Instructions: Complete all problems from the list below. This assignment will be due on Gradescope no later than **7pm on Wednesday, October 12th**. Late work will not be accepted. There will be no exceptions for technology issues, so I suggest you upload your homework at least one hour before the deadline. Please make sure you've done all of the following before submitting your work:

* **Do not** write your name anywhere on your submission. Gradescope will keep track of your submission, and will allow me to use a blind grading process.
* Type your homework using LaTeX.
* Write up proofs formally and completely.
* If you use any resources (stackexchange, tutors, friends), please include a list of references in your writeup.

Chapter 3 Problems:

11. This problem will help finish the proof of Theorem 3.19: show that for any prime p and integer $\alpha \geq 1$, if $x^2 \equiv 1 (\mathrm{mod}\, p^\alpha)$ then $x \equiv \pm 1 (\mathrm{mod}\, p^\alpha)$.

12. This problem will also help to finish the proof of Theorem 3.19: show that for any prime p and integer $\alpha \geq 1$, $p+1$ has order $p^{\alpha-1}$ in $(\mathbb{Z}/p\mathbb{Z})^\times$. (Hint: use the binomial theorem).

14. Use the Miller-Rabin test to determine which of the following integers are prime with at least 99% accuracy. For those that are composite, provide a Miller-Rabin witness.

    a) $n = 294409$

    b) $n = 294439$

    c) $n = 118901509$

    d) $n = 118915387$

15. Use the Lucas-Lehmer test to show that the Mersenne numbers M_n are prime when $n = 17$ and $n = 19$.

Chapter 4 Problems:

3. Show that the only integral solution to $X^2 + Y^2 = (4a+3)Z^2$ is $(0,0,0)$ for any $a \in \mathbb{Z}$.

4. Show that the Mordell equation $Y^2 = X^3 - 5$ has no integral solutions. *(Hint: rewrite this equation as $Y^2 + 4 = X^3 - 1$ and look modulo 4).*

Bonus Problem: Is there a characterization of the solution set of a linear Diophantine equation in n variables, similar to the characterization in two variables from Theorem 4.1? Please provide and statement and either a proof or a reference.