Sample questions for Exam 3
Math 126, Spring 2015

Our class has now diverged significantly from what I have done in previous classes, so this sample exam is merely a guideline and should not be considered to be representative in either content or style.

1. (12 points) Let p be an odd prime.

(a) Let a be an integer such that $\gcd(a, p) = 1$. Define what it means for a to be a quadratic residue mod p.

(b) State the Quadratic Residue Multiplication Rule. (This describes the result of multiplying two quadratic residues, etc.)

2. (12 points) Find an integer x such that $0 \leq x \leq 24$ and $x^7 \equiv 4 \pmod{25}$. Show all your work.

3. (20 points) Suppose we are using the RSA algorithm with modulus $m = 187 = 11 \cdot 17$. Note that

$$\begin{aligned} 160 \cdot 5 &= 800, && (1) \\ 9 \cdot 89 &= 801, && (2) \\ 89 &= 64 + 16 + 8 + 1, && (3) \\ 9 &= 8 + 1. && (4) \end{aligned}$$

Suppose $\gcd(a, 187) = 1$, and suppose someone sends the message a as the encoded message $b = a^9$. In a few sentences and equations, briefly **EXPLAIN:**

- How to decode the encoded message $b = a^9$ to recover the original message a; and
- Why the decoding method you describe works.

In particular:

- If at some point you employ the method of successive squaring, **EXPLAIN** how that would work in this example.
- If you use any of the equations (1)–(4), indicate how each equation is used. ("By (2), we have that...")

4. (12 points) **PROOF QUESTION.** Let p be an odd prime, let b be an integer, and suppose that p divides $b^2 + 2$. Prove that either $p \equiv 1 \pmod 8$ or $p \equiv 3 \pmod 8$.