```
>> L := select(Liste,f);
              [1,5,11,13,17,19,23,25,29,31,37,41]
>> Einheitengruppe := map(L,R);
   [1 mod 42,  5 mod 42, 11 mod 42, 13 mod 42, 17 mod 42,
              19 mod 42,-19 mod 42,-17 mod 42,-13 mod 42,
                        -11 mod 42, -5 mod 42, -1 mod 42]
```

Für die Elementare Zahlentheorie, wie sie in diesem Buch behandelt wird, mag die Fähigkeit von MuPAD, die Restklassenringe von $\mathbb{Z}$ als algebraische Strukturen zu definieren, nicht von wesentlicher Bedeutung sein. MuPAD erlaubt es aber auch, etwa über einem Restklassenkörper $\mathbb{F}$ von $\mathbb{Z}$ den Ring $M(n;\mathbb{F})$ der quadratischen Matrizen einer bestimmten Zeilenzahl n zu erklären, und weiß dann, wie man darin rechnet, und auch, wie man den Rang, die Determinante oder das charakteristische Polynom einer Matrix aus $M(n;\mathbb{F})$ oder die Lösungsmenge eines linearen Gleichungssystems über dem Körper $\mathbb{F}$ berechnet. Darüber informiert die Dokumentation für die MuPAD-Library `linalg`.

5 Primitivwurzeln

(5.1) In diesem Paragraphen werden die natürlichen Zahlen m charakterisiert, für die die Einheitengruppe $E(\mathbb{Z}/m\mathbb{Z})$ des Restklassenrings $\mathbb{Z}/m\mathbb{Z}$ zyklisch ist. Außerdem wird für jedes $m \in \mathbb{N}$ die maximale Elementordnung in der Gruppe $E(\mathbb{Z}/m\mathbb{Z})$ berechnet.

(5.2) Bemerkung: Es sei p eine Primzahl. Der Restklassenring $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ ist ein Körper mit p Elementen, und seine Multiplikativgruppe

$$\mathbb{F}_p^\times \;=\; E(\mathbb{Z}/p\mathbb{Z}) \;=\; \big\{[1]_p, [2]_p, \ldots, [p-1]_p\big\}$$

ist eine zyklische Gruppe (vgl. (3.14)). Also gibt es ein $g \in \{1, 2, \ldots, p-1\}$ mit $\mathbb{F}_p^\times = \langle [g]_p \rangle$.

(5.3) Definition: Es sei p eine Primzahl. $g \in \mathbb{Z}$ heißt eine Primitivwurzel modulo p, wenn g nicht durch p teilbar ist und $\mathbb{F}_p^\times = \langle [g]_p \rangle$ gilt.

(5.4) Bemerkung: (1) Die Primitivwurzeln modulo 2 sind die ungeraden ganzen Zahlen.
(2) Es sei p eine ungerade Primzahl; es sei $g \in \mathbb{Z}$ mit $p \nmid g$. Die folgenden Aussagen sind äquivalent:

(a) g ist eine Primitivwurzel modulo p.
(b) Es ist $\operatorname{ord}([g]_p) = p - 1$.
(c) Es ist $\min(\{i \in \mathbb{N} \mid g^i \equiv 1 \pmod p\}) = p - 1$.
(d) Für jeden Primteiler q von $p-1$ gilt $g^{(p-1)/q} \not\equiv 1 \pmod p$.

Beweis: Daß (a), (b) und (c) äquivalent sind, ist klar.
(c) $\Rightarrow$ (d): Ist $\min(\{i \in \mathbb{N} \mid g^i \equiv 1 \pmod p\}) = p-1$, so gilt für jeden Primteiler q von $p-1$: Es ist $g^{(p-1)/q} \not\equiv 1 \pmod p$.
(d) $\Rightarrow$ (b): $d := \operatorname{ord}([g]_p)$ teilt $p-1$ (vgl. (4.21)(1)). Ist $d < p-1$, so gibt es einen Primteiler q von $(p-1)/d$, und hierfür gilt $q \mid p-1$ und $d \mid (p-1)/q$, also $[g]_p^{(p-1)/q} = [1]_p$ (vgl. (3.5)(3)), also $g^{(p-1)/q} \equiv 1 \pmod p$.

(5.5) Bemerkung: (1) Es sei p eine Primzahl, und es sei $g \in \mathbb{Z}$ eine Primitivwurzel modulo p. Dann ist

$$\mathbb{F}_p^\times = \{[1]_p, [g]_p, [g]_p^2, \dots, [g]_p^{p-2}\}.$$

Für $i \in \{0,1,\dots,p-2\}$ gilt $\mathbb{F}_p^\times = \langle [g]_p^i \rangle = \langle [g^i]_p \rangle$ genau dann, wenn i und $p-1$ teilerfremd sind (vgl. (3.9)(3)). Somit ist

$$\{g^i \bmod p \mid i \in \{0,1,\dots,p-2\};\ \operatorname{ggT}(i,p-1) = 1\}$$

die Menge aller Primitivwurzeln modulo p in $\{0,1,\dots,p-1\}$. Es gibt also in der Menge $\{0,1,\dots,p-1\}$ genau $\varphi(p-1)$ verschiedene Primitivwurzeln modulo p.
(2) Es sei p eine Primzahl, und es sei $g(p)$ die kleinste positive Primitivwurzel modulo p. Ist $p = 2$, so ist $g(p) = 1$; ist $p \geq 3$, so ist $2 \leq g(p) \leq p - \varphi(p-1)$. Man kann mit vergleichsweise einfachen Mitteln beweisen: Es ist

$$g(p) < 2^{1+\omega(p-1)}\sqrt{p},$$

worin $\omega(p-1)$ die Anzahl der verschiedenen Primteiler von $p-1$ ist. Beweise dafür findet man in den Büchern von Hua ([47], Kap. VII, § 9) und Narkiewicz ([73], Kap. II, § 2). Diese Abschätzung ist, jedenfalls für kleine Primzahlen, recht pessimistisch. Es gilt nämlich, wie man mit viel Geduld mittels MuPAD bestätigen kann: Es ist

$$\begin{aligned}
\max(\{g(p) \mid p \text{ Primzahl};\ p < 5\,000\,000\}) &= g(760\,321) = 73,\\
\max(\{g(p) \mid p \text{ Primzahl};\ p < 50\,000\,000\}) &= g(45\,024\,841) = 111,\\
\max(\{g(p) \mid p \text{ Primzahl};\ p < 500\,000\,000\}) &= g(324\,013\,369) = 137,\\
\max(\{g(p) \mid p \text{ Primzahl};\ p < 5\,000\,000\,000\}) &= g(1\,685\,283\,601) = 164.
\end{aligned}$$

Wesentlich rascher erhält man mittels MuPAD folgendes Ergebnis: Für 29 341 der 78 498 Primzahlen $p < 1\,000\,000$ ist $g(p) = 2$, für 17 814 von ihnen ist $g(p) = 3$, und für 10 882 von ihnen ist $g(p) = 5$; nur für weniger als 1.6 % von ihnen ist $g(p) > 20$.
(3) Auch die Theorie liefert bessere Ergebnisse. So zeigte Y. Wang im Jahr 1959 (vgl. [111]): Für jedes $\varepsilon > 0$ gilt

$$g(p) = O(p^{1/4+\varepsilon}).$$

Wenn die sogenannte verallgemeinerte Riemannsche Vermutung, die etwas über die Lage der Nullstellen von Funktionen aussagt, die mit der Riemannschen ζ-Funktion verwandt sind, und zu deren Formulierung auf die Bücher [17] von J. Brüdern oder [10] von E. Bach und J. Shallit verwiesen sei, richtig ist, so gilt sogar

$$g(p) \;=\; O\big(\omega(p-1)^6 \cdot (\log p)^2\big),$$

was ebenfalls von Y. Wang gezeigt wurde.

