A Primitive Elemente und Quadratreste

In diesem mathematischen Einschub werden einige mathematische Probleme geschlossen behandelt, die in der Kryptologie eine Rolle spielen und die multiplikative Gruppe eines Restklassenrings betreffen. Z. B. beruhen die Sicherheitsaussagen für manche kryptographische Verfahren auf der Nichtexistenz effizienter Algorithmen für einige dieser Probleme.

Die hier behandelten Probleme und ihre (nur z. T. behandelten) Lösungen sind:

1. Finden eines primitiven Elements.
   - Die Komplexität ist im allgemeinen Fall unbekannt.
   - Die vollständige Suche ist aber effizient, falls die erweiterte RIEMANNsche Vermutung richtig ist.
   - Es gibt einen sehr effizienten probabilistischen Algorithmus, der aber im schlechtesten Fall nicht einmal terminiert.
   - Für viele Primzahlmoduln ist die Lösung trivial.
   - Der Nachweis der Primitivität ist effizient, wenn die Primfaktoren der Ordnung der multiplikativen Gruppe bekannt sind; sonst ist die Komplexität unbekannt.
   - Der Fall eines zusammengesetzten Moduls ist auf den seiner Primfaktoren reduzierbar, falls diese bekannt sind.
2. Erkennen von Quadratresten.
   - Für Primzahlmoduln gibt es einen effizienten Algorithmus.
   - Der Fall eines zusammengesetzten Moduls ist auf den seiner Primfaktoren reduzierbar, falls diese bekannt sind.
   - Für zusammengesetzte Moduln ist die Komplexität unbekannt, wenn die Primfaktoren nicht bekannt sind; vermutlich ist das Problem hart (so hart wie die Primzerlegung).
3. Finden eines quadratischen Nichtrests.
   - Die Komplexität ist im allgemeinen Fall unbekannt.
   - Die vollständige Suche ist aber effizient, falls die erweiterte RIEMANNsche Vermutung richtig ist.
   - Es gibt einen sehr effizienten probabilistischen Algorithmus, der aber im schlechtesten Fall nicht einmal terminiert.
   - Für die meisten Primzahlen ist die Lösung trivial.
   - Der Fall eines zusammengesetzten Moduls ist auf den seiner Primfaktoren reduzierbar, falls diese bekannt sind.

Ein ähnliches Problem, das Ziehen von Quadratwurzeln in Restklassenringen, wird in Abschnitt 5 behandelt.

A.1 Primitive Elemente für Zweierpotenzen

Die Fälle $n = 2$ oder 4 sind trivial: $\mathbb{M}_2$ ist die einelementige Gruppe, $\mathbb{M}_4$ zyklisch von der Ordnung 2. Sei also bis auf weiteres $n = 2^e$ mit $e \geq 3$. Da $\mathbb{M}_n$ dann gerade aus den Restklassen der ungeraden Zahlen besteht, ist $\varphi(n) = 2^{e-1}$. Wir benötigen zwei Hilfssätze.

Hilfssatz 1 *Sei $n = 2^e$ mit $e \geq 2$.*

(i) *Ist a ungerade, so*

$$a^{2^s} \equiv 1 \pmod{2^{s+2}} \quad \textit{für alle } s \geq 1.$$

(ii) *Ist $a \equiv 3 \pmod 4$, so $n \mid 1 + a + \cdots + a^{n/2-1}$.*

Beweis. (i) Ist $a = 4q + 1$, so $a^2 = 16q^2 + 8q + 1$; ist $a = 4q + 3$, so $a^2 = 16q^2 + 24q + 9 \equiv 1 \pmod 8$. Damit ist die Behauptung für $s = 1$ bewiesen. Der allgemeine Fall folgt durch Induktion:

$$a^{2^{s-1}} = 1 + t2^{s+1} \Longrightarrow a^{2^s} = (a^{2^{s-1}})^2 = 1 + 2t2^{s+1} + t^2 2^{2s+2}.$$

(ii) Es ist $2n = 2^{e+1} \mid a^{n/2} - 1$ nach (i). Da in $a - 1$ nur die erste Potenz von 2 aufgeht, folgt

$$n = 2^e \mid \frac{a^{n/2} - 1}{a - 1},$$

wie behauptet. $\diamond$

Hilfssatz 2 *Sei p eine Primzahl und e eine natürliche Zahl mit $p^e \geq 3$. Sei p^e die größte p-Potenz, die in $x - 1$ aufgeht. Dann ist p^{e+1} die größte p-Potenz, die in $x^p - 1$ aufgeht.*

Beweis. Es ist $x = 1 + tp^e$ mit einer ganzen Zahl t, die kein Vielfaches von p ist. Nach der Binomialformel ist

$$x^p = 1 + \sum_{k=1}^{p} \binom{p}{k} t^k p^{ke}.$$

Da p alle Binomialkoeffizienten $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ für $k = 1, \ldots, p-1$ teilt, kann man aus der Summe sogar p^{e+1} ausklammern:

$$x^p = 1 + tp^{e+1}s$$

mit einer ganzen Zahl s. Also geht p^{e+1} in $x^p - 1$ auf. Zu zeigen ist noch, dass s kein Vielfaches von p ist. Dazu sieht man sich s genauer an:

$$\begin{aligned} s &= \sum_{k=1}^{p} \frac{1}{p}\binom{p}{k} \cdot t^{k-1} p^{e(k-1)} \\ &= 1 + \frac{1}{p}\binom{p}{2} \cdot tp^e + \cdots + \frac{1}{p} \cdot t^{p-1} p^{e(p-1)}. \end{aligned}$$

Da $p^e \geq 3$, ist $e(p-1) \geq 2$, also $s \equiv 1 \pmod{p}$. $\diamond$

Aus Hilfssatz 1 folgt insbesondere

$$a^{2^{e-2}} \equiv 1 \pmod{n} \quad \text{für alle ungeraden } a.$$

Daher ist der Exponent $\lambda(n) \leq 2^{e-2}$ und $\mathbb{M}_n$ schon mal nicht zyklisch. Genauer gilt:

Satz 1 *Sei $n = 2^e$ mit $e \geq 3$. Dann gilt:*

(i) *In $G = \mathbb{M}_n$ hat -1 die Ordnung 2 und 5 die Ordnung 2^{e-2}, und G ist das direkte Produkt der von -1 und 5 erzeugten zyklischen Gruppen.*

(ii) *Wenn $e \geq 4$, sind die primitiven Elemente* mod n *genau die ganzen Zahlen $a \equiv 3, 5 \pmod{8}$. Insbesondere ist ihre Anzahl $n/4$.*

Beweis. (i) Da $\operatorname{Ord} 5 \mid 2^e$ und $\operatorname{Ord} 5 \leq 2^e - 2$, ist $\operatorname{Ord} 5$ eine Zweierpotenz $\leq 2^{e-2}$. Da 2^2 die größte Zweierpotenz in $5-1$ ist, ist 2^3 die größte Zweierpotenz in $5^2 - 1$ (nach Hilfssatz 2) und sukzessive 2^{e-1} die größte Zweierpotenz in $5^{2^{e-3}} - 1$. Also ist die 2^{e-2}-te Potenz von 5 die kleinste, die $\equiv 1 \pmod{2^e}$ ist. Das Produkt der beiden Untergruppen ist direkt, weil -1 keine Potenz von 5 ist – wäre $5^k \equiv -1 \pmod{n}$, so wegen $e \geq 2$ auch $5^k \equiv -1 \pmod{4}$, Widerspruch zu $5 \equiv 1 \pmod{4}$. Das direkte Produkt ist ganz G, weil es die Ordnung $2 \cdot 2^{e-2}$ hat.

