# MAT310 Final, Spring 2006

**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). **Note**: you may of course use your calculators, but the use of the calculator without analysis will not result in many points. **Good luck!**

**Today's Special**: You may skip one problem, any problem! Write "skip" across it.

**Problem 1**. Given integers $a$ and $b$, $d = \gcd(a, b)$. Then there exist integers $x$ and $y$ for which

$$ax + by = d.$$

Prove that $\gcd(x, y) = 1$.

**Problem 2**. Given $p = 11$, choose $q$ to create an RSA scheme for encoding words (letter by letter), on a 26 letter alphabet with the following coding:

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |

1. Fill in the following table, encoding the word "finished". Show any calculations, and justify any choices you need to make.

| p | q | n | k | j | finished |
|---|---|---|---|---|---|
| 11 | | | | | |

2. (3 points) Bring me your $k$ and $n$ and I'll "send you a message (word)". Decode the word.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Ciphertext | | | | | | | | |
| Decoded (number) | | | | | | | | |
| Plaintext | | | | | | | | |

3. (1 point) On what fundamental point does the RSA encryption scheme hinge?

**Problem 3**. Consider a new cipher on the alphabet of 26 letters (i.e. Problem 2) as follows:

- The first letter is encoded by adding to its value the number of letters in the message;
- each succeeding letter is encoded by adding to its value the encoded letter preceding it.
- Example: to encode abz, we'd find the length of the string (3); then
  1. encode a by a+3, or d (using letters and number interchangeably);
  2. encode b by b+d, or e;
  3. encode z by z+e, or d.

1. (3 points) What are the equations that one would use to decode the message "ded"? (Use the notation $n_i$ for the numerical value for the $i^{th}$ letter of the plaintext.)

2. (4 points) Use this scheme to decode the message "owldwar".

3. (3 points) Compare and contrast this method with the other methods we studied: advantages, disadvantages, and which does it most closely resemble?

**Problem 4.**

1. (6 points) Find all solutions to the following linear system (show your work!)

$$3x + 2y \equiv 7 (\text{mod } 26)$$
$$4x + 3y \equiv 10 (\text{mod } 26)$$

2. (4 points) How does this problem relate to one of our encryption schemes? If by 7 we mean "h" and by 10 we mean "k", describe an encryption/decryption problem whose solution would be represented using this system.

**Problem 5**.

1. Use Fermat's theorem to verify that 19 divides $11^{110} - 7$. You should not use your calculator.

2. Use Euler's theorem to confirm that, for any integer $n \geq 0$,

$$133 \mid 12^{108n+9} + 1$$

**Problem 6**. Numbers $n$ such that $\sigma(\sigma(n)) = 2n$ are called *superperfect numbers.*

1. (4 points) If $n = 2^k$ for $2^{k+1} - 1$ prime, prove that $n$ is superperfect.

2. (1 point) Write the first three such values of $n$.

3. (5 points) Compute $\sigma(\sigma(n))$ for $n = 2^{k-1}(2^k - 1)$, $2^k - 1$ prime, and so demonstrate that there are no even perfect numbers that are also superperfect.

**Problem 7**. Short answer (but please do explain!):

1. How many solutions are there (in integers) of

$$22x - 14y = 1?$$

2. Can $s = 656370$ and $t = 12673$ be used to create a primitive Pythagorean triple?

3. What is the gcd of $u_{128}$ and $u_{28}$?

4. Find the smallest natural number evenly divisible by 2, 3, 9, and 11.

5. Are there any even numbers both perfect and triangular?

**Problem 8.**

1. (5 points) Prove (hint: directly) that the Fibonacci numbers satisfy the relationship

$$u_n^2 - u_{n+1}u_{n-1} = (-1)(u_{n-1}^2 - u_n u_{n-2})$$

for $n \geq 3$. [Hint: $u_n^2 = u_n u_n$.]

2. (5 points) From this demonstrate that

$$u_n^2 = u_{n+1}u_{n-1} + (-1)^{n-1}$$

for all $n \geq 2$. (You can do this even if you didn't get part 1!)

**Problem 9**. For the Fibonacci sequence, establish that

$$u_{n+5} \equiv 3u_n (\text{mod } 5)$$

What conclusions can you draw from this?