3. Multiplikative Struktur der Restklassenringe

In jedem Ring R mit Einselement können wir die Einheitengruppe $R^\times$ betrachten. Speziell für $R = \mathbb{Z}_n$ ist $\mathbb{Z}_n^\times$ eine endliche abelsche Gruppe, die genau aus denjenigen Restklassen $[x]$ modulo n besteht, für die x teilerfremd zu n ist. Die Elementezahl von $\mathbb{Z}_n^\times$ ist daher gerade die Anzahl derjenigen natürlichen Zahlen $1 \le x \le n$, die teilerfremd zu n sind. Da diese Anzahl in vielen Zusammenhängen eine Rolle spielt, führen wir eine eigene Bezeichnung ein.

(3.1) Definition. *Für $n \in \mathbb{N}$ bezeichne $\varphi(n)$ die Anzahl derjenigen natürlichen Zahlen $1 \le x \le n$, die zu n teilerfremd sind, also die Bedingung $\mathrm{ggT}(x,n) = 1$ erfüllen. Die Funktion $\varphi : \mathbb{N} \to \mathbb{N}$ wird als* **Eulersche Funktion** *bezeichnet.*

Der folgende Satz ergibt sich daraus, daß für eine endliche Gruppe stets $x^{|G|} = e$ für alle $x \in G$ gilt.

(3.2) Satz von Euler. *Es sei $n \in \mathbb{N}$ beliebig. Ist $a \in \mathbb{Z}$ teilerfremd zu n, so gilt $a^{\varphi(n)} \equiv 1$ modulo n.*

Beweis. Die Gruppe $G = \mathbb{Z}_n^\times$ hat die Ordnung $|G| = \varphi(n)$. Nach Voraussetzung liegt die Restklasse $[a]$ von a modulo n in $\mathbb{Z}_n^\times$; also gilt $[a]^{\varphi(n)} = [1]$. Das ist schon die Behauptung. ∎

Als Spezialfall von (3.2) ergibt sich die folgende Aussage.

(3.3) Kleiner Fermatscher Satz. *Es sei p eine Primzahl. Ist $a \in \mathbb{Z}$ nicht durch p teilbar, so gilt $a^{p-1} \equiv 1$ modulo p.*

Beweis. Wende (3.2) mit $n = p$ an. ∎

Wir stellen einige Eigenschaften der Eulerschen Funktion zusammen.

(3.4) Satz. *Die Eulersche Funktion hat die folgenden Eigenschaften.*

(a) *Sind m und n teilerfremd, so gilt $\varphi(mn) = \varphi(m)\varphi(n)$.*

(b) *Ist p eine Primzahl, so gilt für alle Exponenten $k \in \mathbb{N}$ die Gleichung $\varphi(p^k) = p^k - p^{k-1}$. Insbesondere gilt also $\varphi(p) = p - 1$.*

(c) *Für alle $n \ge 3$ ist $\varphi(n)$ eine gerade Zahl.*

(d) *Für alle $n \in \mathbb{N}$ gilt $\sum_{d|n} \varphi(d) = n$, wobei die Summe über alle Teiler $1 \le d \le n$ von n gebildet wird.*

Beweis. (a) Nach dem Chinesischen Restsatz gilt $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$ (als Ringisomorphismus); hieraus folgt dann $\mathbb{Z}_{mn}^\times \cong \mathbb{Z}_m^\times \times \mathbb{Z}_n^\times$ (als Gruppenisomorphismus). Es ergibt sich

$$\begin{aligned}\varphi(mn) &= |\mathbb{Z}_{mn}^\times| = |\mathbb{Z}_m^\times \times \mathbb{Z}_n^\times| \\ &= |\mathbb{Z}_m^\times| \cdot |\mathbb{Z}_n^\times| = \varphi(m)\varphi(n).\end{aligned}$$

(b) Von den p^k Zahlen $1, 2, 3, \ldots, p^k$ sind genau diejenigen nicht teilerfremd zu p^k, die durch p teilbar sind; dies sind die p^{k-1} Zahlen px mit $1 \le x \le p^{k-1}$. Es verbleiben dann $p^k - p^{k-1}$ Zahlen, die zu p^k teilerfremd sind.

