1.1

1.1 Matrices over Finite Fields

1.1 Matrices over Finite Fields

Throughout this report p is assumed to be prime.

All programs are attached at the end of the report.

Question 1:

A typical test output is shown below.

```
Inv =

     1     6     4     3     9     2     8     7     5    10
```

Figure 1, a typical output for $p = 11$ case.

To speed up this procedure we can skip all values that are already other numbers' inverses when computing a number's inverse. This still gives the inverse of each number since there is a 1 - 1 correspondence between numbers and their inverses *mod* p but upper bounds the number of operations for number i by p - i. This modification speeds up the procedure by a factor of 2 because there are at most $\sum_{i=1}^{p-1} i = \frac{(p-2)(p-1)}{2}$ operations.(cf. Question 2)

Question 2:

Note that for each number there are at most p - *1* operations, and there are p-*1* numbers to test. Hence the complexity is p^2.

Question 3:

Using a program that reduces a matrix into its row echelon form, we produce the following row echelon forms for different matrices:

$$\underset{p\,=\,11\text{ case}}{\begin{bmatrix} 1 & 0 & 3 & 0 & 0 \\ 0 & 1 & 7 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}} \quad \underset{p\,=\,19\text{ case}}{\begin{bmatrix} 1 & 0 & 0 & 0 & 13 \\ 0 & 1 & 0 & 0 & 6 \\ 0 & 0 & 1 & 0 & 3 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix}} \quad \underset{p\,=\,23\text{ case}}{\begin{bmatrix} 1 & 0 & 0 & 9 & 11 & 19 \\ 0 & 1 & 0 & 10 & 5 & 5 \\ 0 & 0 & 1 & 9 & 14 & 7 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}}$$

Since row operations do not alter the row space of a matrix, we see that matrix A_1 has rank 4 when $p = 11$ or 19 and matrix A_2 has rank 3 when $p = 23$. The bases for row spaces of matrices A_1 and A_2 for different p can be read off from their row echelon forms:

$$B_{A_1,11} = \left\{ \begin{bmatrix} 1 \\ 0 \\ 3 \\ 0 \\ 0 \end{bmatrix}^T, \begin{bmatrix} 0 \\ 1 \\ 7 \\ 0 \\ 0 \end{bmatrix}^T, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}^T, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}^T \right\} \quad B_{A_1,19} = \left\{ \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 13 \end{bmatrix}^T, \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 6 \end{bmatrix}^T, \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 3 \end{bmatrix}^T, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}^T \right\}$$

$$B_{A_2,23} = \left\{ \begin{bmatrix} 1 \\ 0 \\ 0 \\ 9 \\ 11 \\ 19 \end{bmatrix}^T, \begin{bmatrix} 0 \\ 1 \\ 0 \\ 10 \\ 5 \\ 5 \end{bmatrix}^T, \begin{bmatrix} 0 \\ 0 \\ 1 \\ 9 \\ 14 \\ 7 \end{bmatrix}^T \right\}, \text{where } T \text{ denotes tranpose.}$$

Question 4:

A program that outputs the basis of the kernel of a matrix is written for Question 4. The outputs of the program for different examples are shown below:

$$\underset{p\,=\,13 \text{ case}}{\left\{ \begin{bmatrix} 7 \\ 2 \\ 1 \\ 2 \\ 1 \end{bmatrix} \right\}} \quad \underset{p\,=\,17 \text{ case}}{\left\{ \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \right\}} \quad \underset{p\,=\,23 \text{ case}}{\left\{ \begin{bmatrix} 6 \\ 6 \\ 9 \\ 9 \\ 9 \\ 1 \end{bmatrix} \right\}}$$

My program for this question works as follows:
1: Transform the matrix into row echelon form.
2: Eliminate all rows with zero entries.
3: From the result in step 2, use Matlab's symbolic expression feature to express all pivotal variables in terms of other variables inductively.
4: Assign specific values to non-pivotal variables to obtain a basis. (Let one variable = 1 and others = 0.)

Question 5:

The sum of the dimension of U and the dimension of U^o is equal to the number of columns of the matrix.

Question 6:

For U the row space of A_1 mod 19, U^o is the kernel of A_1. Use the program for question 4 we find it to be $\left\{ \begin{bmatrix} 6 & 13 & 16 & 18 & 1 \end{bmatrix}^T \right\}$.

