Math 494, Homework 5: due Feb 25

(1) We can write every positive integer n in exactly one way as $2^a \cdot \prod_{j=1}^{r} p_j^{e_j} \cdot \prod_{\ell=1}^{s} q_\ell^{f_\ell}$ where $a, r, s \in \mathbb{N}_0$, the p_j's are primes congruent to 1 mod 4 with $p_1 < p_2 < \cdots < p_r$, and the q_ℓ's are primes congruent to 3 mod 4 with $q_1 < q_2 < \cdots < q_s$. For each $n \in \mathbb{N}$, give a formula for the number of pairs (x, y) of nonnegative integers such that $x^2 + y^2 = n$ and $0 \le x \le y$.

Hint: The formula should only involve the values of a, the e_j's, and the f_ℓ's. Use unique factorization in $\mathbb{Z}[i]$. Also use the fact proved in class, that every prime number congruent to $3 \bmod 4$ is a prime in $\mathbb{Z}[i]$, and every prime number p which is not congruent to $3 \bmod 4$ can be written as $p = a^2 + b^2$ with $a, b \in \mathbb{N}$, in which case $a + bi$ and $a - bi$ are primes in $\mathbb{Z}[i]$. Moreover, every prime in $\mathbb{Z}[i]$ is a unit times one of the primes named in the previous sentence. Also use that if $x \in \mathbb{Z}[i]$ and $\bar{x}$ is its complex conjugate then $N(x) := x\bar{x}$ is a nonnegative integer such that $N(x) = 0$ precisely when $x = 0$, and $N(x) = 1$ precisely when x is a unit, and also $N(xy) = N(x) \cdot N(y)$. The last assertion follows from the analogous assertion about absolute values, or more directly from the easy-to-verify fact that $\overline{xy} = \bar{x} \cdot \bar{y}$.

(2) Describe the prime elements in $\mathbf{Z}[\sqrt{-2}]$, and then use this description to give a formula for the number of ways to express a positive integer n as $x^2 + 2y^2$ with $x, y \in \mathbb{N}_0$. You may use without proof the fact that if p is an odd prime then -2 is a square in $(\mathbb{Z}/p\mathbb{Z})^*$ if and only if p is congruent to 1 or 3 mod 8 (I will prove this fact in a piazza post).

(3) Check via computer that $f(x) := x^4 + 3x^2 + 7x + 4$ is not irreducible in $\mathbb{F}_p[x]$ for any small prime p. But use the factorizations in $\mathbb{F}_p[x]$ to show that $f(x)$ is irreducible in $\mathbb{Z}[x]$. (You don't need to write anything about the first sentence, but I encourage you to familiarize yourself with this type of computer usage; for the benefit of those of you who aren't already expert programmers, I'll make a piazza post showing how to use Magma to factor polynomials in $\mathbb{F}_p[x]$, but if you prefer to use a different computer package then feel free to do so.)

(4) Problems 3.6, 4.4, 4.10(a,e,j,k), 5.1, 5.3 from chapter 12 of Artin.