

M328K Final Exam, May 10, 2003

1. “Bibonacci” numbers. The Bibonacci numbers b_1, b_2, \dots 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 , $b_n \leq 2^{n-1}$.

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

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.

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, \dots, 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.

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

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

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

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

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

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

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

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

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

c) If $y = 24$, what is x ?

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.

b) Compute $\phi(n)$.

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 $x = y^k \pmod{n}$).