The annihilator of U^o, $(U^o)^o$, is the set of all row vectors $\mathbf{t}$ such that $\mathbf{ts} = 0$, where $\mathbf{s}$ is the basis vector we just found. By taking the transpose of this relation we have $\mathbf{s}^T\mathbf{t}^T = 0$, i.e. $\mathbf{t}^T$ is in the kernel of the matrix $\begin{bmatrix} 6 & 13 & 16 & 18 & 1 \end{bmatrix}$.

Using the program for question 4 we find that $(U^o)^o$ has a basis

$$B_{(U^o)^o,19} = \left\{ \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}^T, \begin{bmatrix} 10 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}^T, \begin{bmatrix} 16 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}^T, \begin{bmatrix} 3 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}^T \right\}$$

To show that A_1 spans the row space of $B_{(U^o)^o,19}$, we put these basis vectors and rows in the row echelon form of A_1 in one matrix and perform Gaussian elimination: (using program from question 1)

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 13 \\ 0 & 1 & 0 & 0 & 6 \\ 0 & 0 & 1 & 0 & 3 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 10 & 0 & 1 & 0 & 0 \\ 16 & 0 & 0 & 1 & 0 \\ 3 & 0 & 0 & 0 & 1 \end{bmatrix} \xrightarrow{\text{Gaussian Elimination}} \begin{bmatrix} 1 & 0 & 0 & 0 & 13 \\ 0 & 1 & 0 & 0 & 6 \\ 0 & 0 & 1 & 0 & 3 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

From the result of Gaussian elimination we can see that all basis vectors of $(U^o)^o$ are in the row space of A_1. Since $(U^o)^o$ and A_1 have the same dimension we conclude that they are equal.

Question 7:

A program is written for Quesiton 7. The program takes 2 matrices and a prime number p as inputs and outputs their row spaces, the intersection and the sum of their row spaces.

My program for this question works as follows:
1. Transform the input matrices A and B into row echelon forms to obtain bases for their row spaces.
2. Join the two matrices obtained in step 1 together to obtain a new matrix consisting of a spanning set of $U + W$, where U and W are row spaces of the input matrices.
3. Perform Gaussian elimination on the new matrix to obtain a basis for $U + W$
4. Find bases for the kernels of the two input matrices and transpose them. Apply step 1, 2, 3 to obtain a matrix H consisting of a transposed basis for

$U^o + W^o$. The kernel of the matrix H is $(U^o + W^o)^o = U \cap W$, which can be found by using the program for question 4.

The outputs of the program for different examples are shown below:(X, Y, Z, and W represent bases for $U, W, U + W$ and $U \cap W$)
When $A = A_1$, $B = B_1$, $p = 11$:

$$X = \left\{ \begin{bmatrix}1\\0\\3\\0\\0\end{bmatrix}^T, \begin{bmatrix}0\\1\\7\\0\\0\end{bmatrix}^T, \begin{bmatrix}0\\0\\0\\1\\0\end{bmatrix}^T, \begin{bmatrix}0\\0\\0\\0\\1\end{bmatrix}^T \right\}, \qquad Y = \left\{ \begin{bmatrix}1\\0\\0\\2\\0\end{bmatrix}^T, \begin{bmatrix}0\\1\\0\\3\\0\end{bmatrix}^T, \begin{bmatrix}0\\0\\1\\4\\0\end{bmatrix}^T, \begin{bmatrix}0\\0\\0\\0\\1\end{bmatrix}^T \right\}$$

$$Z = \left\{ \begin{bmatrix}1\\0\\0\\0\\0\end{bmatrix}^T, \begin{bmatrix}0\\1\\0\\0\\0\end{bmatrix}^T, \begin{bmatrix}0\\0\\1\\0\\0\end{bmatrix}^T, \begin{bmatrix}0\\0\\0\\1\\0\end{bmatrix}^T, \begin{bmatrix}0\\0\\0\\0\\1\end{bmatrix}^T \right\} \qquad W = \left\{ \begin{bmatrix}7\\5\\1\\0\\0\end{bmatrix}^T, \begin{bmatrix}8\\6\\0\\1\\0\end{bmatrix}^T, \begin{bmatrix}0\\0\\0\\0\\1\end{bmatrix}^T \right\}$$

