M328K Final Exam Solutions, May 10, 2003

1. "Bibonacci" numbers. The Bibonacci numbers $b_1, b_2, \ldots$ are defined by $b_1 = 1$, $b_2 = 1$, and, for $n > 2$, $b_n = b_{n-1} + 2b_{n-2}$.

a) Prove that, for all positive integers n, $b_n \leq 2^{n-1}$.

The proof is by generalized induction. It is true for $n = 1$ and $n = 2$. Now suppose it is true for all n up to $k - 1$. Then $b_{n-1} \leq 2^{n-2}$ and $b_{n-2} \leq 2^{n-3}$, so $b_n = b_{n-1} + 2b_{n-2} \leq 2^{n-2} + 22^{n-3} = 2^{n-1}$.

b) Prove that, for all positive integers n, $b_n \geq 2^{n-2}$.

The proof is also by generalized induction. It is true for $n = 1$ and $n = 2$. Now suppose it is true for all n up to $k - 1$. Then $b_{n-1} \geq 2^{n-3}$ and $b_{n-2} \geq 2^{n-4}$, so $b_n = b_{n-1} + 2b_{n-2} \geq 2^{n-3} + 22^{n-4} = 2^{n-2}$.

Note: The exact formula works out to $b_n = (2^n - (-1)^n)/3$, which also can be proven by induction.

2. The following theorem-proof combination is erroneous. Find the errors (there are at least two). Then, rewrite the proof (and, if necessary, the statement of the theorem) so that it really does prove the theorem.

"Theorem" Every positive integer is divisible by a prime.

"Proof" Let n be a positive integer. If n is prime, then n is divisible by the prime n, and we are done. If n is composite, then $n = ab$, where a and b are integers less than n. If a is prime, then $a|n$, and we are done. If a is composite, write a as a product of two smaller integers, and examine the first of these. Repeat this process, dividing composite factors into products of still smaller factors, and examining the first sub-factor, until you get a factor that cannot be divided further, and is therefore prime.

The first error is that not all positive integers are prime or composite. The integer 1 is neither prime nor composite, and if n is equal to 1, then n *isn't* divisible by a prime. The second error is that we never show that the process of dividing into factors ever stops. Why can't you keep dividing into smaller factors forever without reaching a prime? The answer requires the Well-Ordering Principle.

Here is a corrected theorem, and two versions of the corrected proof, one using induction and the other using the well-ordering principle directly:

Theorem Every integer *greater than 1* is divisible by a prime.

Proof 1 We prove this by induction. It is true for $n = 2$, since $2|2$. Now suppose it is true for all n from 2 to $k - 1$. We must show that k is divisible by a prime. If k is prime, then k is divisible by the prime k, and we are done. If k is not prime, it must be composite, since $k > 1$. Thus $k = ab$, where a and b are integers less than k and greater than 1. By the inductive

hypothesis, a is divisible by a prime p, hence k is also divisible by p.

Proof 2 Let n be a positive integer greater than one. If n is prime, then n is divisible by the prime n, and we are done. If n is composite, then $n = a_1 b_1$, where a_1 and b_1 are integers less than n. If a_1 is prime, then $a_1|n$, and we are done. If a_1 is composite, write $a_1 = a_2 b_2$ as a product of two integers, each bigger than 1 and smaller than a_1, and examine the first factor a_2. Repeat this process, dividing composite factors into products of still smaller factors, and examining the first sub-factor. The set $\{a_1, a_2, \ldots\}$ is nonempty. By the Well-Ordering Principle, this set has a smallest elements a_k. This implies that a_k is prime, for if a_k were composite, a_{k+1} would exist and would be smaller than a_k. Since $a_k|a_{k-1}|\cdots|a_1|n$, n is divisible by a prime.

3. Matrix products. It is a known fact that, if A and B are matrices such that the product AB makes sense, then $(AB)^T = B^T A^T$. (That is, the transpose of the product is the product of the transposes, in the opposite order). Taking this fact as given, prove the following statement:

Claim: Let $n > 1$ and let $M_1, \ldots M_n$ be an ordered n-tuple of matrices such that the product $M_1 \cdots M_n$ is defined. Then $(M_1 \cdots M_n)^T = (M_n)^T \cdots (M_1)^T$, i.e., the transpose of the product is the product of the transposes with the order reversed.

This is yet another proof by induction on n. (In this case it is regular induction, not generalized induction). The base case is $n = 2$, which is given. Now suppose it is true for $n = k - 1$. Then $(M_1 \cdots M_{k-1})^T = M_{k-1}^T \cdots M_1^T$. Take $A = M_1 \cdots M_{k-1}$ and $B = M_k$. Then $(M_1 \cdots M_k)^T = (AB)^T = B^T A^T = M_k^T (M_{k-1}^T \cdots M_1^T) = M_k^T \cdots M_1^T$.