(c) Jede Zahl $n \ge 3$ enthält einen ungeraden Primfaktor p oder ist durch eine Zweierpotenz 2^m mit $m \ge 2$ teilbar. Im ersten Fall enthält $\varphi(n)$ den Faktor $p - 1$, im zweiten Fall den Faktor $2^m - 2^{m-1} = 2^{m-1}$. In jedem Fall ist also $\varphi(n)$ durch 2 teilbar.

(d) Es sei $X := \{1, \ldots, n\}$. Für jeden Teiler d von n sei S_d die Menge aller $x \in X$ mit $\mathrm{ggT}(x,n) = d$. Die Mengen S_d bilden dann eine Partition der Menge X, so daß $n = |X| = \sum_{d|n} |S_d|$ gilt. Für jeden Teiler d von n sei $d_\star := n/d$ der zugehörige komplementäre Teiler; dann gilt

$$\begin{aligned}S_d &= \{x \in X \mid \mathrm{ggT}(x,n) = d\} \\ &= \{x \in X \mid \mathrm{ggT}(x, dd_\star) = d\} \\ &= \{d\xi \mid 1 \le \xi \le d_\star,\ \mathrm{ggT}(\xi, d_\star) = 1\}\end{aligned}$$

und daher $|S_d| = \varphi(d_\star)$. Durchläuft d die Menge aller Teiler von n, so durchläuft auch $d_\star$ die Menge aller Teiler von n. Es gilt daher

$$n = \sum_{d|n} |S_d| = \sum_{d|n} \varphi(d_\star) = \sum_{d_\star|n} \varphi(d_\star),$$

und das ist die Behauptung. ∎

Wir wollen klären, für welche Werte von n die Gruppe $\mathbb{Z}_n^\times$ zyklisch ist, und betrachten dazu zunächst einige Beispiele.

(3.5) Beispiel: $n = 9$. Wegen $\varphi(9) = \varphi(3^2) = 3^2 - 3^1 = 9 - 3 = 6$ hat $\mathbb{Z}_9^\times$ sechs Elemente. Insbesondere gilt also $a^6 = 1$ für alle $a \in \mathbb{Z}_9^\times$. Wir berechnen die Potenzen aller Elemente der Gruppe.

a	a^2	a^3	a^4	a^5	a^6	$\mathrm{ord}(a)$
1	1	1	1	1	1	1
2	4	8	7	5	1	6
4	7	1	4	7	1	3
5	7	8	4	2	1	6
7	4	1	7	4	1	3
8	1	8	1	8	1	2

Es gibt zwei Elemente der Ordnung 6, nämlich 2 und 5. Insbesondere ist $\mathbb{Z}_9^\times$ zyklisch; sowohl 2 als auch 5 ist ein Erzeuger von $\mathbb{Z}_9^\times$.

(3.6) Beispiel: $n = 18$. Wegen $\varphi(18) = \varphi(2 \cdot 3^2) = \varphi(2)\varphi(3^2) = 1 \cdot 6 = 6$ hat $\mathbb{Z}_{18}^\times$ sechs Elemente. Insbesondere gilt also $a^6 = 1$ für alle $a \in \mathbb{Z}_{18}^\times$. Wir berechnen die Potenzen aller Elemente der Gruppe.

a	a^2	a^3	a^4	a^5	a^6	$\mathrm{ord}(a)$
1	1	1	1	1	1	1
5	7	17	13	11	1	6
7	13	1	7	13	1	3
11	13	17	7	5	1	6
13	7	1	13	7	1	3
17	1	17	1	17	1	2

Es gibt zwei Elemente der Ordnung 6, nämlich 5 und 11. Insbesondere ist $\mathbb{Z}_{18}^\times$ zyklisch; sowohl 5 als auch 11 ist ein Erzeuger von $\mathbb{Z}_{18}^\times$.

