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.

(6.3) Satz: *Es sei $f \in \mathbb{Z}[X]$, es sei $m \in \mathbb{N}$, und es sei $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ die Primzerlegung von m. Es gilt*

$$N(f,m) \;=\; N(f,p_1^{\alpha_1})\,N(f,p_2^{\alpha_2}) \cdots N(f,p_r^{\alpha_r}).$$

Beweis: (a) Ist x eine ganze Zahl und gilt $f(x) \equiv 0 \pmod{m}$, so gilt auch $f(x) \equiv 0 \pmod{p_i^{\alpha_i}}$ für jedes $i \in \{1,2,\ldots,r\}$.
(b) Es seien $x_1, x_2, \ldots, x_r \in \mathbb{Z}$, und es gelte $f(x_i) \equiv 0 \pmod{p_i^{\alpha_i}}$ für jedes $i \in \{1,2,\ldots,r\}$. Der Chinesische Restsatz (vgl. (4.14)) liefert eine ganze Zahl x mit $0 \le x \le m-1$ und mit $x \equiv x_i \pmod{p_i^{\alpha_i}}$ für jedes $i \in \{1,2,\ldots,r\}$. Für jedes $i \in \{1,2,\ldots,r\}$ gilt $f(x) \equiv f(x_i) \equiv 0 \pmod{p_i^{\alpha_i}}$, und daher ist $f(x) \equiv 0 \pmod{m}$.
(c) Es seien $x, x_1, \ldots, x_r$ und $y, y_1, \ldots, y_r$ ganze Zahlen, für die gilt: Für jedes $i \in \{1,2,\ldots,r\}$ gilt $f(x_i) \equiv 0 \pmod{p_i^{\alpha_i}}$ und $x \equiv x_i \pmod{p_i^{\alpha_i}}$, sowie $f(y_i) \equiv 0 \pmod{p_i^{\alpha_i}}$ und $y \equiv y_i \pmod{p_i^{\alpha_i}}$. Es gilt $y \equiv x \pmod{m}$ genau dann, wenn $y \equiv x \pmod{p_i^{\alpha_i}}$ für jedes $i \in \{1,2,\ldots,r\}$ gilt, also genau dann, wenn $y_i \equiv x_i \pmod{p_i^{\alpha_i}}$ für jedes $i \in \{1,2,\ldots,r\}$ gilt.

(6.4) Bemerkung: Es sei

$$f \;=\; \sum_{j=0}^{n} a_j X^j \;=\; a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \;\in\; \mathbb{Z}[X]$$

ein Polynom, und es sei $m \in \mathbb{N}$. $N(f,m)$ ist die Anzahl der verschiedenen Nullstellen des Polynoms

$$[a_n]_m X^n + [a_{n-1}]_m X^{n-1} + \cdots + [a_1]_m X + [a_0]_m \;\in\; (\mathbb{Z}/m\mathbb{Z})[X]$$

im Ring $\mathbb{Z}/m\mathbb{Z}$.
Der Satz in (6.3) führt die Untersuchung der Kongruenz $f(X) \equiv 0 \pmod{m}$ auf die Untersuchung von Kongruenzen $f(X) \equiv 0 \pmod{p^\alpha}$ zurück, in denen jeweils p eine Primzahl und α eine natürliche Zahl ist.

(6.5) Satz: *Es sei $f = \sum_{j=0}^{n} a_j X^j \in \mathbb{Z}[X]$, und es sei $f' = \sum_{j=1}^{n} j a_j X^{j-1}$ die Ableitung von f; es sei p eine Primzahl, es sei $\alpha \in \mathbb{N}$, es sei $x \in \mathbb{Z}$, und es gelte $f(x) \equiv 0 \pmod{p^\alpha}$.*
(1) Ist $f'(x) \not\equiv 0 \pmod{p}$, so gibt es genau ein $z \in \{0,1,\ldots,p^{\alpha+1}-1\}$ mit $z \equiv x \pmod{p^\alpha}$ und mit $f(z) \equiv 0 \pmod{p^{\alpha+1}}$, und zwar gilt: Es gibt ein eindeutig bestimmtes $y \in \{0,1,\ldots,p-1\}$ mit

$$f'(x)\,y \;\equiv\; -\frac{f(x)}{p^\alpha} \pmod{p},$$

und damit gilt $z = x + yp^\alpha$.

