Nadezda Karimenko **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):

   `DO GO YL LX LX LC LB PT FC EK OY WV LB`

   given that "bananas" appears in it.

2. Find q, r with $0 \leq r < a$, so that $b = a \cdot q + r$ with:
   (a) $a = 302295, b = 1992074$
   (b) $a = 499062, b = -564999$.
   (c) $a = 408221, b = 13378$.

3. Find the inverse of 11 (mod 38) (that is, find c such that $11c \equiv 1 \pmod{38}$) or explain why it does not exist.

4. Break the message:

   `UQZL OBBR ZLLZ AAN`

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

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 $ac \equiv bd \pmod{m}$.