a_k \rangle$ Produkt zyklischer Gruppen. □

Satz 2.3.8 (Struktursatz) *Sei A eine endlich erzeugte abelsche Gruppe.*

i) Es gibt $r, s \geq 0$ mit

$$A \cong \mathbb{Z}^r \times \mathbb{Z}/q_1 \times \ldots \times \mathbb{Z}/q_s,$$

dabei sind $q_1 = p_1^{e_1}, \ldots, q_s = p_s^{e_s}$ (nicht notwendig verschiedene) Primzahlpotenzen.

ii) Die Zahlen r, s und $q_1, \ldots, q_s$ sind durch A eindeutig (bis auf die Reihenfolge von $q_1, \ldots, q_s$) bestimmt.

Beweis: i) Nach dem vorigen Satz ist A isomorph zu einem Produkt zyklischer Gruppen. Wir dürfen also annehmen, dass A zyklisch ist. Wenn $A \cong \mathbb{Z}$, dann gilt i) mit $r = 1$, $s = 0$. Sei also $A \cong \mathbb{Z}/m$. Wir haben eine Primfaktorzerlegung

$$m = q_1 \cdot \ldots \cdot q_s,$$

wobei $q_1 = p_1^{e_1}, \ldots, q_s = p_s^{e_s}$ mit paarweise verschiedenen Primzahlen $p_1, \ldots, p_s$ ist. Nach dem Chinesischen Restsatz gilt

$$\mathbb{Z}/m \cong \mathbb{Z}/q_1 \times \ldots \times \mathbb{Z}/q_s.$$

Also gilt i) hier mit $r = 0$.

ii) Sei p eine feste Primzahl. Für $e \in \mathbb{N}$ gebe $r(e)$ an, wie oft p^e vorkommt in $q_1, \ldots, q_s$. Es ist zu zeigen, dass r sowie $r(1), r(2), \ldots$ durch A eindeutig bestimmt sind. Für wieviele $a \in A$ gilt $p^e a = 0$?

- Nur für $a = 0$, falls $A \cong \mathbb{Z}$ oder $A \cong \mathbb{Z}/m$ mit $p \not| m$ ist.
- Für alle $a \in A$, falls $A \cong \mathbb{Z}/p^f$ mit $f \leq e$ ist.
- Die Anzahl ist p^e, falls $A \cong \mathbb{Z}/p^f$ mit $f \geq e$ ist.

Also gilt im Allgemeinen: Die Anzahl der $a \in A$ mit $p^e a = 0$ ist

$$p^{r(1)} \cdot p^{2r(2)} \cdot \ldots \cdot p^{er(e)} \cdot p^{er(e+1)} \cdot p^{er(e+2)} \cdot \ldots$$

Daher ist für alle e die Zahl

$$n(e) := r(1) + 2r(2) + \ldots + er(e) + er(e+1) + \ldots$$

eindeutig bestimmt durch A. Folglich sind auch

$$n(e) - n(e-1) = r(e) + r(e+1) + r(e+2) + \ldots$$

und

$$r(e) = (n(e) - n(e-1)) - (n(e+1) - n(e))$$

eindeutig bestimmt. Das zeigt die Eindeutigkeit von $s, q_1, \ldots, q_s$.

Zu r: Finde eine natürliche Zahl n mit

$$\mathrm{ggT}(n, q_1) = \ldots = \mathrm{ggT}(n, q_s) = 1.$$

Welche Ordnung hat A/nA?

- $|A/nA| = n$, falls $A \cong \mathbb{Z}$ ist.
- $nA = A$, falls $A \cong \mathbb{Z}/q$ mit $\mathrm{ggT}(n, q) = 1$ ist.

Also im Allgemeinen:

$$|A/nA| = n^r.$$

Folglich ist r eindeutig. □

Beispiel Sei $A = (\mathbb{Z}/15)^*$. Es ist $|A| = \varphi(15) = 8$. Nach dem Struktursatz ist A isomorph zu

$$\mathbb{Z}/8,\ \mathbb{Z}/4 \times \mathbb{Z}/2 \quad \text{oder} \quad \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2.$$

$(\mathbb{Z}/15)^*$ hat 3 Elemente der Ordnung 2 und 4 Elemente der Ordnung 4. Folglich ist

$$(\mathbb{Z}/15)^* \cong \mathbb{Z}/4 \times \mathbb{Z}/2.$$

2.4 Polynome

Definition 2.4.1 *Ein* Ring $R = (R, +, \cdot)$ *(kommutativ, mit Eins) besteht aus einer abelschen Gruppe* $(R, +)$ *und einer weiteren Abbildung*

$$\cdot : R \times R \to R \quad , \quad (a, b) \mapsto a \cdot b =: ab$$

mit folgenden Eigenschaften:

(1) Kommutativität: $a \cdot b = b \cdot a$ *für alle* $a, b \in R$.

(2) Assoziativität: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ *für alle* $a, b, c \in R$.

(3) Einselement: Es gibt ein $1 \in R$*, so dass*

$$1 \cdot a = a \qquad \text{für alle } a \in R \text{ gilt.}$$

(4) Distributivität: $(a + b) \cdot c = a \cdot c + b \cdot c$ *für alle* $a, b, c \in R$.

Beispiele für Ringe $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \{0\}$ und $\mathbb{Z}/m$ mit $m \in \mathbb{N}$.

Definition 2.4.2 *Ein Element* a *eines Ringes* R *heißt* Einheit*, falls es ein* $b \in R$ *gibt mit* $ab = 1$. $R^* \subseteq R$ *bezeichnet die Menge aller Einheiten.*

Notiz 2.4.3 *Ist* $(R, +, \cdot)$ *ein Ring, so ist* $(R^*, \cdot)$ *eine abelsche Gruppe.*

Beweis: Wir brauchen eine Abbildung $\cdot : R^* \times R^* \to R^*$. Seien also $a, a' \in R^*$. Es ist zu zeigen, dass $a \cdot a' \in R^*$ ist. Da a, a' Einheiten sind, gibt es $b, b' \in R$ mit $ab = 1 = a'b'$. Damit folgt

$$(aa')(bb') = (ab)(a'b') = 1 \cdot 1 = 1,$$

also $a \cdot a' \in R^*$ wie benötigt.
Wir haben jetzt $\cdot : R^* \times R^* \to R^*$. Die Multiplikation ist kommutativ und assoziativ, da R ein Ring ist. $1 \in R$ liegt in R^* und ist dort neutral bzgl. Multiplikation. Nach Definition von R^* hat jedes Element ein inverses bzgl. Multiplikation. □

Beispiele

(1) Für $R = \mathbb{Z}$ ist $R^* = \{-1, 1\}$.

(2) Für $R = \mathbb{Z}/m$ ist $R^* = (\mathbb{Z}/m)^*$.

Definition 2.4.4 *Ein* Körper *ist ein Ring $K = (K, +, \cdot)$, für den $K^* = K \setminus \{0\}$ gilt. D.h. zu jedem $a \in K$ mit $a \neq 0$ gibt es ein $b \in K$ mit $ab = 1$.*

Insbesondere ist jeder Körper K nullteilerfrei, d.h. für $a, b \in K$ mit $a \neq 0 \neq b$ gilt auch $ab \neq 0$.

Beispiele für Körper $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ und $\mathbb{Z}/p$ mit p Primzahl.

Definition 2.4.5 *Ein* Polynom *über einem Ring R ist eine Folge*

$$f = (a_0, a_1, a_2, \ldots) = (a_n)_{n \geq 0}$$

von Elementen $a_n \in R$, zu der es ein $N \in \mathbb{N}$ gibt mit $a_n = 0$ für alle $n > N$. Wir schreiben

$$f = \sum_{n \geq 0} a_n x^n = a_0 + a_1 x + a_2 x^2 + \ldots + a_N x^N.$$

$R[x]$ bezeichnet die Menge aller Polynome über R.

Definition 2.4.6 *Seien R ein Ring sowie*

$$f = \sum_{n \geq 0} a_n x^n \quad \textit{und} \quad g = \sum_{n \geq 0} b_n x^n$$

zwei Polynome über R. Dann sind die Polynome $f + g$ und $f \cdot g$ definiert durch

$$f + g := \sum_{n \geq 0} (a_n + b_n) x^n$$

und

$$f \cdot g := \sum_{n \geq 0} \left(\sum_{k+l=n} a_k b_l \right) x^n.$$

Proposition 2.4.7 *Für jeden Ring R ist die Menge $R[x]$ zusammen mit*

$$+, \cdot : R[x] \times R[x] \to R[x]$$

wieder ein Ring, der Polynomring *über R.*

Beweis: $(R[x], +)$ ist eine abelsche Gruppe mit neutralem Element $0 = (0, 0, \ldots)$. Die Multiplikation ist kommutativ, und $1 = (1, 0, 0, \ldots) \in R$ ist Einselement. Wir rechnen nun die Distributivität und Assoziativität der Multiplikation nach. Seien

$$f = \sum_{n \geq 0} a_n x^n, g = \sum_{n \geq 0} b_n x^n \text{ und } h = \sum_{n \geq 0} c_n x^n$$

drei Polynome über R. Dann gilt

$$(f+g)h = \sum_{n \geq 0} \left(\sum_{k+l=n} (a_k + b_k) c_l \right) x^n = fh + gh$$

und

$$(fg)h = \sum_{n \geq 0} \left(\sum_{k+l+m=n} a_k b_l c_m \right) x^n = f(gh).$$

□

Definition 2.4.8 (Einsetzen) *Sei $f = a_0 + a_1 x + \ldots + a_N x^N$ ein Polynom über dem Ring R und $a \in R$.*

i) Der Wert von f an der Stelle a *ist*

$$f(a) := a_0 + a_1 a + \ldots + a_N a^N \in R.$$

ii) a heißt Nullstelle von f, *wenn $f(a) = 0$.*

Notiz 2.4.9 *Für alle $f, g \in R[x], a \in R$ gilt:*

$$\begin{aligned} (f+g)(a) &= f(a) + g(a) \quad \textit{und} \\ (f \cdot g)(a) &= f(a) \cdot g(a). \end{aligned}$$

Definition 2.4.10 *Sei $f = a_0 + a_1 x + \ldots + a_N x^N$ ein Polynom über dem Ring R mit $f \neq 0$.*

i) Der Grad *von f ist*

$$\deg(f) := \max\{n : a_n \neq 0\}.$$

ii) Der Leitkoeffizient *von f ist $a_{\deg(f)} \in R$.*

iii) f heißt normiert, *falls $a_{\deg(f)} = 1$ ist.*

Lemma 2.4.11 (Polynomdivision) *Seien $f, g \in R[x]$, dabei sei g normiert. Dann gibt es eindeutig bestimmte Polynome $q, r \in R[x]$ mit*

$$f = qg + r \quad \textit{und} \quad \deg(r) < \deg(g) \textit{ oder } r = 0.$$

Beweis: Wir zeigen die Existenz durch Induktion über $\deg(f)$.
Induktionsanfang: Wenn $\deg(f) < \deg(g)$ ist, dann ist die Behauptung mit $q = 0$ und $r = f$ erfüllt.
Induktionsschritt: Sei $n := \deg(f) \geq \deg(g)$, und sei a der Leitkoeffizient von f. Dann folgt, dass $f_1 := f - ax^{n-\deg(g)} \cdot g$ Grad $\leq n-1$ hat. Nach Induktionsvoraussetzung gibt es $q_1, r \in R[x]$, $\deg(r) < \deg(g)$ oder $r = 0$, mit

$$f_1 = q_1 g + r.$$

Es folgt $f = qg + r$ mit $q := q_1 + ax^{n-\deg(g)}$.

Eindeutigkeit: Angenommen, es gilt $qg + r = f = q'g + r'$ mit $q \neq q'$. Dann folgt

$$\deg(r - r') = \deg(q'g - qg) = \deg(q' - q) + \deg(g) \geq \deg(g),$$

also können r und r' nicht beide Grad kleiner $\deg(g)$ haben oder Null sein. □

Beispiel Für $R = \mathbb{Z}$, $f = 2x^3 + x^2 - x - 1$ und $g = x^2 + 1$ folgt $q = 2x + 1$ und $r = -3x - 2$.

Folgerung 2.4.12 *Sei $a \in R$ eine Nullstelle des Polynoms $f \in R[x]$. Dann gibt es ein Polynom $q \in R[x]$ mit*

$$f = q \cdot (x - a).$$

Beweis: Polynomdivision liefert $q, r \in R[x]$ mit

$$f = q(x - a) + r$$

und $\deg(r) = 0$ oder $r = 0$. So oder so ist $r = a_0 \in R$ ein konstantes Polynom. Einsetzen von $x = a$ ergibt

$$0 = f(a) = q(a) \cdot 0 + r(a) = 0 + a_0,$$

also ist $a_0 = 0$ und r das Nullpolynom. □

Satz 2.4.13 *Sei K ein Körper (allgemeier: ein nullteilerfreier Ring), und sei $0 \neq f \in R[x]$ Polynom vom Grad n. Dann hat f höchstens n verschiedene Nullstellen in K.*

Beweis: Induktion über $n := \deg(f)$. Induktionsanfang für $n = 0$. Hier ist $f = a_0 \in R$ ein konstantes Polynom. Da nach Voraussetzung $a_0 \neq 0$ ist, hat f keine Nullstellen.
Induktionschritt von n auf $n+1$. Sei $\deg(f) = n+1$. Angenommen es gibt ein $a \in K$ mit $f(a) = 0$. Dann folgt

$$f = (x - a) \cdot q,$$

wobei $q \in R[x]$ mit $\deg(q) = n$ ist. Da K nullteilerfrei ist, gilt $f(b) = 0$ nur dann, wenn $b = a$ oder $q(b) = 0$ ist. Nach Induktionsvoraussetzung hat q höchstens n Nullstellen, also hat f höchstens $n + 1$ Nullstellen. □

2.5 Struktur der abelschen Gruppen $(\mathbb{Z}/m)^*$

Satz 2.5.1 *Sei $(K,+,\cdot)$ ein endlicher Körper. Dann ist $(K^*,\cdot)$ eine zyklische Gruppe . Insbesondere ist $(\mathbb{Z}/p)^*$ zyklisch für jede Primzahl p.*

Beweis: Der Struktursatz 2.3.8 besagt, dass

$$K^* \cong \mathbb{Z}/q_1 \times \ldots \times \mathbb{Z}/q_s$$

ist, wobei $q_1, \ldots, q_s$ Primzahlpotenzen sind.

