Vorabskript zur Vorlesung

Angewandte Diskrete Mathematik

Wintersemester 2010/ 11

Prof. Dr. Helmut Maier
Dipl.-Math. Hans- Peter Reck

Institut für Zahlentheorie und Wahrscheinlichkeitstheorie
Universität Ulm

Inhaltsverzeichnis

1 Elementare Zahlentheorie und algebraische Strukturen **4**

1.1 Teilbarkeit ganzer Zahlen 4

1.2 Eindeutigkeit der Primfaktorzerlegung 4

1.3 Berechnung von ggT und kgV anhand der Primfaktorzerlegung 5

1.4 Der Euklidische Algorithmus 6

1.5 Kongruenzen 8

1.6 Das multiplikative Inverse 9

1.7 Das Rechnen mit Kongruenzen 10

1.8 Elementare Teilbarkeitsregeln 11

1.9 Restsysteme, teilerfremde Restklassen, Eulersche φ- Funktion 12

1.10 Lineare Kongruenzen 13

1.11 Der Chinesische Restsatz 14

1.12 Berechnung der Eulerschen φ- Funktion, Multiplikativität 16

1.13 Die Sätze von Euler und Fermat 17

1.14 Algebraische Grundstrukturen 18

1.15 Beispiele in der Zahlentheorie 19

1.16 Untergruppen, zyklische Gruppen, Ordnung und Primitivwurzel 20

1.17 Polynomkongruenzen 27

1.18 Potenzreste 30

2 Anwendungen in der Kryptologie **32**

2.1 Public- Key- Codes, RSA- Verfahren 32

3 Endliche Körper **35**

3.1 Polynomkongruenzen 35

3.2 Endliche Körper 37

4 Fehlerkorrigierende Codes **38**

4.1 Einleitung 38

4.2 Grundlegende Sätze und Definitionen 39

4.3 Lineare Codes 39

4.4 Fehlerkorrektur 42

Kapitel 1

Elementare Zahlentheorie und algebraische Strukturen

1.1 Teilbarkeit ganzer Zahlen

Definition 1.1.1. Eine ganze Zahl b heißt durch eine ganze Zahl $a \neq 0$ teilbar, falls es ein $x \in \mathbb{Z}$ gibt, so daß $b = ax$ ist, und wir schreiben $a|b$. Man nennt a einen Teiler von b, und b heißt Vielfaches von a. Falls b nicht durch a teilbar ist, schreiben wir $a \nmid b$.

Satz 1.1.1. (a) $a|b \Rightarrow a|bc$ *für alle* $c \in \mathbb{Z}$

(b) $a|b$ *und* $b|c \Rightarrow a|c$

(c) $a|b$ *und* $a|c \Rightarrow a|(bx + cy)$ *für alle* $x, y \in \mathbb{Z}$

(d) $a|b$ *und* $b|a \Rightarrow a = \pm b$

(e) $a|b$ *und* $a, b > 0 \Rightarrow a \leq b$

(f) *Ist* $m \neq 0$*, dann gilt:* $a|b \Leftrightarrow ma|mb$.

Beweis. (a) $a|b \Leftrightarrow \exists x \in \mathbb{Z}, b = ax \Rightarrow bc \equiv a \cdot (xc)$ für alle $c \in \mathbb{Z} \Rightarrow a|bc$ für alle $c \in \mathbb{Z}$

(b) $a|b$ und $b|c \Rightarrow \exists x, y \in \mathbb{Z}$: $b = ax, c = by \Rightarrow \exists x, y \in \mathbb{Z}$: $c = a(xy) \Rightarrow a|c$

(c) - (f) ohne Beweis.

□

1.2 Eindeutigkeit der Primfaktorzerlegung

Definition 1.2.1. Eine natürliche Zahl $p \in \mathbb{N}$ heißt Primzahl, wenn p nur die positiven Teiler 1 und p besitzt.

Beispiel 1.2.1. Es ist $n = 91$ keine Primzahl, da $91 = 7 \cdot 13$ gilt.
Dafür ist $p = 17$ eine Primzahl.

Definition 1.2.2. Unter der (kanonischen) Primfaktorzerlegung einer natürlichen Zahl $n > 1$ versteht man eine Darstellung der Gestalt $n = p_1^{\gamma_1} \cdot \ldots \cdot p_r^{\gamma_r}$ mit $p_1 < \ldots < p_r$ und $\gamma_i \in \mathbb{N}$ für $i = 1, \ldots, r$.

Beispiel 1.2.2. Die Zahl $n = 9000$ besitzt die kanonische Primfaktorzerlegung

$$9000 = 2^3 \cdot 3^2 \cdot 5^3.$$

Satz 1.2.1. *(Fundamentalsatz der Arithmetik)*
Die kanonische Primfaktorzerlegung einer natürlichen Zahl $n > 1$ existiert stets und ist eindeutig.

1.3 Berechnung von ggT und kgV anhand der Primfaktorzerlegung

Definition 1.3.1. Es seien $a, b \in \mathbb{Z}$, nicht beide gleich 0.
Der größte gemeinsame Teiler von a und b, $ggT(a, b)$, ist die größte positive ganze Zahl d, für die gilt: $d|a$ und $d|b$.

Es sei nun $a \neq 0$ und $b \neq 0$.
Das kleinste gemeinsame Vielfache von a und b, $kgV(a, b)$, ist die kleinste positive Zahl V, für die gilt: $a|V$ und $b|V$.

Satz 1.3.1. *Es seien $m = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$ und $n = p_1^{\beta_1} \cdot \ldots \cdot p_r^{\beta_r}$ mit p_i verschiedene Primzahlen, $\alpha_i, \beta_i \in \mathbb{Z}$, $\alpha_i \geq 0$ und $\beta_i \geq 0$.*
Dann ist

$$\begin{aligned} ggT(m,n) &= p_1^{\gamma_1} \cdot \ldots \cdot p_r^{\gamma_r} \\ kgV(m,n) &= p_1^{\delta_1} \cdot \ldots \cdot p_r^{\delta_r} \end{aligned}$$

mit $\gamma_i = \min(\alpha_i, \beta_i)$ und $\delta_i = \max(\alpha_i, \beta_i)$.

Bemerkung 1.3.1. Die obige Darstellungen stellen nicht unbedingt die kanonische Primfaktorzerlegung von m und n im Sinne von Definition 1.2.2 dar, bei der alle Exponenten positiv sein müssen. In manchen Fällen ist es nötig, Potenzen p_i^0 einzufügen, um zu gewährleisten, daß die in beiden Produkten vorkommenden Primzahlen dieselben sind.

Beispiel 1.3.1. Es sei

$$\begin{array}{lllllll} m = 90090 & = 2 \cdot 3^2 & \cdot 5 & \cdot 7 & \cdot 11 & \cdot 13 & \\ n = 2300 & = 2^2 & \cdot 5^2 & & & & \cdot 23 \end{array}$$

Bestimme $ggT(m, n)$ und $kgV(m, n)$.

Lösung:
Wir schreiben m und n so als Produkte, daß die in ihnen vorkommenden Primzahlen dieselben sind:

$$\begin{array}{lllllllll} m = 90090 & = 2^1 & \cdot 3^2 & \cdot 5^1 & \cdot 7^1 & \cdot 11^1 & \cdot 13^1 & \cdot 23^0 \\ n = 2300 & = 2^2 & \cdot 3^0 & \cdot 5^2 & \cdot 7^0 & \cdot 11^0 & \cdot 13^0 & \cdot 23^1 \end{array}$$

Nach Satz 1.3.1 ist

$$\begin{array}{lllllllll} ggT(m,n) & = 2^1 & \cdot 3^0 & \cdot 5^1 & \cdot 7^0 & \cdot 11^0 & \cdot 13^0 & \cdot 23^0 & = 10 \\ kgV(m,n) & = 2^2 & \cdot 3^2 & \cdot 5^2 & \cdot 7^1 & \cdot 11^1 & \cdot 13^1 & \cdot 23^1 & = 20720700 \end{array}$$

1.4 Der Euklidische Algorithmus

Der *ggT* zweier natürlicher Zahlen m und n kann mittels des Euklidischen Algorithmus bestimmt werden. Dieser besteht in einer wiederholten Anwendung der Division mit Rest.

Satz 1.4.1. *(Division mit Rest)*
Es seien $a \in \mathbb{Z}$ und $b \in \mathbb{N}$.
Dann gibt es $q \in \mathbb{N}_0$, so daß $a = q \cdot b + r$ mit $0 \leq r < b$.
Es ist $b|a$ genau dann, wenn $r = 0$ ist.
Man nennt q auch den Quotienten und r den Rest der Division durch b.
Wir sagen auch: a läßt bei Division durch b den Rest r.

Beispiel 1.4.1. Für $a = 17$ und $b = 5$ erhalten wir: $17 = 3 \cdot 5 + 2$, also $q = 3$ und $r = 2$.
Die Zahl 17 läßt also bei Division durch 5 den Rest 2.

Satz 1.4.2. *(Euklidischer Algorithmus)*
Es seien $a, b \in \mathbb{Z}$, $b > 0$.
Durch wiederholte Anwendung der Division mit Rest erhält man eine Reihe von Gleichungen:

$$\begin{aligned}
a &= q_1 \cdot b + r_1, \quad 0 \leq r_1 < b \\
b &= q_2 \cdot r_1 + r_2, \quad 0 \leq r_2 < r_1 \\
r_1 &= q_3 \cdot r_2 + r_3, \quad 0 \leq r_3 < r_2 \\
&\vdots \quad\quad \vdots \\
r_{n-2} &= q_n \cdot r_{n-1} + r_n, \quad 0 \leq r_n < r_{n-1} \\
r_{n-1} &= q_{n+1} \cdot r_n
\end{aligned}$$

Dann ist r_n, also der letzte von 0 verschiedene Rest, der größte gemeinsame Teiler von a und b, es gilt somit $r_n = ggT(a, b)$. Durch sukzessives Auflösen der obigen Gleichungen nach r_i läßt sich r_n als ganzzahlige Linearkombination von a und b ausdrücken: $r_n = ax + by$ mit $x, y \in \mathbb{Z}$.

Beweis. Es gilt

$$\begin{aligned}
t|a, t|b \quad &\underset{S.1.1.1c)}{\Leftrightarrow} \quad t|b, t|a - q_1 b = r_1 \Leftrightarrow t|r_1, t|b - q_2 r_1 = r_2 \Leftrightarrow \ldots \Leftrightarrow t|r_{n-1}, t|r_n \\
&\underset{\substack{r_{n-1}=q_{n+1}r_n \\ S.1.1.1b)}}{\Leftrightarrow} \quad t|r_n.
\end{aligned}$$

□

Eng mit dem Euklidischen Algorithmus ist die Theorie der linearen Diophantischen Gleichungen verbunden. Der Begriff Diophantische Gleichung bezieht sich nicht auf die Form der Gleichung, sondern auf die Fragestellung: man interessiert sich nur für ganzzahlige Lösungen. Eine lineare Diophantische Gleichung ist eine der Gestalt $ax + by = c$ mit $a, b, c \in \mathbb{Z}$.

Satz 1.4.3. *Es seien $a, b, c \in \mathbb{Z}$ und a, b nicht beide gleich 0.*
Die lineare Diophantische Gleichung $ax + by = c$ ist genau dann lösbar, wenn $ggT(a, b)|c$.
Eine Lösung kann gefunden werden, indem man die Gleichung $ax + by = d$ mit $d = ggT(a, b)$ mit dem Euklidischen Algorithmus löst und die Lösung mit $\frac{c}{d}$ multipliziert.

Beispiel 1.4.2. Man bestimme den ggT von $a = 294$ und $b = 201$ und drücke ihn als ganzzahlige Linearkombination von a und b aus.

Lösung:
Der Euklidische Algorithmus ergibt:

$$\begin{aligned} 294 &= 201 + 93 \\ 201 &= 2 \cdot 93 + 15 \\ 93 &= 6 \cdot 15 + 3 \\ 15 &= 5 \cdot 3 \end{aligned}$$

Also ist $ggT(294, 201) = 3$.
Die Linearkombination wird durch sukzessive (rückwärtige) Auflösung der Gleichungskette erhalten:

$$\begin{aligned} 3 &= 93 - 6 \cdot 15 = 93 - 6 \cdot (201 - 2 \cdot 93) \\ &= 13 \cdot 93 - 6 \cdot 201 = 13 \cdot (294 - 201) - 6 \cdot 201 \\ &= 13 \cdot 294 - 19 \cdot 201 \end{aligned}$$

Eine Lösung der Diophantischen Gleichung $294x + 201y = 3$ ist also $x = 13$ und $y = -19$.

Beispiel 1.4.3. Finde eine Lösung der Diophantischen Gleichung $73685x + 25513y = 10$ oder zeige, daß sie unlösbar ist.

Lösung:
Der Euklidische Algorithmus ergibt:

$$\begin{aligned} 73685 &= 2 \cdot 25513 + 22659 \\ 25513 &= 1 \cdot 22659 + 2854 \\ 22659 &= 7 \cdot 2854 + 2681 \\ 2854 &= 1 \cdot 2681 + 173 \\ 2681 &= 15 \cdot 173 + 86 \\ 173 &= 2 \cdot 86 + 1 \\ 86 &= 86 \cdot 1 \end{aligned}$$

Also ist $ggT(73685, 25513) = 1$.

Wir lösen nun zunächst die Gleichung $73685x' + 25513y' = 1$:

$$\begin{aligned} 1 &= 173 - 2 \cdot 86 = 173 - 2 \cdot (2681 - 15 \cdot 173) \\ &= 31 \cdot 173 - 2 \cdot 2681 = 31 \cdot (2854 - 2681) - 2 \cdot 2681 \\ &= -33 \cdot 2681 + 31 \cdot 2854 = 31 \cdot 2854 - 33 \cdot (22659 - 7 \cdot 2854) \\ &= 262 \cdot 2854 - 33 \cdot 22659 = 262 \cdot (25513 - 22659) - 33 \cdot 22659 \\ &= -295 \cdot 22659 + 262 \cdot 25513 = -295 \cdot (73685 - 2 \cdot 25513) + 262 \cdot 25513 \\ &= -295 \cdot 73685 + 852 \cdot 25513 \end{aligned}$$

Die Diophantische Gleichung $73685x' + 25513y' = 1$ hat also die Lösung $x' = -295$ und $y' = 852$.
Eine Lösung von $73685x + 25513y = 10$ ergibt sich daraus durch Multiplikation mit 10:
$x = -2950$ und $y = 8520$.

In einer tabellarischen Darstellung sieht die Lösung folgendermaßen aus:

q_{i+1}	r_i	x_i	y_i
	73685	1	0
2	25513	0	1
1	22659	1	-2
7	2854	-1	3
1	2681	8	-23
15	173	-9	26
2	86	143	-413
86	1	-295	852

1.5 Kongruenzen

Die Division mit Rest ergibt eine Partition der Menge $\mathbb{Z}$ der ganzen Zahlen in Äquivalenzklassen, Restklassen oder Kongruenzklassen genannt.

Definition 1.5.1. Es sei $m \in \mathbb{N}$ und $a, b \in \mathbb{Z}$. Wir sagen a ist kongruent zu b modulo m, wenn $m|(b-a)$ gilt, und wir schreiben $a \equiv b \bmod m$ (bzw. $a \not\equiv b \bmod m$, falls $m \not| (b-a)$ ist). Für die Menge aller b mit $a \equiv b \bmod m$ schreiben wir $a \bmod m$. In diesem Zusammenhang nennt man m den Modul der Kongruenz $a \equiv b \bmod m$.

Satz 1.5.1. *Es seien $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$ und die Divisionen*

$$\begin{aligned} a &= q_1 m + r_1 \text{ mit } 0 \leq r_1 < m \\ b &= q_2 m + r_2 \text{ mit } 0 \leq r_2 < m \end{aligned}$$

durch m mit Rest vorgelegt. Dann gilt $a \equiv b \bmod m$ genau dann, wenn $r_1 = r_2$ ist.

Bemerkung 1.5.1. Zwei Zahlen $a, b \in \mathbb{Z}$ sind also genau dann kongruent modulo m, wenn sie bei der Division durch m den gleichen Rest haben.

Definition 1.5.2. Zwei Zahlen gehören zur selben Kongruenzklasse oder Restklasse modulo m, falls sie modulo m kongruent sind.

