Zahlentheorie: Übungsblatt 5
(für die Übungen am 22./23. November 2012)

Aufgabe 1 (schriftlich)**.** Finden Sie alle Primitivwurzeln modulo 19.

Aufgabe 2 (mündlich)**.** (a) Entscheiden Sie mit Hilfe des (i) Gaußschen Lemmas und von (ii) Euler's Kriterium, ob 7 ein quadratischer Rest modulo 13 ist.

(b) Sei p eine Primzahl mit $p \equiv 3 \pmod 4$. Weiterhin habe p die Eigenschaft, dass $q = 2p+1$ ebenfalls eine Primzahl ist. Zeigen Sie, dass dann q die Zahl $2^p - 1$ teilt. Folgern Sie, dass $2^{251} - 1$ keine Primzahl sein kann.

Aufgabe 3 (mündlich)**.** Beweisen Sie, dass es unendlich viele Primzahlen der Form $8k - 1$ ($k \in \mathbb{N}$) gibt. [Hinweis: Betrachten Sie die Zahl $N = (4p_1p_2 \cdots p_n)^2 - 2$.]

Aufgabe 4 (schriftlich)**.** (a) Die Indextabelle zu einer Primitivwurzel r modulo n gibt zu jeder zu n teilerfremden Zahl a den zugehörigen Index bezüglich r an. Erstellen Sie eine Indextabelle für $n = 13$ und $r = 2$.

(b) Benutzen Sie die Rechnung aus Teil (a), um die Kongruenz $4x^9 \equiv 7 \pmod{13}$ zu lösen.

Aufgabe 5 (mündlich)**.** Sei p eine ungerade Primzahl, $a \in \mathbb{Z}$ sei teilerfremd zu p und $b \equiv a \pmod p$. Zeigen Sie, dass a genau dann ein quadratischer Rest modulo einer Primzahlpotenz p^n ist, wenn das Legendre-Symbol (b/p) gleich 1 ist. Sei jetzt q eine weitere ungerade Primzahl. Wenn das Produkt von Legendre-Symbolen $(a/p) \cdot (a/q)$ gleich 1 ist, ist dann a ein quadratischer Rest modulo pq?

http://www.mathematik.uni-stuttgart.de/studium/infomat/ZahlTheo-Koenig/