Math 126, Number Theory

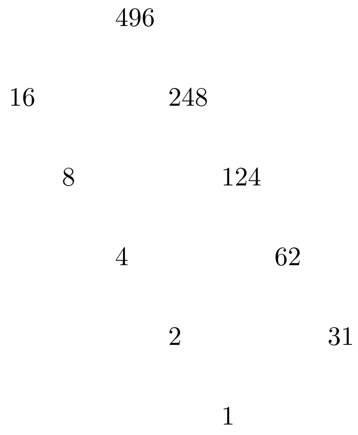
First Test

22 Feb 2006

Scale. 90–101 A. 80–89 B. 60–79 C. Median 94.

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

a. Draw the Hasse diagram of the divisors of $496 = 2^4 \cdot 31$.



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

$d(496)$ is the number of divisors of 496, and you can see in your diagram in part a that there are are 10 of them. $\sigma(496)$ is the sum of those divisors, which you could compute by adding all the divisors, but there's an easier way. Since 2^4 and 31 are relatively prime, therefore $\sigma(496) = \sigma(2^4)\sigma(31) = 31 \cdot 32 = 992$.

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

A number n is perfect if $\sigma(n) = 2n$. Since $\sigma(496) = 992 = 2 \cdot 496$, therefore 496 is perfect.

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.

$$\begin{aligned} 19 &= 304 - 3 \cdot 95 \\ &= 304 - 3 \cdot (399 - 304) \\ &= 4 \cdot 304 - 3 \cdot 199 \\ &= 4 \cdot (703 - 399) - 3 \cdot 399 \\ &= 4 \cdot 703 - 7 \cdot 399 \end{aligned}$$

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

From part a a particular solution to the equation is

$$x_0 = -7, \qquad y_0 = 4.$$

Therefore, the general solution is

$$x = x_0 + \frac{b}{d}\,t, \quad y = y_0 + \frac{a}{d}\,t$$

where $a = 399$, $b = 703$, and $d = (a, b) = 19$, and t is an arbitrary integer, so we can write the general solution as

$$x = 4 + 37t, \quad y = 4 - 21t.$$

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 $a|b$.

There are various ways you can prove this theorem. If you're careful, you can prove both the statement and its converse in the same time by using only if and only if statements. Here's a proof where each half is proved separately.

Proof $\Longrightarrow$*:* Suppose that $a|b$. Then there exists an integer c such that $ac = b$. Multiplying both sides of that equation by d we find that $adc = bd$. Therefore, $ad|bd$.

Proof $\Longleftarrow$*:* Suppose that $ad|bd$. Then there exists an integer c such that $adc = bd$. Since d is positive, we can divide both sides of that equation by d to find that $ac = b$. Therefore $a|b$. Q.E.D.

Problem 4. True or false. [15; 3 points each part]

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

False. The correct statement should have "whenever $(a,b) = 1$." Note that a can divide b but $f(ab) \neq f(a)f(b)$.

b. If $a|c$ and $b|c$ then $(a+b)|c$.
False. The correct statement should be "if $c|a$ and $c|b$ then $c|(a+b)$." Note that $2|6$ and $3|6$ but $5 \nmid 6$.

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.
True. There are other forms of mathematical induction, but this is the standard one.

d. The square root of any prime is an irrational number.
True. This is a special case of a general theorem we proved.

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.
True. We noted this when we looked at the greatest common divisor of three integers (a,b,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.

It's amazing that $f(n)$ is prime for so many values of n, but it isn't prime for all of them. It's fairly easy to see that when $n = 41$ that, since 41 divides $41^2 + 41 + 41$, $f(41)$ has 41 as a factor and so is composite. You can also show that 41 is a factor of $f(40)$, but that's a bit harder to see.

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	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.

Each of x^3 and y^3 is congruent to 0, 1, or -1 modulo 7, so their sum can range from -2 through 2, but can't be 3 or 4.