Fakultät für Mathematik
Universität Bielefeld
Joa Weber

WS 2010/11

Elementare Zahlentheorie

Musterlösung zur Präsenzübung 13

von Daniel Heinrich

Sei im Folgenden $p \in \mathbb{P}$ eine ungerade Primzahl. Das Legendre-Symbol ist für $a \in \mathbb{Z}$ definiert als

$$\left(\frac{a}{p}\right) := \begin{cases} 0 & \text{falls } p \mid a \\ 1 & \text{falls } p \nmid a \text{ und } a \text{ ist quadratischer Rest mod } p \\ -1 & \text{falls } p \nmid a \text{ und } a \text{ ist quadratischer Nichtrest mod } p \end{cases}$$

Für das Rechnen mit dem Legendre-Symbol gibt es einige Rechenregeln, die einem das Leben erleichtern. Das Legendre-Symbol ist zum Beispiel stark multiplikativ, denn es gilt

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

für alle ganzen Zahlen a und b. (Diese müssen nicht notwendig teilerfremd sein. Warum nicht?) Insbesondere gilt für Primzahlpotenzen q^e:

$$\left(\frac{q^e}{p}\right) = \left(\frac{q}{p}\right)^e = \begin{cases} 1 & \text{falls } e \in \mathbb{N} \text{ gerade} \\ \left(\frac{q}{p}\right) & \text{falls } e \in \mathbb{N} \text{ ungerade} \end{cases}$$

Für die Zahlen -1 und 2 gelten weiter die folgenden Ergänzungssätze

$$\left(\frac{-1}{p}\right) = 1 \iff p \equiv 1\,(4)$$

und

$$\left(\frac{2}{p}\right) = 1 \iff p \equiv \pm 1\,(8)$$

Ist $q \in \mathbb{P}$ eine weitere ungerade Primzahl, so gilt das Gauß'sche Reziprozitätsgesetz:

$$\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right) \iff p \equiv q \equiv 3\,(4)$$

oder äquivalent:

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) \iff p \equiv 1\,(4) \text{ oder } q \equiv 1\,(4)$$

Zum Schluss ist noch das Euler-Kriterium hilfreich. Für $a \in \mathbb{Z}$ mit $p \nmid a$ gilt

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

Aufgabe 1 Für $n = 2$ gibt es offensichtlich zwei Quadrate in $R := \mathbb{Z}_n$, nämlich $\overline{0}$ und $\overline{1}$. Ist n eine ungerade Primzahl, so gibt es in R genau $\frac{n+1}{2}$ Quadrate. Davon stammen $\frac{n-1}{2}$ aus R^* und dazu kommt das Element $\overline{0}$. Denn betrachtet man alle $n-1$ Elemente von R^* (das sind für n Primzahl alle Elemente außer $\overline{0}$), so gilt

$$\begin{aligned} 1^2 &= (-1)^2 &&\equiv a_1\,(n) \\ 2^2 &= (-2)^2 &&\equiv a_2\,(n) \\ &\vdots \\ \left(\frac{n-1}{2}\right)^2 &= \left(-\tfrac{n-1}{2}\right)^2 &&\equiv a_{\frac{n-1}{2}}\,(n) \end{aligned}$$

mit $a_1, \ldots, a_{\frac{n-1}{2}} \in \{0, \ldots, n-1\}$. Die Restklassen der Elemente $a_1, \ldots, a_{\frac{n-1}{2}}$ sind alle verschieden, da $\mathbb{Z}_n$ ein Körper ist und somit die Gleichung $X^2 = \overline{a_i}$ höchstens zwei Lösungen in $\mathbb{Z}_n$ besitzt. Damit ist die Anzahl der Quadrate für die jeweiligen n:

$$\begin{aligned} n = 2 &\implies 2 \\ n = 3 &\implies 2 \\ n = 5 &\implies 3 \\ n = 19 &\implies 10 \\ n = 97 &\implies 49 \end{aligned}$$

Aufgabe 2 Man benutzt die beiden Ergänzungssätze für das Legendre-Symbol

$$\left(\frac{-1}{2129}\right) = 1, \text{ denn } p \equiv 1\,(4)$$

$$\left(\frac{2}{2129}\right) = 1, \text{ denn } p \equiv 1\,(8)$$

$$\left(\frac{-1}{2131}\right) = -1, \text{ denn } p \equiv 3\,(4)$$

$$\left(\frac{2}{2131}\right) = -1, \text{ denn } p \equiv 3\,(8)$$

Damit sind -1 und 2 Quadrate modulo 2129 und keine Quadrate modulo 2131.