(ii) Jedes Element $a \in G$ lässt sich nach (i) eindeutig in der Form $a = (-1)^r 5^s$ schreiben mit $r = 0$ oder 1 und $0 \leq s < 2^{e-2}$. Damit ist a^k genau dann 1 in $\mathbb{Z}/n\mathbb{Z}$, wenn kr gerade und ks ein Vielfaches von 2^{e-2} ist, also wenn ks ein Vielfaches von 2^{e-2} ist. Also ist a genau dann primitiv, wenn s ungerade ist, und das bedeutet $a \equiv \pm 5 \pmod{8}$. $\diamond$

Insbesondere ist $\lambda(2^e) = 2^{e-2}$ für $e \geq 4$ und $\lambda(8) = 2$.

A.2 Primitive Elemente für Primzahlmoduln

Schwieriger (und mathematisch interessanter) ist die Suche nach den primitiven Elementen für einen Primzahlmodul. Man kann sich dabei auf die Suche nach *einem* solchen Element beschränken; alle übrigen erhält man durch Potenzieren mit einem Exponenten, der zu $p-1$ teilerfremd ist, insbesondere gibt es genau $\varphi(p-1)$ Stück davon. Im üblichen Sprachgebrauch nennt man die primitiven Elemente zu einem Modul n im Falle, dass $\mathbb{M}_n$ zyklisch ist, auch **Primitivwurzeln** $\bmod n$. Das Problem, eine Primitivwurzel $\bmod p$ zu finden, hat schon GAUSS beschäftigt.

Die einfachste, aber noch nicht bestmögliche Methode heißt: Probiere $x = 2, 3, 4, \ldots$; teste, ob $x^d \neq 1$ für jeden echten Teiler d von $p-1$. Die Anzahl der dazu nötigen Tests wird verringert durch:

Hilfssatz 3 *Sei p eine Primzahl ≥ 5. Eine ganze Zahl x ist genau dann Primitivwurzel* $\bmod p$*, wenn für jeden Primfaktor q von $p-1$ gilt $x^{(p-1)/q} \neq 1$ in $\mathbb{F}_p$.*

Beweis. Die Ordnung von x ist ein Teiler von $p-1$, und jeder echte Teiler von $p-1$ teilt einen solchen Quotienten $\frac{p-1}{q}$. $\diamond$

Um dieses Kriterium anwenden zu können, braucht man also die Primzerlegung von $p-1$. Hat man diese, ist das kriterium effizient: Es gibt höchstens ${}^2\log(p-1)$ Primfaktoren, und für jeden wird die fragliche Potenz durch binäres Potenzieren berechnet.

Beispiel. Für $p = 41$ ist $p - 1 = 40 = 2^3 \cdot 5$, also x genau dann Primitivwurzel, wenn $x^{20} \neq 1$ und $x^8 \neq 1$. In $\mathbb{F}_{41}$ laufen dann folgende Rechenschritte ab:

$$
\begin{array}{lllll}
x = 2: & x^2 = 4, & x^4 = 16, & \left\{ \begin{array}{l} x^8 = 10, \\ x^{20} = x^8 x^8 x^4 = 1. \end{array} \right. \\
x = 3: & x^2 = 9, & x^4 = 81, & x^4 = -1, \ x^8 = 1. \\
x = 4: & x = 2^2, & \text{also} & x^{20} = 1. \\
x = 5: & x^2 = 25, & x^4 = 10 & \left\{ \begin{array}{l} x^8 = 18, \\ x^{20} = x^8 x^8 x^4 = 1. \end{array} \right. \\
x = 6: & x^2 = 36, & x^4 = 25 & \left\{ \begin{array}{l} x^8 = 10, \\ x^{20} = x^8 x^8 x^4 = -1. \end{array} \right.
\end{array}
$$

Also ist 6 *Primitivwurzel für $p = 41$.*

Es stellt sich die Frage, wie lange man auf diese Weise nach einer Primitivwurzel suchen muss. Hier einige Aspekte. Sei

$$\alpha(p) := \min\{x \in \mathbb{N} \mid x \text{ ist Primitivwurzel für } p\}.$$

Dann kann man zeigen: Die Funktion α ist nicht beschränkt. Nach einem Ergebnis von Burgess 1962 ist (etwas vergröbert)

$$\alpha(p) = \mathrm{O}(\sqrt[6]{p}).$$

Falls die erweiterte Riemannsche Vermutung richtig sein sollte, kann man diese immer noch exponentielle Schranke zu einer polynomialen verbessern; das beste bekannte Ergebnis scheint von Shoup 1990 zu stammen und besagt etwas vergröbert:

$$\alpha(p) = \mathrm{O}(\log(p)^6(1 + \log\log(p))^4).$$

Es gibt einige weitere offene Probleme:

- Ist 2 für unendlich viele Primzahlen Primitivwurzel?
- Ist 10 für unendlich viele Primzahlen Primitivwurzel? Das wurde von Gauss vermutet.

Allgemeiner besagt eine *Vermutung von* Artin: Sei $a \in \mathbb{N}$, a kein Quadrat (also $a \neq 0, 1, 4, 9, \ldots$). Dann ist a für unendlich viele Primzahlen Primitivwurzel.

Relevante Literatur:

- D. R. Heath-Brown: Artin's conjecture for primitive roots. Quart. J. Math. Oxford 37 (1986), 27–38.
- M. Ram Murty: Artin's conjecture for primitive roots. Math. Intelligencer 10 (1988), 59–67.
- V. Shoup: Searching for primitive roots in finite fields. Proc. 22nd STOC 1990, 546–554.
- Murata: On the magnitude of the least prime primitive root. J. Number Theory 37 (1991), 47–66.

A.3 Primitive Elemente für Primpotenzen

Für die Primzahlpotenzen braucht man einen weiteren Hilfssatz.

Hilfssatz 4 *Sei p eine Primzahl ≥ 3, k eine ganze Zahl und $d \geq 0$. Dann gilt*

$$(1+kp)^{p^d} \equiv 1 + kp^{d+1} \pmod{p^{d+2}}.$$

Beweis. Für $d = 0$ ist die Aussage trivialerweise richtig. Weiter schließt man durch Induktion: Sei $d \geq 1$ und

$$(1+kp)^{p^{d-1}} = 1 + kp^d + rp^{d+1}.$$

Dann folgt

$$(1+kp)^{p^d} = (1+(k+rp)p^d)^p \equiv 1+p\cdot(k+rp)\cdot p^d \equiv 1+kp^{d+1} \pmod{p^{d+2}},$$

da $d+2 \leq 2d+1$ und $p \geq 3$. $\diamond$

Satz 2 *Sei p eine Primzahl ≥ 3, e ein Exponent ≥ 2 und a eine Primitivwurzel* mod p. *Dann gilt:*

(i) *Genau dann erzeugt a die Gruppe $\mathbb{M}_{p^e}$, wenn $a^{p-1} \bmod p^2 \neq 1$.*

(ii) *a oder $a+p$ erzeugt $\mathbb{M}_{p^e}$.*

(iii) *$\mathbb{M}_{p^e}$ ist zyklisch und $\lambda(p^e) = \varphi(p^e) = p^{e-1}(p-1)$.*

Beweis. (i) Sei t die multiplikative Ordnung von $a \bmod p^e$. Sie ist sicher ein Vielfaches der von $a \bmod p$, also von $p-1$. Andererseits teilt sie $\varphi(p^e) = p^{e-1}(p-1)$. Daher ist $t = p^d(p-1)$ mit $0 \leq d \leq e-1$. Ist nun k so gewählt, dass $a^{p-1} = 1 + kp$, so folgt nach Hilfssatz 4

$$(a^{p-1})^{p^{e-2}} \equiv 1 + kp^{e-1} \equiv 1 \pmod{p^e} \iff p|k \iff a^{p-1} \equiv 1 \pmod{p^2}.$$

Das ist genau dann nicht der Fall, wenn $d = e-1$.