Satz 1.5.2. *Es sei $m \in \mathbb{N}$. Dann gibt es genau m Kongruenzklassen modulo m. Jede ganze Zahl ist zu genau einer der Zahlen $0, 1, \ldots, m-1$ kongruent.*

Beispiel 1.5.1. Die Kongruenzklassen modulo 2 sind

$$\begin{aligned} 0 \bmod 2 &= \{\ldots, -4, -2, 0, 2, 4, \ldots\} \text{ (gerade Zahlen)} \\ 1 \bmod 2 &= \{\ldots, -3, -1, 1, 3, 5, \ldots\} \text{ (ungerade Zahlen).} \end{aligned}$$

Die Kongruenzklassen modulo 10 sind

$$\begin{aligned} 0 \bmod 10 &= \{\ldots, -20, -10, 0, 10, 20, \ldots\} \\ 1 \bmod 10 &= \{\ldots, -19, -9, 1, 11, 21, \ldots\} \\ &\vdots \quad\quad \vdots \\ 9 \bmod 10 &= \{\ldots, -11, -1, 9, 19, 29, \ldots\} \end{aligned}$$

Allgemein sind Kongruenzklassen modulo m arithmetische Progressionen der Form

$$a \bmod m = \{\ldots, a-3m, a-2m, a-m, a, a+m, a+2m, \ldots\}$$

Definition 1.5.3. Es sei $m \in \mathbb{N}$. Die Menge aller Restklassen modulo m bezeichnen wir mit $\mathbb{Z}/m\mathbb{Z}$.

Es ist möglich, Restklassen zu addieren und zu multiplizieren:
Die Addition läßt sich einfach auf geometrische Weise veranschaulichen. Wickelt man die Zahlengerade über einem Kreis des Umfangs m auf, so bestehen Restklassen mod m genau aus den Zahlen, die über demselben Punkt des Kreises zu liegen kommen.
Die Summe $a \bmod m + b \bmod m$ erhält man, indem man auf dem Kreis nacheinander a Schritte und b Schritte in die negative Richtung geht.

Beispiel 1.5.2. Das Rechnen mit Uhrzeiten bedeutet Rechnen mit Restklassen mod 24 oder bei der alten Weise, bei der die Stunden nur von $1-12$ numeriert werden, Rechnen mit Restklassen mod 12. Welche Uhrzeit haben wir sieben Stunden nach 9 Uhr? Die Antwort erhalten wir, wenn wir den Stundenzeiger von 9 Uhr um sieben Stunden im Uhrzeigersinn (dem negativen Sinn) bewegen: 4 Uhr. Mittels Addition von Restklasen ergibt sich das Resultat wie folgt:

$$9 \bmod 12 + 7 \bmod 12 = 4 \bmod 12.$$

Beispiel 1.5.3. Das Rechnen mit Wochentagen bedeutet Rechnung mit Restklassen mod 7:
Der 2. November 2010 ist ein Dienstag. Auf welchen Wochentag fällt der 24. November 2010?
Lösung:
Ordnen wir die Sonntage der Restklasse 0 mod 7 zu, so gehört der 2. November zur Restklasse 2 mod 7. Die Aufgaben läuft auf die Addition $2 \bmod 7 + 22 \bmod 7 = 2 \bmod 7 + 1 \bmod 7 = 3 \bmod 7$ hinaus. Der 24. November 2010 fällt also auf einen Mittwoch.

Addition und Multiplikation von Restklassen können mit Hilfe von Verknüpfungstafeln tabelliert werden:

Beispiel 1.5.4. $m = 5$:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

und

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

1.6 Das multiplikative Inverse

Definition 1.6.1. (multiplikatives Inverses)
Es sei $m \in \mathbb{N}$ und $a \in \mathbb{Z}$. Es heißt $x \bmod m$ muliplikatives Inverses von $a \bmod m$, falls $ax \equiv 1 \bmod m$ ist.
Wir schreiben dann auch $x \bmod m = a^{-1} \bmod m$.

Beispiel 1.6.1. Die Multiplikationstafel in Beispiel 1.5.4 zeigt, daß das multiplikative Inverse von $2 \bmod 5$ gerade $3 \bmod 5$ ist. Also gilt $2^{-1} \bmod 5 = 3 \bmod 5$.

Das multiplikative Inverse braucht nicht immer zu existieren. Näheres ergibt sich aus dem folgenden

Satz 1.6.1. *Es sei $m \in \mathbb{N}$ und $a \in \mathbb{Z}$. Das multiplikative Inverse $a^{-1} \bmod m$ existiert genau dann, wenn $ggT(a, m) = 1$ ist.*
Zur Berechnung des multiplikativen Inversen von $a \bmod m$ löst man die Diophantische Gleichung $ax + by = 1$ mit $b = m$ nach dem in Satz 1.4.3 beschriebenen Verfahren. Dann ist $x \bmod m = a^{-1} \bmod m$.

Beispiel 1.6.2. Bestimme das multiplikative Inverse von 23 mod 79.
Lösung:
Wir müssen die Diophantische Gleichung

$$23x + 79y = 1 \qquad (*)$$

lösen.
Der Euklidische Algorithmus ergibt

$$\begin{aligned} 79 &= 3 \cdot 23 + 10 \\ 23 &= 2 \cdot 10 + 3 \\ 10 &= 3 \cdot 3 + 1 \end{aligned}$$

Auflösen der Gleichungen ergibt

$$1 = 10 - 3 \cdot 3 = 10 - 3 \cdot (23 - 2 \cdot 10) = 7 \cdot 10 - 3 \cdot 23 = 7 \cdot (79 - 3 \cdot 23) - 3 \cdot 23 = 7 \cdot 79 - 24 \cdot 23$$

Eine Lösung von $(*)$ ist also durch $x = -24$ und $y = 7$ gegeben.
Das multiplikative Inverse von 23 mod 79 ist also $23^{-1} \bmod 79 = -24 \bmod 79 = 55 \bmod 79$.

1.7 Das Rechnen mit Kongruenzen

Kongruenzen machen eine Aussage über die Gleichheit von Restklassen und haben daher viel mit Gleichungen gemeinsam. Man kann mit ihnen weitgehend wie mit Gleichungen rechnen; es gibt jedoch auch Unterschiede. Dies wollen wir im folgenden diskutieren.

Satz 1.7.1. *Es seien $a, b, c, d, m \in \mathbb{Z}$, $m > 0$ mit $a \equiv b \bmod m$ und $c \equiv d \bmod m$. Dann ist*

$$\begin{aligned} a + c &\equiv b + d \mod m \\ a - c &\equiv b - d \mod m \\ a \cdot c &\equiv b \cdot d \mod m \end{aligned}$$

Gemeinsame Faktoren können in Kongruenzen nicht immer gekürzt werden:

Beispiel 1.7.1. Es ist $3 \cdot 5 \equiv 3 \cdot 2 \bmod 9$, aber nicht $5 \equiv 2 \bmod 9$.

Gemeinsame Faktoren können jedoch gekürzt werden, wenn man zu einem anderen Modul übergeht:

Satz 1.7.2. *Es seien $a, b, c, m \in \mathbb{Z}$, $m > 0$ und $d = ggT(c, m)$ und $ac \equiv bc \bmod m$.*
Dann ist $a \equiv b \bmod m/d$.
Spezialfall: Ist $ac \equiv bc \bmod m$ und $ggT(c, m) = 1$, so ist $a \equiv b \bmod m$.

Als Spezialfall von Satz 1.7.1 ergibt sich

Satz 1.7.3. *Es seien $a, b, m \in \mathbb{Z}$, $m > 0$.*
Aus $a \equiv b \bmod m$ folgt $a^k \equiv b^k \bmod m$ für $k \geq 1$.

Satz 1.7.3 erlaubt es, die Restklasse von a^k auch für große Werte von k zu bestimmen. Dazu wird k als Summe von Zweierpotenzen geschrieben. Die Restklassen von a^{2^δ} werden durch wiederholtes Quadrieren bestimmt.

Beispiel 1.7.2. Man bestimme $7^{52} \mod 53$.
Lösung:
Es ist $52 = 32 + 16 + 4$. Man berechnte 7^{32}, 7^{16} und 7^4 durch wiederholtes Quadrieren:

$$\begin{aligned} 7^2 &\equiv 49 \equiv -4 \bmod 53 \\ 7^4 &\equiv (-4)^2 \equiv 16 \bmod 53 \\ 7^8 &\equiv 16^2 \equiv -9 \bmod 53 \\ 7^{16} &\equiv (-9)^2 \equiv -25 \bmod 53 \\ 7^{32} &\equiv (-25)^2 \equiv -11 \bmod 53, \end{aligned}$$

also $7^{52} \equiv 7^{32} \cdot 7^{16} \cdot 7^4 \equiv (-11) \cdot (-25) \cdot 16 \equiv 275 \cdot 16 \equiv 10 \cdot 16 \equiv 1 \bmod 53$.

1.8 Elementare Teilbarkeitsregeln

Die elementaren Teilbarkeitsregeln lassen sich durch Rechnen mit Kongruenzen leicht beweisen. Wir legen unseren Überlegungen die Darstellung natürlicher Zahlen im Dezimalsystem zugrunde.

Satz 1.8.1. *Jede natürliche Zahl $n \in \mathbb{N}$ kann eindeutig geschrieben werden als $n = \sum_{k=0}^{m} a_k 10^k$ mit $a_k \in \{0, 1, \ldots, 9\}$ und $a_m \neq 0$. Die a_k heißen die Ziffern von n (im Dezimalsystem).*

Beispiel 1.8.1.

$$n = 283967 = 2 \cdot 10^5 + 8 \cdot 10^4 + 3 \cdot 10^3 + 9 \cdot 10^2 + 6 \cdot 10 + 7.$$

Definition 1.8.1. Unter der Quersumme einer Zahl $n = \sum_{k=0}^{m} a_k 10^k$ mit Ziffern a_k versteht man $Q(n) = \sum_{k=0}^{m} a_k$.

Unter der alternierenden Quersumme versteht man $AQ(n) = \sum_{k=0}^{m} (-1)^k a_k$.

Satz 1.8.2. (a) *Eine natürliche Zahl n ist genau dann durch 2 teilbar (gerade), wenn die letzte Ziffer durch 2 teilbar (gerade) ist.*

(b) *Eine Zahl n ist genau dann durch 5 teilbar, wenn die letzte Ziffer 0 oder 5 ist.*

(c) *Eine Zahl n ist genau dann durch 3 teilbar, wenn ihre Quersumme durch 3 teilbar ist.*

(d) *Eine Zahl n ist genau dann durch 9 teilbar, wenn ihre Quersumme durch 9 teilbar ist.*

(e) *Eine Zahl n ist genau dann durch 11 teilbar, wenn ihre alternierende Quersumme durch 11 teilbar ist.*

Beweis. Wir nehmen $n = \sum_{k=0}^{m} a_k 10^k$, $a_k \in \{0, 1, \ldots, 9\}$ und $a_m \neq 0$ an.

(a) Wegen $10^k \equiv \begin{cases} 0 \mod 2, & \text{für } k \geq 1 \\ 1 \mod 2, & \text{für } k = 0 \end{cases}$ folgt $n \equiv a_0 \mod 2$.

(b) Wegen $10^k \equiv \begin{cases} 0 \mod 5, & \text{für } k \geq 1 \\ 1 \mod 5, & \text{für } k = 0 \end{cases}$ folgt $n \equiv a_0 \mod 5$.

(c) Es ist $10 \equiv 1 \bmod 3$. Nach Satz 1.7.3 folgt $10^k \equiv 1 \bmod 3$. Damit ist nach Satz 1.7.1 dann $n = \sum_{k=0}^{m} a_k 10^k = \sum_{k=0}^{m} a_k \bmod 3$.

(d) Es ist $10 \equiv 1 \bmod 9$. Die Behauptung folgt wie in c), wenn Kongruenzen mod 3 durch Kongruenzen mod 9 ersetzt werden.

(e) Es ist $10 \equiv -1 \bmod 11$. Nach Satz 1.7.3 folgt $10^k \equiv (-1)^k \bmod 11$.
Damit ist $n = \sum_{k=0}^{m} a_k 10^k = \sum_{k=0}^{m} (-1)^k a_k \bmod 11$.

□

1.9 Restsysteme, teilerfremde Restklassen, Eulersche φ- Funktion

Wir haben in Satz 1.5.2 gesehen, daß es genau m Kongruenzklassen modulo m gibt und daß jede ganze Zahl zu genau einer der Zahlen $0, 1, \ldots, m-1$ kongruent ist. Jede Restklasse mod m wird also durch genau ein Element der Menge $R_m = \{0, 1, \ldots, m-1\}$ repräsentiert. Die Menge R_m ist ein (wichtiger) Spezialfall eines vollständigen Restsystems modulo m.

Definition 1.9.1. Ein vollständiges Restsystem mod m ist eine Menge ganzer Zahlen, so daß jede ganze Zahl zu genau einer dieser Zahlen der Menge kongruent mod m ist.

Beispiel 1.9.1. Das vollständige Restsystem $\{0, 1, \ldots, m-1\}$ heißt auch die Menge der kleinsten nichtnegativen Reste mod m.
Es sei m eine ungerade positive Zahl. Dann ist die Menge der absolut kleinsten Reste
$\{-\frac{m-1}{2}, -\frac{m-3}{2}, \ldots, -1, 0, 1, \ldots, \frac{m-3}{2}, \frac{m-1}{2}\}$ ein vollständiges Restsystem mod m.
Für $m = 5$ ist also die Menge der kleinsten nichtnegativen Reste mod 5 die Menge $\{0, 1, 2, 3, 4\}$, und die Menge der absolut kleinsten Reste mod 5 ist die Menge $\{-2, -1, 0, 1, 2\}$.
Ein weiteres vollständiges Restsystem mod 5 ist die Menge $\{100, -24, 12, 33, -71\}$.

Eine wichtige Frage ist nun: Welchen größten gemeinsamen Teiler beitzen die Elemente eines vollständigen Restsystems mod m mit dem Modul m?

Beispiel 1.9.2. $m = 12$:

a	0	1	2	3	4	5	6	7	8	9	10	11
$ggT(a, 12)$	12	1	2	3	4	1	6	1	4	3	2	1

Der $ggT(a, 12)$ hängt nur von der Restklasse a mod 12 ab:
Für alle Elemente von 0 mod 12 $= \{\ldots, -12, 0, 12, 24, 36, \ldots\}$ ist $ggT(a, 12) = 12$.
Für alle Elemente von 3 mod 12 $= \{\ldots, -9, 3, 15, 27, \ldots\}$ ist $ggT(a, 12) = 3$.
Es ist $ggT(a, 12) = 1$ für die Elemente der vier teilerfremden Restklassen 1 mod 12, 5 mod 12, 7 mod 12 und 11 mod 12.

Diese Tatsachen ergeben sich als Spezialfall aus

Satz 1.9.1. *Es sei $m \in \mathbb{N}$. Ist $a \equiv b$ mod m, so ist $ggT(a, m) = ggT(b, m)$, d.h. $ggT(a, m) = ggT(b, m)$ für alle $b \in a$ mod m.*

Definition 1.9.2. Es sei $m \in \mathbb{N}$. Gilt $ggT(b, m) = 1$ für ein Element $b \in a$ mod m (und damit auch für alle Elemente), so heißt a mod m eine teilerfremde Restklasse mod m. Die Anzahl der teilerfremden Restklassen wird mit $\varphi(m)$ bezeichnet. Dabei heißt $\varphi(m)$ Eulersche φ- Funktion.
Ein reduziertes Restsystem mod m ist darüberhinaus eine Menge ganzer Zahlen, so daß jede zu m teilerfremde ganze Zahl zu genau einer dieser Zahlen der Menge kongruent ist.

Beispiel 1.9.3. Beispiel 1.9.2 zeigt, daß $\varphi(12) = 4$ ist. Ein reduziertes Restsystem ist durch $\{1, 5, 7, 11\}$ gegeben. Ein anderes reduziertes Restsystem ist $\{-23, 17, 31, 47\}$.

1.10 Lineare Kongruenzen

Es seien $a, b, m \in \mathbb{Z}$ mit $m > 0$. Wir suchen alle ganzen Zahlen x, welche die lineare Kongruenz

$$ax \equiv b \bmod m \qquad (*)$$

erfüllen.
Ob x eine Lösung von $(*)$ ist, hängt nur von der Restklasse mod m von x ab: $(*)$ wird entweder von allen Elementen einer Restklasse mod m gelöst oder von keinem. Alles läuft daher auf die Frage hinaus: Welche Restklassen sind Lösungen? Man spricht auch von Lösungen mod m.

Satz 1.10.1. *Es seien $a, b, m \in \mathbb{Z}$ mit $m > 0$ und $d = ggT(a, m)$. Dann ist die Kongruenz $ax \equiv b$ mod m genau dann lösbar, wenn $d|b$. Ist diese Bedingung erfüllt, so bilden die Lösungen eine arithmetische Progression mit Differenz m/d. Es gibt also d Lösungen mod m.*

Bemerkung 1.10.1. Im Falle der Lösbarkeit können die Lösungen mittels Satz 1.7.2 erhalten werden:
Die Kongruenz $ax \equiv b$ mod m ist äquivalent zu $a/d\ x \equiv b/d$ mod m/d.
Die Kongruenz kann gelöst werden, in dem man mit der Methode von Abschnitt 2.2 das multiplikative Inverse von a/d mod m/d bestimmt- bei kleinen Werten von m/d auch durch Probieren.