(3.7) Beispiel: $n = 20$. Wegen $\varphi(20) = \varphi(2^2 \cdot 5) = \varphi(2^2)\varphi(5) = 2 \cdot 4 = 8$ hat $\mathbb{Z}_{20}^\times$ acht Elemente. Insbesondere gilt also $a^8 = 1$ für alle $a \in \mathbb{Z}_{20}^\times$. Wir berechnen die Potenzen aller Elemente der Gruppe.

a	a^2	a^3	a^4	a^5	a^6	a^5	a^8	$\mathrm{ord}(a)$
1	1	1	1	1	1	1	1	1
3	9	7	1	3	9	7	1	4
7	9	3	1	7	9	3	1	4
9	1	9	1	9	1	9	1	2
11	1	11	1	11	1	11	1	2
13	9	17	1	13	9	17	1	4
17	9	13	1	17	9	13	1	4
19	1	19	1	19	1	19	1	2

Wir sehen, daß kein Element der Ordnung 8 auftritt; die Gruppe $\mathbb{Z}_{20}^\times$ ist daher nicht zyklisch.

(3.8) Definition. *Wenn die Gruppe $\mathbb{Z}_n^\times$ zyklisch ist, so nennen wir jeden Erzeuger dieser Gruppe eine* **Primitivwurzel** *modulo n.*

(3.9) Bemerkung. Ist allgemein G eine endliche zyklische Gruppe der Ordnung m und ist g ein Erzeuger von G, so sind die paarweise verschiedenen Erzeuger von G genau die Elemente g^k mit $\mathrm{ggT}(k, m) = 1$, und davon gibt es $\varphi(m)$. Eine zyklische Gruppe der Ordnung m hat also genau $\varphi(m)$ Erzeuger. Ist also $\mathbb{Z}_n^\times$ zyklisch, so gibt es wegen $|\mathbb{Z}_n^\times| = \varphi(n)$ genau $\varphi\big(\varphi(n)\big)$ Erzeuger. Anders ausgedrückt: Existiert überhaupt eine Primitivwurzel modulo n, so gibt es exakt $\varphi\big(\varphi(n)\big)$ solcher Primitivwurzeln.

Wir wollen als erstes zeigen, daß $\mathbb{Z}_n^\times$ jedenfalls dann zyklisch ist, wenn n eine Primzahl ist. Dazu benötigen wir den folgenden Satz.

(3.10) Satz. *Es sei G eine endliche Gruppe mit n Elementen. (Wir schreiben G multiplikativ mit dem Neutralelement 1.) Gibt es für jeden Teiler $d|n$ höchstens d Elemente $x \in G$ mit $x^d = 1$, so ist G zyklisch.*

Beweis. Es sei $a \in G$ ein Element mit der Ordnung d. Nach dem Satz von Lagrange ist d ein Teiler von n. Die Elemente $a, a^2, \ldots, a^d = 1$ sind dann paarweise verschieden und erfüllen allesamt die Gleichung $x^d = 1$; nach Voraussetzung kann es in G andere Lösungen dieser Gleichung nicht geben. Jedes beliebige Element in G, das die Ordnung d hat, erfüllt nun die Gleichung $x^d = 1$, ist somit zwangsläufig eines der Elemente $a, a^2, \ldots, a^d$. Von diesen Elementen haben aber genau diejenigen Potenzen a^k die Ordnung d, für die der Exponent k teilerfremd zu d sind. Dies zeigt, daß es zu jeder in G auftretenden Ordnung d genau $\varphi(d)$ Elemente gibt, die diese Ordnung haben. Wenn es also in G überhaupt ein Element der Ordnung d gibt, so gibt es genau $\varphi(d)$ solcher Elemente.

