MAT115 Test 1 (Fall 2005): 1.1-2.5

Name:

Directions: Show your work! Answers without justification will likely result in few points. Your written work also allows me the option of giving you partial credit in the event of an incorrect final answer (but good reasoning). Indicate clearly your answer to each problem (e.g., put a box around it).

Work exactly 10 of the 12 problems. Write "skip" on the other two. You must skip two! Don't do them all and suppose that I'll drop the two lowest....

Good luck!

Problem 1 The two public numbers in your RSA code are 7 and 143.

1. Explain how would you encode the message "3".

2. Now actually encode the message "3".

3. Without actually performing the calculation, explain how you would you use the secret decoding number 103 to decode the encrypted message?

Problem 2. A game of Fibonacci Nim begins with 42 sticks.

1. If you are player 1, and employ the winning strategy, how many sticks should you take? Why?

2. Suppose you are player 2: if the game starts with 42 sticks, and player 1 starts by taking 7 sticks, how many sticks would you choose to assure your victory? Why?

Problem 3 A porch is designed to hold at most 2000 pounds. Your kids have a "kiddy pool" that is 8 feet in diameter, and which gets filled 2.5 feet deep with water. Should you put the pool on the porch and fill it with water? (Hint: Area of a circle: πr^2; volume of a cylinder: $\pi r^2 h$, where r is the radius, and h the height; $\pi \approx 3.14$).

Problem 4. A man, a tame lion, a goat, and a basket of corn arrive at the river where the cannibals and the missionaries once stood. There stands the boat, with blood on it (because the student who tried to get them all safely across screwed up, and the cannibals feasted on the missionaries). The lion will eat the goat if given half a chance, and the goat will feast upon the corn if left unattended. The man can row only one of the items across with himself. How can he get all safely to the other side?

Problem 5 The UPC on my Sun-Maid raisons is 04114302870 – or is it? Recalling that the weights for a UPC follow the pattern "3 1 3 1 3 1 3 1 3 1 3", and that the modulus used is 10, check the UPC and see if appears to be a valid UPC.

Problem 6. Determine whether or not the following expression prime:

$$1 \times 2 \times 3 \times 4 \times 5 \times 6 + 1$$

If it is not prime, find its prime factorization.

Problem 7 Monty Hall concocts a devilish new game: instead of three doors, there are now four doors! What a concept. The game is played precisely as before, only now there are three doors with donkeys behind them and one door with the car. You choose your door, Monty shows you a door behind which a donkey is standing, and you are invited to switch to one of the other doors. Do you switch? Why or why not?

Problem 8. My birthday this year was on a Friday. What day of the week will my birthday fall on in 8 years? Explain!

Problem 9 If you use primes $p = 3$ and $q = 5$ in the RSA algorithm, find legitimate choices of e and d for encoding and decoding.

Problem 10. Demonstrate that there are an infinite number of non-prime numbers.

Problem 11 In a standard deck of cards (4 suits of 13 cards each), what is the smallest number of cards you must draw to guarantee that you will have

1. 1 card of any one suit (this one's easy!);

2. 2 cards of any one suit;

3. 3 cards of any one suit;

4. n cards of any one suit ($n \leq 13$)?

Problem 12. Draw the spirals in the following picture, and demonstrate that they are in a relationship of consecutive Fibonacci numbers. (Photo thanks to R. Knott)