MAT310, Spring 2006, Test 3: Sections 6.1, 7.2, 7.3, 7.5

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).

Note: you may of course use your calculator or Mathematica, but the use of the calculator without analysis – without showing what you're doing on Mathematica and why – will not result in many points. **Good luck!**

Problem 1 (10 pts) Prove that

$$\phi(3n) = 3\phi(n) \iff 3|n$$

Problem 2 (10 pts). We know that ϕ, σ, and τ are multiplicative functions, each with a well-defined and intuitive meaning. I'm curious about other combinations of functions:

1. Consider the function ψ defined as

$$\psi : n \to \sum_{d|n} \sigma(d)$$

   - Is ψ multiplicative?

   - Whether multiplicative or not, we can attempt to characterize the function ψ: how would you describe ψ intuitively in a single sentence?

   - Compute

     (a) $\psi(2)$

     (b) $\psi(5)$

     (c) $\psi(p)$, p a prime

     (d) $\psi(30)$

2. Is the composition $c = \sigma \circ \sigma$

$$c : n \to \sigma(\sigma(n))$$

multiplicative? (Give your reason(s)! A yes or no answer will yield nothing....)

Problem 3 (10 pts). Demonstrate (using Euler's Theorem) that $33 \mid 125^{20007} + 28$.

While you can check this with Mathematica, you should be able to break it down using Euler's so that no calculations are required on a calculator – so that everything can clearly be easily done by hand.

Problem 4 (10 pts). A message is to be encoded using RSA, and the person to whom you wish to send the message has chosen the humongous primes $p = 5$ and $q = 7$ as their primes, with $k = 11$.

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

- Why is this a reasonable choice for k?

- Encode the message "curiouser and curiouser", letter by letter, in the table below. Illustrate your technique with a few of the letters....

c	u	r	i	o	u	s	e	r	a	n	d	c	u	r	i	o	u	s	e	r
2	20	17	8	14	20	18	4	17	0	13	3	2	20	17	8	14	20	18	4	17

- What value of j will the target of your message need to use to decode the message?

- Explain why this would be a bad cipher (apart from the small values of p and q).

Problem 5 (10 pts).

$$\text{Let us use Hill's Cipher with the encoding matrix } A = \begin{bmatrix} 6 & 23 \\ 3 & 20 \end{bmatrix}$$

- What makes this a reasonable choice for an encryption matrix?

- In the table below, encrypt the message *no curious coincidence*, ignoring spaces. Illustrate your technique with a few of the letters....

n	o	c	u	r	i	o	u	s	c	o	i	n	c	i	d	e	n	c	e
13	14	2	20	17	8	14	20	18	2	14	8	13	2	8	3	4	13	2	4

- Find the inverse of the Hill matrix A.

- Decipher the message *“kheqadyayqiuubnglmai”*.

k	h	e	q	a	d	y	a	y	q	i	u	u	b	n	g	l	m	a	i
10	7	4	16	0	3	24	0	24	16	8	20	20	1	13	6	11	12	0	8

- Encrypt the same message, *“kheqadyayqiuubnglmai”*.

k	h	e	q	a	d	y	a	y	q	i	u	u	b	n	g	l	m	a	i
10	7	4	16	0	3	24	0	24	16	8	20	20	1	13	6	11	12	0	8

- What makes this a bad choice for an encryption matrix?

Extra Credit (3 pts). Fill in the blanks:

- "______________________ calculated without apparent effort, just as men breath, as eagles sustain themselves in the air." Arago.

- "Mathematicians are like ______________________: whatever you say to them they translate into their own language and forthwith it is something entirely different." ______________________