

Math 453: Homework # 9

Due Friday, 29 March 2019 in class

In writing your proofs, fully explain all the important steps. Use full and grammatically correct English sentences. Be clear and concise.

Exercise numbers are from the end-of-section exercise sets in the **2002** reissue of *Elementary Number Theory* by James K. Strayer.

1. (5 points) Exercise Set 4.1, # **6**

2. (5 points) Exercise Set 4.1, # **7 (a) and (b)** *Hint for (b):* One way to approach this is to use the fact that the sum $1^2 + 2^2 + 3^2 + \cdots + (p-1)^2$ can be split into the sum of squares of the quadratic residues, plus the sum of the squares of the quadratic nonresidues. To express the quadratic nonresidues in terms of the quadratic residues, you may use the following lemma, even though we haven't proved it yet. (The proof of this lemma is not so difficult.)

Lemma: *Let a be a fixed quadratic nonresidue modulo p . For every quadratic residue e modulo p , the integer ae is a quadratic nonresidue modulo p .*

3. (5 points) Exercise Set 4.1, # **8**

4. (5 points) Exercise Set 4.2, # **15** (Hint: Euler's Criterion can be useful.)

5. (5 points) Exercise Set 4.2, # **18**