Auf der anderen Seite kann man zeigen: Zu jeder reellen Zahl $M > 0$ gibt es eine Primzahl p mit $g(p) > M$ (vgl. dazu Aufgabe 4 in (11.24)). In Wirklichkeit weiß man wesentlich mehr: Es gibt eine positive reelle Zahl c mit

$$g(p) \;>\; c \cdot \log p \quad \text{für unendlich viele Primzahlen } p.$$

Wenn die verallgemeinerte Riemannsche Vermutung richtig ist, so gilt sogar: Zu jedem reellen $\varepsilon > 0$ gibt es unendlich viele Primzahlen p mit

$$g(p) \;>\; \Big(\frac{1}{2} - \varepsilon\Big) \cdot \log p.$$

(vgl. dazu Narkiewicz [73], Kap. II, § 2).

(5.6) Bemerkung: (1) Man kennt keinen schnellen Algorithmus zur Berechnung von Primitivwurzeln. Die in (5.5)(2) angegebene Beobachtung legt das folgende Verfahren nahe, das zu einer Primzahl p und einer ganzen Zahl a die kleinste Primitivwurzel g modulo p mit $g \geq a$ ermittelt, für $a = 1$ also die kleinste positive Primitivwurzel $g(p)$ modulo p bestimmt. Dieses Verfahren setzt die Kenntnis der Primzerlegung von $p-1$ voraus.

(PW1) Ist $p = 2$, so setzt man

$$g \;:=\; \begin{cases} a+1, & \text{falls } a \text{ gerade ist,} \\ a, & \text{falls } a \text{ ungerade ist,} \end{cases}$$

und bricht ab.

(PW2) Man berechnet alle Primteiler von $p-1$ und setzt $g := a$.

(PW3) Ist g durch p teilbar, so setzt man $g := g+1$.

(PW4) Ist $g^{(p-1)/q} \not\equiv 1 \pmod{p}$ für jeden Primteiler q von $p-1$, so bricht man ab. (Nach (5.4)(2) ist g dann eine Primitivwurzel modulo p). Findet man aber einen Primteiler q von $p-1$ mit $g^{(p-1)/q} \equiv 1 \pmod{p}$, so setzt man $g := g+1$ und geht zu (PW3).

(2) **MuPAD:** Die Funktion `numlib::primroot` berechnet Primitivwurzeln: Ist p eine Primzahl, so liefert `numlib::primroot(p)` die kleinste positive Primitivwurzel modulo p, während `numlib::primroot(a,p)` für $a \in \mathbb{Z}$ die kleinste

Primitivwurzel $g \in \mathbb{Z}$ modulo p mit $g \geq a$ berechnet. `numlib::primroot` verwendet im wesentlichen die in (1) beschriebene Methode (vgl. (5.25)(2)).
(3) Von C. F. Gauß wurde in [37], Artikel 73, eine andere Methode zur Berechnung einer Primitivwurzel modulo einer Primzahl p angegeben. Diese Methode ist in der ersten Aufgabe in (5.26) beschrieben.

(5.7) Es sei p eine ungerade Primzahl, und es sei $g \in \mathbb{Z}$ eine Primitivwurzel modulo p. Dann gilt

$$\begin{aligned} \mathbb{F}_p^\times &= \langle [g]_p \rangle = \{[g]_p^i \mid 0 \leq i \leq p-2\} \quad \text{und} \\ \{1, 2, \ldots, p-1\} &= \{g^i \bmod p \mid 0 \leq i \leq p-2\}. \end{aligned}$$

(1) Es sei $a \in \mathbb{Z}$ nicht durch p teilbar. Es gibt eine eindeutig bestimmte Zahl $\operatorname{ind}(a) \in \{0, 1, \ldots, p-2\}$ mit $[a]_p = [g]_p^{\operatorname{ind}(a)}$, also mit $a \equiv g^{\operatorname{ind}(a)} \pmod{p}$. Die Zahl $\operatorname{ind}(a)$ heißt der Index oder der diskrete Logarithmus von a zur Primzahl p und zur Primitivwurzel g. Für $b \in \mathbb{Z} \setminus p\mathbb{Z}$ gilt $\operatorname{ind}(b) = \operatorname{ind}(a)$, genau wenn $b \equiv a \pmod{p}$ gilt.
(2) Kennt man $\operatorname{ind}(a)$ für jedes $a \in \{1, 2, \ldots, p-1\}$, so beherrscht man das Rechnen in der Gruppe $\mathbb{F}_p^\times$ vollständig: Für alle $a, b \in \{1, 2, \ldots, p-1\}$ gilt

$$\operatorname{ind}(ab) = \big(\operatorname{ind}(a) + \operatorname{ind}(b)\big) \bmod (p-1),$$

und für jedes $a \in \{1, 2, \ldots, p-1\}$ gilt (vgl. (3.7)(2))

$$\operatorname{ord}\big([a]_p\big) = \frac{p-1}{\operatorname{ggT}\big(\operatorname{ind}(a), p-1\big)}.$$

(3) Will man für jedes $a \in \{1, 2, \ldots, p-1\}$ den Index $\operatorname{ind}(a)$ von a zur Primzahl p und zur Primitivwurzel g ermitteln, so könnte man so vorgehen: Man berechnet für jedes $i \in \{0, 1, \ldots, p-2\}$ die Zahl $a(i) := g^i \bmod p$ und zwar rekursiv: Man setzt $a(0) := 1$ und

$$a(i) := \big(g \cdot a(i-1)\big) \bmod p \quad \text{für jedes } i \in \{1, 2, \ldots, p-2\}.$$

Die Abbildung

$$i \mapsto a(i) : \{0, 1, \ldots, p-2\} \to \{1, 2, \ldots, p-1\}$$

ist bijektiv, und ihre Umkehrabbildung ist

$$a \mapsto \operatorname{ind}(a) : \{1, 2, \ldots, p-1\} \to \{0, 1, \ldots, p-2\}.$$

Der Aufwand dieses Verfahrens, alle Indizes zu p und g zu berechnen und zu tabellieren, ist offensichtlich proportional zu p; es ist daher nur brauchbar, wenn p klein ist.

(4) Auch das folgende Ergebnis ist eher eine Kuriosität und höchstens dann für das praktische Rechnen geeignet, wenn p klein ist: Zu jedem $i \in \{1,2,\ldots,p-2\}$ gibt es ein und nur ein $b_i \in \{1,2,\ldots,p-1\}$, für das $(1-g^i)\,b_i \equiv 1 \pmod{p}$ gilt, und es ist

$$\operatorname{ind}(a) = \begin{cases} 0 & \text{für } a = 1, \\ \left(\sum_{i=1}^{p-2} b_i\, a^i \right) \bmod p & \text{für jedes } a \in \{2,3,\ldots,p-1\} \end{cases}$$

(vgl. Wells [113]). Auch hier erfordert die Berechnung von $\operatorname{ind}(a)$ einen Aufwand, der zu p proportional ist. In den folgenden Abschnitten werden Verfahren behandelt, die brauchbarer sind als die, die in diesem Abschnitt geschildert wurden.

