整一道题里的矩阵都是在一个质数field里的，就是说如果他给我一个矩阵mod p，那那个矩阵里所有的元素都是在（0,1,2，。。。。。p-1）里取的。

第一题他让我算每个数(0除外)的inverse并保存下来，inverse就是a\*a^(-1)=1 mod p.

function b = Inverse(p)

b = zeros(1,p-1);

for i=1:p-1

for j=1:p-1

if mod(i\*j,p) == 1

b(i) = j;

break;

end

end

end

end

第三题他是让我把一个矩阵通过row operation变成echelon的形式，这个形式你可能得自己去google一下，题目要求了要用row operation，就是什么一行加一行，一行换一行，一行加另一行乘个数之类的。然后这个echelon形式是上矩阵上三角形式的高级版(但类似)。

一个n\*n的矩阵，先看第一列里面有没有1，如果有1就把有1的那一行跟矩阵的第一行交换位子，交换完之后矩阵的第一行第一列就是1了，如果第一列里没有1的话那就将整个第一行乘以第一个数的inverse，乘完之后第一行的元素mod p一下之后，第一行就是以一开头的了，第一行第一列的那个数字是1了之后，就把他下面的所有数字用row operation消成0.例如整个矩阵是mod 5的话，a11=1了，a21=2,那就将第二行\*2+第一行 或者 第二行+第一行\*（5-2），同样的把剩下的a31,a41….都消成0。这样第一行的操作就完成了，之后就不用再管第一行了。开始第二行操作，a21=0,a31=0…..现在要先判断a22等不等于0，如果a22=0,那么接下来就要a22那一列下面的东西都消成0，然后从把a23变成1然后下面变成0.如果a22不等于0那就跟第一行的操作一样了，看有没有=1的，有的话就换行，没有的话就用别的row operation变成1.。。。。。。。

记得要mod p

我给你发的题里面有讲echelon是什么样子的。

最后整个矩阵操作完之后，要判断最后有多少行的全部=0的，有多少行=0.题目中要输出的rank = n-等于0的行数。题目中还要求输出basis for row space，操作完之后的nonzero rows（为0的那些行） are a basis for the row space

Q4说要找kerA的basis，We know that x is in the kernel is equivalent to Ax = 0. That’s equivalent to echelon(A)x = 0. 然后kerA basis里元素的数量=n-rank，就是说echelon最后有几行0，kerA basis里就有几个vector。Wiki上有找basis的方法。

例子：

首先要把A化成echelon的形式

A=\left[ \begin{array}{cccccc}
1 & 0 & -3 & 0 &  2 & -8 \\
0 & 1 &  5 & 0 & -1 & 4 \\
0 & 0 &  0 & 1 & 7 & -9 \\
0 & 0 & 0 & 0 & 0 & 0 \end{array} \,\right]. 

然后弄一个新的矩阵，在A下面加一个I

 \left[\begin{array}{c}A\\\hline I\end{array}\right]=
\left[\begin{array}{cccccc}
1 & 0 & -3 & 0 &  2 & -8 \\
0 & 1 &  5 & 0 & -1 & 4 \\
0 & 0 &  0 & 1 & 7 & -9 \\
0 & 0 & 0 & 0 & 0 & 0 \\
\hline
1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 
\end{array}\right]. 

然后做column echelon形式，就是说现在是column operation不是row的了。

在这个例子里就是交换第三列和第四列。Column echelon 形式的意思就是如果一个矩阵的transpose是在row echelon形式的话，这个矩阵就是在column echelon的形式。

Putting the upper part in column echelon form by column operations on the whole matrix gives

 \left[\begin{array}{c}B\\\hline C\end{array}\right]=
\left[\begin{array}{cccccc}
1 & 0 &  0 & 0 &  0 & 0 \\
0 & 1 &  0 & 0 &  0 & 0 \\
0 & 0 &  1 & 0 &  0 & 0 \\
0 & 0 &  0 & 0 &  0 & 0 \\
\hline
1 & 0 &  0 & 3 & -2 & 8 \\
0 & 1 &  0 & -5 & 1 & -4 \\
0 & 0 &  0 & 1 & 0 & 0 \\
0 & 0 &  1 & 0 & -7 & 9 \\
0 & 0 &  0 & 0 & 1 & 0 \\
0 & 0 &  0 & 0 & 0 & 1 
\end{array}\right]. 

The last three columns of *B* are zero columns. Therefore, the three last vectors of *C*,

\left[\!\! \begin{array}{r} 3 \\ -5 \\ 1 \\ 0 \\ 0 \\ 0 \end{array} \right],\;
\left[\!\! \begin{array}{r} -2 \\ 1 \\ 0 \\ -7 \\ 1 \\ 0 \end{array} \right],\;
\left[\!\! \begin{array}{r} 8 \\ -4 \\ 0 \\ 9 \\ 0 \\ 1 \end{array} \right] 

are a basis of the null space of *A*.