Directions: Solve the following problems. See the course syllabus and the Homework Webpage on the course website for general directions and guidelines.

1. [IR 5.{26,27,28}] Let p be a prime such that $p \equiv 1 \pmod 4$. An integer c is called a biquadratic residue modulo p if $p \nmid c$ and $x^4 \equiv c \pmod p$ has a solution. Since $p \equiv 1 \pmod 4$, from an exercise on HW3, we know that $p = a^2 + b^2$ for some integers a and b with $1 \le a, b < \sqrt{p}$. By symmetry, we may assume that a is odd and b is even.
   (a) Prove that $\left(\frac{a}{p}\right) = 1$ and $\left(\frac{a+b}{p}\right) = (-1)^{((a+b)^2-1)/8}$. [Hint: since a and $a+b$ are odd, the Jacobi symbols $\left(\frac{p}{a}\right)$ and $\left(\frac{p}{a+b}\right)$ are well defined.]
   (b) Prove that $(a+b)^2 \equiv 2ab \pmod p$ and conclude that $(a+b)^{(p-1)/2} \equiv (2ab)^{(p-1)/4} \pmod p$.
   (c) Let f be an integer such that $b \equiv af \pmod p$. Show that $f^2 \equiv -1 \pmod p$ and that $2^{(p-1)/4} \equiv f^{ab/2} \pmod p$.
   (d) Show that c is a biquadratic residue modulo p if and only if $c^{(p-1)/4} \equiv 1 \pmod p$.
   (e) Show that (for $p \equiv 1 \pmod 4$), the integer 2 is a biquadratic residue modulo p if and only if $p = A^2 + 64B^2$ for some integers A and B.
2. [IR 6.1] Show that $\sqrt{2} + \sqrt{3}$ is an algebraic integer. [Hint: closure properties.]
3. [IR 6.2] Let α be an algebraic number. Show that there is an integer n such that $n\alpha$ is an algebraic integer.
4. [IR 6.{4,5,7}] Algebraic integers in $\mathbb{Q}[\sqrt{D}]$ for a square-free integer D.
   (a) Gauss's Lemma. A polynomial $f \in \mathbb{Z}[x]$ is *primitive* if the greatest common divisor of its coefficients is 1. Prove that the product of primitive polynomials is again primitive. [Hint: let f_1 and f_2 be primitive polynomials in $\mathbb{Z}[x]$ and let p be a prime. Since f_i is primitive, there is a least integer r_i such that the coefficient of x^{r_i} in f_i is not divisible by p. Argue that the coefficient of $x^{r_1+r_2}$ in $f_1 f_2$ is not divisible by p.]
   (b) Let α be an algebraic number and let $f \in \mathbb{Q}[x]$ be the minimal polynomial of α. Use part (a) to prove that α is an algebraic integer if and only if $f \in \mathbb{Z}[x]$. [Hint: for the forward direction, suppose α is an algebraic integer and let $g \in \mathbb{Z}[x]$ be a monic polynomial having α as a root. Use that in $\mathbb{Q}[x]$, we have $g = fh$ for some h.]
   (c) Let D be a positive square-free integer, and recall that $\mathbb{Q}[\sqrt{D}] = \{a + b\sqrt{D} \colon a, b \in \mathbb{Q}\}$. Prove the following. If D is congruent to 2 or 3 modulo 4, then the set of algebraic integers in $\mathbb{Q}[\sqrt{D}]$ is $\{a + b\sqrt{D} \colon a, b \in \mathbb{Z}\}$. If $D \equiv 1 \pmod 4$, then the set of algebraic integers in $\mathbb{Q}[\sqrt{D}]$ is $\{a + b((-1+\sqrt{D})/2) \colon a, b \in \mathbb{Z}\}$. [Hint: Show that $r + s\sqrt{D}$ is a root of $x^2 - 2rx + (r^2 - Ds^2)$, and apply part (b).]
5. [IR 6.8] Let $\omega = e^{2\pi i/3}$ and recall that ω is a root of $\omega^3 - 1$. Show that $(2\omega+1)^2 = -3$ and use this to determine $\left(\frac{-3}{p}\right)$ by the new method of congruence over the algebraic integers (see Section 6.2 in the text). [Hint: begin by raising both sides to the power $(p-1)/2$.]
6. [IR 6.16] Let $f \in \mathbb{Q}[z]$ be a monic, irreducible polynomial. Show that f has distinct roots over $\mathbb{C}$. [Hint: if $f = (x-\alpha)^2 g$ for some $\alpha \in \mathbb{C}$, then show that $f'(\alpha) = 0$ where f' is the derivative of f.]
7. [IR 6.19] Find the conjugates of $\cos(2\pi/5)$.