(5.8) Es sei p eine ungerade Primzahl.
(1) Es sei $q := \lceil \sqrt{p} \rceil$. Es gilt: Zu jedem $n \in \{0,1,\ldots,p-2\}$ gibt es ein $r \in \{0,1,\ldots,q-1\}$ und ein $s \in \{0,1,\ldots,q\}$ mit $n = qs - r$.
Beweis: Es sei $n \in \{0,1,\ldots,p-2\}$. Dazu gibt es Zahlen $s' \in \mathbb{N}_0$ und $r' \in \{0,1,\ldots,q-1\}$ mit $n = qs' + r'$. Dabei gilt

$$s' = \frac{n-r'}{q} \leq \frac{n}{q} \leq \frac{p-2}{q} \leq \frac{p-2}{\sqrt{p}} < \sqrt{p},$$

also $s' \leq \lfloor \sqrt{p} \rfloor = \lceil \sqrt{p} \rceil - 1 = q-1$. Ist $r' = 0$, so setzt man $s := s'$ und $r := 0$; ist $r' > 0$, so setzt man $r := q - r'$ und $s := s' + 1$. Es gilt $n = sq - r$, $0 \leq r \leq q-1$ und $0 \leq s \leq q$.
(2) Es sei g eine Primitivwurzel modulo p, es sei $a \in \mathbb{Z} \setminus p\mathbb{Z}$, und es sei $n := \operatorname{ind}(a)$ der Index von a zu p und g. Für jedes $i \in \{0,1,\ldots,q-1\}$ sei

$$y_i := ag^i \bmod p,$$

und für jedes $k \in \{0,1,\ldots,q\}$ sei

$$x_k := (g^q)^k \bmod p.$$

Nach (1) gibt es ein $r \in \{0,1,\ldots,q-1\}$ und ein $s \in \{0,1,\ldots,q\}$ mit $n = qs - r$, und dafür gilt

$$y_r \equiv ag^r \equiv g^{n+r} = g^{qs} = (g^q)^s \equiv x_s \pmod{p},$$

also $y_r = x_s$. Gilt $y_i = x_k$ für ein Paar $(i,k) \in \{0,1,\ldots,q-1\} \times \{0,1,\ldots,q\}$, so gilt

$$g^{qk+r} \equiv x_k g^r = y_i g^r = ag^{i+r} = y_r g^i = x_s g^i \equiv g^{qs+i} \pmod{p},$$

wegen $\mathrm{ord}([g]_p) = p-1$ folgt $qk + r \equiv qs + i \pmod{(p-1)}$, und daher gilt

$$qk - i \equiv qs - r = \mathrm{ind}(a) \pmod{(p-1)},$$

also $\mathrm{ind}(a) = (qk - i) \bmod (p-1)$. Man findet $n = \mathrm{ind}(a)$ daher folgendermaßen: Man sucht ein Paar $(i,k) \in \{0,1,\ldots,q-1\} \times \{0,1,\ldots,q\}$ mit $y_i = x_k$ und berechnet damit $\mathrm{ind}(a) = (qk - i) \bmod (p-1)$.
(3) Das in diesem Abschnitt behandelte Verfahren zur Berechnung von Indizes geht auf eine Methode zurück, die D. Shanks 1969 zur Berechnung von Ordnungen in endlichen zyklischen Gruppen verwendet hat. Es nützt besondere Eigenschaften der Primzahl p nicht aus. In den beiden folgenden Abschnitten wird ein Verfahren beschrieben, das besonders gut für den Fall geeignet ist, daß $p-1$ nur kleine Primteiler besitzt.

(5.9) Es sei p eine ungerade Primzahl, und es sei $g \in \mathbb{Z}$ eine Primitivwurzel modulo p; es sei $a \in \mathbb{Z} \setminus p\mathbb{Z}$.
(1) Es sei q ein Primteiler von $p-1$. Für jedes $k \in \{0,1,\ldots,q-1\}$ sei

$$r(q,k) := g^{k(p-1)/q} \bmod p.$$

Da g eine Primitivwurzel modulo p ist, sind die q Restklassen

$$[r(q,0)]_p,\ [r(q,1)]_p,\ \ldots,\ [r(q,q-1)]_p$$

paarweise verschiedene Elemente von $\mathbb{F}_p^\times$.
(2) Es sei q ein Primteiler von $p-1$, und es sei $\alpha := v_q(p-1)$ der Exponent von q in der Primzerlegung von $p-1$. Es ist $\beta_q := \mathrm{ind}(a) \bmod q^\alpha \in \{0,1,\ldots,q^\alpha - 1\}$, also existieren eindeutig bestimmte Zahlen $k_0, k_1, \ldots, k_{\alpha-1} \in \{0,1,\ldots,q-1\}$ mit

$$\beta_q = k_0 + k_1 q + \cdots + k_{\alpha-1} q^{\alpha-1}.$$

Es gilt

$$\mathrm{ind}(a) \cdot \frac{p-1}{q} \equiv \beta_q \cdot \frac{p-1}{q} \equiv k_0 \cdot \frac{p-1}{q} \pmod{(p-1)}$$

und daher

$$a^{(p-1)/q} \equiv g^{\mathrm{ind}(a)(p-1)/q} \equiv g^{k_0(p-1)/q} \equiv r(q,k_0) \pmod{p}.$$

Für jedes $j \in \{1,2,\ldots,\alpha-1\}$ ergibt sich analog: Für

$$a_j := \left(a \cdot g^{(p-1)-(k_0+k_1 q+\cdots+k_{j-1}q^{j-1})}\right) \bmod p$$

gilt

$$\begin{aligned}
&\operatorname{ind}(a_j) \cdot \frac{p-1}{q^{j+1}} \equiv \\
&\equiv \left(\operatorname{ind}(a) + (p-1) - (k_0 + k_1 q + \cdots + k_{j-1} q^{j-1})\right) \cdot \frac{p-1}{q^{j+1}} \equiv \\
&\equiv \left(\beta_q - (k_0 + k_1 q + \cdots + k_{j-1} q^{j-1})\right) \cdot \frac{p-1}{q^{j+1}} \equiv \\
&\equiv k_j \cdot \frac{p-1}{q} \pmod{(p-1)}
\end{aligned}$$

und daher

$$a_j^{(p-1)/q^{j+1}} \equiv g^{\operatorname{ind}(a)(p-1)/q^{j+1}} \equiv g^{k_j(p-1)/q} \equiv r(q, k_j) \pmod{p}.$$

Also gilt $a^{(p-1)/q} \bmod p = r(q, k_0)$ und

$$a_j^{(p-1)/q^{j+1}} \bmod p = r(q, k_j) \quad \text{für jedes } j \in \{1, 2, \ldots, \alpha - 1\}.$$

(5.10) Es sei p eine ungerade Primzahl, und es sei $g \in \mathbb{Z}$ eine Primitivwurzel modulo p; es sei $a \in \mathbb{Z} \setminus p\mathbb{Z}$.
(1) Der folgende Algorithmus, der 1978 von B. Silver und von S. C. Pohlig und M. E. Hellman angegeben wurde (vgl. [82]), berechnet den Index $\operatorname{ind}(a)$ von a zur Primzahl p und zur Primitivwurzel g:

(SPH1) Zu jedem Primteiler q von $p-1$ und zu jedem $k \in \{0, 1, \ldots, q-1\}$ berechnet man die Zahl $r(q, k) := g^{k(p-1)/q} \bmod p$.

(SPH2) Für jeden Primteiler q von $p-1$ berechnet man

(a) $\alpha := v_q(p-1)$,

(b) die Zahl $k_0 \in \{0, 1, \ldots, q-1\}$ mit $a^{(p-1)/q} \bmod p = r(q, k_0)$.

