Kurze Einführung in Gruppen- und Zahlentheorie

Johannes Blömer

Wintersemester 2003/04

1 Grundlegendes aus der Gruppentheorie

Definition 1.1 *Eine abelsche oder kommutative Gruppe $(G, e, \circ)$ ist eine Menge G mit einem ausgezeichneten Element $e \in G$, genannt das neutrale Element der Gruppe, und einer Verknüpfung*

$$\begin{aligned} \circ : G \times G &\longrightarrow G \\ (g_1, g_2) &\longmapsto g_1 \circ g_2, \end{aligned}$$

die folgende Eigenschaften haben:

1) $g \circ e = e \circ g = g$ *für alle* $g \in G$
2) $g_1 \circ g_2 = g_2 \circ g_1$ *für alle* $g_1, g_2 \in G$
3) *Zu jedem* $g \in G$ *existiert ein* $h \in G$ *mit* $g \circ h = h \circ g = e$. h *ist das Inverse von* g, *geschrieben* $h = g^{-1}$.
4) $(g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3)$.

Die Gruppe heisst endlich, falls G nur endlich viele Elemente enthält.

Da wir in dieser Vorlesung nur endliche abelsche Gruppe kennenlernen werden, wird in Zukunft der Zusatz "abelsch" fallengelassen. In der Regel werden wir eine Gruppe nur durch die zugrunde liegende Menge G und nicht durch das Tripel $(G, e, \circ)$ identifizieren.

Zwei Typen von Gruppen, die immer wieder auftauchen werden, sind die Gruppen $\mathbf{Z}_n$ und $\mathbf{Z}_n^*$, $n \in \mathbb{N}$. Die zu $\mathbf{Z}_n$ gehörige Menge ist $\{0, 1, \ldots, n-1\}$, die zugehörige Verknüpfung ist die Addition modulo n, und das neutrale Element demnach 0. Das zu $g \in \mathbb{Z}$ gehörige Inverse ist $n - g$, wobei hier die normale Subtraktion in $\mathbb{Z}$ gemeint ist.

Die zu $\mathbf{Z}_n^*$ gehörige Menge ist

$$\{a \in \mathbb{N} | 1 \leq a \leq n-1,\ a \text{ und } n \text{ sind teilerfremd}\},$$

die Verknüpfung ist die Multiplikation modulo n, und das neutrale Element ist die 1. Im Moment mag es noch nicht klar sein, dass Multiplikation zweier Elemente in $\mathbf{Z}_n^*$ wieder ein solches Element liefert, oder dass es zu jedem Element in $\mathbf{Z}_n^*$ ein Inverses gibt. Dieses wird im nächsten Abschnitt bewiesen werden.

Definition 1.2 *Sei $(G, e, \circ)$ eine Gruppe. Eine Untergruppe U von $(G, e, \circ)$ ist eine Teilmenge von G, die e enthält, und zusammen mit der Verknüpfung $\circ$ selbst eine Gruppe ist. Insbesondere muss gelten $u_1 \circ u_2 \in U$ für alle $u_1, u_2 \in U$.*

Falls d ein Teiler von n ist, so bilden alle Vielfachen von d die zwischen 0 und $n-1$ liegen, eine additive Untergruppe von $\mathbf{Z}_n$.

Gegeben G und eine Untergruppe U von G kann man eine Äquivalenzrelation auf G wie folgt definieren:

$$g_1 \equiv g_2, \text{ falls } g_1 \circ g_2^{-1} \in U.$$

Für $g \in G$ ist die Menge aller zu g äquivalenten Elemente gegeben durch $gU = \{g \circ u | u \in U\}$. Zwei Äquivalenzklassen sind entweder identisch (als Mengen), oder aber sie sind disjunkt. Man sieht auch recht leicht, dass alle Äquivalenzklassen dieselbe Anzahl von Elementen enthalten.

