1. Show that the following diophantine equations have no integer solutions by using modular arithmetic.

$$y^5 + 6 = x^2 + 11x$$

$$y^6 - y = x^2 + 1$$

2. Suppose you wanted to determine the integer solutions to the equation

$$y^5 = x^2 - 1$$

Outline an approach to this problem. If it helps, only consider the case where y is an odd number. Hint: $x^2 - 1 = (x + 1)(x - 1)$.

3. In general a diophantine equation of the form

$$y^d = f(x)$$

for a polynomial $f(x)$ with integer coefficients is called a *hyperelliptic equation*. Can you outline a general approach to these equations along the lines of your answer to the previous question?

Hint: first think about $y^5 = x^2 + 1$ and what you would want to do in order to treat it as being analogous to $y^5 = x^2 - 1$.

4. Recall the classical statement of quadratic reciprocity:

(Quadratic Reciprocity) Given two odd (positive) prime numbers p and q, define $q^* = -q$ if $q = 3 \bmod 4$ and $q^* = q$ otherwise.

Then p is a square modulo q if and only if q^* is a square mod p.

Using this fact, determine whether or not p is a square mod q for the following:

$$p = 3, q = 103 \qquad p = 5, q = 42491 \qquad p = 7, q = 773$$

5. About a month ago, we proved the following fact:

If p is a prime number, then there is some number $\bar{a}$ mod p such that every nonzero number mod p can be written as a power of $\bar{a}$. (In other words, the list $\bar{a}, \bar{a}^2, \bar{a}^3, ...$ eventually includes all of $\bar{1}, \bar{2}, ..., \overline{p-1}$). Additionally, we know that $\bar{a}^{p-1} = \bar{1}$.

(a) If p is an odd prime, then $p - 1$ is even, so $\frac{p-1}{2}$ is an integer.

Show that $\bar{b} = \bar{a}^{\frac{p-1}{2}} = -1$. Hint: show that $\bar{b}^2 = 1$, in other words $\bar{b}$ is a root of $x^2 - 1 = (x + 1)(x - 1)$, so $\bar{b} = 1$ or $\bar{b} = -1$. Why is $\bar{b} \neq 1$?

(b) Along the same lines as (a), suppose that $p = 1$ mod 4, and so $\frac{p-1}{4}$ is an integer. Show that $\bar{b} = \bar{a}^{\frac{p-1}{4}}$ is a square root of -1. In other words, we can think of it as being similar to the imaginary number i.

6. Suppose that $p = 3$ mod 4. Show that, in contrast to 5(b), *there is no $\bar{b}$ modulo p such that $\bar{b}^2 = -1$*. In other words, there is no number like i in the integers mod p when $p = 3$ mod 4.

Hint: we can write $\bar{b} = \bar{a}^k$ for some integer k between 1 and $p-1$. But then

$$-1 = \bar{b}^2 = (\bar{a}^k)^2 = \bar{a}^{2k}$$

On the other hand, $-1 = \bar{a}^{\frac{p-1}{2}}$. Since k is between 1 and $p-1$, and we can always modify exponents by $p-1$, this means that either $2k = \frac{p-1}{2}$ or $2k - (p-1) = \frac{p-1}{2}$. Show that this is incompatible with $p = 3$ mod 4.

7. Summarize the Chinese Remainder Theorem in your own words. Apply it to decompose the integers modulo $n = 45$.

8. (challenge problem) Let p be an odd prime. Let $(\mathbb{Z}/p^2\mathbb{Z})^*$ be the elements $\bar{a}$ of $\mathbb{Z}/p^2\mathbb{Z}$ such that a is not divisible by p. Show that $(\mathbb{Z}/p^2\mathbb{Z})^*$ can be multiplicatively generated by one element. Can you extend your proof to p^3? What happens for $p = 2$?

Hint: Start with an element $\bar{a}$ such that when it is further reduced to an integer mod p that $\bar{a}$ generates by multiplication everything in $(\mathbb{Z}/p\mathbb{Z})^*$. What does this mean about the powers of the original $\bar{a}$ modulo p^2?

9. Briefly explain in your own words how modular arithmetic helps you study questions in number theory.

10. Briefly explain in your own words how the complex integers help you study questions in number theory.

11. (challenge) Write out a complete multiplication and addition table for $\mathbb{Z}[i]/3\mathbb{Z}[i]$, the complex integers mod 3. Is it a field?

12. (challenge) Write out a complete multiplication and addition table for $\mathbb{Z}[i]/2\mathbb{Z}[i]$, the complex integers mod 2. Do you notice anything interesting? Is it a field?