

## Written Homework 02

**Assigned:** Thu 05 Oct 2006

**Due:** Thu 12 Oct 2006

### Instructions:

- The assignment is due at the *beginning* of class on the due date specified, i.e., 1:35pm for Prof. Aslam's section and 4:35pm for Prof. Fell's section. Late assignments will be penalized 50%, as stated in the course information sheet. Late assignments *will not be accepted* after the solutions have been distributed.
- Problem 2 requires graph paper. Printable graph paper may be found at the following URL:

<http://www.pdfpad.com/graphpaper/pdf/c-i-14.pdf>

### Problem 1 [36 pts]: Cryptography.

A spy has been captured, but all attempts to interrogate him have failed: he speaks a very strange language, unintelligible to any translator. However, this spy was caught with a number of documents. Linguists who have studied these documents believe that they were written in the spy's language, but that they have been encrypted. Decrypting these documents to obtain valid text in the spy's language would be incredibly helpful; your job is to decrypt the spy's documents and hopefully determine where he's from and what language he speaks.

Linguists analyzing the spy's documents have determined that the spy's language consists of 26 linguistic units (analogous to English letters), where each unit consists of one or more case-sensitive English letters or punctuation marks. The units of the spy's language, numbered from 0 to 25, are given below.

|    |    |    |    |    |    |    |     |    |    |    |    |    |
|----|----|----|----|----|----|----|-----|----|----|----|----|----|
| 0  | 1  | 2  | 3  | 4  | 5  | 6  | 7   | 8  | 9  | 10 | 11 | 12 |
| a  | b  | ch | D  | e  | gh | H  | I   | j  | l  | m  | n  | ng |
| 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20  | 21 | 22 | 23 | 24 | 25 |
| o  | p  | q  | Q  | r  | S  | t  | tlh | u  | v  | w  | y  | '  |

You suspect that the spy has used a linear encryption scheme with  $m = 15$  and  $k = 3$  since symbols representing these values were found tattooed on the spy's scalp. Finally, the linguists and interrogators are particularly interested in following phrase, which was written on the top of each document the spy possessed:

rebDng wDq lDghjDp

- Parse the phrase above to obtain the individual linguistic units of the spy's language, i.e., "r" followed by "e" followed by "b" and so on. Note the multi-letter combinations which correspond to individual linguistic units.

- ii. Encode each linguistic unit with its corresponding number from the table given above, e.g.,  $r \rightarrow 17$  and so on.
- iii. Since you suspect that these values were encrypted using the function

$$a \rightarrow (15 \cdot a + 3) \pmod{26}$$

you must subtract 3 and then multiply by the multiplicative inverse of 15 (mod 26) in order to decrypt these values. Start by determining the multiplicative inverse of 15 (mod 26).

- iv. Decrypt each value by inverting the linear encryption.
- v. Decode these values using the table given above to obtain a phrase in the spy's language. (It will *not* be intelligible to most people.)
- vi. Conduct some research on the web to see if you can determine what this phrase means. (Try typing the decrypted words or the entire phrase into Google.) What is the English translation of this phrase? Where does our spy come from and what language does he speak?

**Problem 2 [32 pts]: Mod Addition and Multiplication Patterns.**

- i. Construct the addition and multiplication tables for mod 8, in a manner similar to those for mod 3 and mod 4 given in the text on pg. 33.
- ii. Using graph paper,<sup>1</sup> create patterns from these  $8 \times 8$  tables (ignoring the row and column headers) by leaving each square corresponding to an even number white while shading in each square corresponding to an odd number.

Discuss any patterns you see and why they occur.

**Problem 3 [32 pts]: Euclidean Algorithm.**

Compute the following greatest common divisors via the Euclidean Algorithm. Show *all* of your work.

- i.  $\gcd(212, 121)$
- ii.  $\gcd(154, 98)$
- iii.  $\gcd(391, 247)$
- iv.  $\gcd(585, 495)$

---

<sup>1</sup>The instructions for this assignment (see pg. 1) give a link to printable graph paper.