Honors Algebra II, Courant Institute, Spring 2022
http://www.math.nyu.edu/faculty/goodman/teaching/HonorsAlgebraII2022/HonorsAlgebraII.html
Check the class forum for corrections and hints

Assignment 5

Due: Thursday, March 10.
As an experiment, this assignment has fewer hints than earlier assignments to emphasize the problem solving aspect. Feel free to ask for hints on the Brightspace discussion board after you have tried for a while. Many "simple tricks" are hard to see. Section 12.5 of the text, which is covered in class on Tuesday, will be a big help in solving this.

This sequence of steps shadows the discussion in the text about which *rational primes* ($p \in \mathbb{Z}$) are prime in the Gaussian integers $\mathbb{Z}[i]$. Here, it is done for the ring of algebraic integers in $\mathbb{Q}[\zeta_3]$, with $\zeta_3 = e^{2\pi i/3}$ being a primitive third root of unity. The result is striking: a certain diophantine equation involving a prime p does or does not have a solution depending on whether $p \equiv 1$ or $p \equiv 2$ mod 3.

1. If $R \in \mathbb{F}$ (a ring contained in a field), an element $\alpha \in \mathbb{F}$ is an *algebraic integer* "in $\mathbb{F}$ over R" if there is a monic $f \in \mathbb{R}[X]$ with $f(\alpha) = 0$. We will call this ring A, though it is often denoted by $\mathfrak{o}$ (the letter "o" in Fraktur font). In particular, let A be the ring of algebraic integers over $\mathbb{Z}$ in $\mathbb{Q}[\zeta_3$. Show that $A = \mathbb{Z}[\zeta_3]$. *Discussion.* "Clearly" $\alpha = a + b\zeta_3 \in A$ if $\alpha \in \mathbb{Z}[\zeta_3]$ (so $a, b \in \mathbb{Z}$); why? One approach to the harder direction is first to show that it suffices to consider $\deg(f) = 2$ and then to use the coefficient of ζ_3 in $f(\alpha)$ to show that b is a rational integer.
2. Suppose $\alpha \in A$ and $n \in \mathbb{Z}$. Show that $\alpha \mid n$ if and only if $\overline{\alpha} \mid n$. Here, $\overline{\alpha}$ is the complex conjugate of α.
3. Show that if $\alpha \mid p$ and $\alpha \notin \mathbb{Z}$ then $\alpha\overline{\alpha} = \pm p$.
4. Show that 2 in prime in A.
5. Find a non-trivial factorization of 3 in A.
6. Show that $\Phi(X) = X^2 + X + 1$ is irreducible in $\mathbb{F}_p[X]$, with $p \geq 5$, if and only if $p - 1 \equiv 1$ mod 3.
7. Let R be the quotient ring $R = A/(p)$. Show that R is isomorphic to $\mathbb{F}_p[X]/(\Phi)$.
8. Show that Φ is irreducible in $\mathbb{F}_p[X]$ if and only if p is prime in A.
9. Show that $a^2 + b^2 - ab = p$ has integer solutions (solutions with $a, b \in \mathbb{Z}$) if and only if $p \equiv 1$ mod 3.
10. Find integer solutions for the quadratic diophantine equation $a^2+b^2-ab = p$ for $p = 7$ and $p = 13$.