Übungen zur **Blatt 10**
Elementaren Zahlentheorie 19.12.2014

Falko Lorenz, Karin Halupczok WiSe 2014/15

Abgabetermin: Freitag, 9. Januar 2015, bis 10:10 Uhr in die Briefkästen

Aufgabe 37:

Laut welcher Resultate der Vorlesung ist der Ring $\mathbb{Z}[i]$ faktoriell?
Bestimme die Primfaktorzerlegung von $6 + 14i$ in $\mathbb{Z}[i]$.

Aufgabe 38:

Sei a quadratischer Rest mod p. Man zeige:

(a) Ist $p \equiv 3 \bmod 4$, so hat die Kongruenz $X^2 \equiv a \bmod p$ eine Lösung der Gestalt $x = a^n$.

(b) Ist $p \equiv 5 \bmod 8$, so hat die Kongruenz $X^2 \equiv a \bmod p$ eine Lösung der Gestalt $x = a^n$ oder $x = 2^m a^n$.

Aufgabe 39:

Wie oben stehe p für eine Primzahl. Man zeige die Äquivalenz der folgenden Aussagen:

(i) $2p + 1$ ist ein Teiler von $M_p = 2^p - 1$,

(ii) $2p + 1$ ist eine Primzahl und $p \equiv 3 \bmod 4$.

Man gebe zwei Mersennesche Zahlen M_p an, die aufgrund dieser Feststellung keine Primzahlen sind (und für 2 Fleißpunkte extra auch noch eine dritte).

Aufgabe 40:

(a) Welche der Zahlen $a_1 = 16993$, $a_2 = 17993$ sind quadratische Reste mod 65537?
(Inwieweit muß man dazu wissen, daß $F_4 = 65537$ eine Primzahl ist, was man mit Aufgabe 27 nachprüfen kann; 2P extra).

(b) Für welche Primzahlen p ist 13 quadratischer Rest mod p? (Zur Vorübung auf die Klausur suche man nach einer völlig korrekten und doch konzisen Form der Antwort; 2P extra.)