(2) *Wenn* $f'(x) \equiv 0 \pmod{p}$ *und* $f(x) \not\equiv 0 \pmod{p^{\alpha+1}}$ *gilt, so existiert kein* $z \in \{0, 1, \ldots, p^{\alpha+1} - 1\}$ *mit* $z \equiv x \pmod{p^\alpha}$ *und mit* $f(z) \equiv 0 \pmod{p^{\alpha+1}}$.
(3) *Wenn* $f'(x) \equiv 0 \pmod{p}$ *und* $f(x) \equiv 0 \pmod{p^{\alpha+1}}$ *gilt, so gibt es genau* p *verschiedene Zahlen* $z \in \{0, 1, \ldots, p^{\alpha+1} - 1\}$, *für die* $z \equiv x \pmod{p^\alpha}$ *und* $f(z) \equiv 0 \pmod{p^{\alpha+1}}$ *gilt, und zwar sind dies die Zahlen*

$$x, \quad x + p^\alpha, \quad x + 2p^\alpha, \quad \ldots \quad , \quad x + (p-1)p^\alpha.$$

Beweis: (a) Für jedes $y \in \mathbb{Z}$ gilt: Für jedes $j \in \mathbb{N}$ ist

$$\begin{aligned}(x + yp^\alpha)^j &= \sum_{i=0}^{j} \binom{j}{i} x^{j-i} y^i p^{\alpha i} = x^j + jx^{j-1} yp^\alpha + \sum_{i=2}^{j} \binom{j}{i} x^{j-i} y^i p^{\alpha i} \equiv \\ &\equiv x^j + jx^{j-1} yp^\alpha \pmod{p^{\alpha+1}},\end{aligned}$$

und daher ist

$$\begin{aligned}f(x + yp^\alpha) &= \sum_{j=0}^{n} a_j (x + y\,p^\alpha)^j = \sum_{j=0}^{n} a_j x^j + yp^\alpha \sum_{j=1}^{n} j a_j x^{j-1} = \\ &= f(x) + yp^\alpha f'(x) \pmod{p^{\alpha+1}}.\end{aligned}$$

(b) Es gelte $f'(x) \not\equiv 0 \pmod{p}$, also $p \nmid f'(x)$. Dann gibt es ein eindeutig bestimmtes $y \in \{0, 1, \ldots, p-1\}$ mit

$$f'(x)\, y \equiv -\frac{f(x)}{p^\alpha} \pmod{p}$$

(vgl. (4.9)(2)). Für $z := x + yp^\alpha$ gilt $0 \leq z \leq p^{\alpha+1} - 1$ und $z \equiv y \pmod{p^\alpha}$ und

$$f(z) \equiv f(x) + yp^\alpha f'(x) \equiv f(x) - f(x) \equiv 0 \pmod{p^{\alpha+1}}.$$

Gilt $w \in \{0, 1, \ldots, p^{\alpha+1} - 1\}$ und $w \equiv x \pmod{p^\alpha}$ und $f(w) \equiv 0 \pmod{p^{\alpha+1}}$, so gibt es ein $v \in \{0, 1, \ldots, p-1\}$, für das $w = x + vp^\alpha$ ist, und es gilt $f(x) + vp^\alpha f'(x) \equiv f(w) \equiv 0 \pmod{p^{\alpha+1}}$, also $f'(x)v \equiv -f(x)p^{-\alpha} \pmod{p}$, also $v = y$, und daher ist $w = x + yp^\alpha = z$.
(c) Es gelte $f'(x) \equiv 0 \pmod{p}$ und $f(x) \not\equiv 0 \pmod{p^{\alpha+1}}$. Zu jeder Zahl $z \in \{0, 1, \ldots, p^{\alpha+1} - 1\}$, für die $z \equiv x \pmod{p^\alpha}$ gilt, gibt es eine Zahl $y \in \{0, 1, \ldots, p-1\}$ mit $z = x + yp^\alpha$, und es gilt

$$f(z) = f(x + yp^\alpha) \equiv f(x) + yp^\alpha f'(x) \equiv f(x) \not\equiv 0 \pmod{p^{\alpha+1}}.$$

(d) Es gelte $f'(x) \equiv 0 \pmod{p}$ und $f(x) \equiv 0 \pmod{p^{\alpha+1}}$. Dann gilt für jedes $y \in \{0, 1, \ldots, p-1\}$: Es ist

$$f(x + yp^\alpha) \equiv f(x) + yp^\alpha f'(x) \equiv f(x) \equiv 0 \pmod{p^{\alpha+1}}.$$

(6.6) Bemerkung: Es sei

$$f = \sum_{j=0}^{n} a_j X^j = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$$

ein Polynom in einer Unbestimmten X über dem Ring $\mathbb{Z}$.
(1) Es sei $m \in \mathbb{N}$. Der Beweis in (6.3) zeigt, daß man alle $x \in \{0, 1, \ldots, m-1\}$ mit $f(x) \equiv 0 \pmod{m}$ berechnen kann, wenn man für jeden Primteiler p von m alle $x \in \{0, 1, \ldots, p^{v_p(m)} - 1\}$ kennt, für die $f(x) \equiv 0 \pmod{p^{v_p(m)}}$ gilt.
(2) Es sei p eine Primzahl, und es sei $\alpha \in \mathbb{N}$ mit $\alpha \geq 2$. Der Beweis in (6.5) zeigt, wie man alle $x \in \{0, 1, \ldots, p^\alpha - 1\}$ mit $f(x) \equiv 0 \pmod{p^\alpha}$ finden kann, wenn man alle $x \in \{0, 1, \ldots, p^{\alpha-1} - 1\}$ kennt, für die $f(x) \equiv 0 \pmod{p^{\alpha-1}}$ gilt. Man kann also alle $x \in \{0, 1, \ldots, p^\alpha - 1\}$ mit $f(x) \equiv 0 \pmod{p^\alpha}$ berechnen, wenn man alle $x \in \{0, 1, \ldots, p-1\}$ mit $f(x) \equiv 0 \pmod{p}$, also alle Nullstellen $\xi \in \mathbb{F}_p$ des Polynoms