Wir zeigen nun, dass $\mathrm{ggT}(q_1, q_2) = 1$ ist. Angenommen es gibt eine Primzahl p, die q_1 und q_2 teilt. Dann ist die Ordnung der p^2 Elemente

$$([kq_1/p], [lq_2/p], 0, \ldots, 0) \in \mathbb{Z}/q_1 \times \ldots \times \mathbb{Z}/q_s$$

mit $k, l \in \{0, 1, \ldots, p-1\}$ jeweils ein Teiler von p. Aber in K^* gibt es höchstens p Elemente, deren Ordnung p teilt, denn $x^p - 1 \in K[x]$ hat höchstens p Nullstellen. Dies ist ein Widerspruch, deshalb gilt $\mathrm{ggT}(q_1, q_2) = 1$. Genauso folgt $\mathrm{ggT}(q_i, q_j) = 1$ für alle $i \neq j$. Nach dem Chinesischen Restsatz gilt daher $K^* \cong \mathbb{Z}/q_1 \cdot \ldots \cdot q_s$. □

Satz 2.5.2

i) Für alle $e \geq 3$ gilt $(\mathbb{Z}/2^e)^* \cong \mathbb{Z}/2^{e-2} \times \mathbb{Z}/2$.

ii) Ist $p > 2$ eine Primzahl und $e \in \mathbb{N}$, so ist die abelsche Gruppe $(\mathbb{Z}/p^e)^*$ zyklisch.

Beweis: i) Es ist $\varphi(2^e) = 2^{e-1}$. Nach dem Struktursatz 2.3.8 gilt

$$(\mathbb{Z}/2^e)^* \cong \mathbb{Z}/2^{n_1} \times \ldots \times \mathbb{Z}/2^{n_s}$$

mit $n_1 + \ldots + n_s = e - 1$.

Wir zeigen nun, dass $5^{2^n} \equiv 1 + 2^{n+2} \bmod 2^{n+3}$ für alle $n \geq 0$ gilt durch Induktion über n.

Der Induktionsanfang für $n = 0$ ist klar. Induktionsschritt von $n-1$ auf n. Nach Induktionsvoraussetzung gibt es ein $k \in \mathbb{Z}$ mit

$$5^{2^{n-1}} = 1 + 2^{n+1}(1 + 2k).$$

Quadrieren liefert

$$\begin{aligned} 5^{2^n} &= 1 + 2 \cdot 2^{n+1}(1+2k) + 2^{2n+2}(1+2k)^2 \\ &\equiv 1 + 2^{n+2} \bmod 2^{n+3}. \end{aligned}$$

Also hat $[5] \in (\mathbb{Z}/2^e)^*$ die Ordnung 2^{e-2}. Damit folgt

$$(\mathbb{Z}/2^e)^* \cong \mathbb{Z}/2^{e-1} \text{ oder } \mathbb{Z}/2^{e-2} \times \mathbb{Z}/2.$$

Aber $(\mathbb{Z}/2^e)^*$ ist nicht zyklisch, da die Elemente

$$[-1], [2^{e-1} \pm 1] \in (\mathbb{Z}/2^e)^*$$

alle Ordnung zwei haben.

ii) Es ist $\varphi(p^e) = (p-1)p^{e-1}$. Nach dem Struktursatz 2.3.8 gilt

$$(\mathbb{Z}/p^e)^* \cong A_1 \times A_2$$

mit $|A_1| = p-1$ und $|A_2| = p^{e-1}$.

Wir zeigen nun, dass $(1+p)^{p^n} \equiv 1 + p^{n+1} \bmod p^{n+2}$ für alle $n \geq 0$ gilt durch Induktion über n. Der Beweis ist analog zu dem in i).

Also hat $[1+p] \in (\mathbb{Z}/p^e)^*$ die Ordnung p^{e-1}. Damit folgt

$$A_2 \cong \mathbb{Z}/p^{e-1}.$$

Laut Satz 2.5.1 gibt es ein $a \in \mathbb{Z}$, so dass $[a] \in (\mathbb{Z}/p)^*$ die Ordnung $p-1$ hat. Also hat $[a] \in (\mathbb{Z}/p^e)^*$ die Ordnung $(p-1)k$ mit $k \in \mathbb{N}$. Folglich hat $[a^k] \in (\mathbb{Z}/p^e)^*$ die Ordnung $p-1$. Es folgt

$$A_1 \cong \mathbb{Z}/p-1,$$

also zusammen

$$(\mathbb{Z}/p^e)^* \cong \mathbb{Z}/p-1 \times \mathbb{Z}/p^{e-1} \cong \mathbb{Z}/(p-1)p^{e-1}.$$

□

Korollar 2.5.3 *Gegeben sei $m \in \mathbb{N}$. Sei*

$$m = 2^e \cdot p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$$

die Primfaktorzerlegung von m, dabei sind $r, e \geq 0$, $2 < p_1 < \ldots < p_r$ Primzahlen und $e_1, \ldots, e_r \geq 1$. Dann gilt

$$(\mathbb{Z}/m)^* \cong \begin{cases} \mathbb{Z}/(p_1-1)p_1^{e_1-1} \times \ldots \times \mathbb{Z}/(p_r-1)p_r^{e_r-1} & \text{falls } e \leq 1, \\ \mathbb{Z}/(p_1-1)p_1^{e_1-1} \times \ldots \times \mathbb{Z}/(p_r-1)p_r^{e_r-1} \times \mathbb{Z}/2 & \text{falls } e = 2, \\ \mathbb{Z}/(p_1-1)p_1^{e_1-1} \times \ldots \times \mathbb{Z}/(p_r-1)p_r^{e_r-1} \times \mathbb{Z}/2 \times \mathbb{Z}/2^{e-2} & \text{falls } e \geq 3. \end{cases}$$

Aufgaben

(1) (a) Es sei $f : \mathbb{Z}/8 \longrightarrow \mathbb{Z}/3$ ein Homomorphismus. Zeige, dass f die Nullabbildung ist, also $\ker(f) = \mathbb{Z}/8$.

(b) Gib einen Homomorphismus $f : \mathbb{Z}/8 \longrightarrow \mathbb{Z}/6$ an, der nicht die Nullabbildung ist.

(c) Berechne Kern und Bild für den in (b) angegebenen Homomorphismus.

(2) Es seien a und b zwei ganze Zahlen.

(a) Zeige, dass $a\mathbb{Z} + b\mathbb{Z} = \{ax + by,\ x, y \in \mathbb{Z}\}$ eine Untergruppe von $(\mathbb{Z}, +)$ ist.

(b) Zeige, dass $\alpha = 3a+4b$ und $\beta = 2a+3b$ zusammen die Untergruppe $a\mathbb{Z}+b\mathbb{Z}$ erzeugen.

(3) Es sei $f : A \longrightarrow B$ ein Homomorphismus abelscher Gruppen.

(a) Ist U eine Untergruppe von A, so ist $f(U)$ eine Untergruppe von B.

(b) Ist V eine Untergruppe von B, so ist $f^{-1}(V)$ eine Untergruppe von A.

(c) Es sei V eine Untergruppe von B. Zeige, dass die Abbildung

$$g : A/f^{-1}(V) \longrightarrow B/V, [a] \mapsto [f(a)]$$

wohldefiniert und ein injektiver Homomorphismus ist.

(4) (a) Beweise, dass die Betragsfunktion

$$|\cdot| : \mathbb{C}\backslash\{0\} \longrightarrow \mathbb{R}\backslash\{0\}, x + iy \mapsto |x + iy| = \sqrt{x^2 + y^2}$$

ein Homomorphismus abelscher Gruppen ist.

(b) Bestimme Kern und Bild der Betragsfunktion.

(c) Zeige: Sind die ganzen Zahlen a und b jeweils Summe zweier Quadrate ganzer Zahlen, so ist auch ihr Produkt ab Summe zweier Quadrate ganzer Zahlen.

(5) (a) Zeige $|(\mathbb{Z}/7)^*| = |(\mathbb{Z}/9)^*|$ und $|(\mathbb{Z}/5)^*| = |(\mathbb{Z}/8)^*|$.

(b) Beweise $(\mathbb{Z}/7)^* \cong (\mathbb{Z}/9)^*$ und finde einen Isomorphismus zwischen diesen beiden abelschen Gruppen.

(c) Zeige $(\mathbb{Z}/5)^* \ncong (\mathbb{Z}/8)^*$.

(6) Zerlege $(\mathbb{Z}/144)^*$ und $(\mathbb{Z}/91)^*$ jeweils in ein Produkt zyklischer Gruppen von Primzahlpotenzordnung.

(7) Es sei $A = \mathbb{Z}/4 \times \mathbb{Z}/4 \times \mathbb{Z}/3 \times \mathbb{Z}/9$.

(a) Welche Ordnung kann ein Element aus A haben?

(b) Für jede natürliche Zahl m gib die Anzahl der Elemente in A an, welche die Ordnung m haben.

(8) (a) Welches sind die Einheiten von $\mathbb{Z}/2[x]$?

(b) Welches sind die Einheiten von $\mathbb{Z}/6[x]$?

(c) Welches sind die Einheiten von $\mathbb{Z}/4[x]$?

(9) Finde Polynome f, g in $\mathbb{Z}[x]$ mit $(x^2 + x + 1)\cdot f + (2x^2 + 3x + 2)\cdot g = 1$.

3 Endliche Körper und ElGamal-Verfahren

3.1 Diskrete Logarithmen

Sei $K = (K, +, \cdot)$ ein endlicher Körper und $q = |K|$ (z.B. $K = \mathbb{Z}/p$ für eine Primzahl p und $q = p$). Dann ist $(K^* = K \setminus \{0\}, \cdot)$ eine endliche abelsche Gruppe der Ordnung $q - 1$ und nach Satz 2.5.1 auch zyklisch.

Definition 3.1.1 *Sei $g \in K^*$ ein Erzeuger der zyklischen Gruppe K^*, und sei $k \in K^*$ beliebig. Eine ganze Zahl n heißt* diskreter Logarithmus *von k zur Basis g, falls $g^n = k$ gilt.*

Lemma 3.1.2 *Sei K ein endlicher Körper mit q Elementen, g ein Erzeuger der abelschen Gruppe K^* und $k \in K^*$ beliebig.*

i) Es gibt einen diskreten Logarithmus $n \in \mathbb{Z}$ von k zur Basis g.

ii) n ist eindeutig bestimmt bis auf Vielfache von $q - 1$.

Beweis: i) Dies folgt daraus, dass g Erzeuger von K^* ist.
ii) Seien $n, n' \in \mathbb{Z}$ beide diskrete Logarithmen von k. Dann gilt

$$g^{n'-n} = k \cdot k^{-1} = 1,$$

also ist $n' - n$ durch die Ordnung von g in K^* teilbar. K^* wird von g erzeugt, also ist die Ordnung von g gleich $|K^*| = q - 1$. □

Problem des diskreten Logarithmus Es seien gebeben ein endlicher Körper K, ein Erzeuger $g \in K^*$ und ein $k \in K^*$. Die Berechnung eines diskreten Logarithmus n von k zur Basis g ist sehr aufwendig, wenn $q = |K|$ groß ist. Es sind keine effizienten Algorithmen bekannt, z.B. ist die Berechnung ab einer Großenordnung von $q \approx 2^{1000}$ mit heutigen Verfahren und Computern unmöglich.

3.2 Diffie-Hellman-Schlüsselvereinbarung

Alice und Bob wollen verschlüsselte Nachrichten austauschen und dafür ein symmetrisches Verschlüsselungsverfahren benutzen (z.B. multiplikative Chiffre). Wir haben bereits gesehen, dass bei solchen Verfahren der Austausch und die Geheimhaltung vom Schlüssel ein Problem darstellen. Jetzt wollen wir uns einem Verfahren zuwenden, mit dem man dieses Problem in den Griff bekommen kann.

Wir nehmen an, der Schlüsselraum sei $\mathcal{K} = K^*$, wobei K ein endlicher Körper mit q Elementen ist. Folgendes Verfahren nennt man Schlüsselvereinbarung nach Diffie und Hellman (1976) :

Alice und Bob einigen sich auf einen Erzeuger $g \in K^*$ (der nicht geheim sein muss).

Alice wählt eine Zufallszahl $n_A \in \mathbb{N}$, $n_A < q-1$ und berechnet $k_A := g^{n_A} \in K^*$. Dieses k_A sendet sie an Bob. Bob wählt ebenfalls Zufallszahl eine $n_B \in \mathbb{N}$, $n_B < q-1$, berechnet $k_B := g^{n_B} \in K^*$ und sendet k_B an Alice. Dann können beide $k := g^{n_A n_B} \in K^*$ berechnen, nämlich Alice durch $k = k_B^{n_A}$ und Bob durch $k = k_A^{n_B}$. Dieses $k \in K^* = \mathcal{K}$ können Alice und Bob als Schlüssel benutzen.