Beispiel 1.10.1.

$$15x \equiv 6 \bmod 21 \qquad (1)$$

Es ist $a = 15$, $b = 6$ und $m = 21$. Also ist $d = ggT(15, 21) = 3$, somit $d|6$.
Nach Satz 1.7.2 (oder Bemerkung 1.10.1) ist (1) äquivalent zu

$$5x \equiv 2 \bmod 7. \qquad (2)$$

Das multiplikative Inverse von 5 mod 7 ergibt sich als

$$5^{-1} \bmod 7 = 3 \bmod 7,$$

da $5 \cdot 3 \equiv 1$ mod 7.
Damit ist $x \equiv 2 \cdot 5^{-1}$ mod $7 \equiv 2 \cdot 3$ mod $7 \equiv 6$ mod 7 die eindeutige Lösung von (2). Die Lösungen der ursprünglichen Kongruenz (1) sind die drei Restklassen 6 mod 21, 13 mod 21 und 20 mod 21. Deren Elemente ergeben schließlich zusammen die arithmetische Progression $\{\ldots, -15, -8, -1, 6, 13, 20, \ldots\}$ mit der Differenz $m/d = 7$.

1.11 Der Chinesische Restsatz

Der Chinesische Restsatz befaßt sich mit Systemen von Kongruenzen.

Beispiel 1.11.1. Es sei $N = 35 = 5 \cdot 7$.
Erfüllt eine ganze Zahl m eine Kongruenz $\mod 35$, so erfüllt m auch ein Paar von Kongruenzen, eine Kongruenz $\mod 5$ und eine Kongruenz $\mod 7$.
Ist z. B.

$$m \equiv 13 \bmod 35, \tag{1}$$

so folgt

$$\begin{cases} m \equiv 3 \bmod 5 \\ m \equiv 6 \bmod 7. \end{cases} \tag{2}$$

Die folgende Tabelle zeigt, daß auch (1) aus (2) folgt. Schärfer gilt, daß jedem Paar von Restklassen ($a \mod 5$, $b \mod 7$) genau eine Restklasse $c \mod 35$ entspricht.

mod 5 \	0	1	2	3	4	5	6	... mod 7
0	0	15	30	10	25	5	20	
1	21	1	16	31	11	26	6	
2	7	22	2	17	32	12	27	
3	28	8	23	3	18	33	13	
4	14	29	9	24	4	19	34	

Jede Restklasse $\mod 35$ hat somit zwei Komponenten, eine (mod 7)- Komponente und eine (mod 5)- Komponente. Eine ähnliche Situation besteht in der Vektorrechnung: jeder Punkt der Ebene kann mit einem Koordinatenpaar (x, y) oder auch dem Vektor $\vec{v} = (x, y)$ identifiziert werden. Mit Vektoren kann komponentenweise gerechnet werden: Für $\vec{v}_1 = (x_1, y_1)$ und $\vec{v}_2 = (x_2, y_2)$ ist $\vec{v}_1 + \vec{v}_2 = (x_1 + x_2, y_1 + y_2)$.
Dieses „komponentenweise“ Rechnen ist auch bei Kongruenzen möglich:

Beispiel 1.11.2. Man bestimme das Produkt

$$(23 \bmod 35) \cdot (29 \bmod 35).$$

Lösung:
Aus der obigen Tabelle erhalten wir die Entsprechungen

$$\begin{aligned} 23 \bmod 35 &\Leftrightarrow (2 \bmod 7,\ 3 \bmod 5) \\ 29 \bmod 35 &\Leftrightarrow (1 \bmod 7,\ 4 \bmod 5) \end{aligned}$$

Komponentenweises Rechnen ergibt

$$(2 \bmod 7,\ 3 \bmod 5) \cdot (1 \bmod 7,\ 4 \bmod 5) = (2 \bmod 7,\ 2 \bmod 5).$$

Mit der Entsprechung

$$2 \bmod 35 \Leftrightarrow (2 \bmod 7,\ 2 \bmod 5).$$

erhalten wir

$$(23 \bmod 35) \cdot (29 \bmod 35) = 2 \bmod 35.$$

Wir formulieren nun den Chinesischen Restsatz allgemein und geben auch einen Algorithmus, der ein System von Kongruenzen zu einer einzelnen Kongruenz reduziert.

Satz 1.11.1. *(Chinesischer Restsatz) Es seien $m_1, m_2, \ldots, m_r$ natürliche Zahlen, die paarweise teilerfremd sind und $a_1, a_2, \ldots, a_r$ ganze Zahlen. Dann besitzen die r Kongruenzen*

$$\begin{aligned} x &\equiv a_1 \mod m_1 \\ x &\equiv a_2 \mod m_2 \\ &\vdots \\ x &\equiv a_{r-1} \mod m_{r-1} \\ x &\equiv a_r \mod m_r \end{aligned}$$

eine gemeinsame Lösung.
Diese ist nach dem Modul

$$m = m_1 \cdot m_2 \cdots m_r$$

eindeutig bestimmt.
Eine Lösung kann in der Form

$$x_0 = \sum_{j=1}^{r} M_j M_j^{-1} a_j$$

erhalten werden, wobei

$$M_j := \frac{m}{m_j}, \quad \textit{und} \quad M_j M_j^{-1} \equiv 1 \mod m_j$$

ist.

Beispiel 1.11.3. Gesucht ist die kleinste natürliche Zahl x mit

$$\begin{aligned} x &\equiv 4 \mod 7 \\ x &\equiv 1 \mod 11 \\ x &\equiv 6 \mod 13 \end{aligned}$$

Lösung:
Mit den Bezeichnungen von Satz 1.11.1 ist $m_1 = 7$, $m_2 = 11$, $m_3 = 13$, $m = 7 \cdot 11 \cdot 13 = 1001$, $a_1 = 4$, $a_2 = 1$ und $a_3 = 6$. Weiter ist

$$\begin{aligned} M_1 &:= \frac{m}{m_1} = 143 \\ M_2 &:= \frac{m}{m_2} = 91 \\ M_3 &:= \frac{m}{m_3} = 77. \end{aligned}$$

Die Bestimmung der multiplikativen Inversen M_j^{-1} ist wiederum mit der Methode von Abschnitt 2.2, also dem Euklidischen Algorithmus möglich. Da in unserem speziellen Beispiel die Moduln $m_1 = 7$, $m_2 = 11$ und $m_3 = 13$ klein sind, können hier die Lösungen auch durch Probieren gefunden werden:

$$\begin{aligned} 143 \cdot M_1^{-1} \equiv 1 \mod 7 &\Leftrightarrow 3 \cdot M_1^{-1} \equiv 1 \mod 7, \text{ also } M_1^{-1} \equiv -2 \mod 7 \\ 91 \cdot M_2^{-1} \equiv 1 \mod 11 &\Leftrightarrow 3 \cdot M_2^{-1} \equiv 1 \mod 11, \text{ also } M_2^{-1} \equiv 4 \mod 11 \\ 77 \cdot M_3^{-1} \equiv 1 \mod 13 &\Leftrightarrow -M_3^{-1} \equiv 1 \mod 13, \text{ also } M_3^{-1} \equiv -1 \mod 13. \end{aligned}$$

Wir erhalten die Lösung

$$x_0 = \sum_{j=1}^{3} M_j M_j^{-1} a_j = 143 \cdot (-2) \cdot 4 + 91 \cdot 4 \cdot 1 + 77 \cdot (-1) \cdot 6 = -1242.$$

Die allgemeine Lösung hat die Form

$$x = x_0 + k \cdot m = -1242 + 1001k.$$

Die kleinste positive Lösung erhalten wir für $k = 2$, nämlich $x = 760$.

1.12 Berechnung der Eulerschen φ- Funktion, Multiplikativität

Auch die Frage, welche Restklassen eines vollständigen Restsystems reduziert sind, kann mit der Idee des „komponentenweisen Rechnens“, also des Chinesischen Restsatzes beantwortet werden.
Wir kehren zu unserem alten Beispiel $N = 35 = 5 \cdot 7$ zurück. Es ist genau dann $ggT(a, 35) = 1$, wenn $ggT(a, 7) = 1$ und $ggT(a, 5) = 1$ ist. Es gilt $ggT(a, 5) = 1$, wenn die Restklasse a mod 5 nicht in der ersten Zeile der Tabelle in Abschnitt 1.11 zu finden ist, und es gilt $ggT(a, 7) = 1$, wenn die Restklasse a mod 7 nicht in der ersten Spalte besagter Tabelle zu finden ist.
Für die Wahl der Zeilen haben wir also $\varphi(5) = 4$ Möglichkeiten und für die Wahl des Spalten $\varphi(7) = 6$ Möglichkeiten.
Es ist somit

$$\varphi(35) = \varphi(5 \cdot 7) = \varphi(5) \cdot \varphi(7) = 24.$$

Diese Multiplikativität gilt für die Eulersche φ- Funktion allgemein.

Definition 1.12.1. Eine Abbildung $f : \mathbb{N} \to \mathbb{C}$ heißt zahlentheoretische (oder arithmetische) Funktion.
Diese Funktion f heißt additiv, falls

$$f(m \cdot n) = f(m) + f(n) \tag{1}$$

für alle $m, n \in \mathbb{N}$ mit $ggT(m, n) = 1$ gilt.
Sie heißt vollständig additiv, falls (1) ohne Einschränkung gilt.

Die Funktion f heißt multiplikativ, falls

$$f(m \cdot n) = f(m) \cdot f(n) \tag{2}$$

für alle $m, n \in \mathbb{N}$ mit $ggT(m, n) = 1$ gilt.
Sie heißt vollständig multiplikativ, falls (2) ohne Einschränkung gilt.

Satz 1.12.1. *Es sei $n = p_1^{\gamma_1} \cdots p_r^{\gamma_r}$ die kanonische Primfaktorzerlegung von n. Ist f additiv, so ist $f(1) = 0$ und $f(n) = f(p_1^{\gamma_1}) + \ldots + f(p_r^{\gamma_r})$. Ist f multiplikativ, so ist $f(1) = 1$ und $f(n) = f\left(p_1^{\gamma_1}\right) \cdots f\left(p_r^{\gamma_r}\right)$.*
Dies läßt sich nun auf die Eulersche φ- Funktion anwenden. Wir betrachten zuerst ihre Werte für Primzahlpotenzen p^γ. Von der Menge der kleinsten nichtnegativen Reste $\{0, 1, \ldots, p^\gamma - 1\}$ sind genau die $p^{\gamma-1}$ Vielfachen von p nicht teilerfremd zum Modul p^γ. Also ist

$$\varphi\left(p^\gamma\right) = p^\gamma - p^{\gamma-1} = p^\gamma \cdot \left(1 - \frac{1}{p}\right). \tag{1}$$

Ist $n = p_1^{\gamma_1} \cdots p_r^{\gamma_r}$, so folgt aus der Multiplikativität von φ:

$$\varphi(n) = p_1^{\gamma_1} \cdot \left(1 - \frac{1}{p_1}\right) \cdots p_r^{\gamma_r} \cdot \left(1 - \frac{1}{p_r}\right) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right) = n \cdot \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

Satz 1.12.2. *Die Eulersche φ- Funktion ist multiplikativ. Es ist $\varphi(1) = 1$. Ist $n = p_1^{\gamma_1} \cdots p_r^{\gamma_r}$ die kanonische Primfaktorzerlegung von n, so ist*

$$\varphi(n) = \left(p_1^{\gamma_1} - p_1^{\gamma_1 - 1}\right) \cdots \left(p_r^{\gamma_r} - p_r^{\gamma_r - 1}\right) = n \cdot \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

Beispiel 1.12.1. Man bestimme $\varphi(9000)$.

Lösung:
Es ist $9000 = 2^3 \cdot 3^2 \cdot 5^3$.
Also ist $\varphi(9000) = \left(2^3 - 2^2\right) \cdot \left(3^2 - 3\right) \cdot \left(5^3 - 5^2\right) = 2400$.

1.13 Die Sätze von Euler und Fermat

Der kleine Satz von Fermat (Pierre de Fermat, ca. 1607-1665) wurde etwa 100 Jahre vor dem Satz von Euler (Leonhard Euler, 1707-1783) gefunden und ist einfacher zu formulieren. Jedoch ist der kleine Satz von Fermat ein Spezialfall des Satzes von Euler.

Satz 1.13.1. *(Satz von Euler)*
Es sei $m \in \mathbb{N}$, $a \in \mathbb{Z}$ und $ggT(a, m) = 1$. Dann ist

$$a^{\varphi(m)} \equiv 1 \bmod m.$$

Spezialfall (kleiner Fermat):
Es sei p eine Primzahl und $a \in \mathbb{Z}$ nicht durch p teilbar. Dann ist

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

Der Beweis des Satzes von Euler bietet eine gute Gelegenheit zur Anwendung der Konzepte der letzten Abschnitte.

Lemma 1.13.1. *Es sei $m \in \mathbb{N}$ und $R_1 = \{r_1, \ldots, r_{\varphi(m)}\}$ ein reduziertes Restsystem* mod m *und $ggT(a, m) = 1$. Dann ist auch $R_2 = \{ar_1, \ldots, ar_{\varphi(m)}\}$ ein reduziertes Restsystem* mod m.

Bemerkung 1.13.1. Eine entsprechende Behauptung gilt auch für vollständige Restsystem mod m.

Beweis. (Beweis von Lemma 1.13.1:)
Wegen $ggT(a, m) = 1$ folgt nach Satz 1.7.2:

$$ar_i \equiv ar_j \bmod m \Leftrightarrow r_i \equiv r_j \bmod m.$$

Damit sind die teilerfremden Restklassen $(ar_1) \bmod m, \ldots, (ar_{\varphi(m)}) \bmod m$ alle voneinander verschieden. Da die Gesamtzahl aller teilerfremden Restklassen $\varphi(m)$ ist, ist durch R_2 jede von ihnen genau einmal vertreten. □

Beweis. (Beweis von Satz 1.13.1:)
Es sei $R_1 = \{r_1, \ldots, r_{\varphi(m)}\}$ ein reduziertes Restsystem. Damit ist nach Lemma 1.13.1 aber auch $R_2 = \{ar_1, \ldots, ar_{\varphi(m)}\}$ ein reduziertes Restsystem.
Somit folgt

$$\begin{aligned} ar_1 &\equiv r_{i_1} \bmod m \\ ar_2 &\equiv r_{i_2} \bmod m \\ \vdots &\quad \vdots \\ ar_{\varphi(m)} &\equiv r_{i_{\varphi(m)}} \bmod m \end{aligned}$$

wobei die Folge $(i_1, i_2, \ldots, i_{\varphi(m)})$ eine Umordnung der Folge $(1, 2, \ldots, \varphi(m))$ ist. Multiplikation der obigen Kongruenzen ergibt somit

$$a^{\varphi(m)}(r_1 \cdots r_{\varphi(m)}) \equiv (r_1 \cdots r_{\varphi(m)}) \bmod m.$$

Da das Produkt $(r_1 \cdots r_{\varphi(m)})$ teilerfremd zu m ist, kann es gekürzt werden. Wir erhalten

$$a^{\varphi(m)} \equiv 1 \bmod m.$$

□

1.14 Algebraische Grundstrukturen

Definition 1.14.1. Es sei $X \neq \emptyset$. Auf X sei eine (innere) Verknüpfung $\circ$, d.h. eine Abbildung $\circ : X \times X \to X,\ (x, y) \to x \circ y$ definiert.

1. Es heißt $(X, \circ)$ eine Halbgruppe, falls die Verknüpfung $\circ$ dem Assoziativgesetz genügt:

$$\forall x, y, z \in X :\ (x \circ y) \circ z = x \circ (y \circ z).$$

2. Ein $e \in X$ heißt neutrales Element der Halbgruppe, falls $e \circ x = x \circ e = x$ für alle $x \in X$ gilt.

3. Ein $x \in X$ heißt Einheit, falls es ein Inverses $x^{-1} \in X$ mit $x \circ x^{-1} = x^{-1} \circ x = e$ gibt.

4. Die Struktur $(X, \circ)$ heißt abelsche oder kommutative Halbgruppe, falls $x \circ y = y \circ x$ für alle $x, y \in X$ gilt.

5. Jede Halbgruppe mit neutralem Element, die nur Einheiten besitzt, heißt Gruppe.

Beispiel 1.14.1. $(\mathbb{N}, +)$ besitzt die einzige Einheit 0, ist also keine Gruppe, sondern nur eine kommutative Halbgruppe.
$(\mathbb{Z}, +)$ ist hingegen eine kommutative Gruppe- mit neutralem Element 0 und den Negativen $-a$ als Inverse zu $a \in \mathbb{Z}$.
$(\mathbb{N}, \cdot)$ und $(\mathbb{Z}, \cdot)$ sind kommutative Halbgruppen mit neutralem Element 1, aber keine Gruppen.

Bemerkung 1.14.1. Es ist üblich, die Verknüpfung nur dann mit + zu bezichnen, also als Addition zu betrachten, wenn sie kommutativ ist. Existiert ein neutrales Element, so nennt man es 0. Zur Bezeichnung der Inversen verwendet man das Minuszeichen.