Bezeichnen wir nun für eine beliebige endliche Menge S mit $|S|$, die Anzahl der Element in S, so folgt, dass für jede Untergruppe U einer endlichen Gruppe G die Anzahl der Elemente $|U|$ von U die Anzahl der Gruppenelemente $|G|$ teilt. Man nennt $|U|$ auch die *Ordnung von U*. Insbesondere heisst $|G|$ die Gruppenordnung. Also,

Lemma 1.3 *Bei einer endlichen Gruppe teilt die Ordnung jeder Untergruppe die Gruppenordnung.*

Sei $g \in G$. Wir können $g^i, i \in \mathbb{N}$ induktiv wie folgt definieren: $g^0 = e, g^i = g^{i-1} \circ g$. Die *Ordnung von g* ist nun die kleinste natürliche Zahl $m \neq 0$ mit $g^m = e$. Falls die Gruppe G nicht endlich ist, muss es ein solches m nicht geben. Bei einer endlichen Gruppe G existiert ein solches m dagegen für jedes Gruppenelement.

Ist G endlich, $g \in G$ und m die Ordnung von g, so ist $\{g^i | i = 0, \ldots, m\}$ eine Untergruppe von G. Sie heisst *die von g erzeugte Untergruppe*. Die Ordnung, der von g erzeugten Untergruppe, ist also die Ordnung von g. Aus Lemma 1.3 erhalten wir also

Korollar 1.4 *Bei einer endlichen Gruppe teilt die Ordnung jedes Elements der Gruppe die Gruppenordnung.*

Die von einem Element erzeugten Untergruppen nennt man *zyklische Untergruppen*. Die Gruppe G heisst *zyklisch*, falls es ein Element $g \in G$ gibt, so dass die von g erzeugte Untergruppe die gesamte Gruppe G ist. In solch einem Fall nennt man g auch *erzeugendes Element* von G.

Falls $g \in G$ und m die Ordnung von g ist, so gilt $g^d = e$ für jedes Vielfache d von m. Bevor wir zur Zahlentheorie übergehen, wollen wir noch eine Umkehrung dieses Sachverhaltes beweisen.

Lemma 1.5 *Sei G eine endliche Gruppe und $g \in G$ mit Ordnung m. Falls $d \in \mathbb{N}$ mit $g^d = e$, dann wird d von m geteilt.*

Beweis: Es muss gezeigt werden, dass m ein Teiler von d, falls $g^d = e$. Angenommen dieses sei nicht der Fall. Dann ist $r = d \bmod m$ eine positive ganze Zahl, von Null verschieden und echt kleiner als m. Wir können d ausdrücken als $r = d - qm$, $q \in \mathbb{N}$. Dann gilt $g^r = g^{d-qm} = g^d \circ g^{-qm} = e \circ (g^m)^{-q} = e$. Dieses allerdings widerspricht der Tatsache, dass m die *kleinste* positive Zahl mit $g^m = e$ sein sollte. Also ist $r = 0$ und d ist ein Vielfaches von m. □

2 Grundlegendes aus der Zahlentheorie

Zunächst werden wir die allgemeinen Konzepte des letzten Abschnitts auf die Gruppen $\mathbf{Z}_n$ und $\mathbf{Z}_n^*$ anwenden. Hier, wie auch im Rest der Vorlesung, spielt der *grösste gemeinsamer Teiler* ggT zweier Zahlen eine wesentliche Rolle. Sind $n, m \in \mathbb{Z}$, so ist der grösste gemeinsame Teiler $\mathrm{ggT}(n, m)$ die grösste positive ganze Zahl, die sowohl n als auch m teilt. Schreiben wir $d|n$, falls $d \in \mathbb{Z}$ die Zahl $n \in \mathbb{Z}$ teilt, so können wir den ggT zweier Zahlen etwas formaler (und sehr nützlich) auch folgendermassen definieren.

