Math 1111 – Problem Set 4

1. The ciphertext below was enciphered using a "standard" Vigenère cipher. (That is, the Vigenère cipher as described in Singh in which each row of the Vigenère square is a shift cipher.) Use a Kasiski examination to determine the length of the keyword, then identify the keyword and decipher the text. Hint: The plaintext didn't have as many e's as you would expect.

```
TCXRT ESGOR UQBYY MLUYO AIJNR ASEQU EGETH UQWYA EFCVG TRKBF

ULUNT AMCUE RGEQS MLZEO ZZREP XYTVN SRYRL UEYGS ARYNT URWNL

XQFAT TCWYO APEVC WRRXE ERYRI DMEOA DFVCO GLUFO ZRYRF XMFEO

HCIGH QNCNC QUYRR QYJGA IYJJH ULZAG FFVPE YCEGG UTVFO GRRUO

XJFJS ASEQN UABGA WCJGH QZREI ZZFGH TYEQS FFIBW EFZFW TMCRS

FPVAG FFZAT AGKGR KGETT ADFEC QGKGH DMLTH FFVSL AMIVT RGENL

XWXBE ERYEO GEYAI OICRA ZQUBW ZYEQA ERRET XCUUO DPZSI QBCBO

WAFZE EGEUI EDRPE TCGHT EBFJN FFVOA DNZPK ESGNS FYNUO UQWYA

FRVAE PMEGH QDCBO DURGC TGETH UKKNK QQYVS RJRFH XGXUT MLUTO

QQHHI OICLT AURED FFVFT MGIFH QACVM NQINP UBCL
```

2. Consider the affine cipher $y = (mx + b)$ MOD 26, where x is an integer between 0 and 25 representing a letter in the plaintext, y is an integer between 0 and 25 representing the corresponding letter in the ciphertext, and m and b are constants, each integers between 0 and 25. How many unique affine ciphers are there? Justify your answer.

3. Find all integer solutions to the system of modular arithmetic equations:
$y \equiv 2x + 3 \pmod{10}$
$y \equiv 4x + 1 \pmod{10}$

4. Consider the set of integers S = {1, 2, 3, 4}. Define the operation □ on this set as follows: If a and b are integers in the set S, then $a \square b = (ab)$ MOD 5. It can be shown that □ is associative. Show that the three *other* group conditions are satisfied, as well, proving that (S, □) is a group:
   a. Closure: If a and b are in S, then $a \square b$ is also in S.
   b. Identity: There is an element x in S that has the property that $x \square b = b$, for any b in S.
   c. Inverse: Every element a in S has an inverse under the operation □.

5. The "key" for an ADFGVX cipher consists of some arrangement of the 26 letters of the alphabet as well as the digits 0 through 9 in a six-by-six grid, plus a keyword used to determine how certain columns of ciphertext are rearranged at the appropriate point in the enciphering process. Suppose you know that a keyword of length 4 has been used. How many distinct "keys" are there in this case? (Hint: The keywords KNOT and BENT have the same effect on the column rearrangement, so you should treat them as identical in your count of keys.)

6. Suppose the 8 letters V, I, G, E, N, E, R, and E are each written on a tile and placed in a bag. (You can imagine the game Scrabble, if that helps.) If you reach into the bag and draw five tiles at random (without replacement), what is the probability that…
   a. You draw no Es?
   b. You draw exactly 1 E?
   c. You draw at least one E?

7. Consider the following variation on a Vigenère cipher. Start with a 26 x 26 grid of letters, each row consisting of the English alphabet in standard order. Then select 13 of the rows, and shift each of these rows by a different amount (anywhere between 1 and 25 places). When shifting a row, wrap as necessary, just as in a standard shift cipher. This produces the cipher key.

   For example, you might shift the 3rd row by 5 places, the 10th row by 2 places, the 18th row by 11 places, and so on, until 13 rows have been shifted, each by a different number of places.

   How many unique keys are there?

8. Suppose a certain cipher machine has a plugboard, like the Enigma machine, in which pairs of letters (A—Z) can be connected via cables. Two such cables are provided with the machine, and both must be used for the machine to work.

a. How many different plugboard settings are there in which one cable connects two letters in the first half of the alphabet (A-M) and the other connects two letters in the second half (N-Z)?
b. How many different plugboard settings are there in which the letters A and Z are connected, either to each other or to other letters?