(ii) Erzeugt a nicht $\mathbb{M}_{p^e}$, so ist $a^{p-1} \equiv 1 \pmod{p^2}$, also

$$(a+p)^{p-1} \equiv a^{p-1} + (p-1)a^{p-2}p \equiv 1 - a^{p-2} \pmod{p^2},$$

und dies ist sicher nicht $\equiv 1 \pmod{p^2}$.

(iii) folgt direkt aus (ii). $\diamond$

Daraus lässt sich unmittelbar eine analoge Aussage für das Zweifache einer Primzahlpotenz geweinnen:

Korollar 1 *Sei $q = p^e$ eine Potenz der Primzahl $p \geq 3$. Dann gilt:*

(i) *Die multiplikative Gruppe* $\mathbb{M}_{2q}$ *ist natürlich isomorph zu* $\mathbb{M}_q$*, also zyklisch.*

(ii) *Ist* a *Primitivwurzel* $\bmod q$*, so ist* a *Primitivwurzel* $\bmod 2q$*, falls* a *ungerade, und* $a+q$ *Primitivwurzel* $\bmod 2q$*, falls* a *gerade.*

(iii) $\lambda(2p^e) = p^{e-1}(p-1)$.

Beweis. (i) Da q und 2 teilerfremd sind und $\mathbb{M}_2$ die triviale Gruppe ist, ist nach dem chinesischen Restsatz $\mathbb{M}_{2q} \cong \mathbb{M}_2 \times \mathbb{M}_q \cong \mathbb{M}_q$. Die Abbildung ist explizit durch $a \bmod 2q \mapsto a \bmod q$ gegeben.

(ii) Die Umkehrabbildung dieses natürlichen Isomorphismus ist

$$a \mapsto \begin{cases} a, & \text{falls } a \text{ ungerade,} \\ a+q, & \text{falls } a \text{ gerade.} \end{cases}$$

(iii) klar. $\diamond$

A.4 Die Struktur der multiplikativen Gruppe

Damit können wir genau sagen, wann die multiplikative Gruppe $\mathbb{M}_n$ zyklisch ist (d. h., wann eine Primitivwurzel mod n existiert):

Korollar 2 (GAUSS 1799) *Die multiplikative Gruppe $\mathbb{M}_n$ ist für $n \geq 2$ genau dann zyklisch, wenn n eine der Zahlen $2, 4, p^e$ oder $2p^e$ mit einer ungeraden Primzahl p ist.*

Beweis. Das folgt aus Satz 2, Korollar 1 und dem folgenden Hilfssatz 5. $\diamond$

Hilfssatz 5 *Sind $m, n \geq 3$ teilerfremd, so ist $\mathbb{M}_{mn}$ nicht zyklisch und $\lambda(mn) < \varphi(mn)$.*

Beweis. Ist $n \geq 3$, so $\varphi(n)$ gerade; für eine Primzahlpotenz folgt das aus der expliziten Form und allgemein aus der Multiplikativität der φ-Funktion. Damit folgt

$$\mathrm{kgV}(\varphi(m), \varphi(n)) < \varphi(m)\varphi(n) = \varphi(mn),$$

$$\lambda(mn) = \mathrm{kgV}(\lambda(m), \lambda(n)) \leq \mathrm{kgV}(\varphi(m), \varphi(n)) < \varphi(mn).$$

Also ist $\mathbb{M}_{mn}$ nicht zyklisch. $\diamond$

Damit ist die Struktur der multiplikativen Gruppe auch im allgemeinen Fall bekannt; mit $\mathcal{Z}_d$ wird dabei die zyklische Gruppe der Ordnung d bezeichnet.

Satz 3 *Sei $n = 2^e p_1^{e_1} \cdots p_r^{e_r}$ die Primzerlegung der natürlichen Zahl $n \geq 2$ mit $e \geq 0$, $r \geq 0$, $e_1, \ldots e_r \geq 1$ und verschiedenen ungeraden Primzahlen $p_1, \ldots, p_r$. Sei $q_i = p_i^{e_i}$ und $q_i' = p_i^{e_i - 1}(p_i - 1)$ für $i = 1, \ldots, r$. Dann ist*

$$\mathbb{M}_n \cong \begin{cases} \mathcal{Z}_{q_1'} \times \cdots \times \mathcal{Z}_{q_r'}, & \text{falls } e = 0 \text{ oder } 1, \\ \mathcal{Z}_2 \times \mathcal{Z}_{2^{e-2}} \times \mathcal{Z}_{q_1'} \times \cdots \times \mathcal{Z}_{q_r'}, & \text{falls } e \geq 2. \end{cases}$$

Ein primitives Element $a \bmod n$ findet man, indem man primitive Elemente $a_0 \bmod 2^e$ (falls $e \geq 2$) und $a_i \bmod q_i$ wählt und die simultanen Kongruenzen $a \equiv a_i \pmod{q_i}$, gegebenenfalls $a \equiv a_0 \pmod{2^e}$, löst.

Beweis. All dies folgt jetzt aus dem chinesischen Restsatz. $\diamond$

Übungsaufgabe. Leite daraus eine allgemeine Formel für $\lambda(n)$ her.

A.5 Das JACOBI-Symbol

Auf der multiplikativen Gruppe $\mathbb{M}_n = (\mathbb{Z}/n\mathbb{Z})^\times$ für einen Modul $n \geq 2$ ist die Quadrat-Abbildung

$$\mathbf{q} : \mathbb{M}_n \longrightarrow \mathbb{M}_n, \quad x \mapsto x^2 \bmod n,$$

ein Gruppen-Homomorphismus. Die Elemente im Bild von $\mathbf{q}$ heißen die **Quadratreste** mod n. Eine ganze Zahl x ist also Quadratrest mod n, wenn sie mod n invertierbar ist und es eine ganze Zahl u mit $u^2 \equiv x \pmod{n}$ gibt. Die Menge der Quadratreste – als Teilmenge des Restklassenrings $\mathbb{Z}/n\mathbb{Z}$ aufgefasst – ist also $\mathbb{M}_n^2$. (Das ist allerdings keine Standard-Bezeichnung, so wenig wie $\mathbb{M}_n$. Aber jedesmal $((\mathbb{Z}/n\mathbb{Z})^\times)^2$ zu schreiben ist nicht sehr angenehm.)

Bemerkungen und Beispiele

1. Im Fall $n = 2$ ist $\mathbb{M}_n^2 = \mathbb{M}_n = \{1\}$.

2. Für $n \geq 3$ ist $-1 \neq 1$ und $(-1)^2 = 1$, also $\mathbf{q}$ sicher nicht injektiv und daher auch nicht surjektiv; es gibt also Zahlen, die nicht Quadratrest sind.

