Aufgaben zu den Kapiteln 3 bis 5

(1) (a) Es gibt unendlich viele Primzahlen der Form $4n+3$.
(Das braucht keine Theorie. Die Zahl
$N = 4q_1q_2 - q_5 - 1 = 4(q_1q_2 - q_5 - 1) + 3$ für geeignete q_i hilft.)
(b) Es gibt unendlich viele Primzahlen der Form $4n+1$.
(Hier hilft $N = (2q_1 - q_t)^2 + 1$.)

(2) (a) Sei p prim, $p \equiv 7 \pmod 8$. Dann gilt $p \mid (2^{(p-1)/2} - 1)$.
(b) Welche der folgenden Zahlen sind prim?
$2^{179} - 1,\ 2^{239} - 1,\ 2^{251} - 1$

(3) Es soll gezeigt werden, daß $x^2 \equiv 196 \pmod{1357}$ lösbar ist.
(a) Das ist äquivalent zur Lösbarkeit von zwei Gleichungen
$x^2 \equiv 196 \pmod{23}$ und $x^2 \equiv 196 \pmod{59}$
(b) Berechnen Sie geeignete Legendre-Symbole.
(c) Berechnen Sie die Lösungen. Wieviele sind es?

(4) Beweisen Sie Eulers Kriterium 4.2 ohne Verwendung von Primitivwurzeln, aber mit Hilfe des Satzes von Wilson. modulo p ist
(Hinweis: Wenn a ein quadratischer Nichtrest und $c \in \{1, \dots, p-1\}$, sei d so, daß $c \cdot d \equiv a \pmod p$. Zeigen Sie $c \neq d$ und stellen Sie eine Situation für den Satz von Wilson her.)