$$\overline{f} := \sum_{j=0}^{n} [a_j]_p X^j \in \mathbb{F}_p[X]$$

kennt. Es gibt Algorithmen zur Berechnung der Primzerlegung des Polynoms $\overline{f}$ im Polynomring $\mathbb{F}_p[X]$ und damit insbesondere zur Berechnung der Nullstellen $\xi \in \mathbb{F}_p$ von $\overline{f}$. Von diesen Algorithmen, deren Studium jedem an der Algebra besonders interessierten Leser empfohlen wird, kann hier nicht die Rede sein; man findet sie etwa in den Büchern Geddes-Czapor-Labahn [40] und Zippel [115] behandelt.

Wenn man nicht an der vollen Primzerlegung des Polynoms $\overline{f}$ im Ring $\mathbb{F}_p[X]$, sondern nur an seinen Nullstellen in $\mathbb{F}_p$ interessiert ist, so kann man so vorgehen: Da der größte gemeinsame Teiler von $\overline{f}$ und $X^p - X$ im Ring $\mathbb{F}_p[X]$ das Produkt der Faktoren vom Grad 1 in der Primzerlegung von $\overline{f}$ ist, berechnet man mit dem Euklidischen Algorithmus im Ring $\mathbb{F}_p[X]$ diesen größten gemeinsamen Teiler, berechnet seine Primzerlegung in $\mathbb{F}_p[X]$ und liest daran die Nullstellen von $\overline{f}$ in $\mathbb{F}_p$ ab.

(6.7) MuPAD: Die Funktion `numlib::mroots` liefert zu einem Polynom $f \in \mathbb{Z}[X]$ und zu einer natürlichen Zahl m alle Zahlen $x \in \{0, 1, \ldots, m-1\}$ mit $f(x) \equiv 0 \pmod{m}$, bzw. die Ausgabe `FAIL`, falls es keine solchen x gibt; sie

berechnet zuerst zu jedem Primteiler p von m die Zahlen $x \in \{0, 1, \ldots, p-1\}$ mit $f(x) \equiv 0 \pmod{p}$ und benützt dann die in den Beweisen in (6.5) und (6.3) verwendeten Rechenverfahren. `numlib::mroots` verwendet, wie in (6.6)(2) angedeutet, die Funktion `factor`, die die Primzerlegung von Polynomen über dem Ring $\mathbb{Z}$ oder über einem Restklassenkörper von $\mathbb{Z}$ berechnet.

Über das Rechnen mit Polynomen und insbesondere über die Funktion `factor` und die Funktion `gcd`, die größte gemeinsame Teiler von Polynomen berechnet, lese man im MuPAD-Manual [72] nach.

(6.8) Bemerkung: Es sei $f \in \mathbb{Z}[X]$ ein Polynom vom Grad $n \geq 1$. Ist p eine Primzahl, so gibt es höchstens n Elemente $x \in \{0, 1, \ldots, p-1\}$ mit $f(x) \equiv 0 \pmod{p}$, d.h. es ist $N(f, p) \leq n$. Ist aber $m \geq 2$ keine Primzahl, so kann, wie das folgende Beispiel zeigt, $N(f, m) > n$ gelten. Abschätzungen von $N(f, m)$ findet man in Ore [76], in Huxley [48] und in Stewart [106].

(6.9) Beispiel: In diesem Beispiel werden für das Polynom

$$f := X^4 - 18X^2 - 33X - 10 \in \mathbb{Z}[X]$$

und für $m \in \{7, 7^2, 7^3, 7^4, 7^{20}\}$ jeweils die Zahlen $x \in \{0, 1, \ldots, m-1\}$ berechnet, für die

$$f(x) \equiv 0 \pmod{m}$$

gilt.

```
>> f := poly(X^4 - 18*X^2 - 33*X - 10,[X],Dom::Integer);
      poly(X + (-18) X + (-33) X - 10,[X],Dom::Integer)
>> numlib::mroots(f,7);
                                  [5]
>> numlib::mroots(f,7^2);
                     [5,12,19,26,33,40,47]
>> numlib::mroots(f,7^3);
     [5,47,54,96,103,145,152,194,201,243,250,292,299,341]
>> numlib::mroots(f,7^4);
     [5,341,348,684,691,1027,1034,1370,1377,1713,1720,
                                                2056,2063,2399]
>> numlib::mroots(f,7^20);
   [5,11398895185373141,11398895185373148,22797790370746284,
      22797790370746291,34196685556119427,34196685556119434,
      45595580741492570,45595580741492577,56994475926865713,
      56994475926865720,68393371112238856,68393371112238863,
      79792266297611999]
```

(6.10) Definition: Es seien m und n natürliche Zahlen. Eine ganze Zahl a heißt ein n-ter Potenzrest modulo m, wenn a und m teilerfremd sind und es ein $x \in \mathbb{Z}$ mit $x^n \equiv a \pmod{m}$ gibt.