Warum ist dieses Vefahren sicher? Angenommen ein Angreifer kennt K, g und hört k_A sowie k_B ab. Dann steht er vor dem sogenannten Diffie-Hellman-Problem, wenn er k bestimmen möchte. Es lautet:

Es seien gegeben ein endlichen Körper K, ein Erzeuger $g \in K^*$ und zwei Elemente $k_A = g^{n_A}, k_B = g^{n_B} \in K^*$. Berechne $k = g^{n_A n_B} \in K^*$.

Wer diskrete Logarithmen berechnen kann, kann das Diffie-Hellman-Problem lösen. Wenn der Angreifer den diskreten Logarithmus n_A von k_A berechnen kann, kann er auch $k = k_B^{n_A}$ berechnen. Analog: Wenn er n_B berechnen kann, so kann er auch $k = k_A^{n_B}$ berechnen. Neben den diskreten Logarithmen sind keine anderen Verfahren bekannt, das Diffie-Hellman-Problem zu lösen. Wenn $q = |K|$ also groß genug ist, kann niemand die diskreten Logarithmen von k_A, k_B berechnen, und daher kann auch niemand den Schlüssel k berechnen.

3.3 Das ElGamal-Verfahren

Bei dem Verschlüsselungsverfahren, das auf ElGamal (1985) zurückgeht, handelt es sich um ein public-key-Verfahren. Seien Klartext- und Chiffretextalphabet $\mathcal{P} = \mathcal{C} = K^*$, dabei sei K ein endlicher Körper mit q Elementen. Um eine angemessene Sicherheit zu erreichen, muss q groß gewählt werden (z.B. $q \approx 2^{1000}$). Dann läuft das ElGamal-Verfahren nach folgendem Muster ab:

Schlüsselerzeugung: Bob wählt einen Erzeuger g von K^* und erzeugt eine Zufallszahl $n_B \in \mathbb{N}$ mit $n_B < q-1$. Zudem berechnet er $k_B := g^{n_B} \in K^*$. Dann ist (g, k_B) Bobs öffentlicher und n_B Bobs geheimer Schlüssel.

Verschlüsselung: Alice erzeugt eine Zufallszahl $n_A \in \mathbb{N}$, $n_A < q-1$ und berechnet $k_A := g^{n_A}$ sowie $k := k_B^{n_A}$. Sie verschlüsselt ihre Nachricht an Bob durch

$$E : K^* \to K^* \quad , \quad a \mapsto k \cdot a$$

und sendet erst k_A und dann die verschlüsselte Nachricht an Bob.

Entschlüsselung: Bob berechnet $k = k_A^{n_B}$ und entschlüsselt dann durch

$$D : K^* \to K^* \quad , \quad b \mapsto k^{-1} \cdot b.$$

Die Sicherheit dieses Verfahrens beruht wieder auf der praktischen Unlösbarkeit des Diffie-Hellman-Problems. Angenommen ein Angreifer kennt K, g, k_B und hört k_A ab.

Zum Entschlüsseln braucht er k, d.h. er müsste das Diffie-Hellman–Problem lösen, was er wegen des groß gewählten q jedoch nicht kann.

3.4 Konstruktion von Körpern

Gegeben sei ein Körper K, z.B. $K = \mathbb{Z}/p$ mit einer Primzahl p. Wir wollen aus K weitere Körper konstruieren.

Definition 3.4.1 *Sei $f \in K[x]$ ein normiertes Polynom.*

i) $K[x]/f$ bezeichnet die Faktorgruppe der abelschen Gruppe $(K[x], +)$ nach der Untergruppe

$$f \cdot K[x] := \{f \cdot k : k \in K[x]\} \subseteq K[x].$$

ii) Die Elemente von $K[x]/f$ heißen Restklassen modulo f.

Lemma 3.4.2 *Die abelsche Gruppe $(K[x]/f, +)$ zusammen mit der Abbildung*

$$\begin{aligned} \cdot : K[x]/f \times K[x]/f &\to K[x]/f, \\ ([g],[h]) &\mapsto [g \cdot h] \end{aligned}$$

ist ein Ring.

Beweis: Wohldefiniertheit von $\cdot$: Angenommen für $g_1, g_2, h_1, h_2 \in K[x]$ gilt $[g_1] = [g_2]$ und $[h_1] = [h_2]$ in $K[x]/f$. Dann gibt es $k, l \in K[x]$ mit

$$g_2 - g_1 = f \cdot k \quad \text{und} \quad h_2 - h_1 = f \cdot l.$$

Damit folgt

$$\begin{aligned} g_2h_2 - g_1h_1 &= (g_2 - g_1)h_2 + g_1(h_2 - h_1) \\ &= f(kh_2 + g_1l) \in f \cdot K[x], \end{aligned}$$

also $[g_1h_1] = [g_2h_2]$, d.h. $\cdot$ ist wohldefiniert.

Ringaxiome: $\cdot$ ist kommutativ, assoziativ und distributiv, da $\cdot : K[x] \times K[x] \to K[x]$ es ist. $[1] \in K[x]/f$ ist neutral bzgl. $\cdot$, da $1 \in K[x]$ es ist. □

Definition 3.4.3 *Sei K ein Körper und $f \in K[x]$ ein normiertes Polynom. Der eben konstruierte Ring $(K[x]/f, +, \cdot)$ heißt* Restklassenring *modulo f.*

Lemma 3.4.4 *Sei $f \in K[x]$ ein normiertes Polynom vom Grad d. Dann ist die abelsche Gruppe $(K[x]/f, +)$ zusammen mit der Skalarmultiplikation*

$$\begin{aligned} \cdot : K \times K[x]/f &\to K[x]/f \\ (a, [\sum_n b_n x^n]) &\mapsto [\sum_n (ab_n)x^n] \end{aligned}$$

ein d-dimensionaler Vektorraum über dem Körper K.

Beweis: Wohldefiniertheit von "$\cdot$": Seien $g, h \in K[x]$ mit $[g] = [h]$ in $K[x]/f$, und sei $a \in K$. $[g] = [h]$ bedeutet, dass es ein $k \in K[x]$ gibt mit $h - g = kf$. Daraus folgt $ah - ag = (ak)f \in f \cdot K[x]$, d.h. $[ag] = [ah]$ in $K[x]/f$.

Die Vektorraumaxiome

- $1 \cdot [g] = g$ für $1 \in K$ und $[g] \in K[x]/f$,
- $a(b[g]) = (ab)[g]$ für alle $a, b \in K$ und $[g] \in K[x]/f$,
- $(a + b)[g] = a[g] + b[g]$ für alle $a, b \in K$ und $[g] \in K[x]/f$
- und $a([g] + [h]) = a[g] + a[h]$

folgen alle unmittelbar aus den Rechenregeln für Polynome. Also ist $K[x]/f$ Vektorraum über K.

Wir zeigen nun, dass $[1], [x], [x^2], \ldots, [x^{d-1}]$ eine Basis des K-Vektorraums $K[x]/f$ ist.

Lineare Unabhängigkeit: Seien $a_0, a_1, \ldots, a_{d-1} \in K$ mit $a_0[1]+a_1[x]+\ldots+a_{d-1}[x^{d-1}] = 0$. Dann ist $[a_0 + a_1 x + \ldots + a_{d-1}x^{d-1}] = 0$ in $K[x]/f$. Also ist $g := a_0 + a_1 x + \ldots + a_{d-1}x^{d-1} \in K[x]$ durch f teilbar. Wegen $\deg(g) < d = \deg(f)$ folgt aber $g = 0$, d.h. $a_0 = a_1 = \ldots = a_{d-1} = 0$. Also sind die $[1], [x], [x^2], \ldots, [x^{d-1}]$ linear unabhängig.

Sei $[g] \in K[x]/f$. Nach Polynomdivision gibt es Polynome $q, r \in K[x]$ mit $g = qf + r$ und $\deg(r) < \deg(f)$ oder $r = 0$. Folglich ist $[g] = [r]$ in $K[x]/f$ und $r = a_0 + a_1 x + \ldots + a_{d-1}x^{d-1}$ mit $a_0, a_1, \ldots, a_{d-1} \in K$. Also ist $[g] = [r] = a_0[1] + a_1[x] + \ldots + a_{d-1}[x^{d-1}]$. Somit spannen die $[1], [x], [x^2], \ldots, [x^{d-1}]$ den gesamten Vektorraum $K[x]/f$ auf.

Somit hat $K[x]/f$ die Dimension d. □

Korollar 3.4.5 *Ist K ein endlicher Körper mit q Elementen und $f \in K[x]$ normiert vom Grad d, so ist $K[x]/f$ ein endlicher Ring mit q^d Elementen.*

Bemerkung Die Voraussetzung, dass f normiert sein soll, ist nicht wichtig: Ist $f \neq 0$ nicht normiert, so können wir f ersetzen durch das normierte Polynom

$$f^{\text{normiert}} := a^{-1} f.$$

Dabei ist $a \in K$ der Leitkoeffizient von f. Für $f = 0$ setze $f^{\text{normiert}} := 0$.

Bemerkung Seien $f, g \in K[x]$. Dann wird g von f geteilt, genau dann wenn es ein $k \in K[x]$ gibt mit $g = f \cdot k$. Wir schreiben auch $f|g$ oder $g \in f \cdot K[x]$.

Definition 3.4.6 *Ein Polynom $f \in K[x]$ heißt* größter gemeinsamer Teiler (ggT) *zweier Polynomen $g, h \in K[x]$, falls gilt:*

i) f ist normiert.

ii) $f|g$ und $f|h$.

iii) f hat maximalen Grad unter allen Polynomen, für die i) und ii) gelten.

Behauptung Ein solcher ggT existiert und ist eindeutig bestimmt. *Beweis:* Existenz: Es gibt immer ein Polynom f, das i) und ii) erfüllt, z.B. $f = 1$. Wenn $g = h = 0$ sind, dann gibt es kein f, das auch iii) erfüllt. In dem Fall setzen wir $\mathrm{ggT}(0,0) := 0$. Sonst gilt für alle f mit i) und ii)

$$\deg(f) \leq \deg(g) \quad \text{bzw.} \quad \deg(f) \leq \deg(h).$$

Daher gibt es darunter ein f mit maximalem Grad, d.h. es gibt einen ggT von g und h.

Eindeutigkeit und Berechnung des ggT von g und h ergeben sich mit dem Euklidischen Algorithmus. Wir starten mit $g_1 := g^{\text{normiert}}$ und $h_1 := h^{\text{normiert}}$. Wenn $h_n = 0$ ist, dann bricht der Algorithmus ab mit dem Ergebnis g_n. Sonst liefert Polynomdivision $q_n, r_n \in K[x]$ mit

$$g_n = q_n \cdot h_n + r_n \quad \text{und} \quad \deg(r_n) < \deg(h_n).$$

Wir setzen dann $g_{n+1} := h_n$ und $h_{n+1} := r_n^{\text{normiert}}$. Der Beweis der Behauptung folgt nun mit dem folgenden Satz. □

Satz 3.4.7 *Seien $g, h \in K[x]$, und sei $d := \deg(h)$ (bzw. $d = -1$, wenn $h = 0$).*

i) Dieser Algorithmus bricht ab, und zwar im N-ten Schritt mit $N \leq d + 2$.

ii) g_N ist der einzige ggT von g und h.

Beweis: i) Aus $\deg(h_{n+1}) = \deg(r_n) \leq \deg(h_n) - 1$ folgt

$$\deg(h_n) \leq d + 1 - n \quad \text{solange } h_n \neq 0.$$

Also ist spätestens $h_{d+2} = 0$.

ii) Per Konstruktion ist

$$\{f : f|g_n \text{ und } f|h_n\} = \{f : f|h_n \text{ und } f|r_n\} = \{f : f|g_{n+1} \text{und} f|h_{n+1}\},$$

also

$$\{f : f|g \text{ und } f|h\} = \{f : f|g_N\}.$$

Unter diesen f gibt es genau ein normiertes mit maximalem Grad, nämlich $f = g_N$. □

Definition 3.4.8 *$g, h \in K[x]$ heißen* teilerfremd, *wenn* $\mathrm{ggT}(g,h) = 1$ *ist.*

Satz 3.4.9 *Wenn $g, h \in K[x]$ teilerfremd sind, dann gibt es Polynome $u, v \in K[x]$ mit*

$$u \cdot g + v \cdot h = 1.$$

Beweis: Wir verwenden den erweiterten Euklidischen Algorithmus. Seien g_n, h_n, q_n, r_n und N wie eben. Für $u_N = 1$ und $v_N = 0$ gilt

$$u_N g_N + v_N h_N = g_N = \mathrm{ggT}(g,h) = 1.$$

Angenommen, wir haben schon $u_{n+1}, v_{n+1} \in K[x]$ mit

$$u_{n+1} g_{n+1} + v_{n+1} h_{n+1} = 1.$$

Dann liefert Einsetzen von $g_{n+1} = h_n$ und $h_{n+1} = a_n^{-1} r_n = a_n^{-1}(g_n - q_n h_n)$, wobei a_n der Leitkoeffizient von r_n ist, eine Relation der Form

$$u_n g_n + v_n h_n = 1.$$

Schließlich finden wir so $u_1, v_1 \in K[x]$ mit

$$u_1 g_1 + v_1 h_1 = 1.$$

Einsetzen von $g_1 = g^{\mathrm{normiert}}$ und $h_1 = h^{\mathrm{normiert}}$ liefert schon die Behauptung. □

Definition 3.4.10 *Ein normiertes Polynom $f \in K[x]$ heißt* irreduzibel, *wenn* $\deg(f) > 0$ *ist und die einzigen Teiler von f die Polynome a und $a \cdot f$ mit $a \in K^*$ sind.*

Satz 3.4.11 *Sei K ein Körper, und sei $f \in K[x]$ ein irreduzibles normiertes Polynom. Dann ist der Ring*

$$R := K[x]/f$$

ein Körper.

