MATH 573 — SECOND MIDTERM EXAM
(TAKE HOME PORTION)

May 17, 2007

NAME: ____

1. This exam is due Monday, May 21 before the bell rings for class. After the bell rings I will NOT accept the exam.
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. You are welcome to use any non-human sources you choose. (Note, talking to someone on the phone, over the internet, etc. falls under getting human help.) Be sure to cite your sources as unacknowledged sources constitute plagarism and will receive 0 points.

PROBLEM	POINTS	SCORE
1	10	
2	14	
3	16	
4	10	
TOTAL	50	

1.(10 points) Let p and q be odd primes. Define $\epsilon_p = (-1)^{(p-1)/2}$. Prove that $\epsilon_p p$ is a square modulo q if and only if q is a square modulo p.

2. (2+2+5+5 points each) Consider the elliptic curve $E_{161} : y^2 = x^3 - 161^2 x$.

(a) What is the rank of E_{161}?

(b) What are the elements of $E_{161}(\mathbb{Q})_{\mathrm{tors}}$?

(c) Compute $a_{E_{161},n}$ for $1 \leq n \leq 25$. (This does not have to be done by hand!) Use these values to estimate $L(E_{161}, 1)$.

(d) Is 161 a congruent number? If so, find a triangle with rational sides and area 161.

3. (4 points each) In this problem you show that $\frac{x^2-2}{2y^2+3}$ is not an integer for any integers x, y. Suppose that there exists $x, y \in \mathbb{Z}$ so that $\frac{x^2-2}{2y^2+3} \in \mathbb{Z}$.

(a) Show that if p is a prime with $p \mid 2y^2 + 3$, then necessarily $p \equiv \pm 1 \pmod 8$.

(b) Show that $2y^2 + 3 \equiv \pm 1 \pmod 8$.

(c) Show $2 \nmid y$.

(d) Use the previous results in this problem to reach a contradiction, showing that $\frac{x^2-2}{2y^2+3} \notin \mathbb{Z}$ for any $x, y \in \mathbb{Z}$. (Using (c), what form must y be? Use this!)

4. (5+5 points) **(a)** Let p be a prime and let a be an integer so that $\mathrm{ord}_p(a) = 3$. Prove that $1 + a + a^2 \equiv 0 (\bmod p)$.

(b) Prove that $\mathrm{ord}_p(1 + a) = 6$.