4. a) Find the greatest common factor of 50 and 76.

b) Write this number as a linear combination of 50 and 76.

Use the Euclidean algorithm:

$$\begin{array}{lll} & & 76 = 1(76) + 0(50) \\ & & 50 = 0(76) + 1(50) \\ 76 = 1(50) + 26 & 26 = 76 - 50 & 26 = 1(76) - 1(50) \\ 50 = 26 + 24 & 24 = 50 - 26 & 22 = -(76) + 2(50) \\ 64 = 24 + 2 & 2 = 26 - 24 & 2 = 2(76) - 3(50) \end{array}$$

So $(50, 76) = 2 = 2(76) - 3(50)$

c) Find all solutions, mod 76, of the equation $50x \equiv 18 \pmod{76}$.

Since $(-3)50 = 2 \pmod{76}$, we must have $-27(50) = 18 \pmod{76}$. The solution is only defined mod $76/(76, 50) = 38$, so the solutions mod 76 are 11 and 49.

5. a) Find all solutions, in the range $0 \leq x < 735$, to the following system of congruences.

$$\begin{aligned} x &\equiv 28 \pmod{49} \\ x &\equiv 12 \pmod{15} \end{aligned}$$

Use the Euclidean argument to get that $1 = 4(49) - 13(15) = 196 - 195$. A solution is therefore $x = 28(-195) + 12(196) = -3108 \equiv 567 \pmod{735}$.

b) Find all solutions, in the range $0 \leq x < 5005$, to the system of congruences

$$\begin{aligned} x &\equiv 3 \pmod{5} \\ x &\equiv 5 \pmod{7} \\ x &\equiv 2 \pmod{11} \\ x &\equiv 6 \pmod{13} \end{aligned}$$

Use the Euclidean algorithm on the first two equations to get $x = 33 \pmod{35}$. Combine that with the third equation to get $x = 68 \pmod{385}$. Combine that with the last equation to get $x = 838 \pmod{5005}$.

6. a) Compute $17^{883} \pmod{101}$. (Note that 101 is prime)

Since $\phi(101) = 100$, we only care about 883 (mod 100), so we can take the 83rd power instead of the 883rd. By successive squaring (and reduction mod 101), we have $17^1 = 17$, $17^2 = 87$, $17^4 = 95$, $17^8 = 36$, $17^{16} = 84$, $17^{32} = 87$, and $17^{64} = 95$. Then $17^{83} = 17^{64+16+2+1} = 95 * 84 * 87 * 17 = 65$

b) You are told that $y = x^{883} \pmod{101}$ and that $1 \leq x < 101$. Find a positive integer d such that $x = y^d \pmod{101}$.

We seek an inverse to 83 (mod 100). By the Euclidean algorithm (again!) we get $\bar{83} = 47$ (note that $47 \times 83 = 3901 \equiv 1 \pmod{100}$.) So $d = 47$.

c) If $y = 24$, what is x? By successive squaring, we get $x = 24^{47} = 31$ (mod 101). You can check directly, again by successive squaring, that $31^{83} = 24 \pmod{101}$.

7. Let $n = 8999271$. a) What is the prime factorization of n? (Hint: n is the product of more than two primes) You may use your calculators, but you may NOT use a "factor" key or function, and you MUST show how you did the factorization in order to receive credit.

It's clear that $9|n$, so we factor that out to get $n = 9m$, where $m = 999919$. Using Fermat's method we see that this is $1000^2 - 9^2 = 991 \times 1009$. Both 991 and 1009 are prime, so our factorization is $n = 3^2(991)(1009)$

b) Compute $\phi(n)$.

$\phi(n) = 3(3-1)(991-1)(1009-1) = 5987520$.

c) Somebody suggests coding numbers by $y = x^{17} \pmod{n}$, where x is relatively prime to n. Find a key that decodes this (i.e., a number k such that $x = y^k \pmod{n}$.

By the Euclidean argument, $\phi(n) = 352207(17)+1$, so $1 = \phi(n) - 352207$, so our answer is $-352207 \pmod{\phi(n)}$. The smallest positive representative is $k = \phi(n) - 352207 = 5,635,313$.

[In fact, the smaller key $k' = 55440$ will also work. $17k'$ isn't equal to 1 mod $\phi(n)$, but it is equal to 1 mod the least common multiple of 990, 1008 and 6, so taking things to the $17k'$ power preserves their residue class mod 9, mod 991, and mod 1009, and hence mod n.]