Übungen zur Zahlentheorie, WWU Münster, Mathematisches Institut, SoSe 2016
U. Hartl, K. Halupczok **Blatt Nr. 5**, 12.05.16

Abgabe: **Mittwoch, 25. Mai 2016**, bis 11:30 Uhr in die Briefkästen im Hörsaalgebäude

Leseaufgabe: Kapitel 2.3 bis Montag 23.5.

Aufgabe 1

Berechnen Sie die folgenden Legendresymbole unter Verwendung des quadratischen Reziprozitätsgesetzes und der beiden Ergänzungsgesetze. Beachten Sie dabei, dass je nach Beispiel entweder die Reduktion auf den absolut kleinsten Rest oder die Reduktion auf den kleinsten nichtnegativen Rest vorteilhaft sein kann.

$$\left(\frac{13}{239}\right),\ \left(\frac{19}{8513}\right),\ \left(\frac{16993}{65537}\right),\ \left(\frac{7279}{487}\right)$$

An welcher Stelle ist die Faktorisierung $7279 = 29 \cdot 251$ unumgänglich?

Aufgabe 2

(a) Sei p eine ungerade Primzahl. Berechnen Sie $\left(\frac{-2}{p}\right)$, formulieren und beweisen Sie ein Kriterium, unter dem -2 ein quadratischer Rest mod p ist und sonst nicht.

(b) Sei p eine Primzahl mit $p \equiv 3 \bmod 4$, und sei $a \in \mathbb{Z}$, $p \nmid a$, ein quadratischer Rest mod p. Geben Sie die beiden Lösungen der quadratischen Kongruenz $x^2 \equiv a \bmod p$ explizit an. (Finden Sie nämlich eine Potenz von a, deren Quadrat kongruent zu a ist.)
Wie lauten die Lösungen von $x^2 \equiv -2 \bmod 163$?

Aufgabe 3 (Zum Jacobi-Symbol)

Seien $a, b \in \mathbb{Z}$ teilerfremd und $b > 1$ ungerade. Ist $b = p_1 p_2 \dots p_r$ die Primfaktorzerlegung von b (in nicht notwendig verschiedene Primzahlen), so wird das *Jacobi-Symbol* definiert durch

$$\left(\!\!\left(\frac{a}{b}\right)\!\!\right) := \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_r}\right).$$

(Für b prim ist das Jacobi-Symbol identisch mit dem Legendre-Symbol.)
Es kann gezeigt werden, dass das Jacobi-Symbol ebenso wie das Legendre-Symbol gleich bleibt, wenn im „Zähler" eine Reduktion modulo des „Nenners" vorgenommen wird, dass es multiplikativ im „Zähler" ist (vgl. Satz 2.1.6), und darüberhinaus ist es multiplikativ im „Nenner", d. h. sind $a, b, b' \in \mathbb{Z}$, $b, b' > 1$ ungerade mit $(a, bb') = 1$, so gilt

$$\left(\!\!\left(\frac{a}{bb'}\right)\!\!\right) = \left(\!\!\left(\frac{a}{b}\right)\!\!\right)\left(\!\!\left(\frac{a}{b'}\right)\!\!\right).$$

Insbesondere gelten das quadratische Reziprozitätsgesetz und die beiden Ergänzungsgesetze auch für das Jacobi-Symbol (kann mit einigem Aufwand aus den Gesetzen für das Legendre-Symbol hergeleitet werden).

(a) Berechnen Sie unter Ausnutzen dieser Gesetze die folgenden Jacobi-Symbole. Welche Vorteile ergeben sich mit dem Jacobi-Symbol gegenüber dem Legendre-Symbol?

$$\left(\!\!\left(\frac{2435}{7279}\right)\!\!\right),\ \left(\!\!\left(\frac{16993}{65537}\right)\!\!\right)$$

(b) Seien $a, b \in \mathbb{Z}$ teilerfremd und $b > 1$ ungerade. Zeigen Sie: Ist a ein quadratischer Rest mod b, so gilt $\left(\!\!\left(\frac{a}{b}\right)\!\!\right) = 1$, aber die Umkehrung ist falsch.