M328K Second Midterm Exam, April 11, 2003

1. In class we defined the binomial coefficients $\binom{n}{k}$ in four ways, and showed they were equivalent:
1) $\binom{n}{k}$ is the number of words of length n in the letters "a" and "b" with exactly k a's and $n-k$ b's.
2) $\binom{n}{k}$ is the number of ways to choose k items out of n, where the order does not matter,
3) $\binom{n}{k} = \frac{n!}{k!(n-k)!}$
4) $\binom{n}{k}$ is the coefficient of $a^k b^{n-k}$ in the expansion of $(a+b)^n$. That is, $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$.

Taking these properties as given, give a COMPLETE and RIGOROUS proof of the following theorem. [There are MANY ways to do this, some of which use property 1, some of which use property 2, and so on. You are free to use whatever approach you wish.]

Theorem: If $1 \le k \le n$, then $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$.

2. a) Error-correcting codes. Allan wants to send a 5×5 array $\{x_{ij}\}$ of binary digits to Betsy. He adds a check digit x_{i6} to each row and a check digit x_{6j} to each column, and an overall parity bit x_{66} to get a new 6×6 array with the property that, for each i and j, $\sum_i x_{ij} \equiv \sum_j x_{ij} \equiv 0 \pmod 2$.

In transmission, one mistake gets made, and Betsy receives the following array:

0	1	1	0	1	1
1	0	1	0	0	0
0	1	1	0	1	1
1	1	0	1	0	0
1	0	0	1	1	1
1	1	1	1	1	1

Find the mistake, fix it, and report the array that Allan actually sent.

3. Euler's theorem. For purposes of this problem, the phrase "find $x \pmod n$" means "Find a small integer that is congruent to x mod n." Let $y = 2^{84,123}$.

a) Find $y \pmod 3$ and $y \pmod 5$.

b) Use the Chinese Remainder Theorem and the results of part (a) to find $y \pmod{15}$. (You may want to check your results by computing $y \pmod{15}$ directly using Euler's theorem)

c) Find $\phi(175)$ and compute $y \pmod{175}$.

4. Multiplicative properties of $\phi(n)$. Recall that $\phi(n)$ is defined to be the

number of positive integers, less than or equal to n, that are relatively prime to n. Equivalently, $\phi(n)$ is the number of residue classes $\pmod{n}$ that have a multiplicative inverse. Prove property (a) about $\phi(n)$, below. For extra credit, prove property (b). You may NOT assume the formula for $\phi(\Pi_{j=1}^{k} p_j^{\alpha_j})$ that was proved in class. That formula was proved USING property (a).

a) If $(a, b) = 1$, then $\phi(ab) = \phi(a)\phi(b)$.

b) (Extra Credit) If $p_1, \ldots, p_k$ are distinct primes, then $\phi(p_1 p_2 \cdots p_k) = (p_1 - 1)(p_2 - 1) \cdots (p_k - 1)$.