Wir kommen nun zu Strukturen mit zwei inneren Verknüpfungen:

Definition 1.14.2. Es sei $X \neq \emptyset$ eine Menge mit zwei inneren Verknüpfungen, der Addition $+$ und der Multiplikation $\cdot$. Dann definiert man

1. $(X, +, \cdot)$ heißt ein Ring, falls gilt:
   (a) $(X, +)$ ist eine abelsche Gruppe
   (b) $(X, \cdot)$ ist eine Halbgruppe
   (c) es gelten die Distributivgesetze $(a + b) \cdot c = (a \cdot c) + (a \cdot b)$ und $c \cdot (a + b) = (c \cdot a) + (c \cdot b)$ für alle $a, b, c \in X$.

5. Das neutrale Element von $(X, +)$ heißt Null (Schreibweise: 0).

6. Besitzt $(X, \cdot)$ ein neutrales Element, so heißt dieses Eins (Schreibweise: 1).

7. Ist $(X, \cdot)$ abelsch, so heißt $(X, +, \cdot)$ ein kommutativer Ring.

8. Der Ring $(X, +, \cdot)$ heißt nullteilerfrei, falls für alle $x, y \in X$ gilt
$$x \cdot y = 0 \Rightarrow x = 0 \text{ oder } y = 0.$$

9. Ein nullteilerfreier und kommutativer Ring, der mindestens zwei verschiedene Elemente enthält, heißt Integritätsring.

10. Ein Integritätsring mit 1, in dem jedes $a \neq 0$ eine (multiplikative) Einheit ist, heißt Körper.

Beispiel 1.14.2. $(\mathbb{N}, +, \cdot)$ ist kein Ring, da $(\mathbb{N}, +)$ keine Gruppe ist.
Weiter ist $(\mathbb{Z}, +\cdot)$ ein Integritätsring mit 1, aber kein Körper. Die einzigen multiplikativen Einheiten sind 1 und -1.
Es sind $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ bzw. $(\mathbb{C}, +, \cdot)$ die Körper der rationalen, reellen bzw. komplexen Zahlen.

1.15 Beispiele in der Zahlentheorie

Es sei $m \in \mathbb{N}$.
Es ist klar, daß die Restklassenmenge $\mathbb{Z}/m\mathbb{Z}$ eine abelsche Gruppe bzgl. der Addition bildet. Das neutrale Element ist die Restklasse 0 mod m. Es bildet $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ einen kommutativen Ring, der die Restklasse 1 mod m als Einselement hat. Ist m keine Primzahl, so ist der Ring nicht nullteilerfrei. Ist $m = k \cdot l$ mit $1 < k < m$ und $1 < l < m$, so haben wir
$$(k \bmod m) \cdot (l \bmod m) = m \bmod m = 0 \bmod m.$$
Nach Satz 1.6.1 existiert dann das multiplikative Inverse genau dann, wenn a mod m eine reduzierte Restklassemod m ist, d.h. wenn $ggT(a, m) = 1$ ist.
Die Einheiten des Rings $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ sind also genau die reduzierten Restklassenmod m. Ihre Menge bildet eine Gruppe bzgl. der Multiplikation.

Definition 1.15.1. Für $m \in \mathbb{N}$ bezeichnen wir mit $(\mathbb{Z}/m\mathbb{Z})^*$ die Menge der Einheiten des Rings $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$, also
$$(\mathbb{Z}/m\mathbb{Z})^* = \{a \bmod m : \ ggT(a, m) = 1\}.$$
Offenbar hat $(\mathbb{Z}/m\mathbb{Z})^*$ genau $\varphi(m)$ Elemente.
Ist p eine Primzahl, so besteht $(\mathbb{Z}/m\mathbb{Z})^*$ aus allen Restklassen außer der 0- Restklasse 0 mod p. Damit ist aber $((\mathbb{Z}/p\mathbb{Z}), +, \cdot)$ ein endlicher Körper mit p Elementen.

Wir fassen unsere Beobachtungen zusammen:

Satz 1.15.1. *Es sei $m \in \mathbb{N}$. Dann ist $(\mathbb{Z}/m\mathbb{Z}, +)$ eine abelsche Gruppe mit m Elementen und neutralem Element $0 \bmod m$. Es ist weiterhin $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ ein kommutativer Ring mit Einselement $1 \bmod m$. Die Menge $((\mathbb{Z}/m\mathbb{Z})^*, \cdot)$ bildet eine abelsche Gruppe mit $\varphi(m)$ Elementen. Der Ring $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ ist genau dann ein Integritätsring und sogar ein Körper, wenn m eine Primzahl ist.*

1.16 Untergruppen, zyklische Gruppen, Ordnung und Primitivwurzel

Definition 1.16.1. Es sei $(G, \circ)$ eine Gruppe. Unter einer Untergruppe U von G versteht man eine Teilmenge $U \subseteq G$, die bzgl. der Verknüpfung $\circ$ ebenfalls eine Gruppe ist, d.h. $(U, \circ)$ ist eine Gruppe.
Schreibweise: $(U, \circ) \lhd (G, \circ)$.

Beispiel 1.16.1. Untergruppen der Gruppe $(\mathbb{Z}, +)$ sind alle Mengen der Gestalt

$$m\mathbb{Z} := \{m \cdot k : \ k \in \mathbb{Z}\},$$

wobei $m \in \mathbb{Z}$ fest gewählt ist.
Es ist

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

Definition 1.16.2. Es sei $(G, \circ)$ eine Gruppe und $\mathcal{M} \subseteq G$ eine Teilmenge von G. Unter $\langle \mathcal{M} \rangle$, der von $\mathcal{M}$ erzeugten Untergruppe von G (Schreibweise: $\langle \mathcal{M} \rangle$), versteht man die kleinste Untergruppe von G, die $\mathcal{M}$ enthält. Ist $\mathcal{M}$ eine einelementige Menge $\mathcal{M} = \{g\}$ mit $g \in G$, so schreibt man auch anstelle von $\langle \{g\} \rangle$ einfach $\langle g \rangle$.

Beispiel 1.16.2. Es sei $\mathcal{M} = \{9, 15\}$. Dann ist die von $\mathcal{M}$ erzeugte Untergruppe $\langle \mathcal{M} \rangle$ von $(\mathbb{Z}, +)$ gegeben durch

$$\langle \mathcal{M} \rangle = 3\mathbb{Z} = \{\ldots, -6, -3, 0, 3, 6, 9, \ldots\}.$$

Dies sieht man wie folgt:
$\langle \mathcal{M} \rangle$ muß wegen seiner Untergruppeneigenschaft mit 9 und 15 auch die Vielfachen $27 = 9 + 9 + 9$ und $30 = 15 + 15$, und mit 27 und 30 auch die Differenz $3 = 30 - 27$ enthalten.

Definition 1.16.3. Eine Gruppe heißt zyklisch, wenn G von einem einzigen Element erzeugt wird, d.h. wenn gilt, daß $G = \langle g \rangle$ für ein $g \in G$. Dann heißt g auch erzeugendes Element oder auch Erzeugendes von G, und man sagt: G wird von g erzeugt.

Zur Formulierung des nächsten Satzes benötigen wir den Begriff der Potenz eines Elementes.

Definition 1.16.4. Es sei $(G, \circ)$ eine Gruppe mit neutralem Element e. Es sei $g \in G$. Für $m \in \mathbb{Z}$, $m \geq 0$ definieren wir die Potenz g^m durch die Rekursion $g^0 = e$ und $g^{m+1} = (g^m) \cdot g$.
Für $m < 0$ setzen wir: $g^m = (g^{-m})^{-1}$.

Satz 1.16.1. *Es sei $(G, \circ)$ zyklisch mit neutralem Element e, also $G = \langle g \rangle$ für ein $g \in G$. Dann besteht G aus allen Potenzen von g:*

$$G = \{\ldots, g^{-2}, g^{-1}, g^0 = e, g, g^2, \ldots\}.$$

Es gibt nun zwei Hauptfälle:
Fall 1: Alle Potenzen g^k sind verschieden.
Fall 2: Es gibt $k_1 \neq k_2$, so daß $g^{k_1} = g^{k_2}$.

In beiden Fällen gibt es ein „Standardmodell“, von dem sich die gegebene Gruppe G höchstens durch die Namen ihrer Elemente und der Verknüpfung unterscheidet. Die Namensänderung wird durch einen Isomorphismus vermittelt. Dieser Begiff ist auch für andere algebraische Grundstrukturen grundlegend. Wir geben die Definition jedoch nur für Gruppen.

Definition 1.16.5. Es seien $(G, \circ)$ und $(G', *)$ Gruppen. Eine Abbildung $\Phi: (G, \circ) \to (G', *)$ heißt Isomorphismus, wenn Φ bijektiv und relationstreu ist, d.h. wenn gilt

$$\Phi(a \circ b) = \Phi(a) * \Phi(b)$$

für alle $a, b \in G$.
Es heißen $(G, \circ)$ und $(G', *)$ isomorph, wenn ein Isomorphismus $\Phi: G \to G'$ existiert.

Wir kommen nun zur Diskussion der zyklischen Gruppen $(G, \circ)$ mit $G = \langle g \rangle$.

Fall 1:
Alle Potenzen g^k sind verschieden.
Dann ist $(G, \circ)$ isomorph zum „Standardmodell“ $(\mathbb{Z}, +)$. Der Isomorphismus Φ ist gegeben durch $\Phi: \mathbb{Z} \to G$, $n \to g^n$. Insbesondere ist $(\mathbb{Z}, +)$ selbst eine zyklsiche Gruppe mit den Erzeugenden 1 oder -1, d.h. $\mathbb{Z} = \langle 1 \rangle$ oder $\mathbb{Z} = \langle -1 \rangle$.

Fall 2:
Wir beginnen mit einem Beispiel:

Beispiel 1.16.3. Die Gruppe $G = ((\mathbb{Z}/7\mathbb{Z})^*, \cdot)$ wird von der Restklasse 3 mod 7 erzeugt, wie folgende Tabelle zeigt:

k	0	1	2	3	4	5	6	7	
$3^k \mod 7$	1	3	2	6	4	5	1	3	mod 7.

Aus der Tabelle wird auch die Periodizität der Folge der Potenzen ersichtlich, die bei endlichen zyklischen Gruppen immer auftritt. $(\mathbb{Z}/7\mathbb{Z}, \cdot)$ ist isomorph zur Gruppe $(\mathbb{Z}/6\mathbb{Z}, +)$. Der Isomorphismus Φ ist gegeben durch:

$$\Phi: k \bmod 6 \to 3^k \bmod 7.$$

Hier haben wir also eine zyklische Gruppe G der Ordnung 6, die zu $(\mathbb{Z}/6\mathbb{Z}, +)$ isomorph ist. Allgemein ist eine zyklische Gruppe G der Ordnung m zu $(\mathbb{Z}/m\mathbb{Z}, +)$ isomorph.
Ist $G = \langle g \rangle$, so ist $G = \{e, g, \ldots, g^{m-1}\}$ und $\Phi: \mathbb{Z}/m\mathbb{Z} \to G,\ k \mod m \to g^k$ ein Isomorphismus.

Wir fassen unsere Ergebnisse zusammen in

Satz 1.16.2. *Eine unendliche zyklische Gruppe ist stets isomorph zur Gruppe $(\mathbb{Z}, +)$. Die Gruppe $(\mathbb{Z}, +)$ wird erzeugt von den Elementen 1 und -1: $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$. Die Potenzen von 1 bzw. -1 sind alle verschieden.*
Eine endliche zyklische Gruppe ist isomorph zu einer Gruppe $(\mathbb{Z}/m\mathbb{Z}, +)$ für ein festes $m \in \mathbb{N}$.
Es ist $\mathbb{Z}/m\mathbb{Z} = \langle 1 \bmod m \rangle$.
Unter den Potenzen von $1 \mod m$ sind m verschiedene Werte.
Wie schon in Abschnitt 2.1 illustriert wurde, sind endliche zyklische Gruppen auch isomorph zu einer Gruppe von Drehungen. So kann $\mathbb{Z}/12\mathbb{Z}$ durch die Drehungen des Stundenzeigers einer Uhr veranschaulicht werden. Nach 12 Schritten befindet er sich wieder am Ausgangspunkt. Daraus erklärt sich der Name zyklisch.

Definition 1.16.6. Es sei $(G, \circ)$ eine Gruppe mit neutralem Element e. Für $h \in G$ sei $H = \langle h \rangle$ die von h erzeugte Untergruppe. Diese besteht aus allen Potenzen von h: $H = \{\ldots, h^{-1}, e, h, h^2, \ldots\}$ und ist somit eine zyklische Gruppe. Die Mächtigkeit von $H = \langle h \rangle$ nennt man auch die Ordnung von h. Besteht h aus m verschiedenen Potenzen von h, so ist $H = \{e, h, \ldots, h^{m-1}\}$ und $h^m = e$. Dann ist H isomorph zu $(\mathbb{Z}/m\mathbb{Z}, +)$. Die Ordnung von h kann also auch so beschrieben werden: $|\langle h \rangle|$ ist der kleinste natürliche Exponent m, für den $h^m = e$ ist.

Beispiel 1.16.4. Es sei $G = ((\mathbb{Z}/7\mathbb{Z})^*, \cdot)$. Es sei H die von $h = 2 \bmod 7$ erzeugte Untergruppe:

$$H = \{2^0 \bmod 7 = 1 \bmod 7,\ 2 \bmod 7,\ 4 \bmod 7\}.$$

Es ist $2^3 \bmod 7 = 1 \bmod 7$. Damit ist $|\langle 2 \bmod 7 \rangle| = 3$.

Der folgende Satz gibt eine Übersicht über die Untergruppen von zyklischen Gruppen und auch über die Ordnung der von Gruppenelementen erzeugten Untergruppe.

Satz 1.16.3. *Es sei G eine zyklische Gruppe mit neutralem Element e. Jede Untergruppe von G ist ebenfalls zyklisch. Ist G unendlich, so ist jede Untergruppe $U \triangleleft G$ ebenfalls unendlich außer im Fall $U = \{e\}$.*
Ist $|G| = m \in \mathbb{N}$, so gibt es für jeden Teiler $d|m$ genau eine zyklische Untergruppe U von G mit $|U| = d$. Dies sind sämtliche Untergruppen von G.
Ist $G = \langle g \rangle$ und $|G| = m$, so ist

$$|\langle g^r \rangle| = \frac{m}{ggT(r, m)}.$$

Insbesondere ist genau dann $\langle g^r \rangle = G$, wenn $ggT(r, m) = 1$ ist.
Also hat G genau $\varphi(m)$ Erzeugende.

Wir haben schon in Beispiel 1.16.3 gesehen, daß die Gruppe $((\mathbb{Z}/7\mathbb{Z})^*, \cdot)$ zyklisch ist und von der Restklasse 3 mod 7 erzeugt wird. Man sagt auch: 3 ist eine Primitivwurzel mod 7.
Auch der Begriff der Ordnung läßt sich übertragen: Die Tatsache, daß 3 mod 7 die Ordnung 6 hat, drückt man aus durch: $\text{ord}_7\ 3 = 6$.
Beispiel 1.16.4 zeigt, daß $\text{ord}_7\ 2 = 3$.

Definition 1.16.7. Es sei $m \in \mathbb{N}$ und $a \in \mathbb{Z}$. Unter $\text{ord}_m\ a$ versteht man den kleinsten positiven Exponenten k, für den $a^k \equiv 1 \mod m$ ist. Eine ganze Zahl r heißt Primitivwurzel mod m, wenn $\text{ord}_m\ r = \varphi(m)$ ist.

Bemerkung 1.16.1. Es ist $\text{ord}_m\ a$ also die Ordnung der von der Restklasse $a \mod m$ erzeugten Untergruppe von $((\mathbb{Z}/m\mathbb{Z})^*, \cdot)$.
Außerdem ist r genau dann Primitivwurzel mod m, wenn die Restklasse $r \mod m$ die gesamte Gruppe $((\mathbb{Z}/m\mathbb{Z})^*, \cdot)$ erzeugt, wenn also jede reduzierte Restklasse mod m als Potenz von $r \mod m$ geschrieben werden kann.

Das nächste Beispiel zeigt, daß nicht zu jedem Modul m eine Primitivwurzel existiert.

Beispiel 1.16.5. Es sei $m = 12$. Wir betrachten das reduzierte Restsystem $R = \{1, 5, 7, 11\}$. Es ist $\text{ord}_{12}\ 1 = 1$ und $\text{ord}_{12}\ 5 = \text{ord}_{12}\ 7 = \text{ord}_{12}\ 11 = 2$. Die von 1 mod 12 erzeugte Untergruppe von $((\mathbb{Z}/12\mathbb{Z})^*, \cdot)$ hat somit die Ordnung 1 und die von 5 mod 12, 7 mod 12 und 11 mod 12 erzeugten Untergruppen haben jeweils die Ordnung 2. Es gibt keine Restklasse, die die gesamte Gruppe $((\mathbb{Z}/12\mathbb{Z})^*, \cdot)$ erzeugt, also keine Restklasse der Ordnung 4, oder anders ausgedrückt: kein a mit $\text{ord}_{12}\ a = 4$.
Die Gruppe $((\mathbb{Z}/12\mathbb{Z})^*, \cdot)$ ist nicht zyklisch.

