Schüler-Propädeutikum Mathematik 2020
Vortrag 4: Quadratische Reste

Andreas Lochmann

22. Oktober 2020

1 Quadratische Reste

1.1 Definition Seien $m \in \mathbb{N}$, $m > 1$ und $a \in \mathbb{Z} \setminus \{0\}$ teilerfremd zu m. a heißt **quadratischer Rest modulo** m, wenn es ein $x \in \mathbb{Z}$ gibt mit $x^2 \equiv a \pmod{m}$, sonst **quadratischer Nichtrest**.

1.2 Beispiel Wir schreiben eine Wertetabelle modulo $m = 5$ auf (ohne die Null):

x	1	2	3	4
$x^2 \,\%\, 5$	1	4	4	1

Also sind 1 und 4 quadratische Reste modulo 5; 2 und 3 sind quadratische Nichtreste. Auch 19 ist ein quadratischer Rest modulo 5, denn $19 \equiv 4 \equiv 2^2$ (5); ebenso gibt es unendlich viele quadratische Reste und unendlich viele quadratische Nichtreste modulo 5.

Frage: Ist 3 ein quadratischer Rest modulo 11?

1.3 Definition Sei $p > 2$ prim und $a \in \mathbb{Z} \setminus \{0\}$ mit $p \nmid a$. Wir definieren das **Legendre-Symbol**

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{falls } a \text{ ein q.R. mod } p \text{ ist,} \\ -1 & \text{falls } a \text{ ein quadratischer Nichtrest mod } p \text{ ist.} \end{cases}$$

(Aussprache: „a nach p“. Man beachte, dass es sich *nicht* um einen Bruch handelt, „a durch p“ ist also falsch! Es wird nur ein ähnliches Symbol verwendet.)

1.4 Lemma (Erste Rechenregeln) *Sei $p > 2$ prim und $a, b \in \mathbb{Z} \setminus \{0\}$ nicht durch p teilbar. Dann gilt:*

1) Wenn $a \equiv b$ (p) gilt, so gilt auch $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

2) $\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$.

1.5 Lemma (Eulers Kriterium) *Ist $p > 2$ prim und $a \in \mathbb{Z} \setminus \{0\}$ mit $p \nmid a$, dann ist*

$$a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p}.$$

1.6 Satz (Quadratisches Reziprozitätsgesetz) *Seien $p \neq q$ Primzahlen, $p \neq 2$, $q \neq 2$. Dann gilt:*

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

oder anders ausgedrückt:

$$\left(\frac{p}{q}\right) = \begin{cases} -\left(\frac{q}{p}\right) & \text{falls } p \equiv q \equiv 3 \pmod 4, \\ \left(\frac{p}{q}\right) & \text{sonst.} \end{cases}$$

Beweis: Für einen vergleichsweise einfachen Beweis des quadratischen Reziprozitätsgesetzes im Falle von Primzahlen verweise ich auf ein Mathologer-Video:

`https://www.youtube.com/watch?v=X63MWZIN3gM`

1.7 Satz (Erster Ergänzungssatz)
Für alle Primzahlen $p > 2$ gilt: $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

1.8 Satz (Zweiter Ergänzungssatz)
Für alle Primzahlen $p > 2$ gilt: $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

1.9 Beispiel Wir prüfen, ob 17 ein quadratischer Rest modulo 97 ist. Da $17 \equiv 1\ (4)$ und $97 \equiv 1\ (4)$ sind, ist

$$\left(\frac{17}{97}\right) = \left(\frac{97}{17}\right)$$

Rechnen wir jetzt 97 modulo 17, finden wir:

$$\left(\frac{97}{17}\right) = \left(\frac{12}{17}\right)$$

Wir können das quadratische Reziprozitätsgesetz im obigen Sinn nicht anwenden, da sonst eine Nichtprimzahl (nämlich 12) unten stehen würde. Daher müssen wir die 12 in Primfaktoren zerlegen:

$$\left(\frac{12}{17}\right) = \left(\frac{2 \cdot 2 \cdot 3}{17}\right) = \underbrace{\left(\frac{2}{17}\right) \cdot \left(\frac{2}{17}\right)}_{=1} \cdot \left(\frac{3}{17}\right) = \left(\frac{3}{17}\right).$$