Definition 2.1 *Seien $m, n \in \mathbb{Z}$. Die Zahl $d \in \mathbb{N}$ heisst der grösste gemeinsame Teiler von n und m, geschrieben $d = \mathrm{ggT}(n, m)$, falls für jede ganze Zahl $k \in \mathbb{Z}$ mit $k|m$ und $k|n$ gilt, dass auch $k|d$.*

Gemäß dieser Definition ist der grösste gemeinsame Teiler zweier ganzen Zahlen immer eine *positive* ganze Zahl. Zwei ganze Zahlen m, n heissen *teilerfremd* oder auch *relativ prim*, falls $\mathrm{ggT}(m, n) = 1$.

Beispiel 2.2 *1) Der grösste gemeinsame Teiler von* 12 *und* 40 *ist* 4.

2) Der grösste gemeinsame Teiler von 21 *und* 33 *ist* 3.

3) Der grösste gemeinsame Teiler von 123 *und* 17 *ist* 1. *Die beiden Zahlen sind also teilerfremd, oder relativ prim.*

Zurück zunächst zur Gruppe $\mathbf{Z}_n$. Die Operation $\circ$ ist also die Addition modulo n und entsprechend schreiben wir nicht $g^i, g \in \mathbf{Z}_n, i \in \mathbb{Z}$, sondern ig. Die Gruppenordnung ist n. Jedes Element in $\mathbf{Z}_n$ ist ein Vielfaches von 1, und somit ist die von 1 erzeugte Untergruppe die gesamte Gruppe $\mathbf{Z}_n$. 1 ist also erzeugendes Element der Gruppe.

Als nächstes wollen wir für jedes Element $g \in \mathbf{Z}_n$ seine Ordnung bestimmen. Auf diesen speziellen Fall angewendet: Die Ordnung von $g \in \mathbf{Z}_n$ ist die kleinste, von Null verschiedene Zahl m mit $mg \equiv 0 \bmod n$. Nun gilt, dass $m = \frac{n}{\mathrm{ggT}(n,g)}$ in

$\mathbb{Z}$ liegt und die Eigenschaft $mg \equiv 0 \bmod n$ hat. Es folgt aus der Definition des ggT, dass m die kleinste Zahl mit dieser Eigenschaft ist. Also ist die Ordnung von g gegeben durch $n/\mathrm{ggT}(n, g)$.

Falls $\mathrm{ggT}(n, g) = 1$, hat g Ordnung n. Dies bedeutet, dass die von g erzeugte Untergruppe n Elemente besitzt, und damit die gesamte Gruppe $\mathbf{Z}_n$ ist.

Als nächstes wollen wir die Untergruppen von $\mathbf{Z}_n$ bestimmen. Sei also $U \subseteq \{0, 1, \ldots, n-1\}$ eine Untergruppe. Sei g das kleinste Element in dieser Untergruppe. Wir wollen zeigen, dass dann U die von g erzeugte zyklische Untergruppe ist. Dazu müssen wir zeigen, dass sich jedes Element $u \in U$ als ein Vielfaches von g schreiben lässt. Wir benutzen dieselbe Argumentation wie im Beweis von Lemma 1.5. Wir nehmen also an, es gäbe ein u, dass nicht Vielfaches von g ist. Dann gilt $u = qg + r$ mit $0 < r < g \leq n - 1$. Nun liegen aber sicherlich u und qg in der Untergruppe U. Damit aber auch r. Dies widerspricht der Annahme, dass g das kleinste Element in U ist, und wir können folgern, dass U die von g erzeugte zyklische Untergruppe ist.

Dasselbe Resultat bekommen wir auch, indem wir beobachten, dass in jeder zyklischen Gruppe alle Untergruppen zyklisch sein müssen. Die Argumentation von oben hat aber den Vorteil, dass sie uns auch zeigt, wie für eine Untergruppe ein erzeugendes Element gefunden werden kann.

Jetzt kommen wir zu der für uns viel interessanteren, aber auch schwierigeren Gruppe $\mathbf{Z}_n^*$. Die Operation $\circ$ ist also die Multiplikation modulo n, die wir als einfache Multiplikation ab oder $ab \bmod n$ schreiben. Im Moment haben wir noch nicht einmal gezeigt, dass dieses überhaupt eine Gruppe ist, denn wir haben weder die Abgeschlossenheit der Multiplikation noch die Existenz eines Inversen bewiesen. Dies werden wir jetzt nachholen.

