Name:_____

Test 2

Spring 2003

CS/MATH 2610

March 4, 2003

Directions : You have 75 minutes to complete all 7 problems on this exam. There are a possible 100 points to be earned. You may not use your book or any notes. Please be sure to show all pertinent work. *An answer with no work will receive very little credit!* If any portion of the exam is unclear please come to me and I will elaborate provided I can do so without giving away the problem.

(1) (20 points)

Let A be a set and let $a, b, m \in \mathbb{Z}$ with $m > 0$. Answer each of the following questions.

(a) Define what it means for A to be countably infinite.

(b) Define the statement $a \mid b$.

(c) Define $\gcd(a, b)$.

(d) What does it mean to say the integers $a_1, a_2, \ldots, a_n$ are pairwise prime?

(e) Define the statement $a \equiv b \pmod{m}$.

(2) (10 points)

(a) Convert the number 123 from decimal into binary.

(b) Convert the number $(237)_8$ from octal into decimal.

(3) (10 points)

Recall that Caesar's cipher is obtained by enumerating the letters as $A = 0$, $B = 1$, ..., $Z = 25$ and encoding messages by encoding the corresponding numbers by $f(p) = (p+3)$ (mod 26). Suppose that the message "BRY ZLQ" has been encoded with this cipher. Decode the message.

(4) (15 points)

Use the Euclidean Algorithm to compute $\gcd(135, 532)$. (You will receive very few points if you do not use the Euclidean Algorithm).

(5) (10 points)
Solve the following linear congruence.

$$135x \equiv 17 \pmod{532}$$

(6) (15 points)
Prove that if $a, b, c \in \mathbb{Z}$ so that $a \mid b$ and $a \mid (b + c)$, then $a \mid c$.

(7) (20 points)

Is there an integer x that leaves a remainder of 1 when divided by 3, leaves a remainder of 3 when divided by 4, and also leaves a remainder of 5 when divided by 7? If so why? (You can cite a theorem.) If there is more than one such number, what are they?