3. Sei $n = p \geq 3$ eine Primzahl. Dann besteht der Kern von $\mathbf{q}$ genau aus den Nullstellen des Polynoms $X^2 - 1$ im Körper $\mathbb{F}_p$, also aus $\{\pm 1\}$. Daher gibt es genau $\frac{p-1}{2}$ Quadratreste.

4. Allgemeiner sei $n = q = p^e$ Potenz einer ungeraden Primzahl p. Dann ist $\mathbb{M}_n$ zyklisch von der Ordnung $\varphi(q) = q \cdot (1 - \frac{1}{p})$ nach Satz 2. Also hat 1 in $\mathbb{M}_q$ genau die Quadratwurzeln ± 1, und es gibt $\varphi(q)/2$ Quadratreste.

5. Sei n das Produkt zweier verschiedener ungerader Primzahlen p und q. Der chinesische Restsatz sagt dann, dass die natürliche Abbildung $\mathbb{M}_n \longrightarrow \mathbb{M}_p \times \mathbb{M}_q$ ein Isomorphismus ist. Also gibt es in $\mathbb{M}_n$ genau 4 Quadratwurzeln aus 1, und $\mathbb{M}_n^2$ hat den Index 4 in $\mathbb{M}_n$.

6. Ganz allgemein sei $n = 2^e p_1^{e_1} \cdots p_r^{e_r}$ die Primzerlegung mit $e \geq 0$, verschiedenen ungeraden Primzahlen $p_1, \ldots, p_r$ und $e_1, \ldots, e_r \geq 1$. Aus Satz 3 kann man ablesen, dass folgendes die Anzahl der Quadratwurzeln aus 1 in $\mathbb{M}_n$ ist:

$$\begin{array}{ll} 2^r, & \text{falls } e = 0 \text{ oder } 1, \\ 2^{r+1}, & \text{falls } e = 2, \\ 2^{r+2}, & \text{falls } e \geq 3. \end{array}$$

Der naive Algorithmus zur Bestimmung der Quadratrest-Eigenschaft von $a \bmod n$ probiert der Reihe nach $1^2, 2^2, 3^2, \ldots$, bis a gefunden ist. Dazu sind für einen Nicht-Quadratrest stets $\lfloor \frac{n}{2} \rfloor$, für einen Quadratrest im Durchschnitt $n/4$ Schritte nötig. Der Aufwand wächst also exponentiell mit der Stellenzahl $\log n$. Für den Fall, dass n eine *Primzahl* ist, werden bessere Algorithmen hergeleitet. Das Phänomen, dass es für eine *zusammengesetzte* Zahl n keinen effizienten Algorithmus gibt, wird Grundlage für kryptographische Konstruktionen, z. B. des einfachsten perfekten Zufallsgenerators, sein.

Im Falle eines Primzahlmoduls p dient das LEGENDRE**-Symbol** als Anzeiger der Quadratrest-Eigenschaft:

$$(\frac{x}{p}) = \begin{cases} 1, & \text{wenn } x \text{ Quadratrest,} \\ 0, & \text{wenn } p|x, \\ -1 & \text{sonst.} \end{cases}$$

Das LEGENDRE-Symbol definiert also insbesondere einen Homomorphismus

$$(\frac{\bullet}{p}) : \mathbb{M}_p \longrightarrow \mathbb{M}_p/\mathbb{M}_p^2 \cong \{\pm 1\}.$$

Im Spezialfall $p = 2$ ist

$$(\frac{x}{2}) = \begin{cases} 1, & \text{wenn } x \text{ ungerade,} \\ 0, & \text{wenn } x \text{ gerade.} \end{cases}$$

Satz 4 (EULER-Kriterium) *Sei p eine ungerade Primzahl. Dann ist*

$$x^{\frac{p-1}{2}} \equiv (\frac{x}{p}) \pmod{p} \quad \textit{für alle } x.$$

Beweis. Falls $p|x$, sind beide Seiten 0. Andernfalls ist $(x^{\frac{p-1}{2}})^2 = x^{p-1} \equiv 1$, also $x^{\frac{p-1}{2}} \equiv \pm 1$. Sei nun a ein primitives Element $\bmod p$. Dann ist die Behauptung für $x = a$ richtig – beide Seiten sind -1. Da ferner beide Seiten der Behauptung Homomorphismen $\mathbb{F}_p^\times \longrightarrow \{\pm 1\}$ definieren, folgt die Behauptung auch für alle x, die nicht Vielfache von p sind. $\diamond$

Das EULER-Kriterium ergibt schon einen effizienten Algorithmus zur Entscheidung der Quadratrest-Eigenschaft für einen Primzahlmodul: Man hat in $\mathbb{F}_p^\times$ mit $\frac{p-1}{2}$ zu potenzieren. Bekanntlich kann man das mit höchstens $2\lfloor {}^2\log(\frac{p-1}{2}) \rfloor$ Multiplikationen $\bmod p$. Berücksichtigt man den Aufwand für die modularen Multiplikationen, kommt man in die Größenordnung ${}^2\log(p)^3$.

Nach dem EULER-Kriterium ist -1 genau dann ein Quadratrest, wenn $\frac{p-1}{2}$ gerade, also $p \equiv 1 \pmod 4$ ist. Aber schon die Entscheidung, ob 2 oder 3 Quadratrest ist, fällt immer noch schwer. Der Algorithmus lässt sich aber noch verbessern, und das wird im folgenden Abschnitt A.6 beschrieben.

Das LEGENDRE-Symbol wird durch das genauso geschriebene JACOBI-Symbol verallgemeinert: Ist $n > 0$ und $n = p_1 \cdots p_r$ die Primzerlegung, so

$$(\frac{x}{n}) := (\frac{x}{p_1}) \cdots (\frac{x}{p_r}) \quad \text{für } x \in \mathbb{M}_n,$$

insbesondere $(\frac{x}{n}) = 0$, wenn x und n nicht teilerfremd sind. Ergänzt wird das durch $(\frac{x}{1}) = 1$, $(\frac{x}{n}) = (\frac{x}{-n})$, wenn $n < 0$, und $(\frac{x}{0}) = 0$. Dann ist das JACOBI-Symbol eine Funktion

$$(\frac{\bullet}{\bullet}) : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$$

mit Werten in $\{0, \pm 1\}$, und zwar in Zähler und Nenner multiplikativ. Insbesondere definiert das JACOBI-Symbol ebenfalls noch einen Homomorphismus $(\frac{\bullet}{n})$ von $\mathbb{M}_n$ nach $\{\pm 1\}$, ist aber *kein* Anzeiger für die Quadratrest-Eigenschaft mehr. Ist also $\mathbb{M}_n^+ = Kern(\frac{\bullet}{n})$ und $\mathbb{M}_n^- = \mathbb{M}_n - \mathbb{M}_n^+$, so ist $\mathbb{M}_n^2$ im allgemeinen echte Untergruppe von $\mathbb{M}_n^+$. Ihren Index kann man aus dem obigen Beispiel 6 bestimmen: Gibt es 2^k Quadratwurzeln aus 1 und ist dabei $k \geq 1$, so hat $\mathbb{M}_n^2$ in $\mathbb{M}_n^+$ den Index 2^{k-1}. Stets hängt $(\frac{x}{n})$ nur von der Restklasse x mod n ab. Klar ist

$$(\frac{x}{2^k}) = \begin{cases} 1, & \text{wenn } x \text{ ungerade,} \\ 0, & \text{wenn } x \text{ gerade.} \end{cases}$$

A.6 Das quadratische Reziprozitätsgesetz

Die Grundlage zur Berechnung des LEGENDRE- (und JACOBI-) -Symbols sind die folgenden beiden Sätze; zunächst aber ein Hilfssatz, mit dem sich zusammengesetzte Moduln auf Primzahlen reduzieren lassen.

