Danielle Riethmiller **Homework 2** **Due 07-03-2013**

1. Break this chiphertext that was enciphered using Vigenere with a two letter keyword (the keyword will not necessarily be a real dictionary word):

   MJ XO HP DG RF HG LP HV EK DG UC GC GC L

   given that "bananas" appears in it.

2. Find q, r with $0 \leq r < a$, so that $b = a \cdot q + r$ with:
   (a) $a = 332119, b = 3245773$
   (b) $a = 260745, b = -2934468.$
   (c) $a = 584645, b = 145448.$

3. Find the inverse of 14 $\pmod{38}$ (that is, find c such that $14c \equiv 1 \pmod{38}$) or explain why it does not exist.

4. Break the message:

   BHAI CZEY DFCA IIAF FS

   knowing it was encoded with an affine cipher and contains the word "silly".

5. Use the vigenere applet at

   http://math.ucsd.edu/\˜crypto/java/EARLYCIPHERS/Vigenere.html.

   Choose a random ciphertext and try to break it. Write down the keyword.

6. Prove that if $d|a$ and $d|b$ then $d|a+b$ and $d|a-b$.

7. Prove that if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then $a+c \equiv b+d \pmod{m}$, $a-c \equiv b-d \pmod{m}$ and $ac \equiv bd \pmod{m}$.