(6.11) Bemerkung: Es seien $m, n \in \mathbb{N}$, und es sei $a \in \mathbb{Z}$ ein n-ter Potenzrest modulo m.
(1) Jedes $a' \in \mathbb{Z}$ mit $a' \equiv a \pmod{m}$ ist ein n-ter Potenzrest modulo m.
(2) Es sei $x \in \mathbb{Z}$ eine Lösung der Kongruenz $X^n \equiv a \pmod{m}$. Wegen $\mathrm{ggT}(a,m) = 1$ ist $\mathrm{ggT}(x,m) = 1$, und jedes $x' \in \mathbb{Z}$ mit $x' \equiv x \pmod{m}$ ist ebenfalls Lösung dieser Kongruenz.
(3) Es seien $x_1, x_2, \ldots, x_N$ die Lösungen der Kongruenz $X^n \equiv a \pmod{m}$ in $\{0, 1, \ldots, m-1\}$. Für jedes $i \in \{1, 2, \ldots, N\}$ gilt $\mathrm{ggT}(x_i, m) = 1$, und somit ist

$$N \;\leq\; \#\big(\{x \in \mathbb{Z} \mid 0 \leq x \leq m-1;\, \mathrm{ggT}(x,m) = 1\}\big) \;=\; \varphi(m).$$

Es gilt

$$\{x \in \mathbb{Z} \mid x^n \equiv a \pmod{m}\} \;=\; \bigcup_{i=1}^{N} \{x \in \mathbb{Z} \mid x \equiv x_i \pmod{m}\}.$$

(6.12) Bezeichnung: Es seien $m, n \in \mathbb{N}$. Für jedes $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a,m) = 1$ wird

$$\begin{aligned} N_n(a,m) \;&:=\; N(X^n - a, m) \;= \\ &=\; \#\big(\{x \in \mathbb{Z} \mid 0 \leq x \leq m-1;\, x^n \equiv a \pmod{m}\}\big) \end{aligned}$$

gesetzt.

(6.13) Bemerkung: Es seien $m, n \in \mathbb{N}$, und es sei $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a,m) = 1$. a ist genau dann ein n-ter Potenzrest modulo m, wenn es ein $\xi \in E(\mathbb{Z}/m\mathbb{Z})$ mit $\xi^n = [a]_m$ gibt. Ist a ein n-ter Potenzrest modulo m, so gilt

$$\#\big(\{\xi \in E(\mathbb{Z}/m\mathbb{Z}) \mid \xi^n = [a]_m\}\big) \;=\; N_n(a,m).$$

(6.14) Satz: *Es sei $m \in \mathbb{N}$, und es sei $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ die Primzerlegung von m; es seien $n \in \mathbb{N}$ und $a \in \mathbb{Z}$.*
(1) *a ist genau dann ein n-ter Potenzrest modulo m, wenn gilt: Für jedes $i \in \{1, 2, \ldots, r\}$ ist a ein n-ter Potenzrest modulo $p_i^{\alpha_i}$.*
(2) *Ist $\mathrm{ggT}(a,m) = 1$, so gilt*

$$N_n(a,m) \;=\; N_n(a, p_1^{\alpha_1}) N_n(a, p_2^{\alpha_2}) \cdots N_n(a, p_r^{\alpha_r}).$$

Beweis: Man wendet (6.3) auf das Polynom $f := X^n - a \in \mathbb{Z}[X]$ an.

(6.15) Bemerkung: Es sei $n \in \mathbb{N}$, und es sei $a \in \mathbb{Z}$. Mit Hilfe von (6.14) läßt sich die Untersuchung von Kongruenzen der Form $X^n \equiv a \pmod{m}$, in denen m eine natürliche Zahl mit $\mathrm{ggT}(a,m) = 1$ ist, auf die Untersuchung von Kongruenzen $X^n \equiv a \pmod{p^\alpha}$ zurückführen, in denen p eine Primzahl, die a nicht teilt, und α eine natürliche Zahl ist.