Beweis: Sei $[g] \in R$, $[g] \neq 0$. Zu zeigen ist $[g] \in R^*$. Wir wählen einen Repräsentanten $g \in K[x]$ von $[g]$. Damit folgt

$$f \not| g.$$

Da f irreduzibel ist, folgt $\mathrm{ggT}(f,g) = 1$. Wegen Satz 3.4.9 gibt es also $u, v \in K[x]$ mit

$$uf + vg = 1.$$

Das heißt

$$[v][g] = 1 \quad \text{in} \quad K[x]/f.$$

Das zeigt $[g] \in R^*$. □

Korollar 3.4.12 *Sei p eine Primzahl, $K = \mathbb{Z}/p$ und $f \in K[x]$ ein irreduzibles normiertes Polynom vom Grad d. Dann ist $K[x]/f$ ein Körper mit p^d Elementen.*

3.5 Körpererweiterungen

Definition 3.5.1 *Seien R, S Ringe. Eine Abbildung $f : R \to S$ heißt* Ringhomomorphismus, *wenn gilt:*

$$\begin{aligned} f(1) &= 1, \\ f(a+b) &= f(a) + f(b) \quad \textit{und} \\ f(a \cdot b) &= f(a) \cdot f(b) \quad \textit{für alle } a, b \in R. \end{aligned}$$

f heißt Isomorphismus, *wenn f zusätzlich noch bijektiv ist.*

Definition 3.5.2 *Sei K ein Körper. Eine Teilmenge $U \subseteq K$ heißt* Unterkörper, *falls gilt:*

i) U ist Untergruppe von $(K, +)$.

ii) $U \setminus \{0\}$ ist Untergruppe von $(K \setminus \{0\}, \cdot)$.

Dann ist U zusammen mit den Einschränkungen von $+$ und $\cdot$ selbst ein Körper.

Lemma 3.5.3 *Seien K, L Körper, $f : K \to L$ ein Ringhomomorphismus und $U \subseteq L$ das Bild von f.*

i) U ist ein Unterkörper von L.

ii) $f : K \to U$ ist ein Isomorphismus.

Beweis: Wir zeigen zunächst, dass f injektiv ist. Für alle $a \in K^*$ gilt

$$f(a) \cdot f(a^{-1}) = f(a \cdot a^{-1}) = f(1) = 1,$$

also $f(a) \in L^*$. Folglich ist f injektiv.
Weil $f : (K, +) \to (L, +)$ und $f : (K^*, \cdot) \to (L^*, \cdot)$ Homomorphismen abelscher Gruppen sind, sind ihre Bilder $U \subseteq L$ und $U \setminus \{0\} \subseteq L^*$ Untergruppen. Das zeigt i). Da f injektiv, folgt auch ii). □

Definition 3.5.4 *Die* Charakteristik $\mathrm{char}(K)$ *eines Körpers K ist die Ordnung von 1 in der abelschen Gruppe $(K, +)$. Hat 1 unendliche Ordnung in $(K, +)$, so setzen wir* $\mathrm{char}(K) := 0$.

Beispiele

(1) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ haben die Charakteristik Null.

(2) Ist p Primzahl, so hat $\mathbb{Z}/p$ die Charakteristik p.

Proposition 3.5.5 *Sei K ein Körper.*

i) Ist $\mathrm{char}(K) = 0$*, dann gibt es einen Unterkörper* $U \subseteq K$ *mit* $U \cong \mathbb{Q}$*.*

ii) Ist $\mathrm{char}(K) = p \neq 0$*, dann ist* p *eine Primzahl, und es gibt einen Unterkörper* $U \subseteq K$ *mit* $U \cong \mathbb{Z}/p$*.*

Beweis: Die Abbildung

$$\begin{array}{rcl} f : \mathbb{Z} & \to & K \\ 0 < n & \mapsto & \underbrace{1 + \ldots + 1}_{n} \\ 0 & \mapsto & 0 \\ -n & \mapsto & -(\underbrace{1 + \ldots + 1}_{n}) \end{array}$$

ist ein Ringhomomorphismus.

i) Wenn $\mathrm{char}(K) = 0$ ist, dann ist f injektiv. Daraus folgt, dass

$$\begin{array}{rcl} g : \mathbb{Q} & \to & K \\ \frac{k}{n} & \mapsto & \frac{f(k)}{f(n)} \end{array}$$

auch ein Ringhomomorphismus ist. Mit dem vorigen Lemma folgt der Rest.

ii) Wenn $\mathrm{char}(K) = p \neq 0$, dann ist

$$\begin{array}{rcl} g : \mathbb{Z}/p & \to & K \\ [a] & \mapsto & f(a) \end{array}$$

ein injektiver Ringhomomorphismus. Da K nullteilerfrei ist, ist auch $\mathbb{Z}/p$ nullteilerfrei, also ist p eine Primzahl. Mit dem vorigen Lemma folgt die Behauptung. □

Definition 3.5.6 *Eine* Körpererweiterung L/K *besteht aus einem Körper L und einem Unterkörper $K \subseteq L$.*

Wir sagen auch L ist eine *Erweiterung* von K.

Beispiele

(1) $\mathbb{R}/\mathbb{Q}$ und $\mathbb{C}/\mathbb{R}$ sind Körpererweiterungen.

(2) Sei K Körper, $f \in K[x]$ normiert und irreduzibel und $L := K[x]/f$. Dann ist L/K eine Körpererweiterung.

Wir identifizieren dabei $a \in K$ mit $[a] \in K[x]/f = L$.

Notiz 3.5.7 *Ist L/K eine Körpererweiterung, dann ist $(L,+)$ mit der Skalarmultiplikation*

$$\begin{aligned} K \times L &\to L \\ (a,l) &\mapsto a \cdot l \end{aligned}$$

ein Vektorraum über dem Körper K.

Korollar 3.5.8 *Ist K ein endlicher Körper, so ist $q := |K|$ eine Primzahlpotenz.*

Beweis: Sei $p := \mathrm{char}(K)$. Dann ist $(K,+)$ ein Vektorraum über $\mathbb{Z}/p$. Also ist $q = p^d$, wobei d die Dimension ist. □

Definition 3.5.9 *Sei L/K eine Körpererweiterung.*

i) L/K heißt endlich*, wenn L als K-Vektorraum endlichdimensional ist.*

ii) Der Grad $[L:K]$ *von L/K ist die Dimension von L als K-Vektorraum.*

Beispiele

(1) $\mathbb{C}/\mathbb{R}$ ist endlich vom Grad 2.

(2) $\mathbb{R}/\mathbb{Q}$ und $\mathbb{C}/\mathbb{Q}$ sind nicht endlich.

Definition 3.5.10 *Sei L/K eine Körpererweiterung, und sei $\alpha \in L$. Der Unterkörper $K(\alpha)$ von L ist definiert als der Durchschnitt aller Unterkörper $U \subseteq L$, die K und α enthalten.*

Beispiel Sei $K = \mathbb{Q}$, $L = \mathbb{C}$ und $\alpha = i \in \mathbb{C}$. Dann ist $\mathbb{Q}(i) = \{a + bi : a,b \in \mathbb{Q}\} \subseteq \mathbb{C}$.

Definition 3.5.11 *Eine Körpererweiterung L/K heißt* einfach*, wenn es ein $\alpha \in L$ gibt mit $L = K(\alpha)$.*

Beispiele

(1) $\mathbb{C}/\mathbb{R}$ ist einfach, da $\mathbb{C} = \mathbb{R}(i)$ ist.

(2) $\mathbb{R}/\mathbb{Q}$ ist nicht einfach.

Satz 3.5.12 *Ist K ein endlicher Körper, so ist jede endliche Körpererweiterung L/K einfach.*

Beweis: L/K endlich bedeutet, dass L als Vektorraum über K endlichdimensional ist. Also ist L endlicher Körper, und daher ist L^* eine zyklische Gruppe. Sei $\alpha \in L$ ein Erzeuger von L^*. Dann ist

$$L^* \subseteq K(\alpha), \quad \text{also} \quad L = K(\alpha).$$

□

Definition 3.5.13 *Sei L/K eine Körpererweiterung und $\alpha \in L$. Ein Polynom $f \in K[x]$ heißt* Minimalpolynom *von α über K, falls gilt:*

i) Fassen wir f als Polynom mit Koeffizienten aus L auf, so gilt $f(\alpha) = 0$.

ii) f ist normiert.

iii) Es gibt in $K[x]$ kein Polynom mit kleinerem Grad als f, das auch i) und ii) erfüllt.

Lemma 3.5.14 *Sei L/K eine Körpererweiterung und $\alpha \in L$.*

i) Jedes Minimalpolynom f von α über K ist irreduzibel.

ii) α hat höchstens ein Minimalpolynom über K.

iii) Ist L/K endlich, so hat α ein Minimalpolynom über K.

Beweis: i) Angenommen f ist Minimalpolynom von α und nicht irreduzibel. Dann gibt es normierte Polynome $g, h \in K[x]$ mit kleinerem Grad und $f = g \cdot h$. Folglich ist

$$g(\alpha) \cdot h(\alpha) = f(\alpha) = 0,$$

also $g(\alpha) = 0$ oder $h(\alpha) = 0$ im Widerspruch zur Minimalität von f.

ii) Angenommen $f, g \in K[x]$ sind zwei verschiedene Minimalpolynome von α. Dann hat $h := (f - g)^{\text{normiert}} \in K[x]$ eine Nullstelle α. Wegen $\deg(f) = \deg(g)$ hat h kleineren Grad. Das steht im Widerspruch zur Minimalität von f, g.

iii) Sei $n = [L : K]$. Dann sind die $n + 1$ Vektoren

$$1, \alpha, \alpha^2, \ldots, \alpha^n \in L$$

linear abhängig über K (aus Dimensionsgründen), d. h. es gibt ein Polynom

$$0 \neq f = a_0 + a_1 x + \ldots + a_n x^n \in K[x]$$

mit $f(\alpha) = 0$. Dasselbe gilt für f^{normiert}. Also gibt es normierte Polynome in $K[x]$ mit Nullstelle α. Darunter sind solche mit minimalem Grad. □

Beispiele

i) $\alpha := i \in \mathbb{C}$ hat Minimalpolynom $x^2 + 1$ über $\mathbb{Q}$.

ii) Sei K ein Körper, $f \in K[x]$ normiert vom Grad d und irreduzibel sowie $L := K[x]/f$. Dann ist L/K endlich vom Grad d. L/K ist einfach, da $L = K(\alpha)$ mit $\alpha := [x] \in K[x]/f = L$ ist. Das Minimalpolynom von α ist gerade f.

Satz 3.5.15 *Sei L/K eine endliche, einfache Körpererweiterung. Dann gibt es ein irreduzibles normiertes Polynom $f \in K[x]$ mit $L \cong K[x]/f$.*

Beweis: Da L/K einfach ist, gibt es ein $\alpha \in L$ mit $L = K(\alpha)$. Da L/K endlich ist, hat α ein Minimalpolynom $f \in K[x]$ (normiert und irreduzibel). Wir betrachten die Abbildung

$$\begin{aligned} \psi : K[x]/f &\to L \\ [g] &\mapsto g(\alpha). \end{aligned}$$

Diese ist wohldefiniert, da $f(\alpha) = 0$ ist. ψ ist ein Ringhomomorphismus. Mit Lemma 3.5.3 folgt, dass ψ Isomorphismus auf einem Unterkörper U von L ist. Aber es ist

$$\alpha = \psi([x]) \in U,$$

also folgt $K(\alpha) \subseteq U$ und damit $U = L$. Das heißt ψ ist ein Isomorphismus. □

Korollar 3.5.16 *Sei K ein endlicher Körper. Dann gibt es eine Primzahl p und ein irreduzibles normiertes Polynom $f \in \mathbb{Z}/p[x]$ mit $K \cong \mathbb{Z}/p[x]/f$.*

Beweis: Sei p die Charakteristik von K. Nach Proposition 3.5.5 ist p eine Primzahl und K eine Körpererweiterung von $\mathbb{Z}/p$. Da K endlich ist, ist $K/\mathbb{Z}/p$ eine endliche Körpererweiterung. $K/\mathbb{Z}/p$ ist einfach laut Satz 3.5.12. Wir können also den vorigen Satz anwenden. □

3.6 Faktorisierung von Polynomen

Lemma 3.6.1 *Seien K ein Körper und $f, g, h \in K[x]$ Polynome mit $f|g \cdot h$, dabei sei f normiert und irreduzibel. Dann gilt $f|g$ oder $f|h$.*

Beweis: Angenommen $f \not| g$, dann ist zu zeigen $f|h$. Da f irreduzibel ist, folgt $\mathrm{ggT}(f, g) = 1$. Mit Satz 3.4.9 folgt, dass es $u, v \in K[x]$ mit $uf + vg = 1$ gibt, also

$$ufh + vgh = h.$$

Mit $f|gh$ folgt daraus $f|h$. □

Satz 3.6.2 *Sei $f \in K[x]$ ein normiertes Polynom, wobei K ein Körper ist.*

i) f besitzt eine Darstellung der Form

$$f = f_1^{e_1} \cdot f_2^{e_2} \cdot \ldots \cdot f_r^{e_r},$$

wobei die $f_1, \ldots, f_r \in K[x]$ normiert, irreduzibel und paarweise verschieden sind. Zudem ist $r \geq 0$ und $e_1, \ldots, e_r \geq 1$.

ii) Die Darstellung in i) ist eindeutig bestimmt bis auf die Reihenfolge der Faktoren.

