Homework 6 : Due Wednesday, March 7

Problem 1: Let R be a UFD (but perhaps not a PID). Show that every irreducible element of R is prime.
Cultural Aside: Using this, one can prove that ord_p has the usual properties for any irreducible p. Thus, one can carry over many of our arguments to general UFDs. However, although gcd's exist in a general UFD (think about why on your own), it may not be the case that a gcd of a and b can be written as a linear combination of a and b.

Problem 2: Define $f\colon \mathbb{Z}[i]\backslash\{0\} \to \mathbb{N}$ by letting $f(\alpha)$ be the number of elements in the ring $\mathbb{Z}[i]/\langle\alpha\rangle$. In this problem we show that $f(\alpha) = N(\alpha)$ for all $\alpha \in \mathbb{Z}[i]\backslash\{0\}$. Consult the notes to see why $f(n) = n^2$ for all $n \in \mathbb{Z}$.
a. Show that $f(\alpha) = f(\overline{\alpha})$ for all $\alpha \in \mathbb{Z}[i]\backslash\{0\}$ by showing that if $\{\gamma_1, \gamma_2, \dots, \gamma_k\}$ is a set of unique representatives of the cosets of $\mathbb{Z}[i]/\langle\alpha\rangle$, then $\{\overline{\gamma_1}, \overline{\gamma_2}, \dots, \overline{\gamma_k}\}$ is a set of unique representatives of the cosets of $\mathbb{Z}[i]/\langle\overline{\alpha}\rangle$.
b. Show that $f(\alpha\beta) = f(\alpha) \cdot f(\beta)$ for all $\alpha, \beta \in \mathbb{Z}[i]\backslash\{0\}$ by showing if $\{\gamma_1, \gamma_2, \dots, \gamma_k\}$ is a set of unique representatives of the cosets of $\mathbb{Z}[i]/\langle\alpha\rangle$ and $\{\delta_1, \delta_2, \dots, \delta_\ell\}$ is a set of unique representatives of the cosets of $\mathbb{Z}[i]/\langle\beta\rangle$, then

$$\{\gamma_i + \alpha\delta_j : 1 \le i \le k, 1 \le j \le \ell\}$$

is a set of unique representatives for the cosets of $\mathbb{Z}[i]/\langle\alpha\beta\rangle$.
c. Show that $f(\alpha) = N(\alpha)$ for all $\alpha \in \mathbb{Z}[i]\backslash\{0\}$.
Note: It may be useful to use the standard fact that complex conjugation $\alpha \mapsto \overline{\alpha}$ is an automorphism of $\mathbb{C}$, i.e. that it preserves addition and multiplication.

Problem 3:
a. Show how to write 108,290 as the sum of two squares by first factoring the number and then working your way up to a solution. (In other words, saying that you found a solution by exhaustive search won't suffice).
b. Prove that if an integer is the sum of two rational squares then it is the sum of two integer squares (for example, $13 = (1/5)^2 + (18/5)^2 = 2^2 + 3^2$).

Problem 4: Let $p \in \mathbb{N}^+$ be prime. Let R_p be the subring of $\mathbb{Q}$ consisting all rational numbers which can be written with a denominator not divisible by p, i.e.

$$R_p = \{\frac{a}{b} : a, b \in \mathbb{Z} \text{ and } p \nmid b\}$$

You should convince yourself that R_p is a subring of $\mathbb{Q}$.
a. Show that R is a Euclidean domain with Euclidean function $N(\frac{a}{b}) = ord_p(a)$.
b. Classify the units of R_p.
c. Show that p is irreducible in R_p.
d. Show that every irreducible in R_p is an associate of p (so R_p has a unique irreducible up to associates).
Cultural Aside: The ring R_p is called the localization of $\mathbb{Z}$ at p. Studying localizations of a ring is an extremely important part of algebra.

Problem 5: Suppose that $(x, y) \in \mathbb{Z}^2$ satisfies $2x^3 = y^2 + 1$.
a. Show that x and y are both odd.
b. Show that $1 + i$ is a greatest common divisor of $y + i$ and $y - i$ in $\mathbb{Z}[i]$.
c. Show that either $(x, y) = (1, 1)$ or $(x, y) = (1, -1)$.