Hilfssatz 6 *Seien $s, t \in \mathbb{Z}$ ungerade. Dann gilt*

(i) $\frac{s-1}{2} + \frac{t-1}{2} \equiv \frac{st-1}{2} \pmod 2$,

(ii) $\frac{s^2-1}{8} + \frac{t^2-1}{8} \equiv \frac{s^2t^2-1}{8} \pmod 2$.

Beweis. Ist $s = 2k+1$ und $t = 2l+1$, so $st = 4kl + 2k + 2l + 1$,

$$\frac{st-1}{2} = 2kl + k + l.$$

Ferner $s^2 = 4{\cdot}(k^2{+}k){+}1$, $t^2 = 4{\cdot}(l^2{+}l){+}1$, $s^2t^2 = 16{\cdot}\ldots{+}4{\cdot}(k^2{+}k{+}l^2{+}l){+}1$,

$$\frac{s^2t^2-1}{8} = 2 \cdot \ldots + \frac{k^2+k+l^2+l}{2},$$

und daraus folgt direkt die Behauptung. $\diamond$

Satz 5 *Sei n ungerade. Dann gilt:*

(i) $(\frac{-1}{n}) = (-1)^{\frac{n-1}{2}}$,

(ii) $(\frac{2}{n}) = (-1)^{\frac{n^2-1}{8}}$

Beweis. Wendet man den Hilfssatz auf die Primzerlegung von n an, so darf man o. B. d. A. für beide Behauptungen $n = p$ prim annehmen.

(i) folgt direkt aus dem EULER-Kriterium, Satz 4.

(ii) Es ist

$$(-1)^k \cdot k \equiv \begin{cases} k, & \text{falls } k \text{ gerade,} \\ p-k, & \text{falls } k \text{ ungerade,} \end{cases}$$

$$\prod_{k=1}^{\frac{p-1}{2}} (-1)^k \cdot k \equiv 2 \cdot 4 \cdots p-1 = 2^{\frac{p-1}{2}} \cdot (\frac{p-1}{2})!.$$

Andererseits ist

$$\prod_{k=1}^{\frac{p-1}{2}} (-1)^k \cdot k = (\frac{p-1}{2})! \cdot (-1)^{\frac{p^2-1}{8}}, \quad \text{da} \quad \sum_{k=1}^{\frac{p-1}{2}} k = \frac{(p-1)(p+1)}{2 \cdot 2 \cdot 2}.$$

Da $(\frac{p-1}{2})!$ Produkt von Zahlen $< p$ ist, ist es kein Vielfaches von p, darf also wegdividiert werden. Durch Gleichsetzen und mit dem EULER-Kriterium folgt also

$$(-1)^{\frac{p^2-1}{8}} \equiv 2^{\frac{p-1}{2}} \equiv (\frac{2}{p}) \pmod{p}.$$

Da $p \geq 3$, folgt aus der Kongruenz die Gleichheit. $\diamond$

Insbesondere ist 2 genau dann Quadratrest modulo der Primzahl p, wenn $(p^2-1)/8$ gerade, also $p^2 \equiv 1 \pmod{16}$, also $p \equiv 1$ oder $7 \pmod 8$.

Hauptsatz 1 (Quadratisches Reziprozitätsgesetz) *Für je zwei verschiedene ungerade und zueinander teilerfremde natürliche Zahlen m und n gilt*

$$(\frac{m}{n})(\frac{n}{m}) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}.$$

Eine etwas leichter verständliche Form des quadratischen Reziprozitätsgesetzes ist:

$$(\frac{m}{n}) = \begin{cases} -(\frac{n}{m}) & \text{wenn } m \equiv n \equiv 3 \pmod 4, \\ (\frac{n}{m}) & \text{sonst.} \end{cases}$$

Der Beweis folgt. Zunächst wird die Berechnung an einem Beispiel gezeigt: Ist 7 Quadratrest mod 107? Dies wird durch folgende Rechnung verneint:

$$(\frac{7}{107}) = -(\frac{107}{7}) = -(\frac{2}{7}) = -1.$$

Genauso ist 7 kein Quadratrest mod 11:

$$(\frac{7}{11}) = -(\frac{11}{7}) = -(\frac{4}{7}) = -(\frac{2}{7})(\frac{2}{7}) = -1.$$

Also ist 7 auch nicht Quadratrest mod 1177, da $1177 = 11 \cdot 107$. Aber $(\frac{7}{1177}) = 1$.

Der aus dem quadratischen Reziprozitätsgesetz abgeleitete Algorithmus besteht dann aus der folgenden Prozedur:

Prozedur JacobiSymbol

Eingabeparameter

m, n = zwei ganze Zahlen.

Ausgabeparameter

jac $= (\frac{m}{n})$.

Anweisungen

Falls $n = 0$, gib jac $= 0$ aus. **Ende**

Falls $m = 0$, gib jac $= 0$ aus. **Ende**

Falls ggT$(m, n) > 1$, gib jac $= 0$ aus. **Ende**

[Jetzt sind $m, n \neq 0$ teilerfremd, also jac $= \pm 1$.]
jac $= 1$.
Falls $n < 0$, ersetze n durch $-n$.
Falls n gerade, dividiere n durch die größtmögliche Zweierpotenz 2^k.
Falls $m < 0$,
    ersetze m durch $-m$,
    falls $n \equiv 3 \pmod 4$, ersetze jac durch $-$jac.
[Ab jetzt sind m und n teilerfremd und n ist positiv und ungerade;]
[außer dass am Ende der Fall $m = 0$ und $n = 1$ eintreten kann.]
Falls $m > n$, ersetze m durch $m \bmod n$.
Solange $n > 1$:
    Falls m gerade:
        Dividiere m durch die größtmögliche Zweierpotenz 2^k.
        Falls (k ungerade und $n \equiv \pm 3 \pmod 8$) ersetze jac durch $-$jac.
    [Jetzt sind m und n ungerade und teilerfremd, $0 < m < n$.]
    [Das quadratische Reziprozitätsgesetz ist anwendbar.]
    Falls ($m \equiv 3 \pmod 4$ und $n \equiv 3 \pmod 4$)
        ersetze jac durch $-$jac.
    Setze $d = m$, $m = n \bmod m$, $n = d$.

Dieser Algorithmus lässt sich ähnlich wie der Euklidische Algorithmus analysieren: Man benötigt höchstens $5 \cdot \log(m)$ Schritte, wobei jeder Schritt im wesentlichen aus einer Ganzzahl-Division besteht. Da die Größe der Operanden dabei schnell abnimmt, kommt man insgesamt auf einen Aufwand von $O(\log(m)^2)$. Das ist deutlich schneller als die Anwendung des Euler-Kriteriums.

