Math 430-001 (Ellis) **Group Activity 1: Divisibility** Fall 2008

Group Members: ____

Defn. Let $t, s \in \mathbb{Z}$ be integers; t is a *divisor* of s ("t divides s," "$t|s$") if there is an integer u such that $s = t \cdot u$.

(1a) Write the positive divisors of 12.

(1b) Write the negative divisors of 75.

(1c) Write the set of numbers which 0 divides.

(1d) Write the set of numbers which divide 0.

Defn. A *prime* number is a positive integer $p > 1$ such that the only positive divisors of p are 1 and p.

(2) Quickly list all prime numbers between 1 and 60, inclusive. (Hint: share the work.)

Theorem 0.1. Division Algorithm. Let a and b be integers with $b > 0$. Then there exist unique integers q and r with the property that $a = bq + r$, where $0 \leq r < b$.

(3a) Let $a = 45$, $b = 15$. Find the values of q such that $a - bq$ is closest to 0.

q	$\cdots$								$\cdots$
$45 - 15q$	$\cdots$								$\cdots$

(3b) Let $a = 18$, $b = 5$. Find the values of q such that $a - bq$ is closest to 0.

q	$\cdots$								$\cdots$
$18 - 5q$	$\cdots$								$\cdots$

(3c) Let $a = -34$, $b = 6$. Find the values of q such that $a - bq$ is closest to 0.

q	$\cdots$								$\cdots$
$-34 - 6q$	$\cdots$								$\cdots$

(3d) How do we get q and r for the division algorithm from this data? Be precise.

Break I. Well Ordering Principle and existence proof for the division algorithm.

Defn. The *greatest common divisor (gcd)* of two nonzero integers a and b is the largest integer d which divides both a and b. If $\gcd(a, b) = 1$, then we say that a and b are *relatively prime*.

(4a) Name or briefly describe two distinct methods for computing $\gcd(a, b)$.

(4b) Compute $\gcd(60, 490)$ with the first method and $\gcd(-130, 56)$ with the second method.

(Continue to back of page)

Defn. An *integer linear combination* of two integers a and b is some $as + bt$, where s, t are integers.

(5a) Find 3 integer linear combinations of 60 and 490 as close to 0 as possible.

(5b) Find 3 integer linear combinations of -130 and 56 as close to 0 as possible.

(6) Back-solve one of the methods in problem (4b) to get the gcd as an integer linear combination of a and b.

Theorem 0.2. GCD as a Linear Combination. For any nonzero a and b, there exist integers s and t such that $\gcd(a, b) = as + bt$. Moreover, $\gcd(a, b)$ is the smallest positive integer of the form $as + bt$.

Break II. Well Ordering Principle, gcd as an integer linear combination, Euclid's lemma, Fund. Thm. of Arithmetic.

Modular Arithmetic

Defn. Let a and b be integers with $b > 0$. We define a mod b to be the remainder r obtained by dividing a by b in the Division Algorithm.

(7a) Compute a mod 4 for various values of a and complete the table.

a	-3	-2	-1	0	1	2	3	4	5
$a \bmod 4$									
$a - (a \bmod 4)$									

(7b) Make a conjecture from the data generated in third row.

Proposition (Modular computation shortcuts). Let a, b, and n be integers with $n > 0$. Let $a' = a \bmod n$ and $b' = b \bmod n$. Then
(i) $(a + b) \bmod n = (a' + b') \bmod n$, and
(ii) $ab \bmod n = a'b' \bmod n$.

(8) Use the above to compute $(248881 + 100642) \bmod n$ and $(248881 \cdot 100642) \bmod n$.

Mathematical Induction

Theorem 0.4. First Principle of Mathematical Induction. Let S be a set of integers containing a. Suppose S has the property that whenever some integer $n \geq a$ belongs to S, then the integer $n + 1$ also belongs to S. Then, S contains every integer greater than or equal to a.

Theorem 0.5. Second Principle of Mathematical Induction. Let S be a set of integers containing a. Suppose S has the property that n belongs to S whenever every integer les than n and greater than or equal to a belongs to S. Then, S contains every integer greater than or equal to a.

(9) (Write on attached sheet.) Carefully prove using induction that for every positive integer n, $1 + 2 + \cdots + n = n(n + 1)/2$.

(10) Find the largest value of postage which cannot be composed of 4 cent and 9 cent stamps. Prove that this is the largest such value.