Math 5248 Cryptology and number theory
Fall 2006, Vic Reiner
Midterm exam 1- Due Wednesday October 11, in class

Instructions: This is an open book, open library, open notes, take-home exam, but you are *not* allowed to collaborate. The instructor is the only human source you are allowed to consult. Explain your reasoning- answers without justification or proof (where appropriate) will receive **no credit**.

1. (20 points total) Let $m = 672, n = 259245$.

(a) (5 points) Compute $GCD(m, n)$ via Euclid's algorithm.

(b) (10 points) Find integers $a, b \in \mathbb{Z}$ for which $am + bn = GCD(m, n)$, without using brute force.

(c) (5 points) Compute $LCM(m, n)$ without using brute force, and without factoring m or n.

2. (40 points total) The Hawaiian alphabet has the following 13 letters and (approximate) letter frequencies shown here as percentages:

a	e	i	o	u	$'$
26	7	9	11	6	7

h	k	l	m	n	p	w
4	11	4	3	8	3	1.

(a) (10 points) In performing the affine cipher in Hawaiian rather than English, what is the size of the keyspace? That is, how many possible pairs (a, b) are there with $a, b \in \mathbb{Z}/13$ and for which a has a multiplicative inverse (avoiding the silly choice of the pair $(a, b) = (1, 0)$)?

(b) (15 points) Find the key (a, b) if one assumes that the high frequency plaintext letters "a", "k" (identified with $\overline{0}, \overline{7}$ in $\mathbb{Z}/13$, respectively) were encrypted as ciphertext letters "U", "E" (identified with $\overline{4}, \overline{1}$ in $\mathbb{Z}/13$, respectively).

(c) (15 points) Assume y, y' are two strings of "Hawaiian gibberish" of the same length N, that is, they are each produced by picking letters from the Hawaiian alphabet at random, independently, with the above letter frequencies. What is the expected value of their *index of coincidence* $I(y, y')$?

3. (20 points total) Recall that in an affine cipher of English, when choosing the key (a, b) with $a, b \in \mathbb{Z}/26$, it was always assumed that a had a multiplicative inverse. In this problem, let us temporarily *drop this assumption* so that we allow *any* $a \in \mathbb{Z}/26$.

(a) (6 points) Show by example that there is some pair of English plaintext letters which will get encrypted as the same ciphertext letter if one chooses the key $(a, b) = (6, 11)$.

(b)(7 points) Prove that the same thing will happen as long as a is even, that is, if $a \in \{2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24\} \subset \mathbb{Z}/26$.

(c)(6 points) What is the maximum number of *different* ciphertext letters that can result from the encryption of any plaintext with an affine cipher whose key (a, b) has $a = 13$? Justify your answer.
(Hint: try encrypting the whole alphabet using $(a, b) = (13, 3)$, for example, and see what you get.)

4. (20 points total) (a) (12 points) Given that a number N is written with digits $a_k a_{k-1} \cdots a_1 a_0$ in decimal (meaning that a_0 is the ones digits, a_1 is the tens digit, etc.), let $a_1 a_0$ be the number in the range $0 - 99$ represented by its last two digits, let $a_3 a_2$ be the number in the range $0 - 99$ represented by its next two digits, and so on.

Prove that in $\mathbb{Z}/11$ one has

$$\overline{N} = \overline{a_1 a_0 + a_3 a_2 + a_5 a_4 + \cdots}.$$

(b) (8 points) Prove or disprove, using hand calculations only, that $N = 123456123456123456$ is divisible by 11.