Math 126, Number Theory

First Test

22 Feb 2006

Your name: ____________________________

You may use one sheet of prepared notes and a calculator for the test. Points for each problem are in square brackets.

Problem 1. On divisors. [18; 6 points each part]

a. Draw the Hasse diagram of the divisors of $496 = 2^5 \cdot 31$.

b. What are the values of $d(496)$ and $\sigma(496)$.

c. Is the number 496 a perfect number? Why or why not?

Problem 2. On the Euclidean algorithm. [20; 10 points each part] The Euclidean algorithm shows that the greatest common divisor of 399 and 703 is 19. Here are the computations.

$$\begin{aligned} 703 - 399 &= 304 \\ 399 - 304 &= 95 \\ 304 - 3 \cdot 95 &= 19 \\ 95 - 5 \cdot 19 &= 0 \end{aligned}$$

a. Express 19 as a linear combination of 399 and 703.

b. Find all the integral solutions of the linear Diophantine equation $399x + 703y = 19$.

Problem 3. On divisibility. [15] Recall that we say that one positive integer a *divides* another b, written $a|b$, if there exists a third integer c such that $ac = b$. Carefully prove the following theorem. (Note that the theorem has two parts.)

Theorem. Let a, b, and d be positive integers. If $a|b$, then $ad|bd$. Conversely, if $ad|bd$ then $a|b$.

Problem 4. True or false. [15; 3 points each part] Just write the word "true" or the word "false". If it's not clear to you which it is, explain; otherwise no explanation is necessary.

_______ **a.** A function f defined for all positive integers is said to be multiplicative if $f(ab) = f(a)f(b)$ whenever $a|b$.

_______ **b.** If $a|c$ and $b|c$ then $(a+b)|c$.

_______ **c.** The principle of mathematical induction says that if (1) a property holds for the number 1, and (2) whenever it holds for a number it holds for the following number, then (3) it holds for all positive integers.

_______ **d.** The square root of any prime is an irrational number.

_______ **e.** One of the properties of greatest common divisors is that $((a,b),c) = (a,(b,c))$ for all positive integers a, b, and c.

Problem 5. On primes. [15] Here is a table for some of the values of the polynomial $f(n) = n^2 + n + 41$.

n	1	2	3	4	5	6	7	8	9	10	11
$f(n)$	43	47	53	61	71	83	97	113	131	151	173

All the entries in the second row are primes, and it's true that for many more integers $n > 11$ that $f(n)$ is prime. Explain why it cannot be that for every $n \geq 1$ that $f(n)$ is prime.

Problem 6. [18; 9 points each part] On modular arithmetic.

a. Fill in the rest of this table of cubes modulo 7.

a	0	1	2	3	4	5	6
a^3	0	1				-1	-1

b. Use your results in part a to explain why the sum of two cubes cannot be congruent either 3 or 4 modulo 7, that is to say, the congruences $x^3 + y^3 \equiv 3 \pmod 7$ and $x^3 + y^3 \equiv 4 \pmod 7$ have no solutions.

#1.[15]	
#2.[20]	
#3.[18]	
#4.[15]	
#5.[15]	
#6.[18]	
Total	