(c) für jedes $j \in \{1, 2, \ldots, \alpha - 1\}$ die Zahl

$$a_j := \left(a \cdot g^{(p-1)-(k_0+k_1 q+\cdots+k_{j-1}q^{j-1})}\right) \bmod p$$

und die Zahl $k_j \in \{0, 1, \ldots, q-1\}$ mit $a_j^{(p-1)/q^{j+1}} \bmod p = r(q, k_j)$ und setzt

$$\beta_q := k_0 + k_1 q + \cdots + k_{\alpha-1} q^{\alpha-1}.$$

(SPH3) Mit Hilfe des Chinesischen Restsatzes berechnet man die Zahl $i \in \{0, 1, \ldots, p-2\}$ mit $i \equiv \beta_q \pmod{q^{v_q(p-1)}}$ für jeden Primteiler q von $p-1$, gibt i aus und bricht ab.

(2) Daß der Algorithmus SPH das Verlangte leistet, folgt aus (5.9). Er ist offensichtlich nur brauchbar, wenn alle Primteiler q von $p-1$ vergleichsweise klein sind. Eine genaue Diskussion von SPH findet man in [82]. Man kann diesen Algorithmus noch verbessern, wenn man ihn mit dem auf D. Shanks zurückgehenden Trick kombiniert, der in (5.8) beschrieben ist.

(5.11) Bemerkung: Man kennt keinen wirklich schnellen Algorithmus zur Berechnung von Indizes. Weitere Informationen über die Berechnung von Indizes und über ihre Bedeutung für die Kryptologie findet man in dem Übersichtsartikel [68] von K. S. McCurley; neuere Algorithmen findet man in der Arbeit [22] von D. Coppersmith, A. M. Odlyzko und R. Schroeppel.

(5.12) Hilfssatz: *Es sei p eine ungerade Primzahl. Es gibt eine Primitivwurzel $g \in \mathbb{Z}$ modulo p mit $g^{p-1} \not\equiv 1 \pmod{p^2}$, und zwar gilt: Ist $g_0 \in \mathbb{Z}$ eine Primitivwurzel modulo p mit $g_0^{p-1} \equiv 1 \pmod{p^2}$, so ist $g := (1+p)\,g_0$ eine Primitivwurzel modulo p, und es ist $g^{p-1} \not\equiv 1 \pmod{p^2}$.*

Beweis: Es sei $g_0 \in \mathbb{Z}$ eine Primitivwurzel modulo p mit $g_0^{p-1} \equiv 1 \pmod{p^2}$. Es gilt $g := (1+p)\,g_0 \equiv g_0 \pmod{p}$, also $[g]_p = [g_0]_p$, und somit ist auch g eine Primitivwurzel modulo p. Es gilt

$$\begin{aligned} g^{p-1} &= (1+p)^{p-1}\,g_0^{p-1} \equiv (1+p)^{p-1} = \\ &= 1 + \binom{p-1}{1} p + p^2 \sum_{i=2}^{p-1} \binom{p-1}{i} p^{i-2} \equiv \\ &\equiv 1 + (p-1)\,p \equiv 1 - p \not\equiv 1 \pmod{p^2}. \end{aligned}$$

(5.13) Satz: *Es sei p eine ungerade Primzahl, und es sei $\alpha \in \mathbb{N}$ mit $\alpha \geq 2$. Die Gruppe $E(\mathbb{Z}/p^\alpha\mathbb{Z})$ ist zyklisch, und zwar gilt: Ist $g \in \mathbb{Z}$ eine Primitivwurzel modulo p mit $g^{p-1} \not\equiv 1 \pmod{p^2}$, so ist*

$$E(\mathbb{Z}/p^\alpha\mathbb{Z}) = \langle [g]_{p^\alpha} \rangle.$$

Beweis: Es sei $g \in \mathbb{Z}$ eine Primitivwurzel modulo p mit $g^{p-1} \not\equiv 1 \pmod{p^2}$. (Nach (5.12) gibt es ein solches g).
(a) Zu jedem $n \in \mathbb{N}$ gibt es ein $a_n \in \mathbb{Z} \setminus p\mathbb{Z}$ mit $g^{p^{n-1}(p-1)} = 1 + a_n p^n$.
Beweis durch Induktion: Wegen $p \nmid g$ gilt $g^{p-1} \equiv 1 \pmod{p}$ (vgl. (4.21)(1)), also existiert ein $a_1 \in \mathbb{Z}$ mit $g^{p-1} = 1 + a_1 p$, und wegen $g^{p-1} \not\equiv 1 \pmod{p^2}$ gilt $p \nmid a_1$. – Es sei $n \in \mathbb{N}$, und es sei bereits gezeigt: Es gibt ein $a_n \in \mathbb{Z} \setminus p\mathbb{Z}$ mit $g^{p^{n-1}(p-1)} = 1 + a_n p^n$. Dann gilt

$$g^{p^n(p-1)} = \left(g^{p^{n-1}(p-1)}\right)^p = (1 + a_n p^n)^p =$$

$$= 1 + \binom{p}{1} p^n a_n + \binom{p}{2} p^{2n} a_n^2 + \sum_{j=3}^{p} \binom{p}{j} p^{jn} a_n^j =$$

$$= 1 + p^{n+1} a_n + \frac{p-1}{2} p^{2n+1} a_n^2 + \sum_{j=3}^{p} \binom{p}{j} p^{jn} a_n^j =$$

$$= 1 + a_{n+1} p^{n+1}$$

$$\text{mit} \quad a_{n+1} := a_n + p \cdot \left(\frac{p-1}{2} p^{n-1} a_n^2 + \sum_{j=3}^{p} \binom{p}{j} p^{(j-1)n-2} a_n^j \right) \in \mathbb{Z},$$

und wegen $p \nmid a_n$ folgt $p \nmid a_{n+1}$.
(b) $d := \operatorname{ord}([g]_{p^\alpha})$ teilt $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$ (vgl. (4.20)). Es gilt $[g]_{p^\alpha}^d = [1]_{p^\alpha}$, also $g^d \equiv 1 \pmod{p^\alpha}$, also $g^d \equiv 1 \pmod{p}$, also $[g]_p^d = [1]_p$, und somit ist d durch $p-1 = \operatorname{ord}([g]_p)$ teilbar. Daher gibt es ein $\beta \in \{0, 1, \ldots, \alpha-1\}$ mit $d = p^\beta(p-1)$. Nach (a) gibt es ein $a \in \mathbb{Z} \setminus p\mathbb{Z}$ mit $g^d = g^{p^\beta(p-1)} = 1 + ap^{\beta+1}$. Wegen $g^d \equiv 1 \pmod{p^\alpha}$ folgt $p^\alpha \mid ap^{\beta+1}$, also $p^\alpha \mid p^{\beta+1}$, also $\alpha \leq \beta + 1$, und daher ist $\beta = \alpha - 1$. Somit ist

$$\operatorname{ord}([g]_{p^\alpha}) = d = p^{\alpha-1}(p-1) = \varphi(p^\alpha) = \#(E(\mathbb{Z}/p^\alpha\mathbb{Z})),$$

und daher ist $E(\mathbb{Z}/p^\alpha\mathbb{Z}) = \langle [g]_{p^\alpha} \rangle$.

(5.14) Definition: Es sei p eine ungerade Primzahl, und es sei $\alpha \in \mathbb{N}$ mit $\alpha \geq 2$. Eine ganze Zahl g heißt eine Primitivwurzel modulo p^α, wenn g nicht durch p teilbar ist und $E(\mathbb{Z}/p^\alpha\mathbb{Z}) = \langle [g]_{p^\alpha} \rangle$ gilt.