A.7 Beweis des quadratischen Reziprozitätsgesetzes

Nun zum Beweis des quadratischen Reziprozitätsgesetzes. Von den vielen bekannten Beweisen wird hier einer durchgeführt, der auf der Theorie der endlichen Körper nach Ideen von Zolotarev (Nouvelles Annales de Mathematiques 11 (1872), 354–362) und Swan (Pacific J. Math. 12 (1962), 1099–1106) beruht.

Hilfssatz 7 *Sei p eine ungerade Primzahl und a zu p teilerfremd. Dann sind äquivalent:*

(i) *a ist Quadratrest* mod p.
(ii) *Die Multiplikation mit a ist eine gerade Permutation von $\mathbb{F}_p$.*

Beweis. Die Multiplikation sei mit $\mu_a : \mathbb{F}_p \longrightarrow \mathbb{F}_p$, $x \mapsto ax \bmod p$, bezeichnet. Dann ist $a \mapsto \mu_a$ ein injektiver Gruppenhomomorphismus $\mu : \mathbb{F}_p^\times \longrightarrow \mathfrak{S}_p$ in die volle Permutationsgruppe. Ist a primitiv, so hat μ_a genau zwei Zykel: $\{0\}$ und $\mathbb{F}_p^\times$. Da p ungerade ist, hat μ_a das Vorzeichen $\sigma(\mu_a) = (-1)^{p-2} = -1$, ist also ungerade. Da a die Gruppe $\mathbb{F}_p^\times$ erzeugt, folgt die Gleichheit der Homomorphismen

$$(\frac{\bullet}{p}) = \sigma \circ \mu : \mathbb{F}_p^\times \longrightarrow \{\pm 1\},$$

und daraus die Behauptung. $\diamond$

Ein weiteres Hilfsmittel ist die **Diskriminante** eines Polynoms $f = a_n T^n + \cdots + a_0 \in K[T]$. Sie kann in jedem Erweiterungskörper $L \supseteq K$ gebildet werden, der alle Nullstellen $t_1, \ldots, t_n$ von f enthält, und ist dann

$$D(f) = a_n^{2n-2} \cdot \prod_{1 \le i < j \le n} (t_i - t_j)^2.$$

(Da sie unter allen Permutationen der Nullstellen invariant ist, liegt sie sogar in K, aber das folgt in dem hier interessanten Fall auch aus der expliziten Berechnung.) Die normale Methode zu ihrer Berechnung aus den Koeffizienten besteht im Vergleich mit der Resultanten von f und der Ableitung f'. Für das Kreisteilungspolynom $f = T^n - 1$ ist die Berechnung aber ganz einfach:

Hilfssatz 8 *Das Polynom $f = T^n - 1 \in K[T]$ (mit* char $K \nmid n$*) hat die Diskriminante*

$$D(f) = (-1)^{\frac{n(n-1)}{2}} \cdot n^n.$$

Beweis. Sei ζ eine primitive n-te Einheitswurzel (in einem geeigneten Erweiterungskörper). Dann ist

$$\begin{aligned} f &= \prod_{i=0}^{n-1}(T-\zeta^i), \\ D(f) &= \prod_{0\le i<j\le n-1}(\zeta^i-\zeta^j)^2 = (-1)^{\frac{n(n-1)}{2}}\cdot\prod_{i\neq j}(\zeta^i-\zeta^j) \\ &= (-1)^{\frac{n(n-1)}{2}}\cdot\prod_{i=0}^{n-1}\left[\zeta^i\cdot\prod_{k=1}^{n-1}(1-\zeta^k)\right]. \end{aligned}$$

Für das Polynom

$$g = T^{n-1}+\cdots+1 = \prod_{k=1}^{n-1}(T-\zeta^k) \in K[T]$$

ist $g(1) = n$. Also folgt

$$D(f) = (-1)^{\frac{n(n-1)}{2}}\cdot\prod_{i=0}^{n-1}[\zeta^i\cdot n] = (-1)^{\frac{n(n-1)}{2}}\cdot n^n,$$

wie behauptet. $\diamond$

Hilfssatz 9 *Sei p eine ungerade Primzahl und n ungerade und zu p teilerfremd. Dann sind äquivalent:*

(i) *Die Diskriminante von $T^n-1 \in \mathbb{F}_p[T]$ ist Quadratrest* mod p.
(ii) $l = (-1)^{(n-1)/2}\cdot n$ *ist Quadratrest* mod p.

Beweis. Die Diskriminante ist $D(f) = l^n$ nach Hilfssatz 8. Ist $n = 2k+1$, so ist $D(f)$ Produkt des Quadratrests l^{2k} mit l. $\diamond$

Die Diskriminante eines Polynoms $f \in K[T]$ ist in dem Erweiterungskörper $L \supseteq K$, der die Nullstellen von f enthält, ein Quadrat:

$$D(f) = \Delta(f)^2 \quad \text{mit} \quad \Delta(f) = a_n^{n-1}\cdot\prod_{i<j}(t_i-t_j).$$

Aber $\Delta(f)$ ändert sich bei einer Permutation der Nullstellen mit dem Vorzeichen der Permutation und liegt daher im allgemeinen nicht in K.

Beweis des Hauptsatzes. Wegen Hilfssatz 6(i) reicht es, das quadratische Reziprozitätsgesetz für zwei verschiedene ungerade Primzahlen p und q zu beweisen. Sei $K = \mathbb{F}_p$, ζ eine primitive q-te Einheitswurzel, $L = K(\zeta)$ und

$f = T^q - 1$. Dann definiert $\zeta \mapsto \zeta^p$ eine Permutation der Einheitswurzeln und einen Automorphismus von L über K. Es folgt:

$$\sigma(\mu_p) \cdot \Delta(f) = \prod_{i<j} (\zeta^{pi} - \zeta^{pj}) = \Delta(f)^p.$$

Damit kann man eine Kette von Äquivalenzen aufstellen:

$$(-1)^{\frac{q-1}{2}} \cdot q \,\text{Quadratrest mod } p \iff D(f) \,\text{Quadratrest mod } p \iff \Delta(f) \in \mathbb{F}_p$$

$$\iff \Delta(f) = \Delta(f)^p \iff \sigma(\mu_p) = 1 \iff p \text{ Quadratrest mod } q.$$

Also ist mit Satz 5 (i)

$$(\frac{p}{q}) = (\frac{(-1)^{\frac{q-1}{2}} q}{p}) = (\frac{q}{p}) \cdot (\frac{-1}{p})^{\frac{q-1}{2}} = (\frac{q}{p}) \cdot (-1)^{\frac{p-1}{2}\frac{q-1}{2}},$$

wie behauptet. $\diamondsuit$

A.8 BLUM-Zahlen

Sei nun $n = pq$ mit verschiedenen Primzahlen $p, q \geq 3$. Dann ist

$$\mathbb{M}_n/\mathbb{M}_n^2 \cong \mathbb{M}_p/\mathbb{M}_p^2 \times \mathbb{M}_q/\mathbb{M}_q^2 \cong \mathcal{Z}_2 \times \mathcal{Z}_2,$$

insbesondere $\#(\mathbb{M}_n/\mathbb{M}_n^2) = 4$. Die Untergruppen $\mathbb{M}_n^2 \leq \mathbb{M}_n^+$ und $\mathbb{M}_n^+ \leq \mathbb{M}_n$ sind jeweils echt und daher vom Index 2. Im Ring $\mathbb{Z}/n\mathbb{Z}$ gibt es genau 4 Einheitswurzeln: $1, -1, \tau, -\tau$ mit

$$\tau \equiv -1 \pmod{p}, \quad \tau \equiv 1 \pmod{q},$$

also $(\frac{\tau}{n}) = -1$; anders ausgedrückt: Der Kern der Quadratabbildung $\mathbf{q} : \mathbb{M}_n \longrightarrow \mathbb{M}_n^2$ ist $K = \{\pm 1, \pm\tau\}$, isomorph zur KLEINschen Vierergruppe.