Für jeden Teiler $d|n$ sei $a(d)$ die Anzahl der Elemente der Ordnung d. Wir haben gezeigt, daß entweder $a(d) = 0$ oder aber $a(d) = \varphi(d)$ gilt. Dies liefert

$$(\star) \qquad n \;=\; |G| \;=\; \sum_{d|n} a(d) \;\le\; \sum_{d|n} \varphi(d) \;=\; n,$$

wobei die letzte Gleichheit wegen (3.4)(d) gilt. Damit $(\star)$ gelten kann, muß $a(d) = \varphi(d)$ für alle $d|n$ gelten; der Fall $a(d) = 0$ kann also nicht auftreten. Insbesondere gilt also $a(n) = \varphi(n) > 0$. Damit ist G zyklisch. ∎

(3.11) Folgerung. *Es seien K ein beliebiger Körper und G eine endliche Untergruppe von $K^\times$. Dann ist G zyklisch.*

Beweis. Die Voraussetzung von (3.10) ist erfüllt, weil es in K höchstens d Lösungen der Gleichungen $x^d = 1$ gibt. Das Polynom $p(X) = X^d - 1$ hat nämlich den Grad d und damit höchstens d Nullstellen in K. ∎

(3.12) Folgerung. *Ist K ein endlicher Körper, so ist die Einheitengruppe $K^\times$ zyklisch. Insbesondere ist für jede Primzahl p die Einheitengruppe $\mathbb{Z}_p^\times$ zyklisch.*

Wir leiten nun eine Bedingung her, unter der $\mathbb{Z}_n^\times$ *nicht* zyklisch ist.

(3.13) Satz. *Gilt $n = ab$ mit teilerfremden Zahlen $a, b \ge 3$, so ist $\mathbb{Z}_n^\times$ nicht zyklisch.*

Beweis. Es sei x eine zu n teilerfremde natürliche Zahl (die ein Element von $\mathbb{Z}_n^\times$ repräsentiert). Nach dem Satz von Euler gelten die Kongruenzen $x^{\varphi(a)} \equiv 1$ modulo a und $x^{\varphi(b)} \equiv 1$ modulo b. Für $k := \mathrm{kgV}\big(\varphi(a), \varphi(b)\big)$ gelten daher die Kongruenzen $x^k \equiv 1$ modulo a und $x^k \equiv 1$ modulo b. Wegen der Teilerfremdheit von a und b gilt daher auch $x^k \equiv 1$ modulo ab; das bedeutet $[x]^k = [1]$ in $\mathbb{Z}_n^\times$. Weil die Zahlen $\varphi(a)$ und $\varphi(b)$ beide gerade sind, gilt $\mathrm{kgV}\big(\varphi(a), \varphi(b)\big) < \varphi(a) \cdot \varphi(b) = \varphi(ab) = \varphi(n)$, also $k < |\mathbb{Z}_n^\times|$. Die Ordnung von $[x]$ in $\mathbb{Z}_n^\times$ ist also kleiner als die Gruppenordnung, so daß $\mathbb{Z}_n^\times$ nicht von $[x]$ erzeugt wird. Da x beliebig war, wird also $\mathbb{Z}_n^\times$ nicht von einem einzelnen Element erzeugt. ∎

Die einzigen Zahlen, die von dem obigen Satz nicht erfaßt werden, sind die Zahlen der Form 2^k, p^k und $2p^k$ mit einer Primzahl $p \geq 3$ und einem Exponenten $k \in \mathbb{N}_0$. Wir betrachten nun den Fall, daß $n = 2^k$ eine Zweierpotenz ist. Offenbar sind die Gruppen $\mathbb{Z}_{2^k}^\times$ zyklisch für $k = 0, 1, 2$. Der folgende Satz zeigt, daß dies für höhere Zweierpotenzen nicht mehr der Fall ist.

(3.14) Satz. *Gilt $n = 2^k$ mit $k \geq 3$, so ist $\mathbb{Z}_n^\times$ nicht zyklisch.*