(5.15) Bemerkung: Es sei p eine ungerade Primzahl.
(1) Es sei $\alpha \in \mathbb{N}$ mit $\alpha \geq 2$. Nach (5.12) und (5.13) findet man auf folgende Weise eine Primitivwurzel g modulo p^α: Man ermittelt eine Primitivwurzel g_0 modulo p und setzt

$$g := \begin{cases} g_0, & \text{falls } g_0^{p-1} \not\equiv 1 \pmod{p^2} \text{ gilt,} \\ (1+p)g_0, & \text{falls } g_0^{p-1} \equiv 1 \pmod{p^2} \text{ gilt.} \end{cases}$$

(2) Ist $\beta \in \mathbb{N}$ mit $\beta \geq 2$ und ist $g \in \mathbb{Z}$ eine Primitivwurzel modulo p^β, so ist g für jedes $\alpha \in \mathbb{N}$ Primitivwurzel modulo p^α (vgl. Aufgabe 6 in (5.26)).
(3) Für die kleinste positive Primitivwurzel $g(p)$ modulo p und die kleinste positive Primitivwurzel $g(p^2)$ modulo p^2 gilt $g(p) \leq g(p^2)$ (wegen (2)). Es gibt Primzahlen p, für die $g(p) < g(p^2)$ ist: Es ist $g(40\,487) = 5$ und $g(40\,487^2) = 10$. Solche Primzahlen scheinen recht selten zu sein.

(5.16) Satz: *Es sei p eine ungerade Primzahl, und es sei $\alpha \in \mathbb{N}$; es sei $g_1 \in \mathbb{Z}$ eine Primitivwurzel modulo p^α, und es sei*

$$g := \begin{cases} g_1, & \text{falls } g_1 \text{ ungerade ist,} \\ g_1 + p^\alpha, & \text{falls } g_1 \text{ gerade ist.} \end{cases}$$

Die Gruppe $E(\mathbb{Z}/2p^\alpha\mathbb{Z})$ ist zyklisch, und zwar gilt

$$E(\mathbb{Z}/2p^\alpha\mathbb{Z}) = \langle [g]_{2p^\alpha} \rangle.$$

Beweis: Wegen $p \nmid g_1$ gilt $p \nmid g$, wegen $2 \nmid g$ folgt $\operatorname{ggT}(g, 2p^\alpha) = 1$, und daher ist $[g]_{2p^\alpha} \in E(\mathbb{Z}/2p^\alpha\mathbb{Z})$. $d := \operatorname{ord}([g]_{2p^\alpha})$ teilt

$$\#\big(E(\mathbb{Z}/2p^\alpha\mathbb{Z})\big) = \varphi(2p^\alpha) = \varphi(2)\varphi(p^\alpha) = \varphi(p^\alpha).$$

Wegen $g^d \equiv 1 \pmod{2p^\alpha}$ gilt auch $g^d \equiv 1 \pmod{p^\alpha}$, also ist d durch $\operatorname{ord}([g]_{p^\alpha})$ teilbar. Wegen $g \equiv g_1 \pmod{p^\alpha}$ gilt $[g]_{p^\alpha} = [g_1]_{p^\alpha}$, und daher gilt $\operatorname{ord}([g]_{p^\alpha}) = \operatorname{ord}([g_1]_{p^\alpha}) = \#(E(\mathbb{Z}/p^\alpha\mathbb{Z})) = \varphi(p^\alpha)$. Es gilt also

$$\operatorname{ord}\big([g]_{2p^\alpha}\big) = d = \varphi(p^\alpha) = \varphi(2p^\alpha) = \#\big(E(\mathbb{Z}/2p^\alpha\mathbb{Z})\big),$$

und somit gilt $E(\mathbb{Z}/2p^\alpha\mathbb{Z}) = \langle [g]_{2p^\alpha} \rangle$.

(5.17) Bemerkung: Es sei p eine ungerade Primzahl, und es sei $\alpha \in \mathbb{N}$. Eine ganze Zahl g heißt eine Primitivwurzel modulo $2p^\alpha$, wenn $2 \nmid g$ und $p \nmid g$ und $E(\mathbb{Z}/2p^\alpha\mathbb{Z}) = \langle [g]_{2p^\alpha} \rangle$ gilt. Wie man aus einer Primitivwurzel modulo p eine Primitivwurzel modulo $2p^\alpha$ gewinnen kann, zeigen (5.15) und (5.16).

(5.18) Hilfssatz: *Für jedes $k \in \mathbb{N}_0$ gilt*

$$5^{2^k} \equiv 1 + 2^{k+2} \pmod{2^{k+3}}.$$

Beweis: Für $k = 0$ ist nichts zu zeigen. Ist k eine natürliche Zahl und gilt $5^{2^{k-1}} \equiv 1 + 2^{k+1} \pmod{2^{k+2}}$, so gibt es ein $a \in \mathbb{Z}$ mit

$$5^{2^{k-1}} = 1 + 2^{k+1} + 2^{k+2}a = 1 + 2^{k+1}(1 + 2a),$$

und es folgt

$$\begin{aligned} 5^{2^k} &= \big(5^{2^{k-1}}\big)^2 = \big(1 + 2^{k+1}(1 + 2a)\big)^2 = \\ &= 1 + 2 \cdot 2^{k+1}(1 + 2a) + 2^{2k+2}(1 + 2a)^2 = \\ &= 1 + 2^{k+2} + 2^{k+3}a + 2^{k+3} \cdot 2^{k-1}(1 + 2a)^2 \equiv 1 + 2^{k+2} \pmod{2^{k+3}}. \end{aligned}$$

(5.19) Satz: *Es sei* $\alpha \in \mathbb{N}$ *mit* $\alpha \geq 3$.
(1) *Es gilt* $\operatorname{ord}([5]_{2^\alpha}) = 2^{\alpha-2}$.
(2) *Für jedes ungerade* $a \in \mathbb{Z}$ *gilt: Es gibt eindeutig bestimmte Zahlen* $i \in \{0,1\}$ *und* $j \in \{0,1,\ldots,2^{\alpha-2}-1\}$ *mit* $a \equiv (-1)^i 5^j \pmod{2^\alpha}$, *also mit* $[a]_{2^\alpha} = [-1]_{2^\alpha}^i \cdot [5]_{2^\alpha}^j$, *und es ist* $\operatorname{ord}([a]_{2^\alpha}) \leq 2^{\alpha-2}$.
(3) *Die Gruppe* $E(\mathbb{Z}/2^\alpha\mathbb{Z})$ *ist nicht zyklisch.*

Beweis: (1) Es gilt $5^{2^{\alpha-2}} \equiv 1 + 2^\alpha \pmod{2^{\alpha+1}}$, also $5^{2^{\alpha-2}} \equiv 1 \pmod{2^\alpha}$, und daher gibt es ein $\beta \in \{0,1,\ldots,\alpha-2\}$ mit $d := \operatorname{ord}([5]_{2^\alpha}) = 2^\beta$ (vgl. dazu (3.5)(3)). Es gilt $5^{2^{\alpha-3}} \equiv 1 + 2^{\alpha-1} \not\equiv 1 \pmod{2^\alpha}$ und daher $2^\beta = d > 2^{\alpha-3}$. Also ist $\beta = \alpha - 2$, d.h. es ist $d = 2^{\alpha-2}$.
(2) (a) Es seien $i, k \in \{0,1\}$ und $j, l \in \{0,1,\ldots,2^{\alpha-2}-1\}$ mit $(-1)^i 5^j \equiv (-1)^k 5^l \pmod{2^\alpha}$. Dann gilt $(-1)^i \equiv (-1)^i 5^j \equiv (-1)^k 5^l \equiv (-1)^k \pmod 2$ und daher $i = k$. Es gilt somit $5^j \equiv 5^l \pmod{2^\alpha}$, also $[5]_{2^\alpha}^j = [5]_{2^\alpha}^l$, also ist $l - j$ durch $\operatorname{ord}([5]_{2^\alpha}) = 2^{\alpha-2}$ teilbar, und es folgt $j = l$.
(b) Nach (a) gilt

$$\#\big(\{[-1]_{2^\alpha}^i \cdot [5]_{2^\alpha}^j \mid 0 \leq i \leq 1;\ 0 \leq j \leq 2^{\alpha-2}-1\}\big) = \\ = 2 \cdot 2^{\alpha-2} = 2^{\alpha-1} = \varphi(2^\alpha) = \#\big(E(\mathbb{Z}/2^\alpha\mathbb{Z})\big),$$

und daher gilt

$$E(\mathbb{Z}/2^\alpha\mathbb{Z}) = \{[-1]_{2^\alpha}^i \cdot [5]_{2^\alpha}^j \mid 0 \leq i \leq 1;\ 0 \leq j \leq 2^{\alpha-2}-1\}.$$