Beweis: i) Induktion über $\deg(f)$. Für $\deg(f) = 0$, oder anders ausgedrückt $f = 1$, erfüllt $r = 0$ die Behauptung. Sei also $\deg(f) > 0$. Wenn f irreduzibel ist, ist die Behauptung trivial. Ist f nicht irreduzibel, so gibt es normierte $g, h \in K[x]$ mit $\deg(g), \deg(h) < \deg(f)$, so dass $f = g \cdot h$. Nach Induktionsvoraussetzung besitzen g und h jeweils eine Zerlegung $g = g_1^{a_1} \cdot \ldots \cdot g_s^{a_s}$ bzw. $h = h_1^{b_1} \cdot \ldots \cdot h_t^{b_t}$ mit irreduziblen und normierten g_i, h_j. Daher ist

$$f = g \cdot h = g_1^{a_1} \cdot \ldots \cdot g_s^{a_s} \cdot h_1^{b_1} \cdot \ldots \cdot h_t^{b_t}.$$

Wir fassen nun die unter den g_i und h_j gleichen irreduziblen Polynome zusammen und erhalten dadurch die gewünschte Darstellung.

ii) Induktion über $\deg(f)$. Der Fall $\deg(f) = 0$ ist trivial. Sei also $\deg(f) > 0$. Angenommen f hat die beiden Darstellungen

$$f_1^{e_1} \cdot \ldots \cdot f_r^{e_r} = f = g_1^{d_1} \cdot \ldots \cdot g_s^{d_s},$$

und f sei minimal mit dieser Eigenschaft, d.h. alle Polynome vom Grad kleiner $\deg(f)$ besitzen eine eindeutige Darstellung gemäß ii). Dann teilt f_1 das Produkt rechts. Mit Lemma 3.6.1 folgt $f_1 | g_i$ für ein i. Folglich ist $f_1 = g_i$, da g_i irreduzibel und normiert ist. Wir erhalten zwei Darstellungen von f/f_1

$$f_1^{e_1 - 1} \cdot f_2^{e_2} \cdot \ldots \cdot f_r^{e_r} = f/f_1 = g_1^{d_1} \cdot \ldots \cdot g_i^{d_i - 1} \cdot \ldots \cdot g_s^{d_s}.$$

Es ist $\deg(f/f_1) < \deg(f)$. Also besitzt f/f_1 eine eindeutige Darstellung gemäß ii). Daher ist auch die Darstellung von f eindeutig. Das ist ein Widerspruch zur Voraussetzung, die an f gestellt wurde. □

Beispiel Sei K ein endlicher Körper mit q Elementen, und sei $f = x^q - x \in K[x]$.

Behauptung Die Zerlegung von f in irreduzible normierte Faktoren lautet

$$f = \prod_{a \in K} (x - a).$$

Beweis: Wir zeigen zunächst $f(a) = 0$ für alle $a \in K$. Es ist $f(0) = 0$. Sei $a \in K^*$. Da $(K^*, \cdot)$ eine abelsche Gruppe der Ordnung $q - 1$ ist, gilt nach dem Satz von Lagrange $a^{q-1} = 1$, also ist $f(a) = a(a^{q-1} - 1) = 0$.

Also ist jedes $a \in K$ Nullstelle von f, d.h.

$$(x - a) | f \quad \text{für alle} \quad a \in K.$$

Da die Zerlegung von f in irreduzible normierte Faktoren eindeutig ist, kommen darin alle $x-a$ vor, d.h.

$$\prod_{a\in K}(x-a)|f.$$

Aber beide Polynome sind normiert vom Grad q, also sind sie gleich, deshalb ist

$$f=\prod_{a\in K}(x-a).$$

□

Definition 3.6.3 *Sei* $0\neq f\in K[x]$ *beliebig, und sei*

$$f^{\text{normiert}}=f_1^{e_1}\cdot f_2^{e_2}\cdot\ldots\cdot f_r^{e_r}$$

die eindeutige Zerlegung von f^{normiert} *in Potenzen paarweise verschiedener irreduzibler normierter Polynome nach dem vorigen Satz 3.6.2. Die* Nullstellenvielfachheit *von* f *an der Stelle* $a\in K$ *ist die Zahl* e_i*, falls der irreduzible Faktor* f_i *gleich* $x-a$ *ist, bzw. die Zahl Null, falls* $x-a$ *nicht unter den irreduziblen Faktoren* $f_1,\ldots,f_r$ *vorkommt.*

Hat f an der Stelle a eine genau n-fache Nullstelle, so gibt es ein Polynom $g\in K[x]$ mit

$$f=(x-a)^n\cdot g\qquad\text{und}\qquad g(a)\neq 0.$$

Analogie zwischen ganzen Zahlen und Polynomen über einem Körper

ganze Zahlen	Polynome über K
Ring $\mathbb{Z}$	Ring $K[x]$
natürliche Zahl	normiertes Polynom
Vorzeichen	Leitkoeffizient
$\|k\|$	f^{normiert}
$\|k\|<\|l\|$	$\deg(f)<\deg(g)$
$m\|a$	$f\|g$
Ring $\mathbb{Z}/m$	Ring $K[x]/f$
Division mit Rest	Polynomdivision
$\text{ggT}(a,b)$	$\text{ggT}(g,h)$
Euklidischer Algorithmus	Euklidischer Algorithmus
Satz 1.2.5 (Bézout)	Satz 3.4.9
$p\in\mathbb{N}$ Primzahl	$f\in K[x]$ normiert und irreduzibel
Körper $\mathbb{Z}/p$	Körper $K[x]/f$
Primfaktorzerlegung (Satz 1.6.3)	Satz 3.6.2

Es gibt aber auch Unterschiede, zum Beispiel:

(1) Aus $k, l \in \mathbb{N}$ folgt $k + l \in \mathbb{N}$, aber aus $f, g \in K[x]$ normiert folgt nicht $f + g$ normiert.

(2) Es ist $|k + l| \leq |k| + |l|$, aber $\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$.

(3) Aus $k, l \in \mathbb{N}$ und $k \neq l$ folgt $k < l$ oder $l < k$, aber aus $f, g \in K[x]$ normiert und $f \neq g$ folgt nicht $\deg(f) < \deg(g)$ oder $\deg(g) < \deg(f)$.

Definition 3.6.4 *Sei K ein Körper und*

$$f = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n \in K[x].$$

Die algebraische Ableitung *von f ist das Polynom*

$$f' := a_1 + 2a_2 x + \ldots + n a_n x^{n-1} \in K[x],$$

wobei $ka := \underbrace{a + \ldots + a}_{k} \in K$ für $k \in \mathbb{N}$ und $a \in K$ ist.

Beispiel Sei $K = \mathbb{Z}/3$ und $f = x^9 - x \in K[x]$. Dann ist $f' = 9x^8 - 1 = -1 \in K[x]$.

Proposition 3.6.5 *Sei K ein Körper. Für alle $f, g \in K[x]$ und $a \in K$ gelten:*

i) (f+g)' = f' + g'

ii) (af)' = a f'

iii) (fg)' = f g' + f' g

Beweis: Seien $f = \sum_{k=0}^{n} a_k x^k$ und $g = \sum_{l=0}^{m} b_l x^l$. Zudem sei ohne Einschränkung $n \geq m$.

i) Es ist

$$f + g = (a_0 + b_0) + (a_1 + b_1)x + \ldots + (a_m + b_m)x^m + a_{m+1}x^{m+1} + \ldots a_n x^n.$$

Damit folgt

$$\begin{aligned}(f+g)' &= (a_1 + b_1)x + \ldots + m(a_m + b_m)x^{m-1} + (m+1)a_m x^{m+1} + \ldots n a_n x^{n-1} \\ &= a_1 + \ldots + m a_m x^{m-1} + \ldots + n a_n x^{n-1} + b_1 + \ldots + m b_m x^{m-1} \\ &= f' + g'.\end{aligned}$$

ii) Es ist

$$af = aa_0 + aa_1 x + \ldots + aa_n x^n.$$

Damit folgt

$$\begin{aligned}(af)' &= aa_1 + 2aa_2 x \ldots + n a a_n x^{n-1} \\ &= a(a_1 + 2a_2 x \ldots + n a_n x^{n-1}) = af'.\end{aligned}$$

iii) Es ist

$$\begin{aligned} f \cdot g &= \sum_{k=0}^{n} a_k x^k \cdot \sum_{l=0}^{m} k_l x^l \\ &= \sum_{k,l} a_k x^k b_l x^l = \sum_{k,l} a_k b_l x^{k+l} \\ &= \sum_{i=0}^{m+n} \left(\sum_{k+l=i} a_k b_l \right) x^i. \end{aligned}$$

Damit folgt

$$\begin{aligned} (f \cdot g)' &= \sum_{i=0}^{m+n} i \left(\sum_{k+l=i} a_k b_l \right) x^{i-1} \\ &= \sum_{i=0}^{m+n} \left(\sum_{k+l=i} (k+l) a_k b_l \right) x^{i-1} \\ &= \sum_{i=0}^{m+n} \left(\sum_{k+l=i} (k a_k) b_l \right) x^{i-1} + \sum_{i=0}^{m+n} \left(\sum_{k+l=i} (l b_l) a_k \right) x^{i-1} \\ &= \sum_{k,l} (k a_k) b_l x^{k+l-1} + \sum_{k,l} (l b_l) a_k x^{k+l-1} \\ &= \sum_{k,l} (k a_k x^{k-1})(b_l x^l) + \sum_{k,l} (a_k x^k)(l b_l x^{l-1}) \\ &= \sum_{k} k a_k x^{k-1} \sum_{l} b_l x^l + \sum_{k} a_k x^k \sum_{l} l b_l x^{l-1} \\ &= f'g + fg'. \end{aligned}$$

□

Korollar 3.6.6 *Sei K ein Körper und $f \in K[x]$. Wenn f und f' teilerfremd sind, dann ist f quadratfrei, d.h. es gibt kein Polynom $g \in K[x]$ mit $\deg(g) > 0$ und $g^2 | f$. Insbesondere hat f dann keine mehrfachen Nullstellen.*

Beweis: Angenommen es ist $f = g^2 h$ mit $g, h \in K[x]$ und $\deg(g) > 0$. Dann gilt

$$\begin{aligned} f' = (g^2 h)' &= (g \cdot (gh))' = g(gh)' + g'(gh) \\ &= g((gh)' + g'h). \end{aligned}$$

Also werden f und f' beide von g geteilt und es gilt $\deg(g) > 0$. Somit sind f und f' nicht teilerfremd. □

Beispiel Sei K ein Körper der Charakteristik $p \neq 0$ und $f = x^q - x \in K[x]$, wobei q ein Vielfaches von p ist. Dann ist f quadratfrei, und hat somit auch keine mehrfachen Nullstellen *Beweis:* Es ist $f' = (x^q - x)' = (x^q)' - x' = qx^{q-1} - 1 = -1$. Also sind f und f' teilerfremd. □

3.7 Klassifikation endlicher Körper

Ziel Wir wollen zeigen, dass es zu jeder Primzahlpotenz q bis auf Isomorphie genau einen Körper mit q Elementen gibt.

Satz 3.7.1 *Seien K und L endliche Körper mit $|K| = |L| =: q$, wobei q eine Primzahlpotenz ist. Dann sind K und L isomorph.*

Beweis: Es sei p die Primzahl, deren Potenz q ist. Dann wissen wir, dass es ein $\alpha \in K$ gibt mit $K = \mathbb{Z}/p(\alpha)$. Es sei $f \in \mathbb{Z}/p[x]$ das Minimalpolynom von α über $\mathbb{Z}/p$. Wegen $\alpha^q = \alpha$ ist f Teiler von $x^q - x$. Da $x^q - x$ über L in Linearfaktoren zerfällt und von f geteilt wird, hat f eine Nullstelle $\beta \in L$. Also ist f das Minimalpolynom von β über $\mathbb{Z}/p$. Daher gilt für den Unterkörper $U := \mathbb{Z}/p(\beta)$ von L

$$U \cong \mathbb{Z}/p[x]/f \cong \mathbb{Z}/p(\alpha) = K.$$

Weil K aber q Elemente hat, hat auch U q Elemente, und somit gilt $U = L$. Also ist auch $K \cong L$. □

Notation Wenn es einen Körper mit q Elementen gibt, wird der mit $\mathbb{F}_q$ bezeichnet. Er ist eindeutig bestimmt bis auf Isomorphie.