Beweis. Es sei x eine ungerade natürliche Zahl, also eine Zahl, die ein Element von $\mathbb{Z}_n^\times$ repräsentiert. Wir behaupten, daß

$$(\star) \qquad x^{2^{k-2}} \equiv 1 \text{ modulo } 2^k$$

gilt, was wir durch Induktion über k beweisen. Für $k = 3$ ist zu zeigen, daß $x^2 - 1$ durch 8 teilbar ist. Dies trifft zu, weil die ungerade Zahl x von der Form $x = 2m + 1$ ist und daher $x^2 - 1 = 4m^2 + 4m = 4m(m + 1)$ gilt. Beim Induktionsschritt $k \to k + 1$ nutzen wir aus, daß es nach Induktionsannahme eine Zahl $u \in \mathbb{N}$ mit

$$x^{2^{k-2}} \;=\; 1 + u \cdot 2^k$$

gibt. Quadrieren dieser Gleichung liefert

$$x^{2^{k-1}} \;=\; 1 + u \cdot 2^{k+1} + 2^{2k} \;\equiv\; 1 \text{ modulo } 2^{k+1},$$

was den Induktionsschritt abschließt. Aus $(\star)$ folgt, daß $[x]^{2^{k-2}} = [1]$ in $\mathbb{Z}_n^\times$ gilt. Die Gruppenordnung ist aber $|\mathbb{Z}_n^\times| = \varphi(n) = \varphi(2^k) = 2^{k-1} > 2^{k-2}$, so daß $[x]$ kein Erzeuger von $\mathbb{Z}_n^\times$ sein kann. Da x beliebig war, ist also $\mathbb{Z}_n^\times$ nicht zyklisch. ∎

(3.15) Satz. *Es sei m eine ungerade Zahl. Genau dann ist $\mathbb{Z}_m^\times$ zyklisch, wenn $\mathbb{Z}_{2m}^\times$ zyklisch ist.*

Beweis. Wir machen die folgenden Beobachtungen, die sich beide daraus ergeben, daß m ungerade ist:

(1) es gilt $\varphi(2m) = \varphi(2)\varphi(m) = \varphi(m)$;
(2) ist $w \in \mathbb{Z}$ ungerade, so gilt für $k \in \mathbb{N}$ genau dann $w^k \equiv 1$ modulo $2m$, wenn $x^k \equiv 1$ modulo m gilt.

Wir beweisen nun den angegebenen Satz.

• Zunächst sei $\mathbb{Z}_{2m}^\times$ zyklisch. Die Zahl $w \in \mathbb{N}$ repräsentiere einen Erzeuger von $\mathbb{Z}_{2m}^\times$; dann ist $\varphi(2m)$ die kleinste Zahl $k \in \mathbb{N}$ mit $w^k \equiv 1$ modulo $2m$. Da w zwangsläufig ungerade ist, ist wegen (1) und (2) daher auch $\varphi(m)$ die kleinste Zahl $k \in \mathbb{N}$ mit $w^k \equiv 1$ modulo m. Also hat w die Ordnung $\varphi(m)$ in $\mathbb{Z}_m^\times$, ist also ein Erzeuger von $\mathbb{Z}_m^\times$. Insbesondere ist $\mathbb{Z}_m^\times$ zyklisch.

• Nun sei $\mathbb{Z}_m^\times$ zyklisch. Die Zahl $w_1 \in \mathbb{N}$ repräsentiere einen Erzeuger von $\mathbb{Z}_m^\times$; dann repräsentiert auch $w_2 := w_1 + m$ einen Erzeuger von $\mathbb{Z}_m^\times$, und genau eine der beiden Zahl w_1 und w_2 ist ungerade. Diese bezeichnen wir mit w. Nach Voraussetzung ist dann $\varphi(m)$ die kleinste Zahl $k \in \mathbb{N}$ mit $w^k \equiv 1$ modulo m. Wegen (1) und (2) ist dann auch $\varphi(2m)$ die kleinste Zahl $k \in \mathbb{N}$ mit $w^k \equiv 1$ modulo $2m$. Daher hat w die Ordnung $\varphi(2m)$ in $\mathbb{Z}_{2m}^\times$, ist also ein Erzeuger von $\mathbb{Z}_{2m}^\times$. Insbesondere ist $\mathbb{Z}_{2m}^\times$ zyklisch. ∎

(3.16) Satz. *Es sei $p \geq 3$ eine Primzahl. Es gibt eine Primitivwurzel w modulo p mit $w^{p-1} \not\equiv 1$ modulo p^2. Jede solche Primitivwurzel modulo p ist dann auch eine Primitivwurzel modulo p^k für alle $k \geq 1$.*

