Math Circle - Spring 2012 - Homework 8

When cryptography is outlawed, qw qukk hyar glcw ri qeurw kujw rgua.

It is the year 2718, and Earth is under attack by Martians. You, a loyal Earthling, are a soldier in the Planetary Security Agency, whose purpose is to process enemy communications and decipher their messages.

1. (10 points) You happen to know that the Martians encrypt their messages using a running key cipher with a two-letter key. Decrypt:

HWS AOHSGG PFT FTOSM PBS GIOIWDBTR PH IVT ZJBPF

2. (10 points) The Martians decide to double their efforts by changing two letters at a time in their encryptions. Treating each letter as a number modulo 26 ($A = 0$, $B = 1$, ..., $Z = 25$), they encrypt as follows. They first split the text into blocks of size two letters each. For each block (α, β) of two letters, the Martians change the letters to $(3\alpha + \beta, 2\alpha + \beta)$ (each number reduced modulo 26).

As an example, consider the text MARS. As a sequence of 4 integers, MARS $= (12, 0, 17, 18)$. The Martians change the numbers (always reducing mod 26):

$$MA = (12, 0) \mapsto (3 \cdot 12 + 0, 2 \cdot 12 + 0) = (36, 24) = (10, 24) = KY$$

$$RS = (17, 18) \mapsto (3 \cdot 17 + 18, 2 \cdot 17 + 18) = (69, 52) = (17, 0) = RA$$

So finally we see that MARS $\mapsto$ KYRA under the Martian cipher.

The Martians are planning a huge attack. The following message was intercepted, and it surely indicates exactly when we can expect the Martian invaders. Your decryption is our only hope of survival:

MISBATLLZOYMQDYYTTBODP

3. (10 points) The Martians have a new chief of cryptography, who orders that they use a turning grille cipher with an 8×8 grid. How many possible keys must you try before being sure to get the right one?

4. (10 points) When not decrypting Martian communications, you and your fellow soldiers enjoy a good card game. You have a deck of 50 cards, each of which is labeled with a number between 1 and 25. In the deck, there are exactly two cards with each label. The cards are shuffled and dealt to 25 soldiers who are sitting at a round table, and each soldiers receives two cards.

On every move of the game, each soldiers takes the card with the smaller number out of his or her hand and passes it to the person on his/her right. Each soldier makes this move at the same time so that everyone always has exactly two cards. The game continues until some soldier has a pair of cards with the same number. Show that this game will eventually end.