Nun ist $3 \equiv 3\ (4)$, aber $17 \equiv 1\ (4)$, es wird also kein Minuszeichen eingefügt, wenn wir die quadratische Reziprozität nutzen:

$$\left(\frac{3}{17}\right) \;=\; \left(\frac{17}{3}\right) \;=\; \left(\frac{2}{3}\right).$$

Aus dem zweiten Ergänzungssatz folgt:

$$\left(\frac{2}{3}\right) \;=\; (-1)^{\frac{9-1}{8}} \;=\; -1\,.$$

Alles zusammen ist also

$$\left(\frac{17}{97}\right) \;=\; -1\,,$$

und folglich ist 17 kein quadratischer Rest modulo 97.

Im Prinzip benötigen wir auf diese Weise nur wenige Schritte, um das Legendre-Symbol auszurechnen, ähnlich wie beim euklidischen Algorithmus. Leider jedoch benötigen wir in obigem Beispiel, und auch ganz allgemein, Primfaktorzerlegungen. Im obigen Beispiel war dies $12 = 2 \cdot 2 \cdot 3$. Für eine größere Zahl ist das natürlich entsprechend langwierig, und dies ist ein Problem.

Glücklicherweise ist es aber möglich, das quadratische Reziprozitätsgesetz auch dann anzuwenden, wenn oben und unten keine Primzahlen stehen. Das Problem ist nur: Dann liegt kein Legendre-Symbol mehr vor, d.h. Symbole wie $\left(\frac{17}{12}\right)$ sagen nichts mehr darüber aus, ob 17 ein quadratischer Rest modulo 12 ist. Der Zusammenhang zur ursprünglichen Idee geht verloren – aber die Rechnung funktioniert erstaunlicherweise trotzdem. Diese Verallgemeinerung des Legendre-Symbols heißt **Jacobisymbol**.

1.10 Beispiel Wir prüfen, ob 15 ein quadratischer Rest modulo 97 ist, zunächst auf herkömmliche Weise, nur unter Verwendung von Legendre-Symbolen:

$$\left(\frac{15}{97}\right) \;=\; \left(\frac{3}{97}\right)\cdot\left(\frac{5}{97}\right) \;=\; \left(\frac{97}{3}\right)\cdot\left(\frac{97}{5}\right) \;=\; \left(\frac{1}{3}\right)\cdot\left(\frac{2}{5}\right) \;=\; 1\cdot(-1)^{\frac{25-1}{8}} \;=\; -1\,.$$

Wenn wir Jacobi-Symbole erlauben, sieht die Rechnung so aus:

$$\left(\frac{15}{97}\right) \;=\; \left(\frac{97}{15}\right) \;=\; \left(\frac{7}{15}\right) \;=\; -\left(\frac{15}{7}\right) \;=\; -\left(\frac{1}{7}\right) \;=\; -1$$

(Dabei bekommen wir wegen $15\%4 = 3$ und $7\%4 = 3$ im zweiten Schritt ein Minuszeichen dazu.)

Beide Rechnungen ergeben das gleiche Ergebnis, aber bei der zweiten Rechnung mussten wir niemals eine Zahl faktorisieren – und man kann beweisen, dass dies immer so möglich ist.

Dadurch kann man auch für sehr große Zahlen schnell feststellen, ob eine Zahl ein quadratischer Rest modulo einer Primzahl ist. Wohlgemerkt: Damit kann man die „Wurzel“ nicht bestimmen; dies ist sogar ein relativ langsamer Prozess, vergleichbar der Faktorisierung einer großen Zahl.