When $A = A_3$, $B = \mathrm{Ker}(A_3)$, $p = 19$:

$$X = \left\{ \begin{bmatrix}1\\0\\0\\0\\0\\6\\1\end{bmatrix}^T, \begin{bmatrix}0\\1\\0\\0\\0\\3\\14\end{bmatrix}^T, \begin{bmatrix}0\\0\\1\\0\\0\\16\\9\end{bmatrix}^T, \begin{bmatrix}0\\0\\0\\1\\0\\0\\8\end{bmatrix}^T, \begin{bmatrix}0\\0\\0\\0\\1\\17\\6\end{bmatrix}^T \right\}, \qquad Y = \left\{ \begin{bmatrix}1\\0\\9\\18\\6\\1\\12\end{bmatrix}^T, \begin{bmatrix}0\\1\\0\\2\\0\\4\\14\end{bmatrix}^T \right\}$$

$$Z = \left\{ \begin{bmatrix}1\\0\\0\\0\\0\\0\\0\end{bmatrix}^T, \begin{bmatrix}0\\1\\0\\0\\0\\0\\0\end{bmatrix}^T, \begin{bmatrix}0\\0\\1\\0\\0\\0\\0\end{bmatrix}^T, \begin{bmatrix}0\\0\\0\\1\\0\\0\\0\end{bmatrix}^T, \begin{bmatrix}0\\0\\0\\0\\1\\0\\0\end{bmatrix}^T, \begin{bmatrix}0\\0\\0\\0\\0\\1\\0\end{bmatrix}^T, \begin{bmatrix}0\\0\\0\\0\\0\\0\\1\end{bmatrix}^T \right\}, \qquad W = \left\{ \begin{bmatrix}0\\0\\0\\0\\0\\0\\0\end{bmatrix}^T \right\}$$

When $A = A_3$, $B = \mathrm{Ker}(A_3)$, $p = 23$:

$$X = \left\{ \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 8 \\ 22 \end{bmatrix}^T, \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 3 \\ 18 \end{bmatrix}^T, \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 21 \\ 6 \end{bmatrix}^T, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 4 \\ 0 \end{bmatrix}^T, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 5 \\ 8 \end{bmatrix}^T \right\}, \qquad Y = \left\{ \begin{bmatrix} 1 \\ 0 \\ 17 \\ 8 \\ 15 \\ 21 \\ 8 \end{bmatrix}^T, \begin{bmatrix} 0 \\ 1 \\ 0 \\ 3 \\ 0 \\ 5 \\ 17 \end{bmatrix}^T \right\}$$

$$Z = \left\{ \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 12 \end{bmatrix}^T, \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 20 \end{bmatrix}^T, \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 20 \end{bmatrix}^T, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 18 \end{bmatrix}^T, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 19 \end{bmatrix}^T, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 7 \end{bmatrix}^T \right\}, \qquad W = \left\{ \begin{bmatrix} 11 \\ 3 \\ 3 \\ 5 \\ 4 \\ 16 \\ 1 \end{bmatrix}^T \right\}$$

The relation between the dimensions of U, W, $U + W$ and $U \cap W$ is $\dim(U)$ + $\dim(W)$ - $\dim(U \cap W) = \dim(U + W)$, where dim denotes dimension.

Question 8:

There are 2 surprising features:

1. The dimensions of $U + W$ and $U \cap W$ change with respect to different modules. This is surprising since dimension of a space is unique for the real field.

2. There exists a nontrivial kernel vector that is a linear combination of row vectors. This is surprising since, for the real field, there is Gram-Schmidt process that reduces a basis to an orthonormal basis by defining the canonical inner product, which implies that all nontrivial linear combination of row vectors cannot be sent to 0 by the matrix.

Reference

Source Code

Callings of functions:

```
A = [0,1,7,2,10;8,0,2,5,1;2,1,2,5,5;7,4,5,3,0]%A1
B = [6,16,11,14,1,4;7,9,1,1,21,0;8,2,9,12,17,7;2,19,2,19,7,12]%A2
C = [4,6,5,2,3;5,0,3,0,1;1,5,7,1,0;5,5,0,3,1;2,1,2,4,0]%B1
D = [3,7,19,3,9,6;10,2,20,15,3,0;14,1,3,14,11,3;26,1,21,6,3,5;0,1,3,19,0,3]%B2
L = [1,0,0,0,3,0,0;0,5,0,1,6,3,0;0,0,5,0,2,0,0;2,4,0,0,0,5,1;4,3,0,0,6,2,6]%A3
s = transpose(KernelBasis(L,19))%kernel of A3 mod 19
t = transpose(KernelBasis(L,23))%kernel of A3 mod 23

%Q3
GaussE(A,11)
GaussE(A,19)
GaussE(B,23)
%Q4
KernelBasis(C,13)
KernelBasis(C,17)
KernelBasis(D,23)
%Q7
[q,w,e,r] = SumIntersection(A,C,11)
[a,b,c,d] = SumIntersection(L,s,19)
[t,y,u,i] = SumIntersection(L,t,23)
```

