Homework 14, due October 9

(1) Find the number of different (good) keys there are for a 2 by 2 Hill cipher without counting them one by one. Remember that the determinant has to be relatively prime to 26. Here's one approach to solving the problem:
   (a) Show that the number of good keys mod 26 is equal to the number of good keys mod 13 times the number mod 2. (Find an explicit one–to–one, onto map between matrices mod 26, and pairs of matrices, where the first is a matrix mod 2 and the second is a matrix mod 13. The Chinese Remainder Theorem might be helpful.)
   (b) Show that the number of non-invertible matrices mod a prime p is $(2p-1)^2+(p-1)^3$ by showing the following claims. Let $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Then A is non-invertible if and only if $ad \equiv bc \pmod{p}$. There are two cases: $ad \equiv bc \equiv 0$ or $ad \equiv bc \not\equiv 0$.
      (i) The first case happens $(2p-1)^2$ times.
      (ii) The second case happens $(p-1)^3$ times.
   (c) From this conclude that the number of good keys is 157248.
(2) Use fast modular exponentiation to compute $3^{75} \pmod{103}$ by hand. Show each step as on page 79 of the text.
(3) (a) Divide 3^{10203} by 101. What is the remainder?
   (b) Find a primitive root modulo 31.