Hierzu beobachten wir zunächst, dass wir mit Hilfe des ggT $\mathbf{Z}_n^*$ auch durch $\mathbf{Z}_n^* = \{g \in \mathbf{Z}_n | \mathrm{ggT}(n, g) = 1\}$ definieren können. Zunächst wollen wir zeigen, dass die Multiplikation abgeschlossen ist, also $a, b \in \mathbf{Z}_n^*$ impliziert $ab \bmod n \in \mathbf{Z}_n^*$ oder $\mathrm{ggT}(ab \bmod n, n) = 1$. Das folgende kleine Lemma ist sehr nützlich und wird implizit immer wieder benutzt.

Lemma 2.3 *Seien $m, n \in \mathbb{Z}$, dann gilt $\mathrm{ggT}(n, m) = \mathrm{ggT}(n \bmod m, m) = \mathrm{ggT}(m \bmod n, n)$.*

Für die Abgeschlossenheit genügt es also zu zeigen, dass mit a und b auch ab zu n teilerfremd ist. Hierzu benutzen wir die folgende wichtige Eigenschaft von Primzahlen.

Lemma 2.4 *Sei p eine Primzahl. Falls p das Produkt ab teilt, so teilt es mindestens einen der beiden Faktoren a, b.*

Falls $\mathrm{ggT}(ab, n) \neq 1$, so gibt es eine Primzahl, die den ggT teilt, nach dem Lemma somit eine Primzahl, die sowohl n als auch a oder b teilt. Entweder a oder b war dann aber nicht zu n teilerfremd.

Schliesslich wollen wir auch zeigen, dass es zu jedem Element $g \in \mathbf{Z}_n^*$ ein Inverses gibt. Für jedes feste, aber beliebige $g \in \mathbf{Z}_n^*$ wollen wir die Existenz eines $h \in \mathbf{Z}_n^*$ mit $gh \equiv 1 \bmod n$ zeigen. Hierzu betrachten wir für g die Menge $\{ag \bmod n | a \in \mathbf{Z}_n^*\}$. Je zwei Elemente dieser Menge sind verschieden, denn wäre

$ag \equiv bg \bmod n$ mit $a < b$, so folgt $(b-a)g \equiv 0 \bmod n$, oder $n|(b-a)g$. Da g zu n teilerfremd ist, muss dann $n|(b-a)$ gelten. $b-a$ ist aber echt kleiner als n und nicht Null, kann also von n nicht geteilt werden. Damit wissen wir, dass in $\{ag \bmod n | a \in \mathbf{Z}_n^*\}$ genauso viele Elemente wie in $\mathbf{Z}_n^*$ liegen. Anderseits ist es aber eine Teilmenge von $\mathbf{Z}_n^*$. Hieraus folgt $\{ag \bmod n | a \in \mathbf{Z}_n^*\} = \mathbf{Z}_n^*$ und es muss ein $a \in \mathbf{Z}_n^*$ mit $ag \equiv 1 \bmod n$ geben. Dieses ist unser gesuchtes Inverses zu g.

Jetzt wissen wir also, dass $\mathbf{Z}_n^*$ eine Gruppe ist. Als nächstes wollen wir etwas über die Gruppenordnung von $\mathbf{Z}_n^*$ sagen.

Definition 2.5 *Die Eulersche ϕ-Funktion ist definiert auf den natürlichen Zahlen $\mathbb{N}$. Der Wert $\phi(n)$ an der Stelle $n \in \mathbb{N}$ ist definiert als die Anzahl der zu n teilerfremden Zahlen in $\mathbf{Z}_n$.*

Nach Definition ist die Ordnung von $\mathbf{Z}_n^*$ genau $\phi(n)$. Es gilt

Lemma 2.6 *Sei $n \in \mathbb{N}$ und sei $n = \prod_{i=1}^{k} p_i^{e_i}$ die Primfaktorzerlegung von n. Dann gilt:*

$$\phi(n) = \prod_{i=1}^{k} (p_i^{e_i} - p_i^{e_i - 1}) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

