Due Date: Thursday, November 3 at 5PM EDT

Carefully read and provide solutions to the problems below, showing all work required to justify any conclusions you make. You are encouraged to collaborate with your classmates, but all solutions turned in should be your own work. If you do collaborate, please record the names of those other students on your submitted work. Finally, your work should be submitted as a PDF on Gradescope before the listed due date.

Textbook problems: 24.1, 24.2, 24.3, 25.1

Optional, but recommended: 25.6

Problem 1. (Lecture 10.1, Exercise 2c) Prove that if n is odd and $n = x^2 + y^2$ for some $x, y \in \mathbb{Z}$, then either n is a square or some prime factor of n is congruent to 1 mod 4.

Problem 2. In this problem, you will develop an alternative proof to the statement

$$\text{“If } p \equiv 1 \pmod 4 \text{ then } p = x^2 + y^2 \text{ for some } x, y \in \mathbb{Z}.\text{”}$$

(a) Starting with a solution to $x^2 \equiv -1 \pmod p$, prove that there are integers $0 < u, v < \sqrt{p}$ satisfying $xu \equiv \pm v \pmod p$. *Hint: show that the set* $\{xu - v \mid 0 \leq u, v < \sqrt{p}\}$ *has more than* p *elements.*

(b) Prove that if u and v are the integers you found in part (a), then $u^2 + v^2 = p$.