Eine Zahl der Form $n = pq$ mit verschiedenen Primzahlen $p, q \equiv 3 \pmod 4$ heißt BLUM-**Zahl** (z. B. die Zahl 1177 in A.6). Für eine solche ist also -1 kein Quadratrest in $\mathbb{M}_p$ und $\mathbb{M}_q$, also auch nicht in $\mathbb{M}_n$, aber

$$(\frac{-1}{n}) = (\frac{-1}{p})(\frac{-1}{q}) = (-1)^2 = 1,$$

also $-1 \in \mathbb{M}_n^+$. Es folgt

$$(\frac{-x}{n}) = (\frac{-1}{n})(\frac{x}{n}) = (\frac{x}{n})$$

für jedes x. Es ist $\mathbb{M}_n^2 \cap K = \{1\}$, also die Einschränkung von $\mathbf{q}$ auf $\mathbb{M}_n^2$ injektiv, also bijektiv, und $\mathbb{M}_n$ ist das direkte Produkt

$$\mathbb{M}_n = K \times \mathbb{M}_n^2, \quad \mathbb{M}_n^+ = \{\pm 1\} \times \mathbb{M}_n^2.$$

Jeder Quadratrest $a \in \mathbb{M}_n^2$ hat in jeder der vier Nebenklassen von $\mathbb{M}_n/\mathbb{M}_n^2$ genau eine Quadratwurzel; ist $x \in \mathbb{M}_n^2$ die eine, so sind $-x, \tau x, -\tau x$ die anderen. Damit ist gezeigt:

Satz 6 *Sei n eine* BLUM*-Zahl. Dann gilt:*

(i) *Ist $x^2 \equiv y^2 \pmod n$ für $x, y \in \mathbb{M}_n$ und sind $x, -x, y, -y \bmod n$ paarweise verschieden, so $(\frac{x}{n}) = -(\frac{y}{n})$.*

(ii) *Die Quadrat-Abbildung $\mathbf{q}$ ist eine Bijektion von $\mathbb{M}_n^2$ auf sich.*

(iii) *Jedes $a \in \mathbb{M}_n^2$ hat genau zwei Quadratwurzeln in $\mathbb{M}_n^+$; ist x die eine, so $-x \bmod n$ die andere, und genau eine von beiden ist selbst Quadratrest. Ferner hat a noch genau zwei weitere Quadratwurzeln, und diese liegen in $\mathbb{M}_n^-$.*

Von den vier Quadratwurzeln eines Quadratrests x ist also genau eine wieder ein Quadratrest. Diese wird als etwas besonderes betrachtet und mit $\sqrt{x} \bmod n$ bezeichnet. Das letzte Bit ("least significant bit") von x, das man auch als Parität von x oder als $x \bmod 2$ beschreiben kann, wird mit $\mathrm{lsb}(x)$ bezeichnet.

Korollar 1 *Sei $x \in \mathbb{M}_n^+$. Dann ist x genau dann Quadratrest, wenn*

$$\mathrm{lsb}(x) = \mathrm{lsb}(\sqrt{x^2} \bmod n).$$

Beweis. Ist x Quadratrest, so $x = \sqrt{x^2} \bmod n$. Ist x kein Quadratrest, so sei $y = \sqrt{x^2} \bmod n$. Nach (iii) muss $y = -x \bmod n = n - x$ sein. Da n ungerade ist, haben x und y verschiedene Parität. $\diamond$

Wie kann man die Quadratrest-Eigenschaft $\bmod n$ entscheiden? Wenn die Primzerlegung $n = pq$ bekannt ist, ist das effizient möglich:

$$x \in Q_n \Longleftrightarrow (\frac{x}{p}) = (\frac{x}{q}) = 1.$$

Es ist kein effizientes Verfahren bekannt, das ohne die Kenntnis der Primfaktoren auskommt; *möglicherweise* ist die Entscheidung der Quadratrest-Eigenschaft zur Primzerlegung komplexitätstheoretisch äquivalent. Allgemein für plausibel gehalten wird jedenfalls die

Quadratrest-Vermutung: Die Entscheidung der Quadratrest-Eigenschaft für BLUM-Zahlen ist hart.

A.9 Quadratische Nichtreste

Wie findet man einen quadratischen *Nichtrest* modulo einer Primzahl p? – Also eine Zahl a mit $p \not| a$, die kein Quadratrest $\bmod a$ ist. Bevorzugt als Lösung wird dabei (natürlich) eine möglichst kleine natürliche Zahl; trotzdem beginnen wir mit der -1:

Satz 7 *Sei $p \geq 3$ eine Primzahl.*

(i) -1 *ist quadratischer Nichtrest* $\bmod p \iff p \equiv 3 \pmod 4$.

(ii) 2 *ist quadratischer Nichtrest* $\bmod p \iff p \equiv 3$ *oder* $5 \pmod 8$.

(iii) (*Für $p \geq 5$*) 3 *ist quadratischer Nichtrest* $\bmod p \iff p \equiv 5$ *oder* $7 \pmod{12}$.

(iv) (*Für $p \geq 7$*) 5 *ist quadratischer Nichtrest* $\bmod p \iff p \equiv 2$ *oder* $3 \pmod 5$.

Beweis. (i) Das kann man aus Satz 5 folgern. Ein noch einfacherer Beweis geht so:

$$\begin{aligned} -1 \in \mathbb{M}_p^2 &\iff \bigvee_{i\in\mathbb{Z}} i^2 \equiv -1 \pmod p \iff \bigvee_{i\in\mathbb{Z}} \operatorname{Ord}_p i = 4 \\ &\iff 4 \mid \#\mathbb{F}_p^\times = p-1 \iff p \equiv 1 \pmod 4. \end{aligned}$$

(ii) Auch dies folgt aus Satz 5: Nach der dort anschließenden Bemerkung ist $2 \in \mathbb{M}_p^2 \iff p \equiv 1$ oder $7 \pmod 8$.