Proposition 3.7.2 *Sei K ein Körper der Charakteristik $p \neq 0$. Dann gilt für alle $a, b \in K$*

$$(a+b)^p = a^p + b^p.$$

Beweis: Nach dem Binomischen Lehrsatz gilt

$$(a+b)^p = a^p + \binom{p}{1} a^{p-1}b + \binom{p}{2} a^{p-2}b^2 + \ldots + \binom{p}{p-1} ab^{p-1} + b^p.$$

Dabei ist

$$\binom{p}{k} = \frac{p!}{k! \cdot (p-k)!}.$$

Daran sieht man, dass $\binom{p}{k}$ für $0 < k < p$ von p geteilt wird. Es ist also $\binom{p}{k} = 0$ in K für $0 < k < p$. Daher ist $(a+b)^p = a^p + b^p$. □

Lemma 3.7.3 *Sei K ein Körper und $f \in K[x]$ ein normiertes Polynom. Dann gibt es eine Körpererweiterung L/K, so dass f als Polynom über L in Linearfaktoren zerfällt.*

Beweis: Durch absteigende Induktion über die Anzahl der irreduziblen Faktoren von f, d.h. über die Summe $e_1 + \ldots + e_r$ der Exponenten in der Zerlegung von f laut Satz 3.6.2. Induktionsanfang: Ist diese Anzahl maximal, d. h. gleich dem Grad von f, so ist bereits $L = K$ die gewünschte Körpererweiterung.
Induktionsschritt: Sei f_1 ein irreduziblen Faktor von f mit $\deg(f_1) \geq 2$. Über dem Erweiterungskörper $K[x]/f_1$ von K zerfällt f in mehr irreduzible Faktoren als über K. Wir können also die Induktionsvoraussetzung anwenden und erhalten eine Erweiterung L von $K[x]/f_1$, über der f in Linearfaktoren zerfällt. □

Nach Korollar 3.5.8 wissen wir bereits, dass q Primzahlpotenz ist, wenn es einen Körper mit q Elementen gibt.

Satz 3.7.4 *Sei q Potenz einer Primzahl p. Dann gibt es einen Körper K mit $q = p^n$ Elementen.*

Beweis: Das vorige Lemma liefert einen Oberkörper L von $\mathbb{Z}/p$, über dem $f = x^q - x$ in Linearfaktoren zerfällt. Es sei $K = \{a \in L, f(a) = 0\}$. Wir zeigen nun, dass K ein Körper mit q Elementen ist. f hat den Grad q, hat keine doppelten Nullstellen und zerfällt vollständig über L. K hat also q Elemente. $a \in L$ ist genau dann aus K, wenn gilt $a^q = a$. Mit Hilfe dieser Eigenschaft zeigen wir, dass K ein Unterkörper von L ist:

- Seien $a, b \in K$. Dann ist $(ab)^q = a^q b^q = ab$ und somit $ab \in K$.
- Sei $a \in K \setminus \{0\}$. Dann ist $(a^{-1})^q = (a^q)^{-1} = a^{-1}$ und somit $a^{-1} \in K$.
- Es ist $0 \in K$ und $1 \in K$.
- Seien $a, b \in K$. Mit Proposition 3.7.2 folgt dann

$$\begin{aligned}(a+b)^q &= (a+b)^{p^n} = ((a+b)^p)^{p^{n-1}} = (a^p + b^p)^{p^{n-1}} \\ &= (a^{p^2} + b^{p^2})^{p^{n-2}} = \ldots = a^{p^n} + b^{p^n} = a^q + b^q = a + b.\end{aligned}$$

  Es ist also $a + b \in K$ und somit auch $-a \in K$.

□

Aufgaben

(1) (a) Zeige, dass [3] ein Erzeuger von $(\mathbb{Z}/31)^*$ ist.

(b) Berechne die diskreten Logarithmen von [10] und [19] zur Basis [3].

(c) Finde sämtliche Lösungen der Kongruenz $10^x \equiv 19 \bmod 31$.

(2) (Diffie-Hellman-Schlüsselvereinbarung) *Alice* und *Bob* wollen einen gemeinsamen, geheimen Schlüssel nach Diffie-Hellman vereinbaren. Sie wählen den Schlüsselraum $(\mathbb{Z}/47)^*$ mit dem Erzeuger $g = [5]$. *Alice* wählt die (geheime) Zufallszahl $n_A = 17$, *Bob* die (geheime) Zufallszahl $n_B = 32$.

(a) Welche Zahl sendet *Alice* an *Bob* und welche *Bob* an *Alice*?

(b) Wie lautet der geheime Schlüssel, den sie vereinbaren?

(3) (ElGamal-Verfahren) *Alice* und *Bob* möchten geheime Botschaften mittels des ElGamal-Verfahrens austauschen. Dazu wählen sie das Chiffretextalphabet (=Klartextalphabet) $(\mathbb{Z}/53)^*$ mit dem Erzeuger $g = [2]$.

(a) *Bob* erzeugt die (geheime) Zufallszahl n_B und errechnet seinen öffentlichen Schlüssel $k_B = g^{n_B} = [12]$. *Alice* erzeugt die (geheime) Zufallszahl $n_A = 16$. Welche Nachricht sendet sie an *Bob*, wenn sie ihm den Klartext [5] verschlüsselt übermitteln will?

(b) *Bob* erhält die verschlüsselte Nachricht $([3], [10])$ von *Alice*. Seine geheime Zufallszahl lautet $n_B = 5$. Welche Botschaft hat *Alice* ihm gesendet?

(c) *Bob* erzeugt die (geheime) Zufallszahl n_B und errechnet seinen öffentlichen Schlüssel $k_B = g^{n_B} = [5]$. *Mister X* belauscht die Botschaft $([11], [2])$ von *Alice* an *Bob*. Er freut sich, da es ihm keine Mühe bereitet, sie zu entziffern. Wie lautet sie?

(4) Es sei $K = \mathbb{Z}/2$, und das Polynom $f \in K[x]$ sei definiert durch $f = x^4 + x + 1$.

(a) Zeige: Gilt für die Polynome $g, h \in K[x]$ die Gleichung $gh = f$, so ist $g = 1$ oder $h = 1$.

(b) Wieviele Elemente besitzt der Ring $R = K[x]/f$?

(c) Zeige $[x] \in R^*$ und ermittle die von $[x]$ erzeugte Untergruppe in R^*.

(d) Zeige, dass R ein Körper ist.

(5) (a) Zeige, dass $g = x^6 + 5x^4 + 6x^2 + 1$ und $h = x^5 + 4x^3 + 3x$ teilerfremd sind in $\mathbb{Q}[x]$.

(b) Finde Polynome $u, v \in \mathbb{Q}[x]$ mit $ug + vh = 1$.

(c) Das Polynom $f = x^3 + 3x + 1$ ist irreduzibel in $\mathbb{Q}[x]$.

(6) Es sei $g = x + 3$ und $h = x + 6$.

(a) Finde $u, v \in \mathbb{Q}[x]$ mit $ug + vh = 1$.

(b) Finde $u, v \in \mathbb{Z}/7[x]$ mit $ug + vh = 1$.

(c) Gibt es $u, v \in \mathbb{Z}/3[x]$ mit $ug + vh = 1$?

(d) Gibt es $u, v \in \mathbb{Z}[x]$ mit $ug + vh = 1$?

(7) Es sei $K = \mathbb{Z}/2$ und $f = x^4 + x + 1 \in K[x]$.

(a) Benutze Aufgabe 4, um zu zeigen, dass f irreduzibel über K ist.

(b) Ist $([1 + x], [x + x^2], [x^3], [x^4])$ eine Basis von $K[x]/f$ über K?

(c) Es sei $b_1 = [1 + x]$, $b_2 = [x + x^2]$, $b_3 = [x^3]$, $b_4 = [1 + x^3]$. Zeige, dass (b_1, b_2, b_3, b_4) eine Basis von $K[x]/f$ über K ist.

(d) Zeige, dass die Abbildung $[g] \mapsto [xg]$ eine lineare Abbildung des K-Vektorraums $K[x]/f$ in sich ist. Berechne die Matrix dieser Abbildung bezüglich der Basis (b_1, b_2, b_3, b_4). Ist die Abbildung invertierbar?

(8) Es sei $\alpha = \sqrt[3]{2} \in \mathbb{R}$ und $\beta = \frac{\sqrt[3]{2}}{2}(-1 + i\sqrt{3}) \in \mathbb{C}$.

(a) Berechne die Minimalpolynome von α und β über $\mathbb{Q}$.

(b) Zeige, dass die Körper $\mathbb{Q}(\alpha) \subset \mathbb{R}$ und $\mathbb{Q}(\beta) \subset \mathbb{C}$ isomorph sind.

(9) (Babystep-Giantstep-Algorithmus) Gegeben sei eine (additiv geschriebene) endliche abelsche Gruppe G, ein Element $P \in G$ der Ordnung n und ein Element $Q \in G$, welches in der von P erzeugten Untergruppe liegt, d.h. es gibt ein $k \in \mathbb{N}$ mit $Q = kP$. Der Babystep-Giantstep-Algorithmus ist eine Methode, k zu bestimmen. Es werden dabei nicht mehr als $2\sqrt{n}$ Operationen benötigt.
Der Algorithmus läuft folgendermaßen ab. Zunächst wird die Liste B der Babysteps berechnet,

$$B = \{(Q - rP, r) \in G \times \mathbb{N}_0, 0 \leq r < m\}.$$

Hierbei ist m die kleinste ganze Zahl größer oder gleich $\sqrt{n}$. Dann werden nacheinander die Giantsteps erzeugt:

$$0{\cdot}mP, 1{\cdot}mP, 2{\cdot}mP, ..., q{\cdot}mP, ..., (m-1){\cdot}mP.$$

Ist $q{\cdot}mP$ erzeugt, wird überprüft, ob $q{\cdot}mP$ als erste Komponente eines Elementes in B auftaucht. Wenn ja, also z.B. $(q{\cdot}mP, r) \in B$, so ist $k = qm + r$ und der Algorithmus bricht ab. Wenn nein, wird der nächste Giantstep erzeugt.

(a) Begünde, warum der Algorithmus tatsächlich k liefert.

(b) Führe den Algorithmus im Beispiel $G = (\mathbb{Z}/53)^*$, $P = [2]$ und $Q = [7]$ durch.

4 Elliptische Kurven

4.1 Verallgemeinertes ElGamal-Verfahren

Definition 4.1.1 *Sei $(A, +)$ eine endliche abelsche Gruppe, $g \in A$ und $k \in \langle g \rangle$, dabei ist $\langle g \rangle \subseteq A$ die von g erzeugte Untergruppe. Eine ganze Zahl n heißt* diskreter Logarithmus *von k zur Basis g, falls $n \cdot g = k$ gilt.*

Bemerkung 4.1.2

i) Im Spezialfall $A = K^*$, wobei K ein endlicher Körper und g ein Erzeuger von K^* ist, ist das Definition 3.1.1 (additiv geschrieben).

ii) So ein n existiert immer, da $k \in \langle g \rangle$ vorausgesetzt ist. n ist eindeutig bis auf Vielfache der Ordnung von g.

Verallgemeinertes ElGamal-Verfahren

Sei $(A, +)$ eine endliche abelsche Gruppe, und seien Klartext- und Chiffretextalphabet $\mathcal{P} = \mathcal{C} = A$. Dann läuft das ElGamal-Verfahren in A folgendermaßen ab:

Schlüsselerzeugung: Bob wählt $g \in A$ und eine Zufallszahl $n_B \in \mathbb{N}$. Er berechnet $k_B := n_B g \in A$. Dann ist (g, k_B) Bobs öffentlicher und n_B Bobs geheimer Schlüssel.

Verschlüsselung: Alice wählt eine Zufallszahl $n_A \in A$. Sie berechnet $k_A := n_A g$ und $k := n_A k_B$ und verschlüsselt ihre Nachricht an Bob durch

$$E : A \to A \quad , \quad a \mapsto a + k.$$

Sie sendet erst k_A und dann die verschlüsselte Nachricht an Bob.

Entschlüsselung: Bob berechnet $k = n_B k_A$ und entschlüsselt dann durch

$$D : A \to A \quad , \quad b \mapsto b - k.$$

Angenommen ein Angreifer kennt g, k_B und hört k_A ab. Wenn er den diskreten Logarithmus n_B von k_B zur Basis g berechnen kann, kann er wie Bob entschlüsseln, analog wenn er n_A berechnen kann. Die Sicherheit dieses Verfahrens beruht darauf, dass der diskrete Logarithmus praktisch unmöglich lösbar ist und keine alternativen Verfahren bekannt sind.

Ziel Wir brauchen endliche abelsche Gruppen A, in denen diskrete Logarithmen schwierig genug zu berechnen sind.

Beispiele Geeignete Gruppen sind zum Beispiel:

(1) $A = K^*$ mit einem endlichen Körper K. Die Sicherheit ist ausreichend z.B. ab $|K| \approx 2^{1000}$.

(2) Wir werden sehen, dass jede sogenannte elliptische Kurve E über einem endlichen Körper K eine endliche abelsche Gruppe A definiert. Ist E geschickt gewählt, so reicht z.B. bereits $|K| \approx 2^{160}$ für eine ausreichende Sicherheit.

Daher ist das ElGamal-Verfahren mit elliptischen Kurven weniger rechenaufwendig als in K^*.

4.2 Affine elliptische Kurven

Definition 4.2.1 *Sei K ein Körper. Die* affine Ebene $\mathbb{A}^2$ *über K ist die Menge aller Paare $P = (x_P, y_P)$ mit $x_P, y_P \in K$.*

Definition 4.2.2 *Sei K ein Körper mit* $\mathrm{char}(K) \neq 2$, *und sei $f \in K[x]$ normiert vom Grad drei mit* $\mathrm{ggT}(f, f') = 1$. *Die (affine)* elliptische Kurve *zu f ist die Punktmenge*

$$E := \{(x, y) \in \mathbb{A}^2 : y^2 = f(x)\} \subset \mathbb{A}^2 .$$

Beispiel $K = \mathbb{R}$ und $f = x^3 - x$.