Wir wollen nun einen Überblick darüber erhalten, für welche Moduln Primitivwurzeln existieren. Dies kann mit algebraischen Hilfsmitteln erreicht werden.

Definition 1.16.8. i) Es sei R ein Ring. Unter dem Polynomring $R[x]$ über R in der Unbestimmten x versteht man die Menge aller Ausdrücke der Form $p(x) = a_0 + a_1x + \ldots + a_nx^n$ mit $a_j \in \mathbb{R}$ und $n \in \mathbb{N}$. Die a_j heißen die Koeffizienten von $p(x)$. Zwei Polynome sind genau dann gleich, wenn sie in allen Koeffizienten übereinstimmen.

ii) Es seien

$$\begin{aligned} p(x) &= a_0 + a_1x + \ldots + a_nx^n \in R[x] \\ q(x) &= b_0 + b_1x + \ldots + b_mx^m \in R[x] \\ r(x) &= c_0 + c_1x + \ldots + c_nx^n \in R[x]. \end{aligned}$$

Unter dem Produkt $p(x) \cdot q(x)$ versteht man

$$p(x) \cdot q(x) = \sum_{j=0}^{m+n} \left(\sum_{l=0}^{j} a_l b_{j-l} \right) x^j.$$

Dabei ist $a_s = 0$ und $b_t = 0$ für $s \notin \{0, \ldots, n\}$ und $t \notin \{0, \ldots, m\}$ zu setzen.
Unter der Summe $p(x) + r(x)$ versteht man

$$p(x) + r(x) = \sum_{j=0}^{n} (a_j + c_j)\, x^j.$$

iii) Ist m der größte Wert von j mit $a_j \neq 0$, so heißt die Zahl m der Grad des Polynoms (Bezeichnung: $\operatorname{grad} p$). Ist $a_j = 0$ für alle j, so setzen wir $\operatorname{grad} p := -\infty$.

iv) Ist $\alpha \in \mathbb{R}$, so heißt $p(\alpha) := a_0 + a_1\alpha + \ldots + a_n\alpha^n$ der Wert des Polynoms p an der Stelle α.

v) Ist $p(\alpha) = 0$, so heißt α Nullstelle des Polynoms.

Satz 1.16.4. *Ist R ein Integritätsring, so hat ein Polynom $p \in R[x]$ mit $\operatorname{grad} p = n$ höchstens n Nullstellen.*

Beweis. Wir beweisen die Behauptung durch Induktion nach n:
$n = 0$:
Das Polynom $p(x) = a_0$ mit $a_0 \neq 0$ hat keine Nullstellen.
$n = 1$:
Das Polynom $p(x) = a_1x + a_0$ mit $a_1 \neq 0$ hat höchstens die Nullstelle $a_1 = -a_0a_1^{-1}$.
$\vdots$
$n - 1 \to n$:
Es sei $p(x) = a_0 + \ldots + a_nx^n$ mit $a_n \neq 0$. Weiter sei α_1 eine Nullstelle von p, d.h. $p(\alpha_1) = 0$. Aus der Identität

$$x^k - \alpha_1^k = (x - \alpha_1) \cdot \left(x^{k-1} + \alpha_1 x^{k-2} + \ldots + \alpha_1^{k-2}x + \alpha_1^{k-1} \right)$$

für alle $k \in \{1, \ldots, n\}$ folgt die Existenz eines Polynoms $q \in R[x]$ mit $\operatorname{grad} q = n - 1$, so daß daraus $p(x) = (x - \alpha_1) \cdot q(x) + r$ mit $r \in R$ folgt. Einsetzen von $x = \alpha_1$ ergibt $0 = p(\alpha_1) = r$. Also ist $p(x) = (x - \alpha_1) \cdot q(x)$. Aus der Nullteilerfreiheit von R folgt

$$p(\alpha) = 0 \Leftrightarrow \alpha = \alpha_1 \quad \text{oder} \quad q(\alpha) = 0.$$

Nach Induktionshypothese hat q höchstens $n - 1$ Nullstellen $\alpha_2, \ldots, \alpha_n$. Damit hat p höchstens n Nullstellen. □

Satz 1.16.5. *Es sei p eine Primzahl. Das Polynom $p(x) = a_0 + \ldots + a_n x^n$ habe ganze Koeffizienten, und es sei $a_n \neq 0 \bmod p$. Dann hat die Kongruenz $p(x) \equiv 0 \bmod p$ höchstens n Lösungen* $\bmod p$.

Beweis. Wir betrachten das Polynom $\tilde{p}(x) = \overline{a_0} + \ldots + \overline{a_n} x^n \in (\mathbb{Z}/p\mathbb{Z})[x]$ mit $\overline{a_j} = a_j \bmod p$.
Es ist $p(x) \equiv 0 \bmod p \Leftrightarrow \tilde{p}(x \bmod p) = 0 \bmod p$. Da nach Satz 1.15.1 $\mathbb{Z}/p\mathbb{Z}$ ein Integritätsring ist, folgt die Behauptung nach Satz 1.16.4. □

Wir werden im folgenden ein Kriterium dafür herleiten, wann eine endliche Gruppe zyklisch ist. Dazu treffen wir erst einige Vorbereitungen. Zunächst geben wir eine Verallgemeinerung des Kongruenzbegriffs für beliebige Gruppen.

Definition 1.16.9. Es sei G eine Gruppe und $H \triangleleft G$. Dann heißen a und b rechtskongruent $\bmod H$ (Schreibweise: $a \equiv_r b \bmod H$), falls $ab^{-1} \in H$ gilt.

Bemerkung 1.16.2. Der Begriff "linkskongruent" kann analog definiert werden:

$$a \equiv_l b \bmod H \Leftrightarrow b^{-1}a \in H.$$

Definition 1.16.10. Es sei G eine Gruppe und $H \triangleleft G$. Unter der Rechtsnebenklasse von a verstehen wir $aH := \{ah \colon h \in H\}$

Bemerkung 1.16.3. Die Rechtsnebenklassen sind gerade die Äquivalenzklassen bzgl. der Äquivalenzrelation $\equiv_r$. Ist G abelsch, so ist die Unterscheidung zwischen "links" und "rechts" unnötig, da in diesem Falle $ab^{-1} = b^{-1}a$ und $aH = Ha$ ist.

Beispiel 1.16.6. Es sei $G = (\mathbb{Z}, +)$ und $H = m\mathbb{Z}$ mit $m \in \mathbb{N}$. Für $a, b \in \mathbb{Z}$ gilt dann

$$a \equiv b \bmod H \Leftrightarrow a - b \in H \Leftrightarrow m | a - b \Leftrightarrow a \equiv b \bmod m.$$

Die Definition 1.5.2 ergibt sich hieraus als Spezialfall. Auch die Restklassen ergeben sich als Spezialfall der Nebenklassen. Für $a \in \mathbb{Z}$ ist $a + m\mathbb{Z} = \{b \in \mathbb{Z} \colon a \equiv b \bmod m\} = a \bmod m$.

Satz 1.16.6. *Es sei G eine Gruppe, $H \triangleleft G$ und $a, c \in H$. Es gilt $aH = cH \Leftrightarrow c \in aH$.*

Beweis. Wir zeigen zunächst

$$c \in aH \Leftrightarrow a \in cH. \qquad (*)$$

"$\Rightarrow$":
Es sei $c \in aH$. Dann existiert ein $h_1 \in H$ mit $c = ah_1$. Also gilt $a = ch_1^{-1}$, und damit ist $a \in cH$.
Vertauschung der Rollen von a und c ergibt
"$\Leftarrow$":
Aus $a \in cH$ folgt $c \in aH$. Damit ist $(*)$ gezeigt.
Nun zeigen wir die eigentliche Aussage:
"$\Leftarrow$":
Es sei nun $c \in aH$. Dann existiert ein $h_3 \in H$ mit $c = ah_3$. Es sei $x \in cH$. Deswegen existiert ein $h_2 \in H$ mit $x = ch_2$. Also hat x eine Darstellung $x = ah_3h_2$, also ist $x \in aH$, woraus $cH \subset aH$ folgt. Mit $(*)$ folgt $aH \subset cH$, und damit ist $aH = cH$.
"$\Rightarrow$":
Es sei nun $aH = cH$. Daraus folgt $c = ce \in cH = aH$. □

Satz 1.16.7. *Es sei $H \triangleleft G$. Zwei Rechtsnebenklassen von H sind entweder identisch oder disjunkt.*

Beweis. Es sei $c \in aH \cap bH$. Nach Satz 1.16.6 ist $cH = aH = bH$. □

Satz 1.16.8. *(Lagrange)*
Es sei G eine endliche Gruppe und $H \triangleleft G$. Dann gilt $|H| \Big| |G|$.

Die Ordnung der Untergruppe einer endlichen Gruppe ist also stets ein Teiler der Gruppenordnung. Dieser Satz hat zahlreiche Anwendungen.

Satz 1.16.9. *Eine Gruppe G mit $|G| = p$, wobei p eine Primzahl ist, ist stets zyklisch. Sie wird von jedem vom neutralen Element e verschiedenen Element g erzeugt.*

Beweis. Es sei $g \in G \backslash \{e\}$ und $\langle g \rangle$ die von g erzeugte zyklische Untergruppe. Nach Satz 1.16.8 gilt $| \langle g \rangle | \Big| G = p$. Wegen $\langle g \rangle \neq \{e\}$ ist $| \langle g \rangle | > 1$, also $| \langle g \rangle | = p$. Damit ist $G = \langle g \rangle$. □

Satz 1.16.10. *Es sei G eine endliche Gruppe und $g \in G$. Dann gilt $| \langle g \rangle | \Big| G$.*

Beweis. Dies folgt unmittelbar aus Satz 1.16.8. □

Als zahlentheoretische Anwendung ergibt sich

Satz 1.16.11. *Es sei $m \in \mathbb{N}$ und $n \in \mathbb{Z}$. Dann gilt* $\mathrm{ord}_m a \Big| \varphi(m)$.

Beweis. Wir betrachten die Gruppe $G = ((\mathbb{Z}/m\mathbb{Z})^*, \cdot)$ und die Untergruppen $H = \langle a \bmod m \rangle$. Es ist $|G| = \varphi(m)$ und $|H| = \mathrm{ord}_m a$. Dann folgt die Behauptung aus Satz 1.16.8. □

Satz 1.16.12. *Es sei G eine endliche Gruppe und $g \in G$. Dann gilt $g^{|G|} = e$.*

Beweis. Nach Definition von $\langle g \rangle$ ist $g^{|\langle g \rangle|} = e$. Nach Satz 1.16.10 gibt es ein $k \in \mathbb{N}$ mit $|G| = k \cdot | \langle g \rangle |$. Damit gilt $g^{|G|} = (g^{|\langle g \rangle|})^k = e^k = e$. □

Aus Satz 1.16.12 ergibt sich ein neuer Beweis des Satzes von Euler (Satz 1.13.1):
Es sei $a \in \mathbb{Z}$, $m \in \mathbb{N}$ und $(a, m) = 1$. Weiter sei $G = ((\mathbb{Z}/m\mathbb{Z})^*, \cdot)$ und $g = \langle a \bmod m \rangle$. Es ist $|G| = \varphi(m)$. Nach Satz 1.16.2 ist

$$(a \bmod m)^{\varphi(m)} \equiv 1 \bmod m, \quad \text{also} \quad a^{\varphi(m)} \equiv 1 \bmod m.$$

Wir geben nun ein Kriterium dafür, daß eine endliche abelsche Gruppe zyklisch ist. Daraus wird sich dann ergeben, daß für eine Primzahl p die Gruppe $((\mathbb{Z}/p\mathbb{Z})^*, \cdot)$ zyklisch ist, woraus die Existenz einer Primitivwurzel $\bmod p$ folgt.

Satz 1.16.13. *Es sei G eine endliche abelsche Gruppe. Diese ist genau dann zyklisch, wenn für alle $k \in \mathbb{N}$ die Gleichung $x^k = e$ höchstens k Lösungen hat.*

Zur Vorbereitung des Beweises von Satz 1.16.13 beweisen wir folgendes Lemma:

Lemma 1.16.1. *Für $m \in \mathbb{N}$ ist* $\displaystyle\sum_{k|m} \varphi(k) = m$, *wobei in $\sum_{k|m}$ über alle Teiler k von m summiert wird.*

Beweis. Wir betrachten die Gruppe $(\mathbb{Z}/m\mathbb{Z}, +)$. Es sei $f(k)$ die Anzahl der Elemente von G mit Ordnung k.

1. Es gelte $k|m$.
   Gilt $|\langle a \bmod m\rangle| = k$ für $a \bmod m \in G$, so ist $ka \bmod m = 0 \bmod m$.
   Somit ist $a \bmod m \in G_k := \{a \bmod m |\ ka \bmod m = 0 \bmod m\}$. Die Menge G_k ist dann nach Satz 1.16.3 eine zyklische Untergruppe von G der Ordnung k. Weiter hat $(a \bmod m)$ genau dann die Ordnung k, wenn $\langle a \bmod m\rangle = G_k$ ist. Nach Satz 1.16.3 ist $f(k) = \varphi(k)$.

2. Für $k \not| m$ ist nach Satz 1.16.10 folglich $f(k) = 0$.

Also gilt $\sum_{k|m} f(k) = m$ und damit $\sum_{k|m} \varphi(k) = m$. □

Beweis. (Beweis von Satz 1.16.13)
"⇒":
Es sei G zyklisch und $|G| = m$. Für alle $k \in \mathbb{N}$ sei $G_k := \{g \in G |\ g^k = e\}$, und es sei $d = ggT(k, m)$. Nach Satz 1.4.3 gibt es $u, v \in \mathbb{Z}$ mit $uk + vm = d$. Also ist $g^d = (g^k)^u (g^m)^v = e$. Somit ist $G_k \subset G_d$. Die Behauptung ist also gezeigt, wenn sie für alle $k|m$ gezeigt ist.
Es sei also $k|m$.
Nach Satz 1.16.3 gibt es eine zyklische Untergruppe $U_k \triangleleft G$ mit

$$|U_k| = k. \tag{1}$$

Es sei $U_k = \langle g_k\rangle$. Dann ist $g_k^k = e$ und $|\langle g_k\rangle| = k$. Also ist $g_k \in G_k$, woraus $G_k \neq \emptyset$ folgt. Weiter folgt mit $g, h \in G_k$ dann $gh^{-1} \in G_k$, und damit ist $G_k \triangleleft G$. Nach Satz 1.16.3 ist auch G_k zyklisch und $|G_k| = |\langle h_k\rangle|$ mit $G = \langle h_k\rangle$. Wegen $h_k^k = e$ ist

$$|G_k| \leq k. \tag{2}$$

Nach Satz 1.16.12 ist

$$U_k \subset G_k. \tag{3}$$

Aus (1), (2) und (3) folgt $G_k = U_k$.
Damit hat die Gleichung $x^k = e$ genau k Lösungen.

"⇐":
Für alle $k \in \mathbb{N}$ gelte, daß $x^k = e$ höchstens k Lösungen $x \in G$ habe.
Für $k \in \mathbb{N}$ sei dann $F(k)$ die Anzahl der Elemente $g \in G$ mit $|\langle g\rangle| = k$. Es ist nach Satz 1.16.10

$$F(k) = 0 \quad \text{für} \quad k \not| m. \tag{1}$$

Es sei $k|m$ und $F(k) \neq 0$ sowie $|\langle g_k\rangle| = k$. Dann ist $\langle g_k\rangle = \{e, g_k, \ldots, g_k^{k-1}\}$ und wegen $g^k = e$ folgt $g \in \langle g_k\rangle$. Nach Satz 1.16.3 ist

$$|\langle g_k^r\rangle| = k \Leftrightarrow ggT(r, k) = 1.$$

Also ist

$$F(k) \leq \varphi(k). \tag{2}$$

Aus (1), (2) und Lemma 1.16.1 folgt

$$m = \sum_{k|m} F(k) \leq \sum_{k|m} \varphi(k) = m.$$

Wäre $F(k) < \varphi(k)$ für ein $k|m$, so wäre $m = \sum_{k|m} F(k) < \sum_{k|m} \varphi(k) = m$, ein Widerspruch.

Also gilt $F(k) = \varphi(k)$ für alle $k|m$.
Insbesondere gilt für $k = m$:

$$F(m) = \varphi(m) > 0.$$

Damit existiert ein $g \in G$ mit $|\langle g \rangle| = m = |G|$. Also ist $G = \langle g \rangle$, d.h. G ist zyklisch. □

Satz 1.16.14. *Es sei p eine Primzahl. Dann existiert eine Primitivwurzel* mod p*, d.h. die Gruppe $((\mathbb{Z}/p\mathbb{Z})^*, \cdot)$ ist zyklisch.*

Beweis. Es sei $k \in \mathbb{N}$. Nach Satz 1.16.5 hat das Polynom $p(x) = x^k - (1 \bmod p)$ höchstens k Nullstellen $x \bmod p$. Damit hat die Gleichung $x^k \equiv 1 \bmod p$ höchstens k Lösungen in $((\mathbb{Z}/p\mathbb{Z})^*, \cdot)$. Nach Satz 1.16.13 ist $((\mathbb{Z}/p\mathbb{Z})^*, \cdot)$ zyklisch. □

Der nächste Satz gibt eine vollständige Auskunft über die Existenz von Primitivwurzeln.

