

Written Homework 02

Assigned: Mon 04 Feb 2008

Due: Wed 13 Feb 2008

Instructions:

- The assignment is due at the *beginning* of class on the due date specified. 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.printfreegraphpaper.com/gp/c-i-14.pdf>

Problem 1 [36 pts]: Cryptography.

A spy has been captured, but all attempts to interrogate him have failed; he seems to speak a foreign language. 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. One piece of encrypted text, in particular, is believed to be the *pass phrase* which the spy uses to authenticate himself to his contacts. Your job is to decrypt and translate the spy's pass phrase, and hopefully determine where he's from and what language he speaks.

The spy's language uses the familiar 26 English letters, which are encoded using the numbers $\{0, \dots, 25\}$ in the usual way. You suspect that the spy has used a linear encryption scheme with $m = 19$ and $k = 7$ since symbols representing these values were found tattooed on the spy's scalp. As mentioned, the linguists and interrogators are particularly interested in the encrypted pass phrase, given below:

asnhlth qfsmf hsf idbah ixurh

- Encode each letter in the above phrase in the usual way, i.e., $a \rightarrow 0$, $b \rightarrow 1$, and so on.
- Since you suspect that these values were encrypted using the function

$$num \rightarrow (19 \cdot num + 7) \pmod{26}$$

you must subtract 7 and then multiply by the multiplicative inverse of 19 (mod 26) in order to decrypt these values. Start by determining the multiplicative inverse of 19 (mod 26).

- Decrypt each value by inverting the linear encryption.
- Decode these values in the usual way to obtain a phrase in the spy's language. (It will *not* be intelligible to most people.)

- v. 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 9, in a manner similar to those for mod 3 and mod 4 given in the text.
- ii. Using graph paper,¹ create patterns from these 9×9 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. $\gcd(355, 65)$
- ii. $\gcd(412, 49)$
- iii. $\gcd(600, 435)$
- iv. $\gcd(910, 553)$

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