MATH 573 — SECOND MIDTERM EXAM
(IN CLASS PORTION)

May 17, 2007

NAME: ____

1. Do not open this exam until you are told to begin.
2. This exam has 5 pages including this cover. There are 4 problems.
3. Do not separate the pages of the exam.
4. Your proofs should be neat and legible. You may and should use the back of pages for scrap work.
5. If you are unsure whether you can quote a result from class or the book, please ask.
6. Please turn **off** all cell phones.

PROBLEM	POINTS	SCORE
1	12	
2	16	
3	10	
4	12	
TOTAL	50	

1. (3 points each) In this problem we will work with the elliptic curve $E_{21} : y^2 = x^3 - 441x$.

(a) If we reduce this curve modulo 5 is the resulting curve nonsingular? If so, prove it. If not, give a singular point.

(b) Though we only defined $a_{E_N,p}$ for primes where $\overline{E}_N$ is an elliptic curve, we can use the exact same definition to define $a_{E_N,p}$ for primes where $\overline{E}_N$ is not an elliptic curve. Keeping this in mind, compute $a_{E_{21},5}$.

(c) Show that the point $(-3, 36)$ is on the curve E_N.

(d) Prove that the number 21 is a congruent number.

2. (4 points each) Let $n > 1$ and $a \in \mathbb{Z}$ so that $\gcd(a, n) = 1$.

(a) Define $\mathrm{ord}_n(a)$.

(b) Prove that $a^h \equiv 1 (\bmod n)$ if and only if $\mathrm{ord}_n(a) \mid h$.

(c) Prove that $a^i \equiv a^j (\bmod n)$ if and only if $i \equiv j (\bmod \mathrm{ord}_n(a))$.

(c) Prove that $\{a, a^2, \ldots, a^{\mathrm{ord}_n(a)}\}$ are all incongruent modulo n.

3. (10 points) Does the congruence $x^2 \equiv 60 \pmod{83}$ have a solution? Be sure to justify your answer as a "yes" or "no" with no justification will receive 0!

4. (4+8 points) **(a)** Prove that $\left(\frac{a^2}{p}\right) = 1$ for all a with $p \nmid a$.

(b) If $p > 7$ is a prime, prove that there are at least 2 consecutive quadratic residues modulo p. (Hint: Consider 4 and 9. Look at the cases $\left(\frac{5}{p}\right) = 1$ and $\left(\frac{5}{p}\right) = -1$.)