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

1. [IR 2.1] Let k be a finite field. Show that $k[x]$ has infinitely many irreducible polynomials.
2. [IR 2.21] Define $f(n)$ to be $\ln p$ when n is a positive power of some prime p and 0 otherwise. For example, $f(2) = f(4) = f(8) = \ln 2$ and $f(3) = f(9) = f(27) = \ln 3$ but $f(1) = f(6) = f(10) = 0$. Prove that $f(n) = \sum_{d|n} \mu(n/d) \ln d$. Hint: first calculate $\sum_{d|n} f(d)$ and then apply Möbius inversion.
3. [IR 2.25, 2.26(a)] Consider the *Riemann zeta function* $\zeta(s)$, defined by $\zeta(s) = \sum_{n\geq 1} \frac{1}{n^s}$. Note: by "formal identity", we mean an identity of formal power series.
   (a) Prove the formal identity $\zeta(s) = \prod_p \frac{1}{1-p^{-s}}$.
   (b) Prove the formal identity $\zeta(s)^{-1} = \sum_{n\geq 1} \frac{\mu(n)}{n^s}$.
4. [IR 2.27] A beautiful proof that $\sum_p 1/p$ diverges. Let S_n be the set of square-free integers in $\{1, 2, \ldots, n\}$. It may help to recall the following: $\sum_{j=1}^{n} 1/j \geq \ln(n+1)$ and $\sum_{j=1}^{\infty} 1/j^2 = \pi^2/6$.
   (a) We have seen that for each positive integer n, there exist integers a and b such that a is square-free and $n = ab^2$. Prove that a and b are determined by n.
   (b) Without using that $\sum_p 1/p$ diverges (or the proof of this fact that we saw in class), show that $\sum_{j\in S_n} 1/j \geq \frac{6}{\pi^2} \ln(n + 1)$.
   (c) Conclude that $\prod_{p\leq n}(1 + 1/p) \geq \frac{6}{\pi^2} \ln(n + 1)$.
   (d) Since $e^x \geq 1 + x$, conclude that $\sum_{p\leq n} 1/p \geq \ln \ln(n + 1) - \ln \frac{\pi^2}{6}$.
5. [IR 3.{4,5}] Show that the following equations have no integer solutions.
   (a) $3x^2 + 2 = y^2$
   (b) $7x^3 + 2 = y^3$
6. [IR 3.{12,13}] Recall that for a nonnegative integer n and elements x, y of a ring, we have that $(x + y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$, where $\binom{n}{k} = \frac{n!}{k!(n-k)!}$.
   (a) Let p be a prime. Show that if $1 \leq k \leq p-1$, then $p \mid \binom{p}{k}$. Deduce that $(a+1)^p \equiv a^p+1 \pmod{p}$.
   (b) Use (a) to give another proof of Fermat's theorem, $a^{p-1} \equiv 1 \pmod{p}$ if $p \nmid a$.
7. [IR 3.{23,24}] Extend the notion of congruence to a ring and prove the following.
   (a) $a + bi$ is congruent to 0 or 1 modulo $1 + i$ in $\mathbb{Z}[i]$.
   (b) $a + b\omega$ is congruent to -1, 0, or 1 modulo $1 - \omega$ in $\mathbb{Z}[\omega]$. Conclude that for all $\alpha \in \mathbb{Z}[\omega]$, we have that $\alpha^3 \equiv \alpha \pmod{\lambda}$.
8. [IR 3.{25,26}] Let $\lambda = 1 - \omega \in \mathbb{Z}[\omega]$.
   (a) Prove that if $\alpha \in \mathbb{Z}[\omega]$ and $\alpha \equiv 1 \pmod{\lambda}$, then $\alpha^3 \equiv 1 \pmod{9}$. Hint: show first that $3 = -\omega^2\lambda^2$.
   (b) Use (a) to show that if $\beta, \gamma, \delta \in \mathbb{Z}[\omega]$ are not zero and $\beta^3 + \gamma^3 + \delta^3 = 0$, then λ divides at least one element in $\{\beta, \gamma, \delta\}$.