Code for Question 1:

```
function [Inv]=InverseModP(p)
Inv = zeros(1,p-1);
for i = 1:p-1
for j = 1:p-1
if mod(i*j,p)==1
```

```
Inv(i)=j;
end
end
end
```

Code for Question 3:

```
function [F]=OneStep(B,p,Inv)% one step of gaussian elimination: reduce a submatrix such that the (1,1) entry is 1 and there is only 1 non-zero entry in the first column
d = size(B);
r = d(1);
c = d(2);
s=0;
E=B;
if B == zeros(r,c)
F=B;
else
for i=1:c
s=i;
if B(1:r,1)==zeros(r,1)
x = size(B);
B = B(1:r,2:(x(2)));
else
break
end
end
if B(1,1)==0
for k=2:r
if B(k,1) =0
z=B(k,:);B(k,:)=B(1,:);B(1,:)=z;
B(1,:)=mod(B(1,:)*Inv(B(1,1)),p);
break
end
end
else
B(1,:)=mod(B(1,:)*Inv(B(1,1)),p);
end
for j=2:r
B(j,:)=mod(B(j,:)-(B(j,1))*(B(1,:)),p);
end
E(1:r,s:c)=B;
F=E;
end
end


function [R]=GaussE(A,p)% apply OneStep function to submatrices of the orig-
```

```
inal matrix
d = size(A);
r = d(1);
c = d(2);
t = InverseModP(p);
for i = 1:r
try %Use try to deal with empty matrix!
A(i:r,i:c)=OneStep(A(i:r,i:c),p,t);
R = A;
catch
break
end
end
```

Code for Question 4:

```
function [B]=KernelBasis(A,p)
R = GaussE(A,p);%Reduced matrix
d = size(R);
r = d(1);
c = d(2);
u = 0;
for i = 1:r
if R(i,1:c)==zeros(1,c)
u = u;
else
u = u + 1;
end
end
R = R(1:u,1:c);%ignore all 0 rows
d = size(R);
r = d(1);
c = d(2);
for i = 1:c
x(i)=sym(['x',num2str(i)]);
end
z = x;
for i = r:-1:1 % find algebraic expressions of non-pivotal vars.
for j = 1:c
if R(i,j)==0
continue
else
if j == c
x(c)=0;
else
s = 0;
```

```
for k = j+1:c
s = s - R(i,k)*x(k);
end
x(j) = s;
break
end
end
end
end
q = zeros(1,c);
for i = 1:r % storing indices of non-pivotal vars
for j = 1:c
if R(i,j)==0
continue
else
q(j) = 1;
break
end
end
end
for i = 1:c
for j = 1:c
C(i,j)=sym(['x',num2str(1),num2str(j)]);
end
end
D=C;
v = transpose(C(1,1:c));
if q == ones(1,c)
C = zeros(c,1);
else
for i = 1:c
if q(i) == 1
continue
else %q(i)==0
z = subs(x,x(i),1);%substitute
for j = 1:c
if (q(j) == 0) & (j  = i)
z = subs(z,z(j),0);
end
C(i,1:c)=z;
end
end
end
end
C = transpose(C);
if q == ones(1,c)
```

```
C = zeros(c,1);
else
for i=1:c
d = size(C);
f = d(2);
for j = 1:f
if C(1:c,j)==v
C(:,j)=[];
break
end
end
end
end
try
C(1,1)%test if C is an empty matrix and use 'try' to deal with the case where
C is empty
B=mod(C,p);
catch
B = zeros(c,1);
end
end%there is some redundancy in the last 40 lines but this program works for
all questions.
```

Code for Question 7:

```
function [A,B,C,D] = SumIntersection(Q,R,p)%A,B are row spaces of Q and R,
C = Q + R, D = Q intersection R
A = GaussE(Q,p);
B = GaussE(R,p);
c = size(A);
d = size(B);
G = zeros(c(1)+d(1),c(2));%Initialize a zero matrix
for i = 1:c(1)
G(i,1:c(2)) = A(i,1:c(2));
end
for i = 1:d(1)
G(c(1) + i,1:c(2)) = B(i,1:c(2));
end
C = GaussE(G,p);
clear c
clear d
N = KernelBasis(Q,p);
M = KernelBasis(R,p);
N = transpose(N);
M = transpose(M);
c = size(N);
```

```
d = size(M);
H = zeros(c(1)+d(1),c(2));
for i = 1:c(1)
H(i,1:c(2)) = N(i,1:c(2));
end
for i = 1:d(1)
H(c(1) + i,1:c(2)) = M(i,1:c(2));
end
S = KernelBasis(H,p);
D = transpose(S);
end
```