(iii) Hierzu wird das quadratische Reziprozitätsgesetz verwendet:

$$\begin{aligned} (\frac{3}{p}) = (-1)^{\frac{p-1}{2}}(\frac{p}{3}) &= \begin{cases} (-1)^{6k}(\frac{1}{3}) = 1, & \text{wenn } p = 12k+1, \\ (-1)^{6k+2}(\frac{2}{3}) = -1, & \text{wenn } p = 12k+5, \\ (-1)^{6k+3}(\frac{1}{3}) = -1, & \text{wenn } p = 12k+7, \\ (-1)^{6k+5}(\frac{2}{3}) = 1, & \text{wenn } p = 12k+11, \end{cases} \\ &= \begin{cases} 1, & \text{wenn } p \equiv 1 \text{ oder } 11 \pmod{12}, \\ -1, & \text{wenn } p \equiv 5 \text{ oder } 7 \pmod{12}. \end{cases} \end{aligned}$$

(iv) Hier ist nach dem quadratischen Reziprozitätsgesetz

$$(\frac{5}{p}) = (\frac{p}{5}) = \begin{cases} 1, & \text{wenn } p \equiv 1 \text{ oder } 4 \pmod 5, \\ -1, & \text{wenn } p \equiv 2 \text{ oder } 3 \pmod 5, \end{cases}$$

wie behauptet. $\diamond$

Korollar 1 241 *ist die einzige ungerade Primzahl* < 400*, für die weder* -1*,* 2*,* 3 *noch* 5 *quadratische Nichtreste sind.*

Korollar 2 *Nur für ungerade Primzahlen* $\equiv 1, 49 \pmod{120}$ *ist weder* -1*,* 2*,* 3 *noch* 5 *quadratischer Nichtrest.*

Die Aussage des Satzes lässt sich auf beliebige, nicht notwendig prime, Moduln übertragen. Dazu:

Hilfssatz 10 *Sei* $n \in \mathbb{N}$*,* $n \geq 2$*. Für* $a \in \mathbb{Z}$ *sei* $(\frac{a}{n}) = -1$*. Dann ist* a *kein Quadrat in* $\mathbb{Z}/n\mathbb{Z}$*.*

Beweis. Sei $n = p_1^{e_1} \cdots p_r^{e_r}$ die Primzerlegung. Dann ist

$$(\frac{a}{n}) = (\frac{a}{p_1})^{e_1} \cdots (\frac{a}{p_r})^{e_r}.$$

Also gibt es ein k, für das der Exponent e_k ungerade und $(\frac{a}{p_k}) = -1$ ist. Also ist a kein Quadrat $\bmod p_k$. Da $\mathbb{F}_{p_k}$ homomorphes Bild von $\mathbb{Z}/n\mathbb{Z}$ ist, ist a erst recht kein Quadrat $\bmod n$. $\diamond$

Korollar 3 *Sei* $n \in \mathbb{N}$*,* $n \geq 2$*, und* n *kein Quadrat. Dann gilt:*

(i) *Ist* $n \equiv 3 \pmod 4$*, so ist* -1 *kein Quadrat in* $\mathbb{Z}/n\mathbb{Z}$*.*

(ii) *Ist* $n \equiv 5 \pmod 8$*, so ist* 2 *kein Quadrat in* $\mathbb{Z}/n\mathbb{Z}$*.*

Usw. Man kommt auf diesem Weg aber nie zu einer vollständigen Erfassung aller Fälle, siehe die Anmerkung unten. Einen Algorithmus zur Bestimmung eines quadratischen Nichtrests braucht man allerdings höchstens, wenn $n \equiv 1 \pmod 8$. Hier gibt es wieder zwei Versionen:

- Einen deterministischen Algorithmus, der $a = 2, 3, 5, \ldots$ durchprobiert. Dieser ist unter der Annahme der erweiterten RIEMANNschen Vermutung – angewendet auf den Charakter $\chi = (\frac{\bullet}{n})$ – polynomial in der Stellenzahl $\log(n)$.

- Einen probabilistischen Algorithmus, der zufällig gewählte a probiert und jeweils mit Wahrscheinlichkeit $\frac{1}{2}$ reüssiert, d. h. $(\frac{a}{n}) = -1$ liefert. Zur Berechnung des JACOBI-Symbols sind $O(log(n)^2)$ Schritte nötig. Im Mittel sind zwei Versuche nötig, bis ein Nichtquadratrest gefunden ist.

Übungsaufgabe. Für welche Primzahlmoduln ist 7, 11 oder 13 quadratischer Nichtrest? Welches ist der kleinste Primzahlmodul, für den dann immer noch kein quadratischer Nichtrest gefunden ist?

Anmerkung. Es gibt keine konstante untere Schranke, bis zu der man mit Sicherheit für alle Moduln n einen quadratischen Nichtrest findet. Ein Satz von CHOWLA/ FRIDLENDER/ SALIÉ besagt, dass es (mit einer Konstanten $c > 0$) unendlich viele Primzahlen gibt, so dass alle Zahlen a mit $1 \leq a \leq c \cdot \log(p)$ Quadratreste mod p sind. RINGROSE/ GRAHAM und – unter der erweiterten RIEMANNschen Vermutung – MONTGOMERY bewiesen noch etwas schärfere Versionen.

Relevante Literatur:

- V. R. FRIDLENDER: On the least n-th power non-residue. Dokl. Akad. Nauk. SSSR 66 (1949), 351–352.
- H. SALIÉ: Über den kleinsten positiven quadratischen Nichtrest nach einer Primzahl. Math. Nachr. 3 (1949), 7–8.
- N. C. ANKENEY: The least quadratic nonresidue. Ann. of Math. 55 (1952), 65–72.
- H. L. MONTGOMERY: *Topics in Multiplicative Number Theory.* Springer LNM 227 (1971).
- J. BUCHMANN/V. SHOUP: Constructing nonresidues in finite fields and the extended Riemann hypothesis. Preprint 1990.
- S. W. GRAHAM/C. RINGROSE: Lower bounds for least quadratic non-residues. In: B. C. BERNDT et al. (Eds): *Analytic Number Theory*, Birkhäuser, Boston 1990, 270–309.
- D. J. BERNSTEIN: Faster algorithms to find non-squares modulo worst-case integers. Preprint 2002.

A.10 Primitivwurzeln für spezielle Primzahlen

Ebenso wie quadratische Nichtreste sind auch Primitivwurzeln für viele Primzahlmoduln besonders leicht zu finden:

Satz 8 *Sei (q, p) ein* Germain-*Paar, d. h., q und $p = 2q + 1$ seien Primzahlen. Dann gilt:*

(i) *$a \in [2 \dots p-2]$ ist $\bmod p$ genau dann Primitivwurzel, wenn es quadratischer Nichtrest ist.*

(ii) *$(-1)^{\frac{q-1}{2}} \cdot 2$ ist Primitivwurzel $\bmod p$.*

Beweis. Für $q = 2$, $p = 5$, ist das klar – 2 und 3 sind sowohl die Primitivwurzeln als auch die quadratischen Nichtreste. Also kann man $q \geq 3$, also $p \geq 7$, annehmen.

(i) Dann ist $p \equiv 3 \pmod 4$ und -1 quadratischer Nichtrest. Da die Gruppenordnung $\#\mathbb{F}_p^\times = p - 1$ gerade ist, ist außerdem jede Primitivwurzel quadratischer Nichtrest. Da dieses $\varphi(p-1) = q - 1$ Stück sind, haben wir damit bereits q quadratische Nichtreste gefunden. Da $q = \frac{p-1}{2}$, sind das alle.

(ii) Im Fall $q \equiv 1 \pmod 4$ ist $p \equiv 3 \pmod 8$, also $2 = (-1)^{\frac{q-1}{2}} \cdot 2$ quadratischer Nichtrest, also auch Primitivwurzel.

Im Fall $q \equiv 3 \pmod 4$ ist $p \equiv 7 \pmod 8$, also 2 quadratischer Rest und -1 quadratischer Nichtrest, also $-2 = (-1)^{\frac{q-1}{2}} \cdot 2$ quadratischer Nichtrest, also auch Primitivwurzel. $\diamond$

Die Leichtigkeit, mit der man hier eine Primitivwurzel findet, ist ein weiterer Grund, in der Kryptologie oft Primzahlen der Form $p = 2q + 1$ zu wählen, wo q also eine Sophie-Germain-Primzahl ist.