Satz 1.16.15. *Eine Primitivwurzel r* mod m *existiert genau dann, wenn $m = 1, 2, 4$ oder wenn für eine Primzahl $p > 2$ und $\gamma \in \mathbb{N}$ gilt: $m = p^\gamma$ oder $m = 2p^\gamma$. In diesen Fällen ist die Gruppe $((\mathbb{Z}/m\mathbb{Z})^*, \cdot)$ zyklisch. Jede reduzierte Restklasse* mod m *ist eine Potenz von r* mod m*.*

Abschließend betrachten wir die Frage, für welche Exponenten k die Kongruenz $a^k \equiv 1 \bmod m$ gilt.

Satz 1.16.16. *Es sei $m \in \mathbb{N}$, $a \in \mathbb{Z}$ und $ggT(a, m) = 1$.*
Es gilt genau dann $a^k \equiv 1 \bmod m$, wenn $\mathrm{ord}_m\ a|\ k$.
Insbesondere ist $\mathrm{ord}_m\ a$ stets ein Teiler von $\varphi(m)$.
Es ist genau dann $a^{k_1} \equiv a^{k_2} \bmod m$, wenn $k_1 \equiv k_2 \bmod ord_m a$.

Beweis. Es sei $k = q \cdot \mathrm{ord}_m\ a + r$ mit $0 \leq r < \mathrm{ord}_m\ a$. Dann ist $a^k = \left(a^{\mathrm{ord}_m\ a}\right)^q \cdot a^r \equiv a^r \bmod m$. Nach Definition 1.16.7 ist $a^r \equiv 1 \bmod m \Leftrightarrow r = 0$.
Der Zusatz folgt wegen $a^{\varphi(m)} \equiv 1 \bmod m$ (Satz 1.13.1, Euler). □

1.17 Polynomkongruenzen

Definition 1.17.1. Unter einer Polynomkongruenz verstehen wir eine Kongruenz der Form

$$P(x) \equiv 0 \bmod m, \qquad (*)$$

wobei P ein Polynom mit ganzzahligen Koeffizienten und m eine natürliche Zahl ist.
Bei der Betrachtung von $(*)$ können in $P(x)$ alle Koeffizienten, die durch m teilbar sind, weggelassen werden.

Beispiel 1.17.1. Die Kongruenz

$$15x^4 + 7x^3 + 5x^2 + 2x + 1 \equiv 0 \bmod 3$$

ist äquivalent zu

$$7x^3 + 5x^2 + 2x + 1 \equiv 0 \bmod 3,$$

da wegen $3|15$ auch $15x^4 \equiv 0 \bmod 3$ gilt.

Dies gibt Anlaß zur folgenden

Definition 1.17.2. Hat $P(x)$ in $(*)$ die Form

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$$

mit $n \in \mathbb{N}$ und $a_n \not\equiv 0 \bmod m$, so nennt man $(*)$ eine Polynomkongruenz vom Grad n.

In Abschnitt 1.10 haben wir die linearen Kongruenzen, welche in der Bezeichnungsweise von Definition 1.17.2 gerade die Kongruenzen vom Grad 1 sind, betrachtet. Wir haben gesehen, daß deren Lösungsmenge sehr gut bekannt ist. Gut erforscht sind weiterhin die quadratischen Kongruenzen, also die Kongruenzen vom Grad 2, und die Theorie der Potenzreste: $x^n - a \equiv 0 \bmod m$. Diese werden wir in den nächsten Abschnitten diskutieren. Über allgemeine Polynomkongruenzen sind nur wenige Tatsachen bekannt. Wir werden einige in diesem Abschnitt zusammenstellen.
Wie bei linearen Kongruenzen hängt die Tatsache, ob x eine Lösung von $P(x) \equiv 0 \bmod m$ ist, nur von der Restklasse von $x \bmod m$ ab.

Beispiel 1.17.2. Es sei

$$P(x) = x^3 - 2x^2 - x - 13.$$

Was sind die Lösungen von $P(x) \equiv 0 \bmod 5$?
Wir berechnen die Werte von $P(x)$ für x aus dem absolut kleinsten Restsystem $\bmod 5$ und erhalten folgende Tabelle:

x	-2	-1	0	1	2
$P(x)$	-27	-15	-13	-15	-15

Die Lösungsmenge von $P(x) \equiv 0 \bmod 5$ besteht also aus den folgenden drei Restklassen $\bmod 5$:

$$x \equiv 1 \bmod 5, \quad x \equiv 2 \bmod 5 \quad \text{und} \quad x \equiv 4 \bmod 5.$$

Ist der Modul m einer Polynomkongruenz das Produkt von teilerfremden Moduln $m = m_1 \cdot m_2 \cdots m_r$, so ist die Kongruenz

$$P(x) \equiv 0 \bmod m \qquad (*)$$

äquivalent zum System der Kongruenzen

$(**)$

$$\begin{aligned} P(x) &\equiv 0 \bmod m_1 \\ &\vdots \quad\quad \vdots \\ P(x) &\equiv 0 \bmod m_r. \end{aligned}$$

Die Lösungen der Kongruenz $(*)$ können aus den Lösungen des Systems $(**)$ mittels des Chinesischen Restsatzes mit dem Algorithmus von Satz 1.11.1 berechnet werden.

Beispiel 1.17.3. Es sei wieder $P(x) = x^3 - 2x^2 - x - 13$.
Man bestimme die Lösungsmenge von

$$P(x) \equiv 0 \bmod 15. \qquad (*)$$

Lösung:
Die Kongruenz $(*)$ ist äquivalent zu dem System

$$\begin{aligned} P(x) &\equiv 0 \bmod 3 \quad (I) \\ P(x) &\equiv 0 \bmod 5 \quad (II) \end{aligned}$$

Man überprüft leicht, daß die Lösungen von (I) aus den beiden Restklassen

$$x \equiv 1 \bmod 3 \quad \text{und} \quad x \equiv 2 \bmod 3$$

besteht.
In Beispiel 1.17.2 wurde gezeigt, daß die Lösungsmenge von (II) aus den drei Restklassen

$$x \equiv 1 \bmod 5, \quad x \equiv 2 \bmod 5 \quad \text{und} \quad x \equiv 4 \bmod 5$$

besteht.
Man erhält sechs mögliche Kombinationen, die in folgender Tabelle dargestellt sind:

.		Lösungen mod 5		
		1	2	4
Lösungen mod 3	1	1	7	4
	2	11	2	14

Die Lösungsmenge von $P(x) \equiv 0 \bmod 15$ besteht also aus den sechs Restklassen

$$\begin{aligned} x &\equiv 1 \bmod 15, \quad x \equiv 2 \bmod 15, \quad x \equiv 4 \bmod 15 \\ x &\equiv 7 \bmod 15, \quad x \equiv 11 \bmod 15, \quad x \equiv 14 \bmod 15. \end{aligned}$$

Die in Beispiel 1.17.3 dargestellten Ideen können leicht zum Beweis des folgenden Satzes verwendet werden:

Satz 1.17.1. *Es sei $P(x)$ ein Polynom mit ganzzahligen Koeffizienten. Es sei $N(m)$ die Anzahl der Lösungen der Kongruenz $P(x) \equiv 0 \bmod m$. Dann ist $N(m)$ eine multiplikative Funktion von m, d.h. für $m = m_1 \cdot m_2$ mit $ggT(m_1, m_2) = 1$ gilt:*

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

Wir schließen mit einem Resultat für Polynomkongruenzen nach Primzahlmoduln.

Satz 1.17.2. *Es sei p eine Primzahl und $P(x) = a_n x^n + a_{n-1} x^{n-1} \ldots + a_0$ mit $a_i \in \mathbb{Z}$ und $a_n \not\equiv 0 \bmod p$. Dann besitzt die Kongruenz n- ten Grades*

$$P(x) \equiv 0 \bmod p$$

höchstens n Lösungen.

Bemerkung 1.17.1. Wie Beispiel 1.17.3 zeigt, gilt diese Aussage nicht, falls der Modul keine Primzahl ist. Die Kongruenz dritten Grades

$$x^3 - 2x^2 - x - 13 \equiv 0 \bmod 15$$

besitzt sechs Lösungen.

1.18 Potenzreste

Definition 1.18.1. Es sei $k, m \in \mathbb{N}$ und $a \in \mathbb{Z}$ mit $ggT(a, m) = 1$. Die Zahl a heißt dann k- ter Potenzrest modulo m, falls die Kongruenz

$$x^k \equiv a \bmod m$$

lösbar ist, andernfalls ein k- ter Potenznichtrest.
Im Fall $k = 2$ spricht man von quadratischen Resten bzw. Nichtresten.

Beispiel 1.18.1. Es sei $k = 3$ und $m = 7$. Die dritten Potenzreste $\bmod 7$ lassen sich durch Berechnen der dritten Potenzreste aller Elemente eines vollständigen Restsystems bestimmen. Wir erhalten folgende Tabelle:

$x \bmod 7$	-3	-2	-1	0	1	2	3
$x^3 \bmod 7$	1	-1	-1	0	1	1	-1

Die dritten Potenzreste $\bmod 7$ bestehen also aus den Restklassen $1 \bmod 7$ und $-1 \bmod 7$.
Die Kongruenz

$$x^3 \equiv a \bmod 7$$

besitzt für $a \equiv 1, -1 \bmod 7$ jeweils drei Lösungen $\bmod 7$ und sonst keine.

Die Theorie der Potenzreste $\bmod m$ ist sehr übersichtlich, wenn m eine Primitivwurzel besitzt.

Satz 1.18.1. *Der Modul $m \in \mathbb{N}$ besitze eine Primitivwurzel. Es sei $k \in \mathbb{N}$ und $d = ggT(k, \varphi(m))$. Dann gibt es genau $\frac{\varphi(m)}{d}$ k- te Potenzreste $\bmod m$. Ist $a \in \mathbb{Z}$ ein k- ter Potenzrest $\bmod m$, d.h. ist $ggT(a, m) = 1$ und*

$$x^k \equiv a \bmod m \qquad (*)$$

lösbar, so hat $(*)$ genau d Lösungen in $x \bmod m$. Zudem ist $a \in \mathbb{Z}$ genau dann ein k- ter Potenzrest, wenn

$$a^{\frac{\varphi(m)}{d}} \equiv 1 \bmod m$$

ist.

Beweis. Es sei r eine Primitivwurzel $\bmod m$. Für jedes Paar (x, a) von ganzen Zahlen mit $ggT(x, m) = ggT(a, m) = 1$ gibt es nach Satz 1.16.16 $\bmod \varphi(m)$ eindeutig bestimmte Zahlen y, j mit

$$x \equiv r^y \bmod m \quad \text{und} \quad a \equiv r^j \bmod m.$$

Nach Satz 1.16.5 entsprechen die Lösungen $x \bmod m$ von (1) umkehrbar eindeutig den Lösungen $y \bmod \varphi(m)$ der linearen Kongruenz

$$ky \equiv j \bmod \varphi(m). \qquad (**)$$

Nach Satz 1.10.1 ist $(**)$ genau dann lösbar, wenn $d|j$ ist. Es gibt dann d Lösungen $\bmod \varphi(m)$:

$$d|j \Leftrightarrow \varphi(m)\Big|j\frac{\varphi(m)}{d} \Leftrightarrow (r^j)^{\varphi(m)/d} \equiv 1 \bmod m.$$

Die Lösbarkeit von $(*)$ ist also äquivalent zu $a^{\varphi(m)/d} \equiv 1 \bmod m$. Es gibt $\frac{\varphi(m)}{d}$ Werte von j, welche die Bedingungen $d|j$ erfüllen. □

Wir formulieren den Spezialfall für $k = 2$, d.h. quadratische Reste, und $m = p > 2$ sei eine ungerade Primzahl.

Satz 1.18.2. *Es sei p eine ungerade Primzahl. Von den $p-1$ Werten a mit $1 \leq a \leq p-1$ sind genau $\frac{p-1}{2}$ quadratische Reste* $\bmod p$ *(d.h. $x^2 \equiv a \bmod p$ ist lösbar) und $\frac{p-1}{2}$ quadratische Nichtreste* $\bmod p$.
Es gilt das Eulersche Kriterium:
a ist quadratischer Rest $\bmod p \quad \Leftrightarrow \quad a^{p-1/2} \equiv 1 \bmod p$.
a ist quadratischer Nichtrest $\bmod p \quad \Leftrightarrow \quad a^{p-1/2} \equiv -1 \bmod p$.

Im Falle $p = 3 \bmod 4$ ergibt sich die Möglichkeit, einem quadratischen Rest $a \bmod p$ die "Quadratwurzel" x, d.h. die Lösung von $x^2 \equiv a \bmod p$ zu berechnen.

Satz 1.18.3. *Es sei $p \equiv 3 \bmod 4$ eine Primzahl und a ein quadratischer Rest* $\bmod p$. *Dann ist $x = a^{p+1/4}$ eine Lösung der Kongruenz $x^2 \equiv a \bmod p$.*

Beweis. Es ist

$$x^2 = a^{p+1/2} = a \cdot a^{p-1/2} \equiv a \bmod p,$$

da nach dem Eulerschen Kriterium $a^{p-1/2} \equiv 1 \bmod p$ ist. □

Kapitel 2

Anwendungen in der Kryptologie

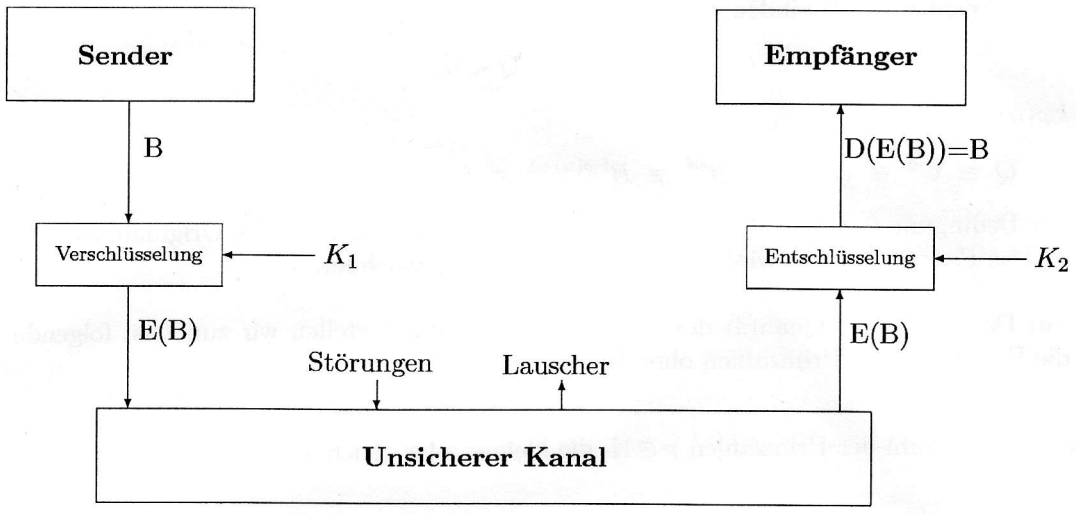
2.1 Public- Key- Codes, RSA- Verfahren

Der Gegenstand der Kryptologie ist die Übermittlung geheimer Botschaften unter Verwendung von Codes. Die Kryptologie besteht aus zwei Teilgebieten:

(i) In der Kryptographie wird der Entwurf von Geheimcodes untersucht.

(ii) In der Kryptoanalyse wird nach Methoden gesucht, diese zu knacken.