(6.16) Satz: *Es sei p eine ungerade Primzahl, und es seien α und n natürliche Zahlen; es sei $d := \mathrm{ggT}(n, \varphi(p^\alpha))$.*

(1) *Es sei $a \in \mathbb{Z} \setminus p\mathbb{Z}$. Folgende Aussagen sind äquivalent:*
   (a) *a ist ein n-ter Potenzrest modulo p^α.*
   (b) *a ist ein d-ter Potenzrest modulo p^α.*
   (c) *Es gilt $a^{\varphi(p^\alpha)/d} \equiv 1 \pmod{p^\alpha}$.*

(2) *Für jeden n-ten Potenzrest $a \in \mathbb{Z}$ modulo p^α gilt*

$$N_n(a, p^\alpha) \;=\; \mathrm{ggT}\big(n, \varphi(p^\alpha)\big).$$

(3) *In $\{0, 1, \ldots, p^\alpha - 1\}$ gibt es genau $\varphi(p^\alpha)/d$ verschiedene n-te Potenzreste modulo p^α.*

Beweis: Es sei $g \in \mathbb{Z}$ eine Primitivwurzel modulo p^α (vgl. (5.2) und (5.16)). (1) und (3): $U := \{\xi^n \mid \xi \in E(\mathbb{Z}/p^\alpha\mathbb{Z})\}$ ist eine Untergruppe der Gruppe $E(\mathbb{Z}/p^\alpha\mathbb{Z})$. Es gilt $E(\mathbb{Z}/p^\alpha\mathbb{Z}) = \langle\, [\,g\,]_{p^\alpha} \,\rangle$ und $U = \langle\, [\,g\,]^n_{p^\alpha} \,\rangle$. Nach (3.7)(2) ist

$$\#(U) \;=\; \#\big(\langle\, [\,g\,]^n_{p^\alpha} \,\rangle\big) \;=\; \mathrm{ord}\big([\,g\,]^n_{p^\alpha}\big) \;=\; \frac{\mathrm{ord}\big([\,g\,]_{p^\alpha}\big)}{\mathrm{ggT}\big(n, \mathrm{ord}([\,g\,]_{p^\alpha})\big)} \;=$$
$$= \frac{\varphi(p^\alpha)}{\mathrm{ggT}\big(n, \varphi(p^\alpha)\big)} \;=\; \frac{\varphi(p^\alpha)}{d} \;=\; \frac{\#(G)}{d}.$$

Nach (3.10) gilt daher einerseits

$$U \;=\; \big\langle\, [\,g\,]^{\#(G)/\#(U)}_{p^\alpha} \,\big\rangle \;=\; \big\langle\, [\,g\,]^d_{p^\alpha} \,\big\rangle \;=\; \big\{\xi^d \mid \xi \in E(\mathbb{Z}/p^\alpha\mathbb{Z})\big\} \;=$$
$$= \big\{[\,a\,]_{p^\alpha} \mid 0 \le a \le p^\alpha - 1;\; a \text{ ist } d\text{-ter Potenzrest modulo } p^\alpha\big\}$$

und andererseits

$$U \;=\; \big\{\eta \in E(\mathbb{Z}/p^\alpha\mathbb{Z}) \mid \eta^{\#(U)} = [\,1\,]_{p^\alpha}\big\} \;=$$
$$= \big\{\eta \in E(\mathbb{Z}/p^\alpha\mathbb{Z}) \mid \eta^{\varphi(p^\alpha)/d} = [\,1\,]_{p^\alpha}\big\} \;=$$
$$= \big\{[\,a\,]_{p^\alpha} \mid 0 \le a \le p^\alpha - 1;\; p \nmid a;\; a^{\varphi(p^\alpha)/d} \equiv 1 \pmod{p^\alpha}\big\}.$$

Damit ist gezeigt, daß die drei Aussagen (a), (b) und (c) in (1) äquivalent sind und daß (3) gilt.

(2) Es sei $a \in \mathbb{Z}$, und es gelte: a ist ein n-ter Potenzrest modulo p^α. Es gibt ein $j \in \{0, 1, \ldots, p^\alpha - 1\}$ mit $a \equiv g^j \pmod{p^\alpha}$. Nach (1) gilt

$$g^{j\varphi(p^\alpha)/d} \equiv a^{\varphi(p^\alpha)/d} \equiv 1 \pmod{p^\alpha},$$

und daher ist $j\varphi(p^\alpha)/d$ durch $\operatorname{ord}([g]_{p^\alpha}) = \varphi(p^\alpha)$ teilbar (vgl. (3.5)(3)). Also ist j durch $d = \operatorname{ggT}(n, \varphi(p^\alpha))$ teilbar, und somit besitzt die Kongruenz $nk \equiv j \pmod{\varphi(p^\alpha)}$ nach (4.9)(3) in $\{0, 1, \ldots, p^\alpha - 1\}$ genau d verschiedene Lösungen $k_1, k_2, \ldots, k_d$. Für jedes $i \in \{1, 2, \ldots, d\}$ gilt

$$x_i := g^{k_i} \bmod p^\alpha \in \{0, 1, \ldots, p^\alpha - 1\}$$

und

$$x_i^n \equiv g^{nk_i} \equiv g^j \equiv a \pmod{p^\alpha},$$

und $x_1, x_2, \ldots, x_d$ sind paarweise verschieden.