(c) Für jedes ungerade $a \in \mathbb{Z}$ gilt nach (b): Es gibt ein $i \in \{0,1\}$ und ein $j \in \{0,1,\ldots,2^{\alpha-2}-1\}$ mit $[a]_{2^\alpha} = [-1]_{2^\alpha}^i \cdot [5]_{2^\alpha}^j$, und wegen $\operatorname{ord}([5]_{2^\alpha}) = 2^{\alpha-2}$ gilt

$$[a]_{2^\alpha}^{2^{\alpha-2}} = \big([-1]_{2^\alpha}^{2^{\alpha-2}}\big)^i \cdot \big([5]_{2^\alpha}^{2^{\alpha-2}}\big)^j = \big([-1]_{2^\alpha}^{2^{\alpha-2}}\big)^i = [1]_{2^\alpha},$$

also $\operatorname{ord}([a]_{2^\alpha}) \leq 2^{\alpha-2}$.
(3) Für jedes ungerade $a \in \mathbb{Z}$ gilt

$$\operatorname{ord}\big([a]_{2^\alpha}\big) \leq 2^{\alpha-2} < 2^{\alpha-1} = \varphi(2^\alpha) = \#\big(E(\mathbb{Z}/2^\alpha\mathbb{Z})\big).$$

In $E(\mathbb{Z}/2^\alpha\mathbb{Z})$ gibt es also kein Element der Ordnung $\#(E(\mathbb{Z}/2^\alpha\mathbb{Z}))$, und daher ist $E(\mathbb{Z}/2^\alpha\mathbb{Z})$ nicht zyklisch.

(5.20) Bemerkung: (1) $E(\mathbb{Z}/2\mathbb{Z}) = \{[1]_2\}$ und $E(\mathbb{Z}/4\mathbb{Z}) = \{[1]_4, [3]_4\}$ sind zyklische Gruppen. $E(\mathbb{Z}/8\mathbb{Z}) = \{[1]_8, [3]_8, [5]_8, [7]_8\}$ ist nicht zyklisch, denn $[3]_8$, $[5]_8$ und $[7]_8$ sind von der Ordnung 2.
(2) Es sei $\alpha \geq 4$, und es sei $a \in \mathbb{Z}$ ungerade. Es gilt $\operatorname{ord}([a]_{2^\alpha}) \leq 2^{\alpha-2}$, und es ist $\operatorname{ord}([a]_{2^\alpha}) = 2^{\alpha-2}$, genau wenn $a \equiv 3 \pmod 8$ oder $a \equiv 5 \pmod 8$ gilt.

Beweis: Nach (5.19)(2) ist $\operatorname{ord}([a]_{2^\alpha}) \leq 2^{\alpha-2}$, und es gibt ein $i \in \{0,1\}$ und ein $j \in \{0,1,\ldots,2^{\alpha-2}-1\}$ mit $a \equiv (-1)^i 5^j \pmod{2^\alpha}$. Wegen $\alpha \geq 4$ ist $(-1)^{2^{\alpha-3}} = 1$, und daher gilt

$$a^{2^{\alpha-3}} \equiv \left((-1)^{2^{\alpha-3}}\right)^i \cdot \left(5^{2^{\alpha-3}}\right)^j = 5^{2^{\alpha-3}j} \pmod{2^\alpha}.$$

Also ist $\operatorname{ord}([a]_{2^\alpha}) = 2^{\alpha-2}$, genau wenn $2^{\alpha-3}j$ nicht durch $\operatorname{ord}([5]_{2^\alpha}) = 2^{\alpha-2}$ teilbar ist, also genau wenn j ungerade ist. Ist j ungerade, so gilt

$$a \equiv (-1)^i \cdot 5 \cdot 25^{(j-1)/2} \equiv (-1)^i \cdot 5 \equiv \begin{cases} 5 \pmod 8, & \text{falls } i = 0 \text{ ist,} \\ 3 \pmod 8, & \text{falls } i = 1 \text{ ist,} \end{cases}$$

und ist j gerade, so gilt

$$a \equiv (-1)^i \cdot 25^{j/2} \equiv (-1)^i \equiv \begin{cases} 1 \pmod 8, & \text{falls } i = 0 \text{ ist,} \\ 7 \pmod 8, & \text{falls } i = 1 \text{ ist.} \end{cases}$$

(5.21) Bezeichnung: Für jedes $m \in \mathbb{N}$ setzt man

$$\begin{aligned} \lambda(m) := \exp\big(E(\mathbb{Z}/m\mathbb{Z})\big) &= \max\big(\{\operatorname{ord}(\alpha) \mid \alpha \in E(\mathbb{Z}/m\mathbb{Z})\}\big) = \\ &= \max\big(\{\operatorname{ord}([a]_m) \mid a \in \mathbb{Z};\ \operatorname{ggT}(a,m) = 1\}\big). \end{aligned}$$

Die Funktion $\lambda : \mathbb{N} \to \mathbb{N}$ heißt Carmichael-Funktion.

(5.22) Satz: (1) *Für jedes $m \in \mathbb{N}$ und jedes $a \in \mathbb{Z}$ mit $\operatorname{ggT}(a,m) = 1$ gilt:* $\operatorname{ord}([a]_m)$ *teilt* $\lambda(m)$, *und es ist* $a^{\lambda(m)} \equiv 1 \pmod m$.
(2) *Sind $m_1, m_2, \ldots, m_n \in \mathbb{N}$ paarweise teilerfremd, so gilt*

$$\lambda(m_1 m_2 \cdots m_n) = \operatorname{kgV}\big(\lambda(m_1), \lambda(m_2), \ldots, \lambda(m_n)\big).$$

Beweis: (1) folgt aus (3.11), und (2) folgt so: Es seien $m_1, m_2, \ldots, m_n \in \mathbb{N}$ paarweise teilerfremd, und es sei $m := m_1 m_2 \cdots m_n$; es sei a eine ganze Zahl mit $\operatorname{ggT}(a,m) = 1$ und mit $\operatorname{ord}([a]_m) = \lambda(m)$. Für jedes $i \in \{1,2,\ldots,n\}$ gilt $\operatorname{ggT}(a,m_i) = 1$, also $a^{\lambda(m_i)} \equiv 1 \pmod{m_i}$, und weil $\lambda(m_i)$ ein Teiler von

$$l := \operatorname{kgV}\big(\lambda(m_1), \lambda(m_2), \ldots, \lambda(m_n)\big)$$

ist, folgt $a^l \equiv 1 \pmod{m_i}$. Hieraus folgt, daß $a^l \equiv 1 \pmod m$ gilt, und daher ist $\operatorname{ord}([a]_m) = \lambda(m)$ ein Teiler von l. Andererseits gibt es zu jedem $i \in \{1,2,\ldots,n\}$ ein $b_i \in \mathbb{Z}$ mit $\operatorname{ggT}(b_i, m_i) = 1$ und mit $\operatorname{ord}([b_i]_{m_i}) = \lambda(m_i)$. Der Chinesische Restsatz in (4.14) liefert eine ganze Zahl b mit $b \equiv b_i \pmod{m_i}$ für jedes $i \in \{1,2,\ldots,n\}$. Es ist $\operatorname{ggT}(b,m) = 1$, und für jedes $i \in \{1,2,\ldots,n\}$ gilt $b_i^{\lambda(m)} \equiv b^{\lambda(m)} \equiv 1 \pmod{m_i}$ und daher $\lambda(m_i) = \operatorname{ord}([b_i]_{m_i}) \mid \lambda(m)$. Also

ist $\lambda(m)$ durch $l = \mathrm{kgV}(\lambda(m_1), \lambda(m_2), \ldots, \lambda(m_n))$ teilbar. Damit ist gezeigt, daß $\lambda(m) = l = \mathrm{kgV}(\lambda(m_1), \lambda(m_2), \ldots, \lambda(m_n))$ ist.