Dieses Lemma werden wir erst später beweisen. Jetzt wollen wir uns nur an Spezialfällen überzeugen, dass es korrekt ist. Betrachten wir den Fall, dass n eine Primzahl ist. Das Lemma sagt, dass $\phi(n) = n-1$. Dieses ist leicht zu überprüfen, denn bis auf 0 sind alle Zahlen in $\mathbf{Z}_n$ zu n teilerfremd. Etwas allgemeiner sei nun $n = p^e$ eine Primzahlpotenz. Das Lemma sagt $\phi(n) = \phi(p^e) = p^e - p^{e-1}$. Nun lassen sich die Zahlen in $\mathbb{Z}_{p^e}$, die nicht zu p^e teilerfremd sind, leicht bestimmen. Es sind dies genau die Zahlen der Form lp, wobei $l = 0, 1, \ldots, p^{e-1} - 1$. Demnach sind p^{e-1} Elemente in $\mathbb{Z}_{p^e}$ nicht zu p^e teilerfremd, und das Lemma gibt auch in diesem Fall die korrekte Antwort. Wir werden in Kürze den Beweis des Lemma mit Hilfe des Chinesischen Restsatzes führen.

Es stellt sich die Frage, ob $\mathbf{Z}_n^*$ wie $\mathbf{Z}_n$ eine sehr einfache Struktur hat, nämlich eine zyklische Gruppe ist. Im allgemeinen stimmt dieses nicht, wie das nächste Lemma zeigt.

Lemma 2.7 *Sei $n \in \mathbb{N}$. Die Gruppe $\mathbf{Z}_n^*$ ist zyklisch genau dann, wenn $n = 2, 4$ ist oder aber die Form $n = p^e, n = 2p^e$ hat, wobei $e \in \mathbb{N}$ beliebig sein kann, und p eine Primzahl $\neq 2$ sein muss.*

Wir werden dieses Lemma nicht beweisen. Einen schönen Beweis gibt es in [**?**].

Beispiel 2.8 *Schauen wir uns $n = 9$ an. Nach dem Lemma ist $\mathbb{Z}_9^*$ zyklisch. $\phi(9) = 9 - 3 = 6$ und die Ordnung von $\mathbb{Z}_9^*$ ist 6. Setzen wir $g = 2$, so erhalten wir folgende Tabelle für die Potenzen von g modulo 9.*

i	0	1	2	3	4	5
g^i	1	2	4	8	7	5

2 ist also ein erzeugendes Element von $\mathbb{Z}_9^*$.

Beispiel 2.9 *Als nächstes betrachten wir $n = 8$. Gemäss dem Lemma ist die Gruppe $\mathbf{Z}_8^*$ nicht zyklisch. Die Gruppenordnung ist $\phi(8) = 4$, und die Elemente der Gruppe sind $1, 3, 5, 7$. Für diese Elemente gilt $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \bmod 8$. Wie erwartet gibt es keine Elemente der Ordnung 4.*

Sehr nützlich ist das folgende, als *Lemma von Euler* bekannte Resultat.

Lemma 2.10 *Für alle $a \in \mathbf{Z}_n^*$ gilt*

$$a^{\phi(n)} \equiv 1 \bmod n.$$

Beweis: Wir wissen aus dem letzten Abschnitt, dass für jede Gruppe G mit neutralem Element e und jedes $g \in G$ gilt, $g^{|G|} = e$. Das Lemma ist der Spezialfall $G = \mathbf{Z}_n^*$. □

Wir wollen uns nun noch die Ordnung von Elementen in $\mathbf{Z}_n^*$ genauer anschauen.

Definition 2.11 *Sei $a \in \mathbf{Z}_n^*$. Die Ordnung von a in der Gruppe $\mathbf{Z}_n^*$ wird mit $\mathrm{ord}_n(a)$ bezeichnet.*

Für $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, n) = 1$ ist die Ordnung von a definiert als die Ordnung von $a \bmod n \in \mathbf{Z}_n^*$. Auch diese Ordnung bezeichnen wir mit $\mathrm{ord}_n(a)$.