Andererseits gilt für jedes $x \in \mathbb{Z}$, für das $x^n \equiv a \pmod{p^\alpha}$ ist: Wegen $p \nmid x$ gibt es ein $k \in \{0, 1, \ldots, \varphi(p^\alpha) - 1\}$ mit $x \equiv g^k \pmod{p^\alpha}$, wegen

$$g^{nk} \equiv x^n \equiv a \equiv g^j \pmod{p^\alpha}$$

gilt $nk \equiv j \pmod{\varphi(p^\alpha)}$, und daher gilt $k \in \{k_1, k_2, \ldots, k_d\}$ und $x \bmod p^\alpha \in \{x_1, x_2, \ldots, x_d\}$. Also gilt

$$\{x \in \mathbb{Z} \mid 0 \le x \le p^\alpha - 1;\ x^n \equiv a \pmod{p^\alpha}\} = \{x_1, x_2, \ldots, x_d\}$$

und $N_n(a, p^\alpha) = d$.

(6.17) Beispiel: (1) Es sei p eine ungerade Primzahl, und es seien α und n natürliche Zahlen. Nach (6.16)(1) ist -1 dann und nur dann ein n-ter Potenzrest modulo p^α, wenn gilt: Es ist

$$(-1)^{\varphi(p^\alpha)/\operatorname{ggT}(n, \varphi(p^\alpha))} \equiv 1 \pmod{p^\alpha}.$$

Da p ungerade ist, ist dies genau dann der Fall, wenn $\varphi(p^\alpha)/\operatorname{ggT}(n, \varphi(p^\alpha))$ gerade ist. Der Exponent von 2 in der Primzerlegung von $\varphi(p^\alpha)$ ist

$$v_2\big(\varphi(p^\alpha)\big) = v_2\big(p^{\alpha-1}(p-1)\big) = v_2(p-1),$$

und der Exponent von 2 in der Primzerlegung von $\operatorname{ggT}(n, \varphi(p^\alpha))$ ist

$$v_2\big(\operatorname{ggT}(n, \varphi(p^\alpha))\big) = \min\big(\{v_2(n), v_2(\varphi(p^\alpha))\}\big) = \min\big(\{v_2(n), v_2(p-1)\}\big).$$

Also ist -1 ein n-ter Potenzrest modulo p^α, genau wenn gilt: Es ist

$$v_2(n) < v_2(p-1).$$

(2) Es sei $m \in \mathbb{N}$ ungerade, und es sei $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ die Primzerlegung von m. Nach (6.14)(1) ist -1 ein n-ter Potenzrest modulo m, genau wenn -1 für jedes $i \in \{1, 2, \ldots, r\}$ ein n-ter Potenzrest modulo $p_i^{\alpha_i}$ ist. Aus (1) folgt daher, daß -1 genau dann ein n-ter Potenzrest modulo m ist, wenn gilt: Für jedes $i \in \{1, 2, \ldots, r\}$ ist $v_2(n) < v_2(p_i - 1)$. Nach (6.14)(2) gilt außerdem: Ist -1 ein n-ter Potenzrest modulo m, so gilt

$$N_n(-1, m) = \prod_{i=1}^{r} N_n\big(-1, p_i^{\alpha_i}\big) = \prod_{i=1}^{r} \operatorname{ggT}\big(n, \varphi(p^{\alpha})\big).$$

(6.18) Satz: *Es sei $n \in \mathbb{N}$, und es sei $a \in \mathbb{Z}$ ungerade.*
(1) *a ist n-ter Potenzrest modulo 2, und es gilt $N_n(a, 2) = 1$.*
(2) *Ist n ungerade, so gilt: a ist ein n-ter Potenzrest modulo 4, und es ist $N_n(a, 4) = 1$; ist n gerade, so ist a genau dann ein n-ter Potenzrest modulo 4, wenn $a \equiv 1 \pmod 4$ gilt, und ist dies der Fall, so ist $N_n(a, 4) = 2$.*
(3) *Es sei α eine natürliche Zahl mit $\alpha \geq 3$, es seien $i \in \{0, 1\}$ und $j \in \{0, 1, \ldots, 2^{\alpha-2} - 1\}$ die Zahlen mit $a \equiv (-1)^i 5^j \pmod{2^{\alpha}}$ (vgl. (5.19)(2)), und es sei $\delta := \min(\{v_2(n), \alpha - 2\})$. Ist n ungerade, so ist a ein n-ter Potenzrest modulo 2^{α}, und es ist $N_n(a, 2^{\alpha}) = 1$; ist n gerade, so ist a ein n-ter Potenzrest modulo 2^{α}, genau wenn $a \equiv 1 \pmod 8$ und $v_2(j) \geq \delta$, gilt, und ist dies der Fall, so ist $N_n(a, 2^{\alpha}) = 2^{\delta} = \operatorname{ggT}(n, 2^{\alpha-2})$.*

Beweis: (1) ist klar, und (2) folgt, indem man die n-ten Potenzen in der Gruppe $E(\mathbb{Z}/4\mathbb{Z}) = \{[1]_4, [3]_4\}$ betrachtet.
(3) (a) Es sei $x \in \mathbb{Z}$ ungerade. Nach (5.19)(2) gibt es eindeutig bestimmte $k \in \{0, 1\}$ und $l \in \{0, 1, \ldots, 2^{\alpha-2} - 1\}$ mit $x \equiv (-1)^k 5^l \pmod{2^{\alpha}}$. Wegen $\operatorname{ord}([5]_{2^{\alpha}}) = 2^{\alpha-2}$ (vgl. (5.20)(1)) gilt

$$x^n \equiv (-1)^{nk} 5^{nl} \equiv (-1)^{nk \bmod 2} \cdot 5^{nl \bmod 2^{\alpha-2}} \pmod{2^{\alpha}}.$$