(5.23) Satz: (1) *Ist α eine natürliche Zahl, so gilt*

$$\lambda(2^\alpha) = \begin{cases} 1, & \text{falls } \alpha = 1 \text{ ist,} \\ 2, & \text{falls } \alpha = 2 \text{ ist,} \\ 2^{\alpha-2}, & \text{falls } \alpha > 2 \text{ ist.} \end{cases}$$

(2) *Für jede ungerade Primzahl p und für jede natürliche Zahl α gilt*

$$\lambda(p^\alpha) = p^{\alpha-1}(p-1) = \varphi(p^\alpha).$$

(3) *Ist m eine natürliche Zahl mit der Primzerlegung $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, so gilt*

$$\lambda(m) = \mathrm{kgV}\big(\lambda(p_1^{\alpha_1}), \lambda(p_2^{\alpha_2}), \ldots, \lambda(p_r^{\alpha_r})\big).$$

Beweis: (1) folgt aus (5.20)(1) und (5.19), (2) folgt aus (5.2) und (5.13), und (3) folgt aus (5.22)(2).

(5.24) Satz: *Es sei m eine natürliche Zahl. Folgende Aussagen sind äquivalent:*
(1) *Die Gruppe $E(\mathbb{Z}/m\mathbb{Z})$ ist zyklisch.*
(2) *Es gilt $\lambda(m) = \varphi(m)$.*
(3) *m ist ein Element der Menge*

$$\mathcal{M} := \{1,2,4\} \cup \{p^\alpha \mid p \in \mathbb{P};\ p \geq 3;\ \alpha \in \mathbb{N}\} \cup \{2p^\alpha \mid p \in \mathbb{P};\ p \geq 3;\ \alpha \in \mathbb{N}\}.$$

Beweis: Daß (1) und (2) äquivalent sind, folgt unmittelbar aus der Definition der Carmichael-Funktion. Daß (1) aus (3) folgt, wurde im Laufe dieses Paragraphen bewiesen.
(2) $\Rightarrow$ (3): (a) Für jedes $m \in \mathbb{N}$ gilt: $\lambda(m)$ ist die Ordnung eines Elements der Gruppe $E(\mathbb{Z}/m\mathbb{Z})$, und daher ist $\lambda(m) \leq \#(E(\mathbb{Z}/m\mathbb{Z})) = \varphi(m)$. Nach (5.23)(1) ist $\lambda(2^\alpha)$ für jede natürliche Zahl $\alpha \geq 2$ gerade. Für jede Primzahl $p \geq 3$ und jede natürliche Zahl α ist $\lambda(p^\alpha) = \varphi(p^\alpha) = p^{\alpha-1}(p-1)$ ebenfalls gerade.
(b) Es sei m ein Element von $\mathbb{N} \setminus \mathcal{M}$, das eine Potenz von 2 ist. Dann gibt es eine natürliche Zahl $\alpha \geq 3$ mit $m = 2^\alpha$, und nach (5.23)(1) gilt

$$\lambda(2^\alpha) = 2^{\alpha-2} < 2^{\alpha-1} = \varphi(2^\alpha).$$

(c) Es sei m ein Element von $\mathbb{N} \setminus \mathcal{M}$, das keine Potenz von 2 ist, es sei $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ die Primzerlegung von m, und es sei $p_1 < p_i$ für jedes

$i \in \{2,3,\ldots,r\}$. Wegen $m \notin \mathcal{M}$ gilt entweder $p_1 \geq 3$ und $r \geq 2$, oder es ist $p_1 = 2$ und $\alpha_1 = 1$ und $r \geq 3$, oder es ist $p_1 = 2$ und $\alpha_1 \geq 2$ und $r \geq 2$. In jedem Fall gibt es daher Indizes $i, j \in \{1,2,\ldots,r\}$ mit $i \neq j$, für die $\lambda(p_i^{\alpha_i})$ und $\lambda(p_j^{\alpha_j})$ beide gerade sind (vgl. (a)). Es gilt

$$\begin{aligned}
\lambda(m) &= \mathrm{kgV}\big(\lambda(p_1^{\alpha_1}), \lambda(p_2^{\alpha_2}), \ldots, \lambda(p_r^{\alpha_r})\big) \leq \\
&\leq \frac{1}{2} \cdot \lambda(p_1^{\alpha_1})\lambda(p_2^{\alpha_2}) \cdots \lambda(p_r^{\alpha_r}) \leq \\
&\leq \frac{1}{2} \cdot \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \cdots \varphi(p_r^{\alpha_r}) = \\
&= \frac{1}{2} \cdot \varphi(m) < \varphi(m).
\end{aligned}$$

(5.25) Bemerkung: (1) Für jedes Element m der in (5.24)(3) angegebenen Menge $\mathcal{M}$ ist die Einheitengruppe $E(\mathbb{Z}/m\mathbb{Z})$ des Restklassenrings $\mathbb{Z}/m\mathbb{Z}$ zyklisch; jede ganze Zahl g mit $\mathrm{ggT}(g,m) = 1$ und mit $E(\mathbb{Z}/m\mathbb{Z}) = \langle\, [\,g\,]_m \,\rangle$ heißt eine Primitivwurzel modulo m.

(2) **MuPAD:** (a) Die Funktion `numlib::primroot` berechnet Primitivwurzeln: Ist m eine natürliche Zahl, so liefern `numlib::primroot(m)` die kleinste positive Primitivwurzel modulo m und `numlib::primroot(a,m)` für $a \in \mathbb{Z}$ die kleinste Primitivwurzel $g \in \mathbb{Z}$ modulo m mit $g \geq a$, falls es überhaupt Primitivwurzeln modulo m gibt, und andernfalls die Ausgabe `FAIL`. Das Verfahren, das dabei verwendet wird, benützt das Ergebnis aus (5.24) und ist eine Verallgemeinerung der in (5.6)(1) beschriebenen Methode.

(b) Für eine natürliche Zahl m berechnet `numlib::lambda(m)` den Wert $\lambda(m)$ der Carmichael-Funktion. `numlib::lambda` verwendet die Funktionen `ifactor` und `ilcm` aus dem MuPAD-Kern.

(5.26) Aufgaben:

Aufgabe 1: Diese Aufgabe behandelt das in (5.6)(3) erwähnte Verfahren zur Berechnung von Primitivwurzeln, das Gauß angegeben hat.

(1) (a) Es seien k, $l \in \mathbb{N}$. Ein Blick auf die Primzerlegungen von k und von l zeigt: Es gibt einen eindeutig bestimmten Teiler $r(k,l) \in \mathbb{N}$ von k mit $\mathrm{ggT}(r(k,l),l) = 1$ und mit: Jeder Teiler $j \in \mathbb{N}$ von k mit $\mathrm{ggT}(j,l) = 1$ teilt $r(k,l)$.

