M328K Second Midterm Exam Solutions, 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 $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$.

$\binom{n+1}{k}$ is the number of words of length $n+1$ with exactly k a's and $n+1-k$ b's. Each such word either ends with an a (and has $k-1$ other a's) or ends with a b (and has k other a's). There are $\binom{n}{k-1}$ words of the first type, since specifying a word of this type is tantamount to specifying its first n letters. Likewise, there are $\binom{n}{k}$ words of the second type, or $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$ words in all.

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.

Since the 4th row and the 4th column add up to 1 (mod 2), the error is in the (4,4) position. The 1 should be a zero.

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 $y \pmod 5$.

Since $\phi(3) = 2$ and $84,123 = 1 \pmod 2$, $y = 2^1 = 2 \pmod 3$. Since $\phi(5) = 4$ and $84,123 = 3 \pmod 3$, $y = 2^3 = 8 = 3 \pmod 5$.

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)

The only number (mod 15) that is 2 (mod 3) and 3 (mod 5) is 8.

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

$175 = 5^2 \times 7$, so $\phi(175 = 5(4)(6) = 120$. Since $84,123 = 3 \pmod{120}$, $y = 2^3 = 8 \pmod{175}$.

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 $\phi(ab) = \phi(a)\phi(b)$.

Step 1: We show that an integer x is relatively prime to ab if and only if it is relatively prime to a and to b. If $(x, ab) = 1$, then 1 is a linear combination of x and ab, so 1 is a linear combination of x and a, so $(a, x) = 1$. Likewise for (b, x). For the converse, suppose that $(a, x) = (b, x) = 1$. Let m be a common factor of x and ab. There is a prime p that divides m, and is therefore a common factor of x and ab. But if $p|ab$, then $p|a$ or $p|b$, in which case p would be a common factor of both x and a, or of both x and b, which is impossible since $(a, x) = (b, x) = 1$.

Step 2: We count the integers, less than or equal to ab, that are relatively prime to ab. By Step 1, these are the integers that are relatively prime to a and relatively prime to b. By the CRT, each such integer x corresponds to a unique pair (x mod a), (x mod b). There are $\phi(a)$ choices for (x mod a) and $\phi(b)$ choices for (x mod b), hence $\phi(a)\phi(b)$ choices in all.

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

This is induction on k, together with the fact that $\phi(p_j) = p_j - 1$. It

is true for $k = 1$ by Fermat. Suppose it is true for $k = n - 1$. Then $\phi(p_1 \cdots p_n) = \phi(p_1 \cdots p_{n-1} p_n) = \phi(p_1 \cdots p_{n-1})\phi(p_n)$, since p_n is relatively prime to $p_1 \cdots p_{n-1}$ (by part (a)). But $\phi(p_1 \cdots p_{n-1}) = (p_1 - 1) \cdots (p_{n-1} - 1)$ by the inductive hypothesis and $\phi(p_n) = p_n - 1$, so we are done.