Also gilt $x^n \equiv a \pmod{2^{\alpha}}$, genau wenn $nk \bmod 2 = i$ und $nl \bmod 2^{\alpha-2} = j$ gilt, also genau wenn $nk \equiv i \pmod 2$ und $nl \equiv j \pmod{2^{\alpha-2}}$ gilt.
(b) Es gelte: n ist ungerade. Dann gibt es ein eindeutig bestimmtes $k \in \{0, 1\}$ mit $nk \equiv i \pmod 2$ und ein eindeutig bestimmtes $l \in \{0, 1, \ldots, 2^{\alpha-2} - 1\}$ mit $nl \equiv j \pmod{2^{\alpha-2}}$ (vgl. (4.9)(2)). Hieraus und aus (a) folgt: Es gibt ein eindeutig bestimmtes $x \in \{0, 1, \ldots, 2^{\alpha} - 1\}$ mit $x^n \equiv a \pmod{2^{\alpha}}$, nämlich $x = (-1)^k 5^l \bmod 2^{\alpha}$. Also ist a ein n-ter Potenzrest modulo 2^{α}, und es ist $N_n(a, 2^{\alpha}) = 1$.
(c) Es gelte: n ist gerade, und es ist $a \not\equiv 1 \pmod 8$. Für jedes ungerade $x \in \mathbb{Z}$ gilt $x^n \equiv 1 \pmod 8$, also $x^n \not\equiv a \pmod 8$, also $x^n \not\equiv a \pmod{2^{\alpha}}$. Somit ist a nicht n-ter Potenzrest modulo 2^{α}.

(d) Es gelte: n ist gerade, es ist $a \equiv 1 \pmod 8$, und es ist $v_2(j) < \delta$. Dann ist j nicht durch $\mathrm{ggT}(n, 2^{\alpha-2}) = 2^\delta$ teilbar, und daher gibt es kein $l \in \mathbb{Z}$ mit $nl \equiv j \pmod{2^{\alpha-2}}$ (vgl. (4.9)(1)). Also existiert nach (a) kein $x \in \mathbb{Z}$ mit $x^n \equiv a \pmod{2^\alpha}$, und somit ist a nicht n-ter Potenzrest modulo 2^α.
(e) Es gelte: n ist ungerade, es ist $a \equiv 1 \pmod 8$, und es ist $v_2(j) \geq \delta$. Es gilt $i = 0$, und j ist gerade (wegen $a \equiv 1 \pmod 8$, vgl. den Beweis in (5.20)(2)). Für $k := 0$ gilt $nk \equiv 0 \equiv i \pmod 2$, und weil j durch $\mathrm{ggT}(n, 2^{\alpha-2}) = 2^\delta$ teilbar ist, gibt es ein $l \in \mathbb{N}_0$ mit $nl \equiv j \pmod{2^{\alpha-2}}$ (vgl. (4.9)(1)). Für $x := (-1)^k 5^l = 5^l$ gilt $x^n \equiv a \pmod{2^\alpha}$, und somit ist a ein n-ter Potenzrest modulo 2^α. Diese Überlegung zeigt auch, daß die Anzahl $N_n(a, 2^\alpha)$ der $x \in \{0, 1, \ldots, 2^\alpha - 1\}$, für die $x^n \equiv a \pmod{2^\alpha}$ gilt, gleich der Anzahl $\mathrm{ggT}(n, 2^{\alpha-2}) = 2^\delta$ der Zahlen $l \in \{0, 1, \ldots, 2^{\alpha-2} - 1\}$ mit $nl \equiv j \pmod{2^{\alpha-2}}$ ist (vgl. (4.9)(3)).

(6.19) Satz: *Es sei p eine ungerade Primzahl, es sei n eine natürliche Zahl, die nicht durch p teilbar ist, und es sei $a \in \mathbb{Z} \setminus p\mathbb{Z}$. Folgende Aussagen sind äquivalent:*
(1) *a ist ein n-ter Potenzrest modulo p.*
(2) *Für jedes $\alpha \in \mathbb{N}$ ist a ein n-ter Potenzrest modulo p^α.*
(3) *Es gibt ein $\alpha \in \mathbb{N}$, für das a ein n-ter Potenzrest modulo p^α ist.*
(4) *Es gilt*

$$a^{(p-1)/\mathrm{ggT}(n,p-1)} \equiv 1 \pmod p.$$

Beweis: Daß (3) aus (2) und (1) aus (3) folgt, ist klar, und nach (6.16)(1) sind (1) und (4) äquivalent.
(1) $\Rightarrow$ (2): Es gelte, daß a ein n-ter Potenzrest modulo p ist. Es sei $\alpha \in \mathbb{N}$, und es sei bereits bewiesen, daß a ein n-ter Potenzrest modulo p^α ist. Dann gibt es eine ganze Zahl x mit $p \nmid x$ und mit $x^n \equiv a \pmod{p^\alpha}$. Für das Polynom $f := X^n - a \in \mathbb{Z}[X]$ gilt