Bei der Übermittlung einer geheimen Nachricht wird zunächst eine Botschaft B in einen Geheimtext $E(B)$ umgeändert. Das Verfahren für die Umänderung bezeichnet man als Verschlüsselung E (von eng. "encryption"). Die verschlüsselte Botschaft wird dann an den Empfänger gesandt. Dieser benutzt ein Entschlüsselungsverfahren D (von engl. "decryption"), um dann die ursprüngliche Botschaft zurück zu gewinnen. Diese sogenannten Chiffrierverfahren sind öffentlich bekannt. Das Verschlüsselungsverfahren wird dabei meist durch einen Schlüssel K_1 gesteuert, die Entschlüsselung durch einen Schlüssel K_2. Die Übermittlung erfolgt also nach folgendem Schema:



Ziel der Chiffrierverfahren ist es, die Nachricht B vor dritten Personen geheimzuhalten und gegen Veränderungen bei der Übertragung zu schützen. Dazu ist es erforderlich, den Schlüssel K_2 vor eventuellen Lauschern geheimzuhalten. Bei den konventionellen Verfahren (den symmetrischen Chiffrierverfahren) ist es möglich, das Entschlüsselungsverfahren aus dem Verschlüsselungsverfahren zu gewinnen (meist sind diese sogar identisch, und es gilt: $K_1 = K_2$). Also war auch K_1 geheimzuhalten. In gewissen Umständen ist es jedoch wünschenswert, auf die Geheimhaltung von K_1 zu verzichten. Haben wir zum Beispiel ein Netzwerk von sehr vielen Teilnehmern, so ist es wünschenswert, daß jeder Teilnehmer T_i an jeden anderen Teilnehmer T_j eine Botschaft schicken kann, ohne sich zunächst bei T_j nach dem Schlüssel zu erkundigen. Dazu veröffentlicht jeder Teilnehmer T_j seinen Schlüssel S_j für die Verschlüsselung in einer Art Telefonbuch. Will ein anderer Teilnehmer T_i eine Botschaft an T_j senden, so benutzt er dazu den Schlüssel S_j. Es muß also ein System gefunden werden, bei dem es unmöglich ist, den Schlüssel für die Entschlüsselung aus S_j zu berechnen. Einen solchen Code nennt man Public- Key- Code oder auch asymmetrisches Chiffrierverfahren. Wir werden das RSA- System (benannt nach Rivest, Shamir und Adleman, die es 1978 vorgeschlagen haben) betrachten.

Der öffentliche Schlüssel $S = (e, n)$ ist ein Zahlenpaar bestehend aus dem Exponenten $e \in \mathbb{N}$ und dem Modulus n, so daß $n = p \cdot q$ das Produkt zweier verschiedener Primzahlen ist und außerdem auch $ggT(e, \varphi(n)) = 1$ gilt. Während e und n allgemein zugänglich sind, ist die Faktorisierung $n = p \cdot q$ und auch $\varphi(n)$ nur dem Empfänger bekannt, dem der öffentliche Schlüssel gehört. Das Verfahren gilt als sicher, wenn p und q groß genug gewählt sind. Aktuelle Schlüssel (Stand: 2005) sind von der Größenordnung 2^{1024}.
Wir beschreiben nun das Verschlüsselungsverfahren: Jeder Buchstabe der Nachricht wird nach einem Standardverfahren in eine Ziffernfolge umgewandelt. Eine feste Anzahl dieser Ziffernfolgen werden aneinander gehängt, so daß sie eine Zahl $B < n$ bilden. Dabei soll B jedoch von derselben Größenordnung wie n sein, d.h. in etwa die gleiche Anzahl an Stellen besitzen. Ist die Botschaft länger, kann sie in Blöcke unterteilt werden. Der Absender berechnet dann die eindeutig bestimmte Zahl C mit $C \equiv B^e \mod n$ mit $0 < C < n$. Die Zahl C ist der Geheimtext, der an den Empfänger gesendet wird.
Wir kommen zur Beschreibung des nur dem Empfänger bekannten Entschlüsselungsverfahrens. Da der Empfänger die Faktorisierung $n = p \cdot q$ kennt, kann er auch $\varphi(n) = (p-1) \cdot (q-1)$ einfach ausrechnen. Da $ggT(e, \varphi(n)) = 1$ ist, kann der Empfänger ein $d > 0$ berechnen, so daß $ed \equiv 1 \mod \varphi(n)$ ist. Erhält er den Geheimtext $C \equiv B^e \mod n$, so berechnet er die eindeutig bestimmte Zahl Q mit $Q \equiv C^d \mod n$ mit $0 < Q < n$.
Dann ist $ed = k\varphi(n) + 1$ für ein $k \in \mathbb{N}_0$, also gilt

$$Q \equiv C^d \equiv (B^e)^d \equiv B^{ed} \equiv B^{k\varphi(n)+1} \equiv \left(B^{\varphi(n)}\right)^k \cdot B \equiv B \mod n.$$

Also ist wegen der Bedingung $0 < Q < n$ dann $Q = B$, d.h. der Empfänger hat die Originalnachricht zurückgewonnen. Das Paar $T = (d, n)$ wird als privater Schlüssel bezeichnet.

Bevor wir nun zur Diskussion der Qualität des RSA- Systems kommen, stellen wir zunächst folgende Tatsache über die Häufigkeit der Primzahlen ohne Beweis fest:

Definition 2.1.1. Für $x > 0$ sei $\pi(x)$ die Anzahl der Primzahlen $p \in \mathbb{N}$, die kleiner oder gleich x sind.

Es gilt:

Satz 2.1.1. *(Primzahlsatz)*

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\log x} = 1,$$

was auch als

$$\pi(x) \sim \frac{x}{\log x}$$

geschrieben werden kann.

Die zweite Tatsache, die wir müssen wissen, ist, daß es sehr schnelle Primzahltests gibt. Die Anzahl der Rechenschritte für einen Primzahltest ist für eine Zahl der Größenordnung 2^k nur von der Größenordnung k. Wir kommen nun zur angekündigten Diskussion der Qualität des RSA- Systems:

(i) Ein öffentlicher Schlüssel (e, n) ist leicht zu konstruieren. Dazu wählt man irgendeine Zahl p der Größenordnung $\sim 2^k$ nach dem Zufallsprinzip. Die Wahrscheinlichkeit, daß p eine Primzahl ist, beträgt nach dem Primzahlsatz

$$\frac{\pi(2^k)}{2^k} \sim \frac{1}{\log(2^k)} \sim \frac{1}{k}.$$

Ein Rechner benötigt daher im Schnitt k Versuche, um eine Primzahl p der gewünschten Größenordnung zu finden. Der Teilnehmer T berechnet zwei verschiedene Primzahlen p und q auf diese Weise und veröffentlicht den Schlüssel (e, n) mit $n = p \cdot q$.

(ii) Verschlüsselung und Entschlüsselung können leicht mit Computern durchgeführt werden, es wird nur die Potenzierung mit einer natürlichen Zahl benötigt, die modulo n effiizient durch wiederholtes Quadrieren durchgeführt werden kann. Das Inverse d zu e kann mit dem Euklidischen Algorithmus berechnet werden, wenn p und q bekannt sind.

(iii) Es gibt zur Zeit kein Verfahren, das die Originalnachricht B aus $C \equiv B^e \mod n$ ohne Kenntnis von $\varphi(n)$ oder der Faktorisierung $n = p \cdot q$ (welche die Kenntnis von $\varphi(n) = (p-1) \cdot (q-1)$ impliziert) mit akzeptablem Aufwand ausrechnen kann.

Kapitel 3

Endliche Körper

3.1 Polynomkongruenzen

Die Theorien der Teilbarkeit und der Kongruenzen von Kapitel 1 können mit Einschränkungen auf Polynomringe $R[x]$ über einem Ring R, die in Definition 1.16.1 eingeführt wurden, übertragen werden. Wir beschränken uns auf den Fall, daß R ein Körper ist.
Im folgenden bezeichne K also stets einen Körper.

Definition 3.1.1. (Teilbarkeit)
Es seien $f, g \in K[x]$, und f sei nicht das Nullpolynom. Man sagt $g|f$, also g teilt f, falls es ein $q \in K[x]$ mit $f(x) = q(x) \cdot g(x)$ gibt. Dann heißt q Teiler von f.

Beispiel 3.1.1. Es sei $K = \mathbb{R}$, $f(x) = x^3 - 1$ und $g(x) = x - 1$. Dann ist $g|f$, da $f(x) = q(x) \cdot g(x)$ mit $q(x) = x^2 + x + 1$.

Beispiel 3.1.2. Es sei $K = (\mathbb{Z}/2\mathbb{Z}, +, \cdot)$. Es bedeute $\overline{a} = a \bmod 2$. Weiter seien $f(x) = x^2 + \overline{1}$ und $g(x) = x + \overline{1}$. Dann ist $g(x)|f(x)$, da $g(x)^2 = x^2 + (x + x) + \overline{1}$ und $x + x = x \cdot (\overline{1} + \overline{1}) = x \cdot \overline{0} = \overline{0}$ ist. Also ist $f(x) = g(x)^2$, und damit gilt $g(x)|f(x)$.

Definition 3.1.2. (Kongruenz)
Es seien $f, g \in K[x]$ und $q \in K[x]\backslash\{0\}$. Dann ist $f \equiv g \bmod q$, falls $q(x)|(f(x) - g(x))$ gilt.

Beispiel 3.1.3. Es sei $K = \mathbb{R}$, $f(x) = x^3 + x^2 - 1$, $g(x) = x^2$ sowie $q(x) = x - 1$. Dann ist $f \equiv g \bmod q$, da $f(x) - g(x) = x^3 - 1 = (x - 1) \cdot (x^2 + x + 1)$ gilt.

Wie bei Zahlkongruenzen können auch bei Polynomkongruenzen Restklassen und Restklassenringe eingeführt werden.

Satz 3.1.1. *Es sei $q \in K[x]$ und $q \neq 0$. Die Relation $\equiv \bmod q$ ist eine Äquivalenzrelation.*

Definition 3.1.3. Es sei $q \in K[x]\backslash\{0\}$. Die Äquivalenzklassen bzgl. der Relation $\equiv \bmod q$ heißen Kongruenzklassen oder Restklassen mod q.

Wiederum ist es möglich, Restklassen zu addieren und zu multiplizieren. Die übersichtliche Darstellung des Produkts zweier Restklassen beruht auf der Division mit Rest.

Satz 3.1.2. *(Division mit Rest)*
Es seien $f, g \in K[x]$ und $g \neq 0$. Dann gibt es $q, r \in K[x]$ mit $\operatorname{grad} r < \operatorname{grad} q$ oder $r = 0$, so daß $f = q \cdot g + r$ gilt.

Die Ermittlung von q und r geschieht mittels der "langen Division":
Wir geben zunächst eine kurze Beschreibung und illustrieren sie dann mit einem Beispiel.

Beschreibung der langen Division:
Es seien $f, g \in K[x]$ mit $g \neq 0$ gegeben.
Gesucht sind $q, r \in K[x]$ mit $\operatorname{grad} r < \operatorname{grad} q$ oder $r = 0$.

Fall 1: $\operatorname{grad} f < \operatorname{grad} g$
Wähle $q = 0$ und $r = f$.

Fall 2: $\operatorname{grad} f \geq \operatorname{grad} g$
Es sei $f(x) = a_n x^n + \ldots + a_0$ und $g(x) = b_m x^m + \ldots + b_0$ mit $a_n, b_m \neq 0$.
1. Schritt:
Bilde $r_1(x) = f(x) - a_n b_m^{-1} x^{n-m} g(x)$. Es ist $\operatorname{grad} r_1(x) < \operatorname{grad} f(x)$.
Weitere Schritte:
Wiederhole diesen Schritt mit $f \to r_1$. Es ergibt sich r_2 mit $\operatorname{grad} r_2(x) < \operatorname{grad} r_1(x)$. Ebenso $r_3, \ldots, r_m$.
Ist $\operatorname{grad} r_m(x) < \operatorname{grad} g(x)$, so ist $r = r_m$.
Ende des Algorithmus.

Beispiel 3.1.4. Es sei $K = \mathbb{R}$, $f(x) = x^5 + x^3 - 2x^2 + 1$ und $g(x) = 2x^3 + 3x - 2$. Dann ist

$$\begin{array}{rrrrl} (x^5 & +x^3 & -2x^2 & +1) & : \quad (2x^3 + 3x - 2) = \frac{1}{2}x^2 - \frac{1}{4} \\ -(x^5 & +\frac{3}{2}x^3 & -x^2) & & \\ \hline & -\frac{1}{2}x^3 & -x^2 & +1 & \\ & -(-\frac{1}{2}x^3 & & -\frac{3}{4}x & +\frac{1}{2}) \\ \hline & & -x^2 & +\frac{3}{4}x & +\frac{1}{2} \end{array}$$

Also ist $f(x) = q(x) \cdot g(x) + r(x)$ mit $q(x) = \frac{1}{2}x^2 - \frac{1}{4}$ und $r(x) = -x^2 + \frac{3}{4}x + \frac{1}{2}$.

Beispiel 3.1.5. Es sei $K = (\mathbb{Z}/3\mathbb{Z}, +, \cdot)$, und $\overline{a}$ bedeute a mod 3. Es seien die Polynome $f(x) = x^2 + \overline{2}$, $g(x) = x^3 + \overline{2}x + \overline{2}$ und $q(x) = x^2 + x + \overline{1}$ gegeben.
Man finde eine Darstellung der Form $(f(x) \bmod q) \cdot (g(x) \bmod q) = p(x) \bmod q$ mit $\operatorname{grad} p < 2$.

Lösung:
Es ist $f(x) \cdot g(x) = x^5 + x^3 + \overline{2}x^2 + x + \overline{1}$. Wir führen die Division mit Rest durch:

$$\begin{array}{rrrrrl} (x^5 & +x^3 & +\overline{2}x^2 & +x & +\overline{1}) & : \quad (x^2 + x + \overline{1}) = x^3 + \overline{2}x^2 + x + \overline{2} \\ -(x^5 & +x^4 & +x^3) & & & \\ \hline & \overline{2}x^4 & +\overline{2}x^2 & +x & & \\ & -(\overline{2}x^4 & +\overline{2}x^3 & +\overline{2}x^2) & & \\ \hline & & x^3 & +x & +\overline{1} & \\ & & -(x^3 & +x^2 & +x) & \\ \hline & & & \overline{2}x^2 & +\overline{1} & \\ & & & -(\overline{2}x^2 & +\overline{2}x + \overline{2}) & \\ \hline & & & & x + \overline{2} & \end{array}$$

Also ist $f(x) \cdot g(x) = (x^3 + \overline{2}x^2 + x + \overline{2}) \cdot q(x) + (x + \overline{2})$. Damit gilt

$$(f(x) \bmod q) \cdot (g(x) \bmod q) = (x + \overline{2}) \bmod q.$$

Definition 3.1.4. Ein Polynom $f \in K[x]$ heißt irreduzibel, falls es nicht das Produkt zweier Polynome kleineren Grades ist.

3.2 Endliche Körper

Die einfachsten endlichen Körper haben wir bereits kennengelernt. Es sind dies die Restklassenringe $GF(p) = (\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ mit einer Primzahl p. Sämtliche endliche Körper sind eng mit diesem Beispiel verbunden.

Satz 3.2.1. *Die Ordnung eines endlichen Körpers ist stets eine Primzahlpotenz $q = p^n$. Der Körper $GF(q)$ ist bis auf Isomorphie eindeutig bestimmt. Es ist*

$$GF(q) \cong (\mathbb{Z}/p\mathbb{Z})[x]/(f_0)$$

mit einem irreduziblen Polynom $f_0 \in (\mathbb{Z}/p\mathbb{Z})[x]$ mit $\operatorname{grad} f_0 = n$.

Beispiel 3.2.1. Finde die Verknüpfungstafeln für den Körper $GF(4)$.

Lösung:
Das Polynom $f_0(x) = x^2+x+\overline{1} \in (\mathbb{Z}/2\mathbb{Z})[x]$ ist irreduzibel. Wäre es ein Produkt von Polynomen ersten Grades, so hätte es eine Nullstelle. Nach Satz 3.2.1 ist $GF(4) \cong (\mathbb{Z}/2\mathbb{Z})[x]/(f_0)$. Es sei $t = x \bmod f_0$. Dann ist $GF(4) = \{\overline{0}, \overline{1}, t, t + \overline{1}\}$.

Die Verknüpfungstabellen für die Addition und die Multiplikation haben die Gestalt

$+$	$\overline{0}$	$\overline{1}$	t	$t+\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	t	$t+\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$	$t+\overline{1}$	t
t	t	$t+\overline{1}$	$\overline{0}$	$\overline{1}$
$t+\overline{1}$	$t+\overline{1}$	t	$\overline{1}$	$\overline{0}$

und

$\cdot$	$\overline{0}$	$\overline{1}$	t	$t+\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	t	$t+\overline{1}$
t	$\overline{0}$	t	$t+\overline{1}$	$\overline{1}$
$t+\overline{1}$	$\overline{0}$	$t+\overline{1}$	$\overline{1}$	t

Das einzige Problem ist die Bestimmung von t^2. Es ist $t^2 = x^2 \bmod f_0$. Division mit Rest ergibt $x^2 = (x^2 + x + \overline{1}) + x + \overline{1}$. Also ist $x^2 \equiv (x + \overline{1}) \bmod f_0$. Alle anderen Summen und Produkte ergeben sich nach den Rechengesetzen für Körper.

Kapitel 4

Fehlerkorrigierende Codes

4.1 Einleitung

Codes werden bei der Übertragung und Umsetzung von Nachrichten aller Art verwendet. Das grundlegende Modell der Nachrichtenübertragung kann wie folgt dargestellt werden:

Viele Kanäle haben dabei folgende Eigenschaften:

i) Übertragen werden Zeichenfolgen aus Zeichen eines endlichen Alphabets.

ii) Nur gewisse Zeichenfolgen sind Codeworte, andere nicht.

