Math 435 Number Theory I
Sample Problems–Midterm 2

Midterm 2 will cover chapters 4–7.4 of Jones and Jones. You should be able to apply quadratic reciprocity but are not responsible for the proof. It may also cover material on public key cryptography and the Rabin-Miller primality test. Notes for this material is on the webpage

`http://www.math.uic.edu/~marker/math435/435comp.pdf`

`http://www.math.uic.edu/~marker/math435/rm.pdf`

I have also posted a list of key concepts and results that you should be familiar with

`http://www.math.uic.edu/~marker/math435/concepts.html`

and a week-by-week syllabus with reading assignments

`http://www.math.uic.edu/~marker/math435/wtw.html`

The questions below are representative of the type of questions I might ask. (Note: This sample is **much** longer than the exam will be.)

1) State the Quadratic Reciprocity Theorem.

2) Define the following concepts.
g is a primitive root in U_n

3) State Fermat's Little Theorem and sketch a proof.

4) Give a brief explanation of RSA public key cryptography.

5) Decide if the following statements are TRUE or FALSE if FALSE give a counterexample or an explanation as to why they are FALSE.
a) -1 is a square mod 23
b) 2 is a square mod 23
c) The group U_n is cyclic for all n.
d) If $x^2 \equiv 1 \pmod{n}$, then $x \equiv \pm 1 \pmod{n}$.

6) Let $f(X) = X^2 + 3X - 10$. Note that $f(4) = 18 \equiv 0 \pmod{9}$. Find x such that $x \equiv 4 \pmod{9}$ and $f(x) \equiv 0 \pmod{27}$.

7) Prove 3 is a primitive root mod 17.

8) Solve $X^{27} \equiv 5 \pmod{41}$.

9) Calcuate $3^{323} \text{mod } 17$.

10) Calculate $\phi(425)$.

11) Calculate $\left(\frac{5}{13}\right)$ using Gauss's Lemma and Euler's crierion.

12) Calculate $\left(\frac{23}{53}\right)$

13) Suppose $p > 2$ is prime.

a) Prove that $(p-2)! \equiv 1 \pmod{p}$.

b) Prove that $(p-3)! \equiv \frac{p-1}{2} \pmod{p}$. [Hint: It might be useful to prove that $(-2)^{-1} = \frac{p-1}{2} \pmod{p}$.]

14) Prove that $\phi(nm) \geq \phi(n)\phi(m)$ for all $n, m \geq 2$.