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

1. [IR 4.{21,4,6}]
   (a) Let g be a primitive root modulo m. Show that the order of g^s in $U(\mathbb{Z}/m\mathbb{Z})$ is $\phi(m)/\gcd(s, \phi(m))$.
   (b) Let p be a prime of the form $4t+1$. Prove that a is a primitive root modulo p if and only if $-a$ is a primitive root modulo p.
   (c) Prove that if p is prime and equals $2^n + 1$ for $n \geq 2$ (i.e. p is a Fermat prime), then 3 is a primitive root modulo p. *Hint*: First show that if 3 is not a primitive root, then $-3 \equiv a^2 \pmod{p}$ for some a. Next, show that there is an integer u such that $2u \equiv -1+a \pmod{p}$ and then argue that u has order 3 in $U(\mathbb{Z}/p\mathbb{Z})$. Apply Lagrange's theorem to the subgroup generated by u.
2. [IR 4.11] Prove that $1^k + 2^k + \cdots + (p-1)^k$ is congruent to 0 modulo p if $p - 1 \nmid k$ and congruent to -1 modulo p if $p-1 \mid k$.
3. [IR 4.19] Determine, without resorting to exhaustive case analysis, the numbers a such that $x^3 \equiv a \pmod{p}$ is solvable for $p \in \{7, 11, 13\}$.
4. [IR 4.22] Show that if a has order 3 modulo p, then $1 + a$ has order 6 modulo p.
5. [IR 5.3] Suppose that $p \nmid a$. Show that the number of solutions to $ax^2 + bx + c \equiv 0 \pmod{p}$ is given by $1 + \left(\frac{b^2-4ac}{p}\right)$.
6. [IR 5.{6,7,8}] Let p be an odd prime.
   (a) Show that the number of solutions to $x^2 - y^2 \equiv a \pmod{p}$ is given by $\sum_{y=0}^{p-1}(1+\left(\frac{y^2+a}{p}\right))$.
   (b) By calculating directly show that the number of solutions to $x^2 - y^2 \equiv a \pmod{p}$ is $p-1$ if $p \nmid a$ and $2p-1$ if $p \mid a$. Hint: use the change of variables $u = x + y$ and $v = x - y$.
   (c) Using (a) and (b), show that
$$\sum_{y=0}^{p-1}\left(\frac{y^2+a}{p}\right) = \begin{cases} -1 & \text{if } p \nmid a \\ p-1 & \text{if } p \mid a \end{cases}.$$
7. [IR 5.13]
   (a) Show that any prime divisor of $x^4 - x^2 + 1$ is congruent to 1 modulo 12. Hint: show that if $p \mid x^4 - x^2 + 1$, then $x^6 \equiv -1 \pmod{p}$. What is the order of x?
   (b) Use part (a) to show that there are infinitely primes congruent to 1 modulo 12.
8. [IR 5.16] Using quadratic reciprocity find the primes for which 7 is a quadratic residue; do the same for 15.
9. [IR 5.{23,24}] Let p be a prime congruent to 1 modulo 4.
   (a) Show that there exist integers s and t such that $pt = s^2 + 1$. Conclude that p is not a prime in $\mathbb{Z}[i]$.
   (b) Show that p is the sum of two squares; that is, $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$. Hint: let $p = \alpha\beta$ for nonunit $\alpha, \beta \in \mathbb{Z}[i]$. Take the magnitude-squared of both sides, and recall the characterization of the units in $\mathbb{Z}[i]$.