INTRODUCTION TO NUMBER THEORY
Exam 1
February 20, 2009

The point value of each problem is given in the margin.

(12) 1. Find the general solution of the linear equation $21x - 15y = 66$, in integers $x, y$.

(12) 2. Use properties of congruences to compute the least residue of the following numbers (mod 5). (Avoid big numbers.)
   (a) $5503 \cdot 69 + 72$

   (b) $78^2 + 72^5$

   (c) $2^{1001}$
3. a) State the well ordering axiom of the natural numbers.

b) Define \( a \equiv b \pmod{m} \):

c) State the three properties showing that congruence \( \pmod{m} \) is an equivalence relationship.

d) Using the fast Euclidean algorithm what is the largest number of steps required to calculate \( \gcd(a, b) \) if \( 1 \leq a, b \leq 1024 = 2^{10} \). (roughly)

e) Suppose that \( \text{lcm}[a, b] = ab \). What can you say about \( \gcd(a, b) \)?

4. Prove the following theorem. If \( a, b, d, x, y \) are integers such that \( d|a \) and \( d|b \) then \( d|(ax + by) \).
5. Let $a = 2^35^47^2$, $b = 2^55^2$. Find the following.

(i) $\gcd(a^2, b) =$ The prime factorization will do!

(ii) $\text{lcm}[a, b] =$ Same comment.

(iii) The value $e$ such that $5^e \mid (a - b)$

6. True, False. Circle T or F. All variables are integers.

T  F  a) If $a \mid bc$ and $\gcd(a, b) = 1$ then $a \mid c$.

T  F  b) If $a \mid b$ and $a \mid c$ then $a^2 \mid bc$.

T  F  c) If $p$ is a prime and $p \mid b^2$ then $p \mid b$.

T  F  d) If $a \equiv b \pmod{m^2}$ then $m \mid (a - b)$.

T  F  e) If $p, q$ are distinct primes then the equation $px + qy = 8$ always has an integer solution.
(10) 7. Prove by induction that the sum of the first $n$ odd numbers is $n^2$, that is $\sum_{k=1}^{n}(2k-1) = n^2$, for any positive integer $n$.

(10) 8. Prove one of the following: a) For any integers $a, b, q$, $\gcd(a - qb, b) = \gcd(a, b)$.

b) The uniqueness part of the Fundamental Theorem of Arithmetic. (You may assume the key lemma needed for this proof.)