Das Problem der Theorie der fehlerkorrigierenden Codes ist, Fehler in der Übertragung zu erkennen und zu korrigieren. Dies ist natürlich nur dann möglich, wenn nicht zu viele Fehler bei der Übertragung auftreten.

Beispiel 4.1.1. Ein Absender schickt seinem Partner eine Nachricht über den Zeitpunkt eines Treffens. Es wurde vereinbart, daß nur der Monatsname übermittelt werden soll. Der Absender möchte die Nachricht `Juni` schicken, macht jedoch einen einzigen Fehler und schickt die Nachricht `Juli`.
Hier kann der Fehler weder erkannt noch korrigiert werden: `Juni` und `Juli` sind beides mögliche Codeworte. Sie besitzen den Hammingabstand 1 und können durch einen einzigen Fehler ineinanderübergehen.

Aus diesem Beispiel ergibt sich eine erste Forderung an einen guten Code: Um Fehler bei der Übertragung erkennen und möglichst korrigieren zu können, sollten zwei verschiedene Codeworte einen nicht zu kleinen Hammingabstand haben.

Beispiel 4.1.2. Die einfachsten Codes, die dies erreichen, sind die sogenannten Repetition-Codes, deren Codeworte durch mehrfaches Aneinanderhängen der ursprünglichen Buchstaben der Nachricht gebildet werden. Der Nachricht `Juni` wird im Falle eines Repetition-Codes der Ordnung 3 der Code `JJJuuunnniii` zugeordnet. Wird nun die Nachricht `JJJuuunlniii` empfangen, so kann der Fehler erkannt werden. Die empfangene Nachricht ist kein Codewort, da der Buchstabe l nur einmal auftritt. Es wird angenommen, daß nur ein einziger Fehler unterlaufen ist. Dieser muß an der Stelle des "l" passiert sein. Die einzige Möglichkeit, die Nachricht durch Abänderung einer einzigen Stelle in ein Codewort umzuwandeln, besteht darin, das "l" durch ein "n" zu ersetzen.

Die Repetition-Codes haben den Nachteil, daß sie sehr ineffizient sind. Im obigen Beispiel wird beim Repetition-Code der Ordnung 3 pro Zeichen nur ein Drittel der Information übertragen. Der Repetition-Code enthält im Verhältnis zu seiner Länge nur wenige Codeworte. Gute Codes sollten folgende Eigenschaften haben:

1. Um möglichst viel Information übertragen zu können, sollte der Code möglichst viele Codeworte (im Vergleich zur Länge) enthalten.
2. Um Fehler bei der Übertragung nachweisen und korrigieren zu können, sollten zwei verschiedene Codeworte einen nicht zu kleinen Hammingabstand besitzen.
3. Die Fehlerkorrektur sollte einfach durchführbar sein.

4.2 Grundlegende Sätze und Definitionen

Wir betrachten im folgenden nur Codes, in denen alle Codeworte die gleiche Länge besitzen (sogenannte Blockcodes).

Definition 4.2.1. Es X eine endliche Menge. Der Hammingabstand auf dem Kartesischen Produkt X^n zweier Tupel $\vec{x} = (x_1, \ldots, x_n)$ und $\vec{y} = (y_1, \ldots, y_n)$ ist durch

$$d(\vec{x}, \vec{y}) \;=\; |\{i \mid x_i \neq y_i\}|$$

definiert.

Satz 4.2.1. *Der Hammingabstand ist eine Metrik auf X^n, d.h. es gilt*

- $d(\vec{x}, \vec{z}) =\leq d(\vec{x}, \vec{y}) + d(\vec{y}, \vec{z})$ *(Dreiecksungleichung),*
- $d(\vec{x}, \vec{y}) = 0 \Leftrightarrow \vec{x} = \vec{y}$ *(Definitheit).*

Beweis. Es seien $\vec{x} = (x_1, \ldots, x_n)$, $\vec{y} = (y_1, \ldots, y_n)$ und $\vec{z} = (z_1, \ldots, z_n)$ Elemente von X^n. Gilt $z_i \neq x_i$, so ist notwendigerweise $y_i \neq x_i$ oder $z_i \neq y_i$, also gilt $\{i \mid z_i \neq x_i\} \subseteq \{i \mid y_i \neq x_i\} \cup \{i \mid z_i \neq y_i\}$. und damit die erste Aussage. Die zweite Aussage ist trivial. □

Definition 4.2.2. Es sei X eine endliche Menge der Mächtigkeit $q \in \mathbb{N}$. Ein $(n, M, d; q)$-Code (oder kürzer (n, M, d)-Code, wenn q klar ist) auf X ist eine M-elementige Teilmenge $C \subseteq X^n$, für die $d(\vec{x}, \vec{y}) \geq d$ für alle $\vec{x}, \vec{y} \in C$ mit $\vec{x} \neq \vec{y}$ gilt, und für die es auch $\vec{x}, \vec{y} \in C$ mit $d(\vec{x}, \vec{y}) = d$ gibt. Die Zahl d heißt Minimalabstand des Codes C.

Wir werden im folgenden sogenannte lineare Codes betrachten:

4.3 Lineare Codes

Bei linearen Codes ist das verwendete Alphabet der endliche Körper $GF(q)$ mit q Elementen. Nach Satz 3.2.1 ist q eine Primzahlpotenz, also $q = p^m$. In der Praxis ist fast nur der Fall $q = 2^m$ von Bedeutung, weil dann die Elemente des Alphabets als Folge von Nullen und Einsen der Länge m geschrieben werden können.

Ein linearer Code C läßt sich dann als linearer Unterraum des Vektorraums $\mathrm{GF}(q)^n$ beschreiben.

Zur Fehlerkorrektur können Methoden der Linearen Algebra verwendet werden. Auch grundlegende Parameter, wie beispielsweise der Minimalabstand, können einfach bestimmt werden.

Definition 4.3.1. Ein $(n, M, d; q)$-Code C über GF(q) heißt linear, wenn C ein Unterraum des Vektorraums GF$(q)^n$ ist.

Satz 4.3.1. *Es ist stets* $M = q^k$ *mit* $k = \dim(C)$.

Beweis. Aus der Linearen Algebra ist bekannt, dass C eine Basis $B = \{\vec{b}_1, \ldots, \vec{b}_k\}$ mit $\vec{b}_i \in C$ besitzt. Dann ist jedes $\vec{x} \in C$ eindeutig als Linearkombination

$$\vec{x} \;=\; \sum_{j=1}^{k} \lambda_j \vec{b}_j \;\;,\;\; \lambda_j \in \mathrm{GF}(q)$$

darstellbar. Für die Wahl eines jeden λ_j gibt es q Möglichkeiten. Insgesamt erhalten wir $|C| = q^k$. $\square$

Beispiel 4.3.1. ($(7,4)$-Hamming-Code)
Wir verwenden das Alphabet $X = \{0, 1\}$, das mit dem Körper GF$(2) = \{0 \bmod 2, 1 \bmod 2\}$ identifiziert wird. Addition und Multiplikation sind auf GF(2) wie folgt definiert:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Der $(7,4)$- Hamming- Code C ist die Menge aller Zeichenfolgen aus $X^7 = \{(x_1, x_2, \ldots, x_7) \colon x_j \in X\}$, die das folgende lineare Gleichungssystem erfüllen:

$$\begin{aligned}
&(1) && x_2 + x_3 + x_4 + x_5 && = 0\\
&(2) && x_1 + x_3 + x_4 + x_6 && = 0\\
&(3) && x_1 + x_2 + x_4 + x_7 && = 0,
\end{aligned}$$

oder in Matrixschreibweise: $H \cdot \vec{x} \;=\; \vec{0}$, mit

$$H \;=\; \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} .$$

Definition 4.3.2. Es sei C ein linearer $(n, q^k, d; q)$-Code. Wenn $\vec{a}_1, \ldots, \vec{a}_k$ eine Basis von C ist, so heißt die Matrix G mit Zeilen $\vec{a}_1, \ldots, \vec{a}_k$ eine Generatormatrix für C.

Die Kontrollmatrix eines Codes C hängt mit dessen zugehöriger Generatormatrix mittels der Konzepte der Orthogonalität und des zu C dualen Codes $C^\perp$ zusammen.

Definition 4.3.3. Es seien $\vec{x} = (x_1, \ldots, x_n), \vec{y} = (y_1, \ldots, y_n) \in \mathrm{GF}(q)^n$. Unter dem inneren Produkt $\langle \vec{x} | \vec{y} \rangle$ verstehen wir

$$\langle \vec{x} | \vec{y} \rangle \;=\; \sum_{i=1}^{n} x_i y_i \;=\; x_1 y_1 + \cdots + x_n y_n \,.$$

Die Vektoren $\vec{x}$ und $\vec{y}$ heißen orthogonal, falls $\langle \vec{x} | \vec{y} \rangle = 0$ ist.

Satz 4.3.2. *Es sei* $C \subset GF(q)$ *ein linearer Code. Die Menge* $C^\perp = \{\vec{y} \in \mathrm{GF}(q)^n \mid \langle \vec{x} | \vec{y} \rangle = 0,\ \forall \vec{x} \in C\}$ *ist ebenfalls ein linearer Code, d.h. ein Unterraum von* GF$(q)^n$.
Es ist $\dim C + \dim C^\perp = n$ *und* $(C^\perp)^\perp = C$.

Beweis. Es sei G eine Generatormatrix von C. Es ist genau dann $\vec{y} \in C^\perp$, wenn $\langle \vec{a}_i | \vec{y} \rangle = 0$ für sämtliche Zeilen von G ist, d.h. wenn

$$G\vec{y} = \vec{0} \qquad (*)$$

ist.
Die Behauptung von Satz 4.3.2 folgt aus der Theorie der linearen Gleichungssysteme. □

Definition 4.3.4. Der Code $C^\perp$ heißt der zu C duale Code. Eine Generatormatrix von $C^\perp$ heißt Kontrollmatrix von C.

Satz 4.3.3. *Es sei $C \subset GF(q)^n$ ein linearer Code mit Generatormatrix G und Kontrollmatrix H. Es sei G vom Typ (k, n). Jede Kontrollmatrix H ist dann vom Typ $(n-k, n)$. Es ist $|C| = q^k$.*

Beweis. Dies folgt aus den Sätzen 4.3.1 und 4.3.2. □

Satz 4.3.4. *Es sei $C \subset GF(q)^n$ ein linearer Code mit Kontrollmatrix H. Dann ist*

$$\vec{x} \in C \;\Leftrightarrow\; H \cdot \vec{x} = \vec{0}\,.$$

Beweis. Dies folgt aus der Tatsache $(*)$ aus dem Beweis von Satz 4.3.2. □

Der Minimalabstand von linearen Codes läßt sich besonders einfach bestimmen. Wir beschreiben im folgenden das Verfahren.

Definition 4.3.5. i) Es sei $\vec{x} \in \mathrm{GF}(q)^n$. Das Gewicht $w(\vec{x})$ ist die Anzahl der Koordinaten ungleich Null in $\vec{x}$.

ii) Ist C ein linearer Code, so ist $\min\{w(\vec{x}) |\ \vec{x} \in C \backslash \{\vec{0}\}\}$ das Minimalgewicht von C.

Satz 4.3.5. *i) Für beliebige $\vec{x}, \vec{y} \in \mathrm{GF}(q)^n$ gilt $d(\vec{x}, \vec{y}) = w(\vec{x} - \vec{y})$.*

ii) Für einen linearen Code ist der Minimalabstand gleich dem Minimalgewicht.

Beweis. i) Es sei $\vec{x} = (x_1, \ldots, x_n)$ und $\vec{y} = (y_1, \ldots, y_n)$. Dann ist genau dann $x_i - y_i \neq 0$, wenn $x_i \neq y_i$ ist. Also ist $d(\vec{x}, \vec{y}) = w(\vec{x} - \vec{y})$.

ii) Es seien w_0 bzw. d_0 Minimalgewicht bzw. Minimalabstand von C sowie $\vec{x}_0 \in C$ mit $w(\vec{x}_0) = w_0$. Dann ist $d(\vec{x}_0, \vec{0}) = w_0$. Also ist $d_0 \leq w_0$.
Weiter seien $\vec{x}_1, \vec{x}_2 \in C$ mit $d(\vec{x}_1, \vec{x}_2) = d_0$. Da C linear ist, ist $\vec{x}_1 - \vec{x}_2 \in C$, also $w(\vec{x}_1 - \vec{x}_2) = d_0$. Folglich ist $w_0 \leq d_0$. Daraus folgt die Behauptung.

□

Satz 4.3.6. *Es sei C ein linearer Code mit Kontrollmatrix H. Dann sind Minimalabstand und Minimalgewicht gleich der Minimalzahl der linear abhängigen Spalten von C.*

Beweis. Die Spalten $\vec{v}_{j_1}, \ldots, \vec{v}_{j_l}$ von H sind genau dann linear abhängig, wenn es ein Codewort $\vec{x}_0 = (x_1, \ldots, x_n)$ mit $x_{j_1}\vec{v}_1 + \ldots + x_{j_l}\vec{v}_l = \vec{0}$ und $x_i = 0$ für $i \notin \{j_1, \ldots, j_l\}$ gibt. □

Beispiel 4.3.2. $((7,4)$-Hamming-Code)
In der Kontrollmatrix

$$H = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

sind die Spalten $\vec{y}_1, \vec{v}_2, \vec{v}_3$ linear abhängig. Es ist $\vec{s}_1 + \vec{s}_2 + \vec{s}_3 = H(1,1,1,0,0,0,0) = \vec{0}$. Es gibt keine einzelne linear abhängige Spalte, da sie alle von $\vec{0}$ verschieden sind. Es gibt keine zwei linear abhängige, da sie alle verschieden sind.

4.4 Fehlerkorrektur

Definition 4.4.1. Es sei C ein (nicht notwendigerweise linearer) Code.
Der Code C heißt e-fehlerkorrigierend, wenn für seinen Minimalabstand d_0 gilt: $d_0 = 2e + 1$.

Beispiel 4.4.1. Der $(7, 4)$- Hamming-Code ist ein 1-fehlerkorrigierender Code, da der Minimalabstand $d = 3 = 2 \cdot 1 + 1$ ist.

Der Name e- fehlerkorrigierend erklärt sich aus folgender Tatsache:

Satz 4.4.1. *Es sei X eine endliche Menge und $C \in X^n$. Für $\vec{x}^* \in X^n$ gibt es genau ein Codewort $\vec{x}_0 \in C$ mit $d(\vec{x}^*, \vec{x}_0) \leq e$.*

Beweis. Es sei $d(\vec{x}^*, \vec{x}_1) \leq e$ und $d(\vec{x}^*, \vec{x}_2) \leq e$. Nach der Dreiecksungleichung ist $d(\vec{x}_1, \vec{x}_2) \leq 2e$ im Widerspruch zur Definition des Minimalabstandes. □

Daraus ergibt sich folgendes Verfahren zur Fehlerkorrektur unter der Annahme, daß bei der Übertragung eines Codeswortes $\vec{x}_0$ höchstens e Fehler unterlaufen sind.

Es sei $\vec{x}^*$ die empfangene Zeichenfolge. Man finde das Codewort $\vec{x}_0$, für das $d(\vec{x}^*, \vec{x}_0)$ minimal ist.

Bei linearen Codes gibt es einen Algorithmus, der dies durchführt: die Syndrommethode.

Definition 4.4.2. Es sei $C \subset GF(q)^n$ linear mit Kontrollmatrix H. Für $\vec{x} \in GF(q)^n$ heißt $\vec{s}(\vec{x}) = H\vec{x}$ das Syndrom von $\vec{x}$. Nach Satz 4.3.4 ist $\vec{x} \in C \Leftrightarrow \vec{s}(\vec{x}) = \vec{0}$.

Anstelle einer systematischen Diskussion erklären wir das Verfahren für den 1- fehlerkorrigierenden $(7, 4)$- Hammingcode.

Beispiel 4.4.2. Bei der Übertragung des Codewortes sei an der j- ten Stelle ein Fehler unterlaufen. Dann lautet die übertragene Zeichenfolge $\vec{x}^* = \vec{x}_0 + \vec{e}_j$ mit dem Fehlervektor $\vec{e}_j = (0, \ldots, 1, \ldots, 0)$ mit einer 1 an der j- ten Stelle. Es ist $H\vec{x}^* = H\vec{x}_0 + H\vec{e}_j = \vec{v}_j$, die j- te Spalte von H. Man ändert also die j- te Stelle und erhält $\vec{x}^* - \vec{e}_j = \vec{x}_0$, das beabsichtigte Codewort.

Beispiel 4.4.3. Es wurde ein Fehler gemacht und $\vec{x}^* = (0, 0, 1, 0, 0, 0, 1)$ übertragen. Man nehme die Fehlerkorrektur vor.

Lösung: Es ist

$$H \cdot \vec{x}' = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = \vec{v}_4 \,.$$

Der Fehler ist also an der vierten Stelle begangen, d.h. die Zeichenfolge $\vec{x}^*$ ist zum Codewort $\vec{x}_0 = (0011001)^T$ zu korrigieren.