(b) Man zeige: Für alle k, $l \in \mathbb{N}$ gilt

$$r(k,l) = r\left(\frac{k}{\mathrm{ggT}(k,l)}, \mathrm{ggT}(k,l)\right).$$

(c) Man schreibe eine MuPAD-Funktion, die zu natürlichen Zahlen k und l mit Hilfe der in (b) angegebenen Rekursionsformel $r(k,l)$ berechnet (ohne vorher die Primzerlegungen von k und l zu berechnen).

(2) Es sei $m \in \mathbb{N}$, es seien a, $b \in \mathbb{Z}$ mit $\mathrm{ggT}(a,m) = \mathrm{ggT}(b,m) = 1$. Mit $k := \mathrm{ord}([\,a\,]_m)$ und $l := \mathrm{ord}([\,b\,]_m)$ setze man

$$\alpha := r\Big(k, \frac{l}{\mathrm{ggT}(k,l)}\Big), \quad \gamma := r\Big(l, \frac{k}{\mathrm{ggT}(k,l)}\Big) \quad \text{und} \quad \beta := \frac{\gamma}{\mathrm{ggT}(\alpha,\gamma)}.$$

Für $c := (a^{k/\alpha}\, b^{l/\beta}) \bmod m$ gilt $\mathrm{ggT}(c,m) = 1$ und $\mathrm{ord}([\,c\,]_m) = \mathrm{kgV}(k,l)$.

Man schreibe eine MuPAD-Funktion, die zu $m \in \mathbb{N}$ und ganzen Zahlen a und b mit $\mathrm{ggT}(a,m) = \mathrm{ggT}(b,m) = 1$ ein $c \in \{1,2,\ldots,m-1\}$ mit

$$\mathrm{ggT}(c,m) = 1 \quad \text{und} \quad \mathrm{ord}\big([\,c\,]_m\big) = \mathrm{kgV}\big(\mathrm{ord}([\,a\,]_m), \mathrm{ord}([\,b\,]_m)\big)$$

berechnet.

(3) Es sei p eine ungerade Primzahl. Das folgende Verfahren liefert eine Primitivwurzel g modulo p mit $g \in \{2,3,\ldots,p-1\}$.

Schritt 1: Man wählt ein $a \in \{2,3,\ldots,p-1\}$, etwa eine Zufallszahl, und ermittelt $k := \mathrm{ord}([\,a\,]_p)$.

Schritt 2: Ist $k := p-1$, so ist a eine Primitivwurzel modulo p; in diesem Fall setzt man $g := a$ und bricht ab.

Schritt 3: Man wählt $b \in \{2,3,\ldots,p-1\} \setminus \{a^i \bmod p \mid i = 1,2,\ldots,k-1\}$ und ermittelt $l := \mathrm{ord}([\,b\,]_p)$. Dann gilt $l \nmid k$, denn sonst wäre $[\,b\,]_p$ ein Element der von $[\,a\,]_p$ erzeugten Untergruppe von $\mathbb{F}_p^\times$ (vgl. (3.10)). Ist $l = p-1$, so ist b eine Primitivwurzel modulo p; in diesem Fall setzt man $g := b$ und bricht ab.

Schritt 4: Man ermittelt mit dem in (2) beschriebenen Verfahren ein $c \in \{2,3,\ldots,p-1\}$ mit $\mathrm{ord}([\,c\,]_p) = \mathrm{kgV}(k,l) =: k'$. (Es ist $k' > k$). Man setzt $a := c$ und $k := k'$ und geht zu Schritt 2 zurück.

Man schreibe zu diesem Verfahren eine MuPAD-Funktion.

Aufgabe 2: Man schreibe eine MuPAD-Funktion, die zu natürlichen Zahlen n und N feststellt, wie oft jede natürliche Zahl als kleinste positive Primitivwurzel $g(p)$ einer Primzahl p mit $n \le p \le N$ vorkommt.

Aufgabe 3: In (5.7)(3) und (5.7)(4) werden zwei Verfahren angegeben, mit deren Hilfe man zu einer kleinen Primzahl p und einer Primitivwurzel modulo p Indizes berechnen kann. Man schreibe dazu MuPAD-Funktionen.

Aufgabe 4: Man schreibe eine MuPAD-Funktion, die mit Hilfe des in (5.8) beschriebenen Verfahrens Indizes berechnet.

Aufgabe 5: Man schreibe eine MuPAD-Funktion, die mit Hilfe des Algorithmus von Silver, Pohlig und Hellman aus (5.10) Indizes berechnet. Man versuche, dieses Verfahren mit dem in Abschnitt (5.8) verwendeten Trick zu kombinieren.

Aufgabe 6: Es sei p eine ungerade Primzahl, es sei $\beta \in \mathbb{N}$ mit $\beta \geq 2$, und es sei g eine Primitivwurzel modulo p^β. Man beweise, daß g für jedes $\alpha \in \mathbb{N}$ eine Primitivwurzel modulo p^α ist.

Aufgabe 7: Es sei $\lambda : \mathbb{N} \to \mathbb{N}$ die Carmichael-Funktion (vgl. (5.21)).

(a) Es sei m eine natürliche Zahl > 1, die keine Primzahl ist. Man zeige, daß m genau dann eine Carmichael-Zahl ist, wenn $m - 1$ durch $\lambda(m)$ teilbar ist (vgl. Carmichael [19]).

(b) Aus der Charakterisierung der Carmichael-Zahlen in (a) folgere man: Ist $m \in \mathbb{N}$ eine Carmichael-Zahl, so besitzt m mindestens drei verschiedene Primteiler und ist nicht durch das Quadrat einer Primzahl teilbar.

(c) Man beweise das von A. Korselt 1899 angegebene Kriterium: Eine natürliche Zahl m ist genau dann eine Carmichael-Zahl, wenn m das Produkt von $r \geq 3$ paarweise verschiedenen Primzahlen $p_1, p_2, \ldots, p_r$ ist und $m - 1$ für jedes $i \in \{1, 2, \ldots, r\}$ durch $p_i - 1$ teilbar ist.

(d) Man schreibe eine MuPAD-Funktion, die mit Hilfe des Kriteriums von Korselt zu natürlichen Zahlen a und b alle Carmichael-Zahlen zwischen a und b findet.

(e) Man zeige: Ist k eine natürliche Zahl und sind $6k + 1$, $12k + 1$ und $18k + 1$ Primzahlen, so ist $(6k + 1) \cdot (12k + 1) \cdot (18k + 1)$ eine Carmichael-Zahl. Man finde Carmichael-Zahlen, die diese Gestalt besitzen.

6 Nichtlineare Kongruenzen

(6.1) In diesem Paragraphen werden zuerst nichtlineare Kongruenzen behandelt. Daran schließt die Theorie der Potenzreste an. Einige Ergebnisse dieser Theorie werden im nächsten Paragraphen bei der Behandlung des Primzahltests von Rabin benötigt. Aber auch für sich betrachtet ist die Theorie der Potenzreste von Interesse; ein Spezialfall, die Theorie der quadratischen Reste, auf die in § 10 ausführlich eingegangen wird, gilt seit Gauß mit Recht als einer der Höhepunkte der Elementaren Zahlentheorie.

(6.2) Bezeichnung: Für ein Polynom $f \in \mathbb{Z}[X]$ und für ein $m \in \mathbb{N}$ wird

$$N(f, m) := \#\big(\{x \in \mathbb{Z} \mid 0 \leq x \leq m - 1; f(x) \equiv 0 \pmod{m}\}\big)$$

gesetzt.