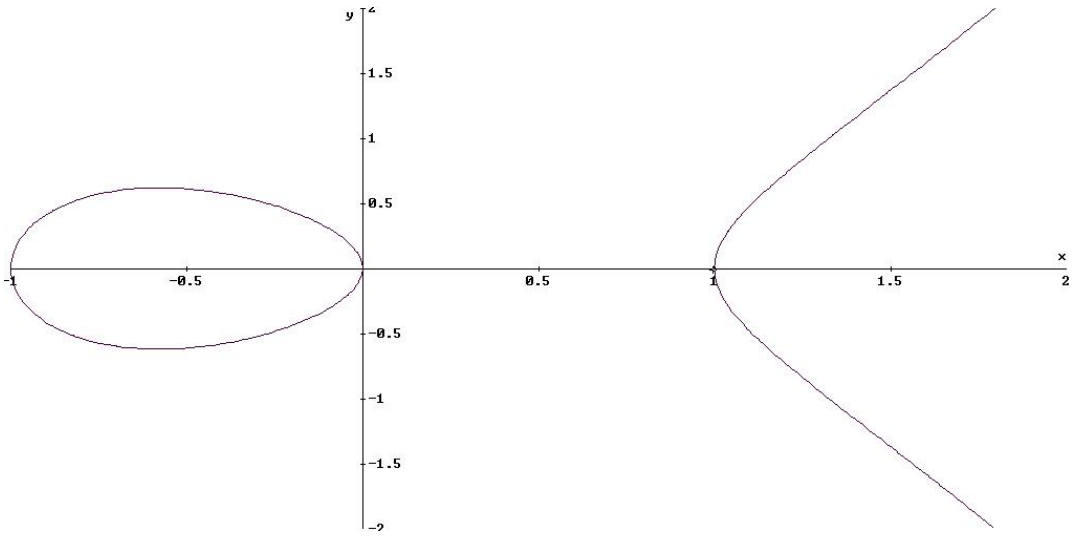

Abbildung 1: Elliptische Kurve $y^2 = x^3 - x$

Bemerkung Einige erste Eigenschaften von elliptischen Kurven:

i) Achsensymmetrie: Wenn $P = (x_P, y_P) \in E$, dann ist auch $-P := (x_P, -y_P) \in E$.

ii) Schnitt mit der x-Achse: $(x_P, 0) \in E$ genau dann, wenn x_P Nullstelle von f ist. (f hat keine mehrfachen Nullstellen, da $\mathrm{ggT}(f, f' = 1)$ ist.)

4.3 Sekanten und Tangenten

Definition 4.3.1 *Sei K ein Körper. Eine Punktmenge $L \subseteq \mathbb{A}^2$ heißt* Gerade, *wenn es $a, b, c \in K$ gibt mit $a \neq 0$ oder $b \neq 0$, so dass*

$$L = \{(x, y) \in \mathbb{A}^2 : ax + by = c\}.$$

Bemerkung Wir unterscheiden die Geraden nach $b \neq 0$ und $b = 0$.

i) Wenn $b \neq 0$ ist, dann ist

$$L = \{(x, y) : y = -\frac{a}{b}x + \frac{c}{b}\}$$

eine Gerade mit Steigung $m = -a/b$.

ii) Wenn $b = 0$ ist, dann ist $a \neq 0$ und

$$L = \{(x, y) : x = \frac{c}{a}\}$$

ist eine senkrechte Gerade.

Notiz 4.3.2 *Seien $P, Q \in \mathbb{A}^2$ zwei verschiedene Punkte. Dann gibt es genau eine Gerade $L \subset \mathbb{A}^2$, die P und Q enthält. Ist $P = (x_P, y_P)$ und $Q = (x_Q, y_Q)$, so gilt*

$$L = \{(x, y) : (y_Q - y_P)(x - x_P) = (x_Q - x_P)(y - y_P)\}.$$

Definition 4.3.3 *Seien K ein Körper mit $\mathrm{char}(K) \neq 2$, $E \subset \mathbb{A}^2$ eine elliptische Kurve und $P, Q \in E$ zwei verschiedene Punkte. Dann heißt die Gerade durch P und Q* Sekante *von E.*

Definition 4.3.4 *Sei K wie eben, $f \in K[x]$ normiert vom Grad drei mit $\mathrm{ggT}(f, f') = 1$ und $E \subset \mathbb{A}^2$ die elliptische Kurve zu f. Die* Tangente *an E im Punkt $P = (x_P, y_P) \in E$ ist die Gerade*

$$T_P E = \{(x, y) : f'(x_P)(x - x_P) = 2y_P(y - y_P)\} \subset \mathbb{A}^2.$$

Bemerkung Wir unterscheiden zwei Fälle.

i) Ist $y_P \neq 0$, dann hat die Tangente $T_P E$ an E in P die Steigung

$$m = \frac{f'(x_P)}{2y_P}.$$

ii) Ist $y_P = 0$, dann ist $f(x_P) = 0$, also $f'(x_P) \neq 0$, da $\mathrm{ggT}(f, f') = 1$ ist. Somit ist die Tangente $T_P E$ an E in P vertikal.

Bemerkung Die Formel für die Tangente stimmt mit der Anschauung überein. Hierzu betrachten wir $K = \mathbb{R}$ und einen Punkt $P = (x_P, y_P) \in E$ mit $y_P \neq 0$, etwa $y_P > 0$. Dann ist $f(x_P) > 0$. Also ist die Funktion

$$g(x) = \sqrt{f(x)}$$

in einer Umgebung von x_P definiert. g ist in x_P differenzierbar, und

$$g'(x_P) = \frac{f'(x_p)}{2\sqrt{f(x_P)}} = \frac{f'(x_P)}{2y_P} = m$$

laut Kettenregel. Also hat die Tangente an E in P in diesem Fall tatsächlich Steigung m.

Definition 4.3.5 *P heißt* Wendepunkt *von E, falls $2y_P^2 f''(x_P) = f'(x_P)^2$ ist.*

Definition 4.3.6 *Sei $L \subset \mathbb{A}^2$ eine Gerade und $P \in L \cap E$. Die Zahl $m_P(L) :=$*

1 *falls* $L \neq T_P E$
2 *falls* $L = T_P E$ *und P kein Wendepunkt*
3 *falls* $L = T_P E$ *und P Wendepunkt*

heißt Schnittvielfachheit *von L und E in P. Wir setzen $m_P(L) = 0$ für alle $P \notin L \cap E$.*

Lemma 4.3.7 *Sei $L = \{(x, y) : y = mx + b\}$ eine nicht senkrechte Gerade und $P = (x_P, y_P) \in L$. Dann hat*

$$h := (mx + b)^2 - f \in K[x]$$

eine genau $m_P(L)$-fache Nullstelle in x_P.

Beweis: Es ist

$$\begin{aligned} h(x_P) &= y_P^2 - f(x_P), \\ h'(x_P) &= 2my_P - f'(x_P), \\ h''(x_P) &= 2m^2 - f''(x_P). \end{aligned}$$

Also ist $h(x_P) = 0$ genau dann wenn $P \in E$. Wenn das gilt, dann ist

$$h'(x_P) = 0 \Leftrightarrow m = \frac{f'(x_P)}{2y_P} \Leftrightarrow L = T_P E.$$

Gilt auch dies, so folgt

$$h''(x_P) = \frac{f'(x_P)^2}{2y_P^2} - f''(x_P),$$

also ist P Wendepunkt genau dann wenn $h''(x_P) = 0$ ist. □

Satz 4.3.8 *Ist L Sekante oder Tangente an E, so gilt*

$$\sum_{P \in L \cap E} m_P(L) = \begin{cases} 2, \textit{ falls } L \textit{ senkrecht ist} \\ 3, \textit{ sonst.} \end{cases}.$$

Beweis: Wir unterscheiden zwei Fälle.

1. Fall: L ist senkrecht. Sei $P = (x_P, y_P) \in L \cap E$. Wenn $y_P = 0$ ist, dann folgt

$$L \cap E = \{P\} \quad \text{und} \quad m_P(L) = 2.$$

Wenn $y_P \neq 0$ ist, dann ist

$$L \cap E = \{P, -P\} \quad \text{und} \quad m_P(L) = 1 = m_{-P}(L).$$

2. Fall: $L = \{(x, y) : y = mx + b\}$. Nach Lemma 4.3.7 enthält $(mx + b)^2 - f \in K[x]$ mindestens zwei Linearfaktoren, also genau 3, da f vom Grad 3 ist. Mit erneuter Verwendung von Lemma 4.3.7 folgt die Behauptung. □

4.4 Gruppenstruktur

Bemerkung In diesem Abschnitt sind mit $L \cap E$ grundsätzlich die Schnittpunkte mit Vielfachheiten gemeint, auch wenn dies nicht immer explizit erwähnt wird.

Definition 4.4.1 *Sei $E \subset \mathbb{A}^2$ eine (affine) elliptische Kurve. Die* (projektive) elliptische Kurve E^* *ist*

$$E^* := E \cup \{O\},$$

wobei $O \notin \mathbb{A}^2$ ist. O heißt unendlich ferner Punkt.

Definition 4.4.2 *Die Abbildung*

$$+ : E^* \times E^* \to E^*$$

ist wie folgt definiert:

i) $O + P := P$ und $P + O := P$ für alle $P \in E^*$.

ii) Seien $P, Q \in E$ und L die Sekante durch P, Q (bzw. $L = T_P E$, falls $P = Q$).

$$P + Q := \begin{cases} O, \textit{ falls } L \textit{ senkrecht ist,} \\ -R, \textit{ falls } L \cap E = \{P, Q, R\} \textit{ ist.} \end{cases}$$

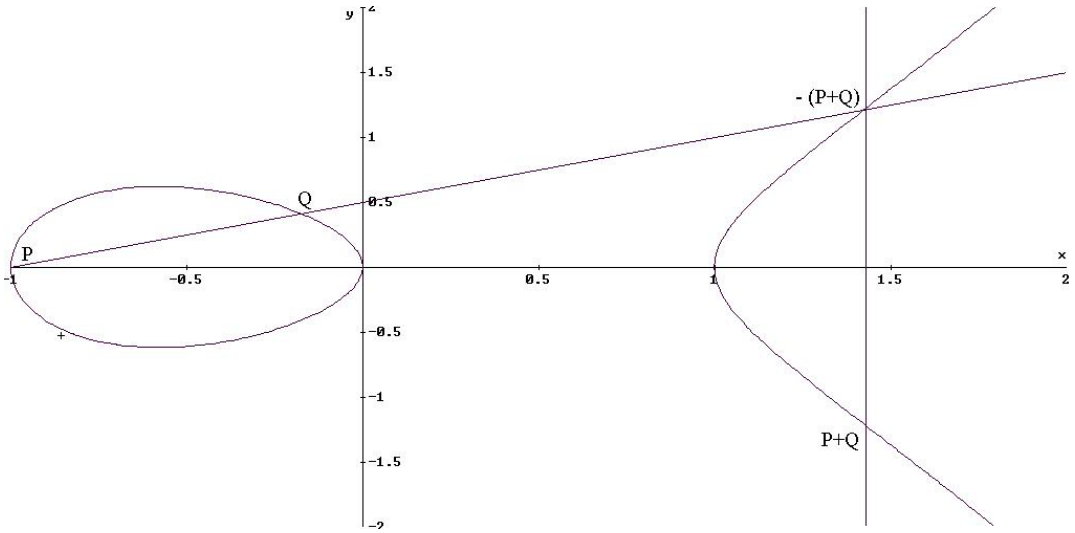

Abbildung 2: Addition auf einer Elliptischen Kurve

Notiz 4.4.3 *Seien $P = (x_P, y_P), Q, R \in E$.*

i) Es ist $P + Q = O$ genau dann, wenn $Q = (x_P, -y_P) = -P$ ist.

ii) Es ist $(P + Q) + R = 0$ genau dann, wenn es eine Gerade L gibt mit

$$L \cap E = \{P, Q, R\}.$$

Satz 4.4.4 *Sei $E^* = E \cup \{O\}$ die projektive elliptische Kurve zu $f \in K[x]$.*

i) $(E^*, +)$ ist eine abelsche Gruppe.

ii) $O \in E^*$ ist das neutrale Element.

iii) Das Inverse zu $P = (x_P, y_P) \in E$ ist $-P = (x_P, -y_P)$.

Beweis: Per Definition ist + kommutativ, $O \in E^*$ neutral und $P + (-P) = O$. Das liefert ii) und iii). Für i) ist noch zu zeigen

$$(P + Q) + R = P + (Q + R)$$

für alle $P, Q, R \in E^*$. oBdA seien $P, Q, R \in E$.

1. Fall: $P + Q = O$. oBdA sei $Q + R \neq O$, d.h. es gibt eine Gerade

$$L = \{(x, y) : y = mx + b\}$$

mit $L \cap E = \{Q, R, -(Q + R)\}$. Für

$$\bar{L} := \{(x, y) : -y = mx + b\}$$

gilt dann $L \cap E = \{P, -R, Q+R\}$, also

$$P + (Q + R) = R = (P + Q) + R.$$

2. Fall: Für $Q + R = O$ folgt die Behauptung analog zum 1. Fall.

3. Fall: Für $(P+Q)+R = O$ oder $P+(Q+R) = O$ folgt die Behauptung aus Notiz 4.4.3.ii).

4. Fall: Den Fall $P + Q$, $Q + R$, $(P + Q) + R$, $P + (Q + R) \neq O$ beweisen wir später. □

4.5 Beweis der Assoziativität

Definition 4.5.1 *Der* Funktionenring *der elliptischen Kurve* $E = \{(x, y) : y^2 = f(x)\}$ *ist*

$$A(E) := K[x, y]/y^2 - f(x).$$

Definition 4.5.2 *Sei* $g \in A(E)$. *Für* $P = (x_P, y_P) \in E$ *ist* $g(P) \in K$ *definiert durch*

$$g(P) := h(x_P, y_P),$$

dabei ist $h \in K[x, y]$ *Repräsentant der Restklasse* g.