Jetzt erhalten wir folgendes Lemma.

Lemma 2.12 *Sei nun $n = 2, 4$ oder $n = p^e, 2p^e$ und somit die Gruppe $\mathbf{Z}_n^*$ zyklisch. Weiter sei g ein erzeugendes Element für $\mathbf{Z}_n^*$ und $a = g^d \in \mathbf{Z}_n^*$. Dann ist*

$$\mathrm{ord}_n(a) = \frac{\phi(n)}{\mathrm{ggT}(\phi(n), d)}.$$

Ähnliche Aussagen haben wir schon vorher bewiesen, daher ist der Beweis eine gute Übungsaufgabe.

Insbesondere sagt das Lemma, dass es für $\mathbb{Z}_p^*$ genau $\phi(p-1)$ viele erzeugende Elemente gibt. Hat man eines, sagen wir g, so sind die anderen gegeben durch g^d, wobei $0 < d < p-1$ zu $p-1$ teilerfremd sein muss.

Beispiel 2.13 *Betrachten wir $p = 7$. Für $p = 7$ und $g = 3$ erhalten wir folgende Tabelle für die Potenzen von g modulo 7.*

i	0	1	2	3	4	5
g^i	1	3	2	6	4	5

$g = 3$ ist also erzeugendes Element. Da $\phi(6) = 2$ gibt es nur ein weiteres erzeugendes Element, nämlich $3^5 \equiv 5 \bmod 7$.

Als nächstes kommen wir zum *Chinesischen Restsatz*.

Satz 2.14 (Chinesischer Restsatz) *Seien $m_1, \ldots, m_k$ paarweise zueinander teilerfremde Zahlen (also $\mathrm{ggT}(m_i, m_j) = 1$ für alle $i \neq j$) und seien $a_1, \ldots, a_k$ beliebige ganze Zahlen. Das System von Kongruenzen*

$$\begin{aligned} x &\equiv a_1 \bmod m_1 \\ &\vdots \\ x &\equiv a_k \bmod m_k \end{aligned}$$

besitzt eine Lösung. Diese Lösung ist modulo $\prod_{i=1}^{k} m_i$ eindeutig bestimmt.

Sowohl die Existenz als auch die Eindeutigkeit ist wichtig an der Aussage dieses Satzes. Statt des Beweises hier ein Beispiel.

Beispiel 2.15 *Seien $m_1 = 5, m_2 = 7, m_3 = 9$ und $a_1 = 1, a_2 = 2, a_3 = 3$. Dann ist die gesuchte Lösung durch $x = 156$ gegeben. Jede andere Lösung y erfüllt $y \equiv 156 \bmod 5 * 7 * 9$.*

Als erste Anwendung des Chinesischen Restsatzes wollen wir Lemma 2.6 beweisen.

Beweis: [Beweis von Lemma 2.6] Wir haben uns schon vorher überlegt, dass $\phi(p^e) = p^e - p^{e-1}$ für Primzahlpotenzen p^e gilt. Sei nun $n \in \mathbb{N}$ beliebig mit Primfaktorzerlegung $n = \prod_{i=1}^{k} p_i^{e_i}$. Sei $a \in \mathbf{Z}_n^*$, dann ist für jedes $i = 1, \ldots, k$ die Zahl $a_i \equiv a \bmod p_i^{e_i}$ ein Element aus $\mathbb{Z}^*_{p_i^{e_i}}$. Wir können also jedem $a \in \mathbf{Z}_n^*$ ein k-tupel in $\mathbb{Z}^*_{p_1^{e_1}} \times \cdots \times \mathbb{Z}^*_{p_k^{e_k}}$ zuordnen.