$$f(x) \equiv 0 \pmod{p^\alpha} \quad \text{und} \quad f'(x) = nx^{n-1} \not\equiv 0 \pmod{p^\alpha},$$

und daher gibt es nach (6.5)(1) ein $z \in \mathbb{Z}$ mit $z^n - a = f(z) \equiv 0 \pmod{p^{\alpha+1}}$. Also ist a auch ein n-ter Potenzrest modulo $p^{\alpha+1}$.

(6.20) Bemerkung: Es sei p eine ungerade Primzahl, es sei n eine natürliche Zahl, die nicht durch p teilbar ist, es sei $a \in \mathbb{Z}$ ein n-ter Potenzrest modulo p, und es sei $\alpha \in \mathbb{N}$. Der Beweis in (6.5) zeigt, wie man aus einer Lösung $x_1 \in \mathbb{Z}$ der Kongruenz $X^n \equiv a \pmod p$ schrittweise eine Lösung $x_\alpha \in \mathbb{Z}$ der Kongruenz $X^n \equiv a \pmod{p^\alpha}$ berechnen kann. Auf diese Weise erhält man alle Lösungen von $X^n \equiv a \pmod{p^\alpha}$: Die Kongruenz $X^n \equiv a \pmod{p^\alpha}$

besitzt nämlich nach (6.16)(2) in $\{0,1,\ldots,p^\alpha-1\}$ genausoviele Lösungen wie die Kongruenz $X^n \equiv a \pmod{p}$ in $\{0,1,\ldots,p-1\}$, denn wegen $p \nmid n$ gilt

$$\begin{aligned} N_n(a,p^\alpha) &= \operatorname{ggT}\big(n,\varphi(p^\alpha)\big) = \\ &= \operatorname{ggT}\big(n,p^{\alpha-1}(p-1)\big) = \operatorname{ggT}(n,p-1) = N_n(a,p). \end{aligned}$$

(6.21) Aufgaben:

Aufgabe 1: Man schreibe MuPAD-Funktionen, die für eine Primzahl p, eine natürliche Zahl n und eine ganze Zahl a, die nicht durch p teilbar ist, feststellen, ob a ein n-ter Potenzrest modulo p ist, und die, falls dies der Fall ist, alle Lösungen $x \in \{0,1,\ldots,p-1\}$ der Kongruenz $X^n \equiv a \pmod{p}$ berechnen. Man verwende dabei einmal die Funktionen zur Berechnung von Primitivwurzeln und von Indizes und zum zweiten die Funktionen `factor` und `gcd` zum Rechnen in Polynomringen über Restklassenkörpern von $\mathbb{Z}$ (wie dies in `numlib::mroots` geschieht, vgl. (6.7)).

Ein Verfahren, das ohne das Rechnen in einem Polynomring auskommt, findet man im Abschnitt 7.3 des Buchs [10] von E. Bach und J. Shallit; für $n = 2$ vergleiche man § 12.

Aufgabe 2: Es sei p eine Primzahl, es sei n eine natürliche Zahl, die nicht durch p teilbar ist, es sei $\alpha \in \mathbb{N}$, und es sei a eine nicht durch p teilbare ganze Zahl. Man schreibe eine MuPAD-Funktion, die die Lösungen $x \in \{0,1,\ldots,p^\alpha-1\}$ der Kongruenz $X^n \equiv a \pmod{p^\alpha}$ berechnet, falls a ein n-ter Potenzrest modulo p^α ist, und die andernfalls `FAIL` ausgibt. (Man lese dazu den Beweis des Satzes in Abschnitt (6.5)).

Aufgabe 3: Es sei p eine Primzahl, es sei n eine natürliche Zahl, die durch p teilbar ist, es sei $\alpha \in \mathbb{N}$, und es sei a eine nicht durch p teilbare ganze Zahl. Man schreibe eine MuPAD-Funktion, die die Lösungen $x \in \{0,1,\ldots,p^\alpha-1\}$ der Kongruenz $X^n \equiv a \pmod{p^\alpha}$ berechnet, falls a ein n-ter Potenzrest modulo p^α ist, und die andernfalls `FAIL` ausgibt. (Man lese dazu den Beweis des Satzes in Abschnitt (6.5)).

Aufgabe 4: Es seien m und n natürliche Zahlen, und es sei a eine ganze Zahl mit $\operatorname{ggT}(a,m) = 1$. Man schreibe eine MuPAD-Funktion, die feststellt, ob a ein n-ter Potenzrest modulo m ist, und die, falls dies der Fall ist, alle Lösungen $x \in \{0,1,\ldots,m-1\}$ der Kongruenz $X^n \equiv a \pmod{m}$ berechnet.