Aufgabe 3 Hier führt wiederholte Anwendung der Gauß'schen Reziprozität sowie der Ergänzungssätze zum Erfolg.

$$\left(\frac{26}{41}\right) = \left(\frac{2}{41}\right) \cdot \left(\frac{13}{41}\right) = 1 \cdot \left(\frac{41}{13}\right) = \left(\frac{2}{13}\right) = -1$$

$$\left(\frac{125}{1009}\right) = \left(\frac{5}{1009}\right)^3 = \left(\frac{5}{1009}\right) = \left(\frac{1009}{5}\right) = \left(\frac{4}{5}\right) = 1$$

$$\left(\frac{225}{3769}\right) = \left(\frac{15}{3769}\right)^2 = 1$$

$$\begin{aligned} \left(\frac{6557}{7919}\right) &= \left(\frac{79}{7919}\right) \cdot \left(\frac{83}{7919}\right) = (-1)^2 \cdot \left(\frac{7919}{79}\right) \cdot \left(\frac{7919}{83}\right) = \left(\frac{19}{79}\right) \cdot \left(\frac{34}{83}\right) \\ &= (-1) \cdot \left(\frac{79}{19}\right) \cdot \left(\frac{2}{83}\right) \cdot \left(\frac{17}{83}\right) = (-1) \cdot \left(\frac{3}{19}\right) \cdot (-1) \cdot \left(\frac{83}{17}\right) \\ &= \left(\frac{3}{19}\right) \cdot \left(\frac{15}{17}\right) = (-1) \cdot \left(\frac{19}{3}\right) \cdot \left(\frac{-1}{17}\right) \cdot \left(\frac{2}{17}\right) = (-1) \cdot \left(\frac{1}{3}\right) \cdot 1 \cdot 1 = -1 \end{aligned}$$

Aufgabe 4 Hier benutzt man das Eulerkriterium, denn $11 = \frac{23-1}{2}$ und damit sind die Potenzen nichts anderes als die entsprechenden Werte des Legendre-Symbols.

$$\begin{aligned}
2^{11} &\equiv \left(\frac{2}{23}\right) = 1\,(23)\\
3^{11} &\equiv \left(\frac{3}{23}\right) = -\left(\frac{23}{3}\right) = -\left(\frac{2}{3}\right) = 1\,(23)\\
4^{11} &\equiv \left(\frac{4}{23}\right) = 1\,(23)\\
5^{11} &\equiv \left(\frac{5}{23}\right) = \left(\frac{23}{5}\right) = \left(\frac{3}{5}\right) = -1\,(23)\\
21^{11} &\equiv \left(\frac{21}{23}\right) = \left(\frac{-2}{23}\right) = \left(\frac{-1}{23}\right)\cdot\left(\frac{2}{23}\right) = (-1)\cdot 1 = -1\,(23)\\
22^{11} &\equiv (-1)^{11} = -1\,(23)
\end{aligned}$$

Aufgabe 5 (a) Natürlich führt hier auch ausprobieren zum Ziel, allerdings geht dies auch systematischer. Die erste Bedingung ist äquivalent zu

$$\left(\frac{3}{q}\right) = 1 \tag{1}$$

und die zweite ist eine andere Formulierung für

$$\left(\frac{q}{3}\right) = -1 \tag{2}$$

Da q kein Quadrat modulo 3 sein soll, bedeutet dies $q \equiv 2\,(3)$, denn $\overline{2}$ ist das einzige Nichtquadrat modulo 3. Weiter folgt aus den Gleichungen (1) und (2)

$$\left(\frac{3}{q}\right) = -\left(\frac{q}{3}\right) \implies q \equiv 3\,(4).$$

Diese beiden Kongruenzen liefern ein System

$$\begin{aligned}
x \equiv\ & 2 \equiv -1 \quad (3)\\
x \equiv\ & 3 \equiv -1 \quad (4),
\end{aligned}$$

das sich mit Hilfe des chinesischen Restsatzes zu $x \equiv -1 \equiv 11\,(12)$ lösen lässt. Die kleinste solche Primzahl ist 11 und man rechnet schnell nach, dass 11 auch wirklich die geforderte Eigenschaft besitzt.

(b) Angenommen es wäre

$$\begin{aligned}
\left(\frac{g}{p}\right) = 1 \quad &\implies \quad 1 = \left(\frac{g}{p}\right) \equiv g^{\frac{p-1}{2}}\,(p)\\
&\implies \quad \operatorname{ord}(g) \leq \frac{p-1}{2} < p-1\\
&\implies \quad g \text{ ist keine Primitivwurzel,}
\end{aligned}$$

was im Widerspruch zu Wahl von g steht. Somit gilt:

$$\left(\frac{g}{p}\right) = -1$$