Beweis. Es sei w_0 *irgendeine* Primitivwurzel modulo p. Gilt $w_0^{p-1} \not\equiv 1$ modulo p^2, so können wir einfach $w := w_0$ wählen. Gilt dagegen $w_0^{p-1} \equiv 1$ modulo p^2, so ist auch $w := w_0 + p$ eine Primitivwurzel modulo p, und unter Benutzung der binomischen Formel erhalten wir

$$\begin{aligned} w^{p-1} &= (w_0 + p)^{p-1} \\ &= w_0^{p-1} + (p-1)w_0^{p-2}p + \text{Terme mit } p^2 \\ &= w_0^{p-1} - w_0^{p-2}p + \text{Terme mit } p^2 \\ &= 1 - w_0^{p-2}p + \text{Terme mit } p^2 \\ &\not\equiv 1 \text{ modulo } p^2 \text{ wegen } p \nmid w_0. \end{aligned}$$

In jedem Fall gibt es also eine Primitivwurzel w modulo p mit $w^{p-1} \not\equiv 1$ modulo p^2. Eine solche Primitivwurzel w sei nun fest gewählt. Wir behaupten zunächst, daß dann

$$(\star) \qquad w^{\varphi(p^k)} \not\equiv 1 \text{ modulo } p^{k+1} \text{ für alle } k \geq 1$$

gilt, und beweisen diese Aussage mit Induktion über k. Der Fall $k = 1$ ist gerade die Voraussetzung über w. Beim Induktionsschritt gehen wir davon aus, daß $w^{\varphi(p^k)} \not\equiv 1$ modulo p^{k+1} gilt. Nach dem Satz von Euler gilt andererseits $w^{\varphi(p^k)} \equiv 1$ modulo p^k. Wir haben daher eine Darstellung $w^{\varphi(p^k)} = 1 + up^k$ mit $p \nmid u$. Wegen $\varphi(p^{k+1}) = p^{k+1} - p^k = p(p^k - p^{k-1}) = p \cdot \varphi(p^k)$ gilt also

$$\begin{aligned} w^{\varphi(p^{k+1})} &= \left(w^{\varphi(p^k)}\right)^p = (1 + up^k)^p \\ &= 1 + up^{k+1} + \text{Terme mit } p^{2k+1} \\ &\not\equiv 1 \text{ modulo } p^{k+2} \text{ wegen } p \nmid u. \end{aligned}$$

Damit ist $(\star)$ gezeigt. Wir wollen nun eine weitere Behauptung beweisen:

$(\star\star)$
Die Ordnung von w modulo p^k ist $\varphi(p^k)$ für alle $k \geq 1$.

Auch diese Aussage beweisen wir mit Induktion über k. Der Induktionsanfang $k = 1$ ergibt sich daraus, daß w nach Voraussetzung eine Primitivwurzel modulo p ist. Nach Induktionsannahme sei $\varphi(p^k)$ die Ordnung von w modulo p^k. Weiter sei m die Ordnung von w modulo p^{k+1}. Nach dem Satz von Lagrange ist dann m ein Teiler von $\varphi(p^{k+1})$. Andererseits folgt aus $w^m \equiv 1$ modulo p^{k+1} erst recht $w^m \equiv 1$ modulo p^k, so daß m ein Vielfaches von $\varphi(p^k)$ ist, da ja nach Induktionsannahme $\varphi(p^k)$ die Ordnung von w modulo p^k ist. Die Zahl m ist also einerseits ein Vielfaches von $\varphi(p^k)$, andererseits ein Teiler von $\varphi(p^{k+1}) = p \cdot \varphi(p^k)$. Dies läßt nur die beiden Möglichkeiten

$m = \varphi(p^k)$ und $m = \varphi(p^{k+1})$ offen. Die erste Möglichkeit scheidet aber wegen $(\star)$ aus, so daß die zweite Möglichkeit eintreten muß. Damit ist der Induktionsschritt zum Nachweis von $(\star\star)$ beendet. Aussage $(\star\star)$ bedeutet aber genau, daß w für jeden Exponenten $k \geq 1$ einen Erzeuger von $\mathbb{Z}_{p^k}^\times$ repräsentiert. ∎

Wir fassen unsere Ergebnisse kurz zusammen.

