UNIQUE FACTORIZATION AND FERMAT'S LAST THEOREM
HOMEWORK 5

Problem 1 (Factorization of prime integers). Let R be an imaginary quadratic integer ring, let $P \subset R$ be a nonzero prime ideal, and let $n = N(P)$, so $n > 1$ is an integer and $P\overline{P} = (n)$.

(i) Show that if $I \subset R$ is a nonzero ideal such that $N(I)$ is prime, then I is prime.

(ii) Let $n = p_1 \cdots p_r$ be the prime factorization of n (as an ordinary integer). Prove that both P and $\overline{P}$ divide the same ideal (p_i) for some i.

(iii) Use (i) to show that that there is a prime integer p such that $n = p$ or $n = p^2$. In the case that $n = p$ is prime, show that p is not a prime element of R and that $(p) = P\overline{P}$. If $n = p^2$ is a prime square, show that p is a prime element of R and that $P = \overline{P} = (p)$.

(iv) Conversely, show that if a prime integer p is not a prime element of R then there exists a prime ideal P of R such that $(p) = P\overline{P}$, and that $\overline{P}$ is also prime.

(v) *Extra credit*: can you determine which prime integers p have the prime factorization $(p) = P^2$ for a prime ideal $P \subset R$?

Problem 2 (The quadratic imaginary integer rings which are PIDs). For each value of D, prove that the ideal class group of the imaginary quadratic integer ring for $-D$ is a principal ideal domain:

$$D = 1,\ 2,\ 3,\ 7,\ 11,\ 19,\ 43,\ 67,\ 163.$$

(We have already treated the cases $D = 1, 2, 3$.)

Problem 3 (A very curious polynomial). Let $\delta = \sqrt{-163}$ and let $\eta = \frac{1}{2}(1+\delta)$, so $R = \mathbf{Z}[\eta]$ is the quadratic imaginary integer ring for -163. Let

$$f(X) = X^2 - X + 41 = (X - \eta)(X - \overline{\eta}).$$

(i) Let $z \in R$ be non-real, i.e. $z \notin \mathbf{R}$. Show that $|z|^2 \geq 41$

(ii) Let $0 \leq a \leq 40$ be an integer. Show that $f(a) = |a - \eta|^2 < 41^2$. Use (i) to conclude that $a - \eta$ is irreducible.

(iii) Again let $0 \leq a \leq 40$ be an integer. Use (ii) and Problem 2 above to prove that $a - \eta$ is prime, then use Problem 1 to prove that $|a - \eta|^2$ is a prime integer.

(iv) Conclude that $f(0), f(1), f(2), \ldots, f(39), f(40)$ are all prime numbers.

Problem 4 (Calculating ideal class groups). For each value of D, calculate the ideal class group of the imaginary quadratic integer ring for $-D$:

$$D = 6,\ 10,\ 13,\ 14,\ 15,\ 17,\ 21.$$