Problem set 1 – Math 699 – Algebraic number theory

(1) (a) For $\alpha \in \mathbf{Z}[i]$, show that $N(\alpha) = 1$ if and only if $\alpha \in \mathbf{Z}[i]^\times$. Here $N(\alpha) = \alpha\overline{\alpha}$ is the norm of α.

(b) Show if that $p \equiv 3 \pmod 4$, then p is prime in $\mathbf{Z}[i]$.

(2) (a) Show that $\mathbf{Z}[\sqrt{-2}]$ is Euclidean. (Hint: use the norm function $N(a+b\sqrt{-2}) = |a + b\sqrt{-2}|^2 = a^2 + 2b^2$.)

(b) Show that $N(\alpha) = 1$ if and only if $\alpha \in \mathbf{Z}[\sqrt{-2}]^\times$. From this, determine $\mathbf{Z}[\sqrt{-2}]^\times$.

(c) Let p be a prime. Show that if $p = a^2 + 2b^2$, with $a, b \in \mathbf{Z}$, then $p = 2$ or $p \equiv 1$ or $3 \pmod 8$. Conclude that if p is odd and $p \equiv 5, 7 \pmod 8$, then p is prime in $\mathbf{Z}[\sqrt{-2}]$.

(d) Let p be an odd prime. Using quadratic reciprocity (or really its so-called "supplements"), show that $p \equiv 1, 3 \pmod 8$ if and only if -2 is a square mod p.

(e) Show that if $p \equiv 1, 3 \pmod 8$, then p is *not* prime in $\mathbf{Z}[\sqrt{-2}]$.

(f) Prove Fermat's theorem that $p = a^2 + 2b^2$ with $a, b \in \mathbf{Z}$ if and only if $p = 2$ or $p \equiv 1, 3 \pmod 8$.

(3) Let ω be the primitive 3rd root of unity $e^{2\pi i/3}$, so a root of $x^2 + x + 1$.

(a) Show that $\mathbf{Z}[\omega]$ is Euclidean. (Hint: use the norm function $N(a + b\omega) = |a + b\omega|^2 = a^2 - ab + b^2$.)

(b) Show that $N(\alpha) = 1$ if and only if $\alpha \in \mathbf{Z}[\omega]^\times$. From this, determine $\mathbf{Z}[\omega]^\times$.

(c) Let p be a prime. Show that if $p = a^2 - ab + b^2$, with $a, b \in \mathbf{Z}$, then $p = 3$ or $p \equiv 1 \pmod 3$. Conclude that if $p \equiv 2 \pmod 3$, then p is prime in $\mathbf{Z}[\omega]$.

(d) Let $p \neq 3$. Using quadratic reciprocity, show that $p \equiv 1 \pmod 3$ if and only if -3 is a square mod p.

(e) Show that if $p \equiv 1 \pmod 3$, then p is *not* prime in $\mathbf{Z}[\omega]$.

(f) Prove that $p = a^2 - ab + b^2$ with $a, b \in \mathbf{Z}$ if and only if $p = 3$ or $p \equiv 1 \pmod 3$.

(4) Why does the argument used in the lecture to show that $\mathbf{Z}[i]$ is Euclidean with respect to the norm function not work for $\mathbf{Z}[\sqrt{-3}]$?