Nach dem Chinesischen Restsatz angewandt mit den Moduli $m_i = p_i^{e_i}$ entspricht aber auch jedem k-Tupel $(a_1, \ldots, a_k) \in \mathbb{Z}^*_{p_1^{e_1}} \times \cdots \times \mathbb{Z}^*_{p_k^{e_k}}$ ein Element a in $\mathbf{Z}_n$. Dieses Element muss aber sogar in $\mathbf{Z}_n^*$ liegen. Wäre dem nicht so, wäre a zu mindestens einem $p_i^{e_i}$ nicht teilerfremd. Deshalb müsste dann für das entsprechende a_i ebenfalls gelten, dass es nicht zu $p_i^{e_i}$ teilerfremd ist, Widerspruch.

Wiederum nach dem Chinesischen Restsatz sind für verschiedene k-Tupel $(a_1, \ldots, a_k)$ die entsprechenden a's in $\mathbf{Z}_n^*$ verschieden. Damit ergibt sich

$$\phi(n) = |\mathbf{Z}_n^*| = |\mathbb{Z}^*_{p_1^{e_1}} \times \cdots \times \mathbb{Z}^*_{p_k^{e_k}}| = \prod_{i=1}^{k} (p^e - p^{e-1}),$$

und Lemma 2.6 ist bewiesen. □

Als zweite Anwendung des Chinesischen Restsatzes wollen wir uns jetzt noch überlegen, dass $\mathbf{Z}_n^*$ nicht zyklisch sein kann, falls $n = pq$, wobei $p \neq 2$ und $q \neq 2$ verschiedene Primzahlen sind. Dies ist ein Spezialfall des Lemmas 2.7. Wäre $\mathbf{Z}_n^*$ zyklisch, so gäbe es in $\mathbf{Z}_n^*$ ein Element der Ordnung $\phi(n)$. Da $n = pq$ ist, gilt

$$\phi(n) = (p-1)(q-1).$$

Wir werden nun zeigen, dass für alle $a \in \mathbf{Z}_n^*$ gilt, $a^{(p-1)(q-1)/2} \equiv 1 \bmod n$.

Zunächst beachte man, dass $p - 1/2$ und $q - 1/2$ beide in $\mathbb{N}$ liegen, da p, q ungerade sind. Sei nun $a_p \in \mathbb{Z}_p^*$ mit $a_p \equiv a \bmod p$ und $a_q \in \mathbb{Z}_q^*$ mit $a_q \equiv a \bmod q$. Es gilt

$$a^{(p-1)(q-1)/2} \equiv a_p^{(p-1)(q-1)/2} \bmod p$$

und analog für q. Nach dem Chinesischen Restsatz gilt $a^{(p-1)(q-1)/2} \equiv 1 \bmod n$, falls $a_p^{(p-1)(q-1)/2} \equiv 1 \bmod p$ und $a_q^{(p-1)(q-1)/2} \equiv 1 \bmod q$.

Wir zeigen nun $a_p^{(p-1)(q-1)/2} \equiv 1 \bmod p$, die Aussage für q folgt analog. Da $\phi(p) = p - 1$, falls p eine Primzahl ist, gilt nach Lemma 2.10

$$a_p^{(p-1)(q-1)/2} \equiv \left(a_p^{p-1}\right)^{(q-1)/2} \equiv 1^{(q-1)/2} \equiv 1 \bmod p.$$

Wie oben schon bemerkt, folgt jetzt das $\mathbf{Z}_n^*$ nicht zyklisch ist.

Zum Abschluss dieses Abschnittes betrachten wir noch den *Euklidischen Algorithmus* und seine Komplexität. Der euklidische Algorithmus berechnet den grössten gemeinsamen Teiler zweier Zahlen.

Euklidischer Algorithmus

`Eingabe:` $m, n \in \mathbb{Z}$

`Ausgabe:` Der grösste gemeinsame Teiler $\mathrm{ggT}(m, n)$ von m und n.

`1. Schritt` Setze $a := m, b := n, r := 0$.

`2. Schritt` Falls $a < 0$, ersetze a durch $-a$. Falls $b < 0$, ersetze b durch $-b$.