Bemerkung $g(P)$ ist wohldefiniert, da $y_P^2 - f(x_P) = 0$ ist.

Notiz 4.5.3 *Jedes* $g \in A(E)$ *hat genau einen Repräsentanten der Form* $u + vy$ *mit* $u, v \in K[x]$.

$$\begin{aligned} A(E) &\to A(E) \\ g &\mapsto \bar{g} := [u - vy] \end{aligned}$$

ist ein Ringisomorphismus.

Bemerkung Wir identifizieren $u \in K[x]$ mit $[u] \in A(E)$. Damit gilt für alle $g = [u + vy] \in A(E)$

$$g \cdot \bar{g} = u^2 - f \cdot v^2 \in K[x].$$

Wir erhalten also eine Abbildung

$$\begin{aligned} N : A(E) &\to K[x] \\ g &\mapsto g \cdot \bar{g}. \end{aligned}$$

Proposition 4.5.4 *$A(E)$ ist nullteilerfrei.*

Beweis: Seien $g, h \in A(E)$ mit $g \cdot h = 0$, dann ist zu zeigen $g = 0$ oder $h = 0$. Es gilt

$$N(g) \cdot N(h) = N(g \cdot h) = N(0) = 0,$$

also ist $N(g) = 0$ oder $N(h) = 0$, da $K[x]$ nullteilerfrei ist. Sei etwa $N(g) = 0$ für $g = [u + vy]$ mit $u, v \in K[x]$, d.h.

$$u^2 = f \cdot v^2 \quad \text{in } K[x].$$

Da $\deg(f) = 3$ ungerade ist, muss $u = v = 0$ sein, also ist $g = 0$. □

Definition 4.5.5 *$P \in E$ heißt* Nullstelle *von $g \in A(E)$, falls $g(P) = 0$ ist.*

Lemma 4.5.6 *Sei $P = (x_P, y_P)$ ein Punkt auf E und $g \in A(E)$ mit*

i) g(P)=0=g(-P), falls $y_P \neq 0$ ist.

ii) bzw. $(x - x_P)^2 | N(g) = g \cdot \bar{g} \in K[x]$, falls $y_P = 0$ ist.

Dann ist g durch $[x - x_P]$ teilbar, d.h. es gibt ein $h \in A(E)$ mit

$$g = [x - x_P] \cdot h \quad \text{in } A(E).$$

Beweis: Schreibe $g = [u + vy]$ mit $u, v \in K[x]$. Wir unterscheiden zwei Fälle.

1. Fall: Sei $y_P \neq 0$. Wir haben $u(x_P) + y_P v(x_P) = 0$ und $u(x_P) - y_P v(x_P) = 0$ in K, also sind $u(x_P) = v(x_P) = 0$, d.h. u, v und damit auch g sind durch $x - x_P$ teilbar.

2. Fall: Sei $y_P = 0$, also $f(x_P) = 0$. Aus

$$(x - x_P)^2 \big| u^2 - f \cdot v^2$$

folgt zunächst $u(x_P) = 0$. Weil auch

$$\frac{N(g)}{x - x_P} = u \cdot \frac{u}{x - x_P} - \frac{f}{x - x_P} \cdot v^2 \in K[x]$$

eine Nullstelle bei x_P hat, $f/(x - x_P)$ aber nicht, folgt $v(x_P) = 0$. □

Satz 4.5.7 *Sei $P = (x_P, y_P)$ ein Punkt auf der elliptischen Kurve E zu $f \in K[x]$. Dann gibt es genau eine Abbildung*

$$v_P : A(E) \setminus \{0\} \to \mathbb{N} \cup \{0\}$$

mit folgenden Eigenschaften:

i) $v_P(g) = 0$, *wenn* $g(P) \neq 0$ *ist.*

ii) $v_P(gh) = v_P(g) + v_P(h)$.

iii) $v_P([x - x_P]) = 1$, *falls* $y_P \neq 0$, *bzw.* $= 2$, *falls* $y_P = 0$ *ist.*

Beweis: Wir unterscheiden zwei Fälle.

1. Fall: $y_P \neq 0$. Wir finden eine nicht senkrechte Gerade

$$L = \{(x, y) : y = mx + b\}$$

mit $-P \in L$ und $L \neq T_{-P}E$. Sei

$$l := [y - mx - b] \in A(E).$$

In dieser Situation benutzen wir das folgende:

Lemma Zu jedem $0 \neq g \in A(E)$ gibt es ein $n \geq 0$ und ein $k \in A(E)$ mit

$$l^n \cdot g = [x - x_P]^n \cdot k.$$

und $k(P) \neq 0$. n ist durch g eindeutig bestimmt.
Beweis: Durch Induktion über die Vielfachheit der Nullstelle x_P von $N(g) \in K[x]$. Sei zunächst $g(P) \neq 0$. Dann erfüllt $n = 0$ die Behauptung, und für $n > 0$ gilt $l^n \cdot g \neq [x - x_P]^n \cdot k$, da die rechte Seite eine Nullstelle in P hat, die linke Seite aber nicht. Das zeigt auch die Eindeutigkeit im Fall $g(P) \neq 0$.
Wenn $g(P) = 0$ ist, dann liefert Lemma 4.5.6 ein $h \in A(E)$ mit

$$l \cdot g = [x - x_P] \cdot h.$$

Da $N(l)$ eine einfache, aber $N([x - x_P])$ eine doppelte Nullstelle bei x_P hat, fällt h unter die Induktionsvorauusetzung. □
Wir kehren zum 1. Fall im Beweis des Satzes zurück.
Eindeutigkeit von v_P: Wenn i) - iii) erfüllt sind, gilt mit den Bezeichnungen des Lemmas $v_P(k) = 0 = v_P(l)$ und deshalb $v_P(g) = n$. Also kann es höchstens eine solche Abbildung v_P geben.
Existenz von v_P: Wegen der Eindeutigkeit von n im Lemma ist $v_P(g) := n$ wohldefiniert. Die so definierte Abbildung v_P erfüllt i) - iii).

2. Fall: Sei $y_P = 0$. Sei $0 \neq g \in A(E)$, und sei $n \geq 0$ die Vielfachheit der Nullstelle x_P von $N(g) \in K[x]$. Nach Lemma 4.5.6 gibt es ein $k \in A(E)$ mit

$$g^2 = [x - x_P]^n \cdot k.$$

Dann hat $N(k) \in K[x]$ keine Nullstelle mehr in x_P, also ist $k(P) \neq 0$. Wenn v_P i) - iii) erfüllt, muss also $v_P(g) = n$ gelten. Es folgt, dass v_P eindeutig bestimmt ist. Umgekehrt kann v_P durch $v_P(g) := n$ definiert werden und erfüllt dann i) - iii). □

Definition 4.5.8 *Die Zahl $v_P(g)$ heißt Vielfachheit der Nullstelle $P \in E$ von $g \in A(E) \setminus \{0\}$.*

Bemerkung Zu jeder Gerade $L = \{(x, y) : ax + by = c\}$ gehört eine "lineare" Funktion $l = [ax + by - c] \in A(E)$.

Proposition 4.5.9 *Sei $L = \{(x, y) : ax + by = c\}$ eine Gerade, und sei $l = [ax + by - c] \in A(E)$. Dann gilt*

$$v_P(l) = m_P(L)$$

für alle $P \in E$.

Beweis: Wenn $P \notin L$ ist, dann gilt $l(P) \neq 0$, also

$$v_P(l) = 0 = m_P(L).$$

Sei also $P = (x_P, y_P) \in L \cap E$. Wir unterscheiden wieder zwei Fälle.

1. Fall: L sei senkrecht, also

$$L = \{(x, y) : x = x_P\}.$$

Wenn $y_P \neq 0$ ist, dann ist

$$v_P(l) = v_P([x - x_P]) = 1 = m_P(L),$$

da $L \neq T_P E$. Wenn $y_P = 0$ ist, dann ist

$$v_P(l) = v_P([x - x_P]) = 2 = m_P(L),$$

da $L = T_P E$.

2. Fall: L ist nicht senkrecht. Nach Lemma 4.3.7 hat $N(l) \in K[x]$ eine genau $m_P(L)$-fache Nullstelle in x_P, also

$$v_P(l \cdot \bar{l}) = m_P(L) \cdot v_P([x - x_P]).$$

Wenn $y_P \neq 0$ ist, dann ist $v_P([x - x_P]) = 1$ und

$$v_P(\bar{l}) = v_{-P}(l) = 0, \quad \text{da } -P \notin L \text{ ist.}$$

Wir erhalten $v_P(l) = m_P(L)$.
Wenn $y_P = 0$ ist, dann ist $v_P([x - x_P]) = 2$ und

$$v_P(\bar{l}) = v_{-P}(l) = v_P(l), \quad \text{da } -P = P \text{ ist.}$$

Wir erhalten $2v_P(l) = 2m_P(L)$. □

Proposition 4.5.10 *Sei $L = \{(x, y) : ax + by = c\}$ eine Sekante oder Tangente an E, und sei $l = [ax + by - c] \in A(E)$. Wenn $g \in A(E)$ die Eigenschaft $v_P(g) \geq v_P(l)$ für alle $P \in E$ hat, ist g durch l teilbar.*

Beweis: Die Behauptung folgt aus Lemma 4.5.6, falls L senkrecht ist. Sei L also nicht senkrecht, $L \cap E = \{Q, R, S\}$ (mit Vielfachheiten). Dann folgt

$$(l \cdot \bar{l})^{\text{normiert}} = (x - x_Q)(x - x_R)(x - x_S)$$

laut Lemma 4.3.7. Für alle $P \in E$ haben wir

$$v_P(g \cdot \bar{l}) \geq v_P(l \cdot \bar{l}).$$

Mit dreimal Lemma 4.5.6 folgt

$$l \cdot \bar{l} | g \cdot \bar{l}$$

und somit $l|g$. □

Satz 4.5.11 *Seien P, Q, R Punkte auf der affinen elliptischen Kurve E mit $P + Q$, $Q + R$, $(P + Q) + R$, $P + (Q + R) \neq O$. Dann gilt*

$$(P + Q) + R = P + (Q + R) \text{ in } E^*.$$

Beweis: Nach Definition von + gibt es Geraden $L_1, M_1, L_2, M_2, L_3, M_3$ mit

$$\begin{aligned}
L_1 \cap E &= \{P, Q, -(P + Q)\} \\
M_1 \cap E &= \{Q, R, -(Q + R)\} \\
L_2 \cap E &= \{Q + R, -(Q + R)\} \\
M_2 \cap E &= \{P + Q, -(P + Q)\} \\
L_3 \cap E &= \{P + Q, R, -((P + Q) + R)\} \\
M_3 \cap E &= \{P, Q + R, -(P + (Q + R))\},
\end{aligned}$$

jeweils mit Vielfachheiten. Seien

$$l_1, m_1, l_2, m_2, l_3, m_3 \in A(E)$$

die zugehörigen linearen Funktionen. Die Nullstellen von $l_1 l_2 l_3$ sind

$$\{P, Q, R, \pm(P + Q), \pm(Q + R), -((P + Q) + R)\},$$

und die Nullstellen von $m_1 m_2 m_3$ sind

$$\{P, Q, R, \pm(P+Q), \pm(Q+R), -(P+(Q+R))\}.$$

Zweimal Proposition 4.5.10 liefert ein $l \in A(E)$ mit

$$l_1 l_2 l = m_1 m_2 m_3.$$

Da N multiplikativ ist, folgt somit $\deg(N(l)) = 3$, d.h. l ist die lineare Funktion zu einer Geraden L, und

$$L \cap E = \{P+Q, R, -(P+(Q+R))\}$$

(mit Vielfachheiten). Es folgt $L = L_3$, also

$$-(P+(Q+R)) = -((P+Q)+R).$$

□

Korollar 4.5.12 *$(E^*, +)$ ist eine abelsche Gruppe. Insbesondere ist $(E^*, +)$ für jede elliptische Kurve E über einem endlichen Körper eine endliche abelsche Gruppe.*

Einige dieser Gruppen eignen sich besonders gut für das ElGamal-Verfahren.

Aufgaben

(1) Es sei $K = \mathbb{Z}/13$ und $f = x^3 + 2x + 1 \in K[x]$.

(a) Berechne $ggT(f, f')$ und begründe, warum f eine elliptische Kurve E definiert.

(b) Bestimme die Punkte von E.

(2) Es sei $K = \mathbb{Z}/7$, $f = x^3 + 4x^2 + 3x + 3 \in K[x]$ und E sei die durch f definierte elliptische Kurve. Es sei $P_1 = (3, 1)$ und $P_2 = (1, 2)$. Weiter seien die Geraden L_1, L_2 und L_3 definiert durch $L_1 = \{(x, y) : 5(x - 3) = 2(y - 1)\}$, $L_2 = \{(x, y) : y = 2\}$ und $L_3 = \{(x, y) : x - 3 = -2(y - 1)\}$.

Für $i = 1, 2, 3$ und $j = 1, 2$ berechne die Schnittvielfachheiten von L_i und E in P_j.

(3) Es sei $K = \mathbb{Z}/5$, $f = x^3 - x - 1 \in K[x]$ und E sei die durch f definierte elliptische Kurve.

(a) Zeige $P = (2, 0) \in E$, $Q = (4, 3) \in E$ und bestimme die Tangenten an E in P und Q, sowie die Sekante durch P und Q.

(b) Berechne $P + P$, $Q + Q$ und $P + Q$.

(4) Es sei E eine elliptische Kurve für die es eine Tangente oder Sekante gebe, die nicht senkrecht ist. Zeige, dass der Funktionenring $A(E)$ nicht faktoriell ist.

Index