(3.17) Zusammenfassung. Die Gruppe $\mathbb{Z}_n^\times$ ist genau in den folgenden Fällen zyklisch:

- $n \in \{1, 2, 4\}$;
- n ist eine Potenz einer ungeraden Primzahl;
- n ist das Doppelte einer Potenz einer ungeraden Primzahl.

Der Beweis zu Satz (3.15) zeigt, wie man eine Primitivwurzel modulo $2m$ findet, wenn eine Primitivwurzel modulo m bekannt ist, und der Beweis zu Satz (3.16) zeigt, wie man eine Primitivwurzel modulo p^k findet, wenn eine Primitivwurzel modulo p bekannt ist. Noch nicht behandelt wurde die Frage, wie man eine Primitivwurzel modulo einer Primzahl p finden kann, ohne mit roher Gewalt alle Möglichkeiten durchzuprobieren. Bei der Beantwortung dieser Frage hilft der folgende Satz.

(3.18) Satz *Es sei G eine beliebige Gruppe. Für ein Element $a \in G$ sind dann die folgenden Aussagen äquivalent:*

(1) $\operatorname{ord}(a) = r$;
(2) $a^r = e$, aber $a^{r/q} \neq e$ für jeden Primteiler $q|r$.

Beweis. Aus (1) folgt trivialerweise (2). Umgekehrt gelte (2), und es sei $m = \operatorname{ord}(a)$. Dann gilt $m|r$. Wäre $m \neq r$, so besäße r/m einen Primteiler q, sagen wir $r/m = qs$ bzw. $r = mqs$. Dann wäre $a^{r/q} = a^{ms} = (a^m)^s = e^s = e$ im Widerspruch zu Voraussetzung (2). Also gilt $m = r$. ∎

(3.19) Folgerung. *Es seien p eine Primzahl und $a \in \mathbb{Z}$ eine nicht durch p teilbare Zahl. Genau dann ist a eine Primitivwurzel modulo p, wenn $a^{(p-1)/q} \not\equiv 1$ modulo p für jeden Primteiler $q|p-1$ gilt.*

Beweis. Wir wenden Satz (3.18) mit $G = \mathbb{Z}_p^\times$ und $r = p-1$ an. Da die Bedingung $[a]^{p-1} = [1]$ in $\mathbb{Z}_p$ nach dem Satz von Euler automatisch erfüllt ist, gilt nach Satz (3.18) genau dann $[a]^{(p-1)/q} \neq [1]$ in $\mathbb{Z}_p$ für jeden Primteiler $q|p-1$, wenn $\operatorname{ord}([a]) = p-1$ gilt. Das ist aber genau die Bedingung dafür, daß a eine Primitivwurzel modulo p ist. ∎

Bevor wir einige konkrete Beispiele betrachten, machen wir noch die folgenden Beobachtungen.

(3.20) Beobachtungen. (a) Ist p eine ungerade Primzahl, so kann kein Quadrat eine Primitivwurzel modulo p sein. Aus $a = b^2$ folgt nämlich $a^{(p-1)/2} = b^{p-1} = 1$ in $\mathbb{Z}_p^\times$, was wegen (3.19) ausschließt, daß a eine Primitivwurzel modulo p ist.

(b) Wenn wir die Primitivwurzeln modulo p suchen, so genügt es, die *kleinste* Zahl $a \in \mathbb{N}$ zu finden, die eine Primitivwurzel modulo p ist (alle anderen Primitivwurzeln sind dann die Zahlen a^k mit $\operatorname{ggT}\big(k, \varphi(n)\big) = 1$). Diese kleinste Zahl a kann nun niemals eine echte Potenz $a = b^N$ sein, denn ist b^N eine Primitivwurzel modulo p, so ist auch b eine.

