Math 335 HW 1 - Due Feb. 9, 2004

1. A *partition* of the integers, $\mathbb{Z}$, is a collection A_i of subsets of $\mathbb{Z}$ such that the union of all of the subsets is all of $\mathbb{Z}$, and if $i \neq j$, then A_i is disjoint from A_j. For example, A_1 the odd numbers and A_2 the even numbers is a partition. A different example is $A_i = \{3i, 3i+1, 3i+2\}$, where i is any integer. You can visualize this partition as $\{.....\{-6,-5,-4\},\{-3,-2,-1\},\{0,1,2\},\{3,4,5\},...\}$.

   An *equivalence relation* on $\mathbb{Z}$ is subset $R \subseteq \mathbb{Z} \times \mathbb{Z}$ such that

   (a) $(a,a) \in R$ for all $a \in \mathbb{Z}$. (R is reflexive.)

   (b) If $(a,b) \in R$, then $(b,a) \in R$. (R is symmetric)

   (c) If $(a,b) \in R$ and $(b,c,) \in R$, then $(a,c) \in r$. (R is transitive).

   An example of an equivalence relation is $R = \{(a,a) \in \mathbb{Z} \times \mathbb{Z}\}$. The subset $R' = \{(a,b) \in \mathbb{Z} \times \mathbb{Z} : a \leq b\}$ is NOT an equivalence relation because $(3,5) \in R'$, but $(5,3) \notin R'$.

   (a) Given a partition A_i of the integers, let $R = \{(a,b) \in \mathbb{Z} : a$ and b are in the same subset of the partition.$\}$. Prove that R is an equivalence relation.

   (b) Let R be an equivalence relation on $\mathbb{Z}$. For each $i \in \mathbb{Z}$ define $A_i = \{j \in \mathbb{Z} : (i,j) \in R.\}$ Show that for every i and j, either $A_i = A_j$, or A_i and A_j are disjoint. Hence, the set of all *distinct* A_i form a partition of $\mathbb{Z}$.

   (c) Fix an integer m. Prove that $R = \{(a,b,) \in \mathbb{Z} \times \mathbb{Z} : a \equiv b \ (\mod m)\}$ is an equivalence relation on $\mathbb{Z}$.

2. Show all work.

   (a) Compute (6188,4709).

   (b) Show that 1234 and 357 are relatively prime. Find the multiplicative inverse of 357 in $\mathbb{Z}_{1234}$.

3. Suppose we are told that the plaintext

   breathtaking

   yields the ciphertext

   RUPOTENTOIFV.

   where the *Hill* cipher is used, but m is not specified. Determine the encryption matrix.

4. Decrypt the following Vigenére Cipher:

   KCCPKBGUFDPHQTYAVINRRTMVGRKDNBVFDETDGILTXRGUD
   DKOTFMBPVGEGLTGCKQRACQCWDNAWCRXIZAKFTLEWRPTYC
   QKYVXCHKFTPONCQQRHJVAJUWETMCMSPKQDYHJVDAHCTRL
   SVSKCGCZQQDZXGSFRLSWCWSJTBHAFSIASPRJAHKJRJUMV
   GKMITZHFPDISPZLVLGWTFPLKKEBDPGCEBSHCTJRWXBAFS
   PEZQNRWXCVYCGAONWDDKACKAWBBIKFTIOVKCGGHJVLNHI
   FFSQESVYCLACNVRWBBIREPBBVFEXOSCDYGZWPFDTKFQIY
   CWHJVLNHIQIBTKHJVNPIST

5. Decrypt the following message. It was encrypted using the Hill cipher with encrypting matrix

$$\begin{bmatrix} 4 & 3 \\ 5 & 1 \end{bmatrix}.$$

   HMSQNNAYXDWKXVWMINET

6. For any $m \geq 1$, $\phi(m)$ is the number of integers a such that $1 \leq a \leq m$ and a is relatively prime to m. This function is called the *Euler* ϕ-function. For instance, if p is prime, then $\phi(p) = p - 1$.

(a) If p is prime, what is $\phi(p^r)$?

(b) Compute $\phi(10), \phi(5), \phi(9), \phi(4), \phi(20), \phi(45), \phi(36)$, and $\phi(40)$.

(c) Suppose that r and s are relatively prime. Find a formula for $\phi(rs)$.
$*$ Can you prove this formula? $*$

7. Write the Euclidean algorithm as follows:

$$\begin{array}{lcllcl} a & = & q_1 b & + & r_1 \\ b & = & q_2 r_1 & + & r_2 \\ \vdots & & \vdots & & \vdots \\ r_{m-2} & = & q_m r_{m-1} & + & r_m \end{array}$$

Prove that $r_i \geq 2r_{i+2}$ whenever this makes sense. Prove that m is $O((\log a)^2)$.