`3. Schritt` Falls $b \neq 0$, setze $r := b, b := a \bmod r, a := r$, sonst `Ausgabe` $\mathrm{ggT}(m, n) = a$.

Die Korrektheit dieses Algorithmus folgt unmittelbar aus der Gleichung $\mathrm{ggT}(m, n) = \mathrm{ggT}(n, m \bmod n)$, die wir schon in Lemma 2.3 beobachtet haben. Eine Laufzeitanalyse findet man in vielen Büchern über Algorithmen, z. B. in [**?**]. Wie notieren hier nur das Ergebnis.

Lemma 2.16 *Seien $m, n \in \mathbb{Z}$ und sei $|n| \geq |m|$, wobei $|n|$ der Absolutbetrag der Zahl n ist. Dann berechnet der euklidische Algorithmus den grössten gemeinsamen Teiler von m und n mit $\mathcal{O}(\log^2(|n|))$ vielen Bitoperationen.*

Eine leicht geänderte Variante des euklidischen Algorithmus kann benutzt werden, um den $\mathrm{ggT}(m, n)$ als ganzzahlige Linearkombination vo m und n darzustellen, d. h. der Algorithmus berechnet $s, t \in \mathbb{Z}$ mit $\mathrm{ggT}(n, m) = sm + tn$.

Erweiterter Euklidischer Algorithmus (EAA)

`Eingabe:` $m, n \in \mathbb{Z}$

`Ausgabe:` Der grösste gemeinsame Teiler $\mathrm{ggT}(m, n)$ von m und n, sowie $s, t \in \mathbb{Z}$ mit $\mathrm{ggT}(m, n) = sm + tn$.

`1. Schritt` Setze $a := m, b := n, s_0 := 1, s_1 := 0, t_0 := 0, t_1 := 1, r := 0, q := 0, u := 0, v := 0$.

`2. Schritt` Falls $a < 0$, ersetze a durch $-a$ und setze $s_0 = -1$. Falls $b < 0$, ersetze b durch $-b$ und setze $t_1 = -1$.

`3. Schritt` Falls $b \neq 0$, setze $r := b, b := a \bmod r, q := a \operatorname{div} r, a := r$. Ausserdem setze man:

$$\begin{aligned} u &:= s_1 \\ v &:= t_1 \\ s_1 &:= s_0 - qs_1 \\ t_1 &:= t_0 - qt_1 \\ s_0 &:= u \\ t_0 &:= v \end{aligned}$$

Sonst `Ausgabe` $\mathrm{ggT}(m,n) = a, s = s_0, t = t_0$.

Die Korrektheit des Algorithmus ist nicht schwer einzusehen. Am Anfang hat man $s_0 m + t_0 n = a$ und $s_1 m + t_1 n = b$. Nun überlegt man sich, dass diese Eigenschaft bei Änderung von a, b durch die entsprechende Änderung von s_0, s_1, t_0, t_1 aufrechterhalten bleibt. Die Laufzeit des erweiterten euklidischen Algorithmus ist dieselbe wie beim euklidischen Algorithmus (siehe wiederum [**?**]).

Lemma 2.17 *Seien $m, n \in \mathbb{Z}$ und sei $|n| \geq |m|$, wobei $|n|$ der Absolutbetrag der Zahl n ist. Dann ist die Laufzeit des erweiterten euklidischen Algorithmus $\mathcal{O}(\log^2(|n|))$.*

Falls $a \in \mathbf{Z}_n^*$, so ist $\mathrm{ggT}(a,n) = 1$. Bei Eingabe a, n berechnet EAA also Zahlen s, t mit $sa + tn = 1$. Nehmen wir diese Gleichung modulo n, erhalten wir $sa \equiv 1 \bmod n$, und somit ist s das Inverse von a in $\mathbf{Z}_n^*$. Wir erhalten als Korollar aus Lemma 2.17

Korollar 2.18 *Sei $a \in \mathbf{Z}_n^*$. Das Inverse von a in $\mathbf{Z}_n^*$ kann in Zeit $\mathcal{O}(\log^2(n))$ berechnet werden.*