Es ist jetzt klar, wie man für eine gegebene Primzahl p eine Primitivwurzel modulo p findet: Man geht die Zahlen $a = 2, 3, 4, 5, 6, \ldots$ der Reihe nach durch und berechnet jeweils alle Potenzen $a^{(p-1)/q}$, für die q ein Primteiler von $p-1$ ist. Sind alle diese Potenzen von 1 modulo p verschieden, so ist a eine Primitivwurzel. Wegen (3.20) dürfen wir dabei beim Durchprobieren der möglichen Werte von a alle echten Potenzen überspringen, also $4, 8, 9, 16, 25, 27$ und so weiter.

(3.21) Beispiele. (a) Es sei $p = 7$. Wir müssen die Zahlen $a = 2, 3, 5, 6$ durchprobieren. Wegen $p-1 = 6 = 2\cdot 3$ müssen wir jeweils überprüfen, ob a^2 und a^3 beide von 1 verschieden sind (modulo 7); genau dann, wenn dies der Fall ist, ist a eine Primitivwurzel modulo 7. Wir erhalten $(2^2, 2^3) = (4, 1)$; also ist $a = 2$ keine Primitivwurzel. Weiter ist $(3^2, 3^3) = (2, 6)$; also ist 3 eine Primitivwurzel. Damit sind wir eigentlich fertig. Wir probieren aber auch noch $a = 5$ und $a = 6$ aus. Wegen $(5^2, 5^3) = (4, 6)$ ist auch 5 eine Primitivwurzel; dagegen ist 6 keine Primitivwurzel, denn $(6^2, 6^3) = (1, 6)$. Die Primitivwurzeln modulo 7 sind also genau 3 und 5. Daß die Anzahl der Primitivwurzeln 2 sein würde, war von Anfang an klar, denn $\varphi\big(\varphi(p-1)\big) = \varphi(6) = 2$.

(b) Es sei $p = 761$. Wir müssen die Zahlen $a = 2, 3, 5, 6, \ldots, 760$ durchprobieren, wobei wir wegen (3.20) echte Potenzen auslassen dürfen. Wegen $p - 1 = 760 = 2^3 \cdot 5 \cdot 19$ müssen wir jeweils überprüfen, ob a^{380}, a^{152} und a^{40} allesamt von 1 verschieden sind (modulo 761); genau dann, wenn dies der Fall ist, ist a eine Primitivwurzel modulo 761. Wir erhalten die folgenden Ergebnisse.

- $(2^{380}, 2^{152}, 2^{40}) = (1, 67, 636)$;
- $(3^{380}, 3^{152}, 3^{40}) = (760, 1, 410)$;
- $(5^{380}, 5^{152}, 5^{40}) = (1, 1, 25)$;
- $(6^{380}, 6^{152}, 6^{40}) = (760, 67, 498)$.

Erstmals für $a = 6$ tritt also keine 1 mehr auf; also ist 6 die kleinste Primitivwurzel modulo 761. Insgesamt gibt es $\varphi\big(\varphi(760)\big) = \varphi\big(\varphi(2^3 \cdot 5 \cdot 19)\big) = \varphi(4 \cdot 4 \cdot 18) = \varphi(2^5 \cdot 3^3) = \varphi(2^5)\varphi(3^3) = 16 \cdot 18 = 288$ Primitivwurzeln modulo 761 (nämlich die Zahlen 6^k, wobei k teilerfremd mit 760 ist).

(c) Es sei $p = 409$. Wir müssen die Zahlen $a = 2, 3, 5, 6, \ldots, 408$ durchprobieren, wobei wir wegen (3.20) echte Potenzen auslassen dürfen. Wegen $p - 1 = 408 = 2^3 \cdot 3 \cdot 17$ müssen wir jeweils überprüfen, ob a^{51}, a^{136} und a^{24} allesamt von 1 verschieden sind (modulo 409); genau dann, wenn dies der Fall ist, ist a eine Primitivwurzel modulo 409. Hier ist eine längere Rechnung erforderlich; als kleinste Primitivwurzel ergibt sich $a = 21$ $\big($mit $(21^{51}, 21^{136}, 21^{24}) = (31, 355, 5)\big)$.