Homework

due on Tuesday, October 23

Read sections 2.3.1-2.3.4, 2.4.2, 7.2.1-7.2.2 in Cameron's book and section 3.5 in Lauritzen's book. Solve the following problems:

Problem 1. Consider the ring $R = \mathbb{Z}[\omega] = \{a+b\omega : a, b \in \mathbb{Z}\}$ of Eisenstein integers, where $\omega = (-1+\sqrt{-3})/2$ (see Homeworks 17, 23 for various facts about R).

a) Let $x = a + b\omega$, $y = c + d\omega$ be elements of R such that $x \neq 0$. Prove that the complex number y/x can be written as $u + w\omega$ for some rational numbers u, w.

b) Consider the map $N : R \longrightarrow \mathbb{Z}$ defined by $N(a + b\omega) = a^2 - ab + b^2$ (so $N(x)$ is just the square of the absolute value of the complex number x). Use N to prove that R is an Euclidean domain (Hint: Mimic the argument from class for the ring of Gaussian integers).

c) Let $x = a + b\omega \in R$. Prove that there exists $c + d\omega \in R$ which is associated with x and such that $c \geq 0$, $d \geq 0$ (Hint: Use d) of Problem 1 from homework 23).

d) Let p be an odd prime such that -3 is a quadratic non-residue modulo p . Prove that p is irreducible in R. (Use h) of Problem 1 from homework 23). Prove the same for $p = 2$.

e) Suppose that p is an odd prime such that -3 is a quadratic residue modulo p. Prove that p is not irreducible in R. Conclude that there exist positive integers a, b such that $p = a^2 - ab + b^2$ (use c)).

f) Use quadrartic reciprocity to prove that -3 is a quadratic residue modulo p iff $p \equiv 1 \pmod 3$.

Problem 2. Let R be a PID. Consider two elements $a, b \in R$. Since R is a PID, there is $d \in R$ such that $aR + bR = dR$. Prove that for any $c \in R$ we have $c|d$ iff $c|a$ and $c|b$. What would be appropriate to call d?