18.786: Topics in Algebraic Number Theory (spring 2006)
Problem Set 1, due Thursday, February 16

Throughout these exercises, let $i \in \mathbb{C}$ be a square root of -1 and let $|\cdot|$ denote the usual absolute value on $\mathbb{C}$. Let $\mathbb{Z}[i]$ (resp. $\mathbb{Q}(i)$) be the subsets of $\mathbb{C}$ consisting of $a+bi$ with $a, b \in \mathbb{Z}$ (resp. $a, b \in \mathbb{Q}$). Then $\mathbb{Z}[i]$ is a ring, the ring of *Gaussian integers*, and $\mathbb{Q}(i)$ is its fraction field, the field of *Gaussian rationals*.

1. Prove the division algorithm for $\mathbb{Z}[i]$: for any $f, g \in \mathbb{Z}[i]$ with $g \neq 0$, there exist (not necessarily unique) $q, r \in \mathbb{Z}[i]$ with $f = qg + r$ and $|r| < |g|$.

2. Use the division algorithm to prove that $\mathbb{Z}[i]$ is a principal ideal domain, by imitating the usual proof for $\mathbb{Z}$.

3. Imitate the previous argument to prove that $\mathbb{Z}[e^{2\pi i/3}]$ and $\mathbb{Z}[\sqrt{-2}]$ are principal ideal domains. (I'll have more to say about this later.)

4. Prove that $\mathbb{Z}[\sqrt{-5}]$ is not a principal ideal domain by showing that the ideal generated by 2 and $1 + \sqrt{-5}$ is not principal. (Hint: if x divides y, then $|x|^2$ divides $|y|^2$.)

5. Use arithmetic in $\mathbb{Z}[i]$ to prove Fermat's theorem: if p is a prime number and $p \equiv 1 \pmod 4$, then there exist $a, b \in \mathbb{Z}$ such that $a^2 + b^2 = p$, which are unique up to sign and order. (Hint: for any odd prime p, you can find $x \in \mathbb{Z}$ such that $(x^{(p-1)/4})^2 + 1 \equiv 0 \pmod p$.)

6. Establish access to SAGE 1.0.0 (or greater) on any of: a computer of your own, an Athena machine, a math department machine. Then using SAGE and the previous exercises, find a representation of the prime $p = 10^{40}+301$ in the form a^2+b^2. Show your work: that is, include the code that you used to obtain the representation. Most likely you want to do this by just printing out your session. (This amounts to implementing the Euclidean algorithm in $\mathbb{Z}[i]$. You may want to warm up with a simpler example!)