MATH 573 — FIRST MIDTERM EXAM

April 18, 2007

NAME: ______________________________

1. Do not open this exam until you are told to begin.
2. This exam has 9 pages including this cover. There are 8 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	10	
2	15	
3	10	
4	10	
5	10	
6	10	
7	20	
8	15	
TOTAL	100	

1.(4+6 points) **(a)** For integers a and b, define the greatest common divisor of a and b.

(b) Prove that $\gcd(a, a+b) = d$ if and only if $\gcd(a, b) = d$.

2. (15 points) Find the simultaneous solutions to the congruences:

$$\begin{aligned} 11x &\equiv 4 \pmod{25} \\ 5x &\equiv 13 \pmod{17} \end{aligned}$$

Be sure to show all your work! Writing down an answer without the steps to arrive at it will receive 0 points!

3. (10 points) Find all solutions to the equation $\phi(n) = 2p$ for n a positive integer and p a prime. Be sure to prove that your list contains all possible solutions. Note a solution is a pair (n, p) for which the equation holds.

4. (10 points) Prove that 5 divides $9 \cdot 2^{4n} + 1$ for every positive integer n.

5. (10 points) Let p be an odd prime and k an integer with $1 \leq k \leq p-2$. Prove that $\binom{p-1}{k} \equiv (-1)^k \pmod{p}$.

6. (10 points) Let p be a prime and suppose that $p|(a^2+b^2)$ for some relatively prime integers a and b. Prove that p must be the sum of two squares.

7. (20 points) Explain the RSA public-key cryptosystem. Your explanation should include why such a system is important and how the system works, including relevant mathematics.

8. (15 points) Find all integer solutions of the equation $x^2 + 3y^2 = 5z^n$ for $n \in \mathbb{Z}_{\geq 1}$. Be sure to prove these are all the solutions!