## 1.1

# Matrices over Finite Fields

## Question 1

Table 1: Inverses of the non-zero elements of $F$ with $p = 11$ and $p = 7$

| Element | Inverse (mod 11) | Inverse (mod 7) |
|---|---|---|
| 1 | 1 | 1 |
| 2 | 6 | 4 |
| 3 | 4 | 5 |
| 4 | 3 | 2 |
| 5 | 9 | 3 |
| 6 | 2 | 6 |
| 7 | 8 | - |
| 8 | 7 | - |
| 9 | 5 | - |
| 10 | 10 | - |

**Modification**. After computing the inverse of an element we can store both the inverse in the position of the element and the element in the position of its inverse. Hence we need to compute the inverses for half the elements, speeding up the procedure by roughly a factor of 2.

## Question 2

**Complexity**. Let the number of steps the mod operation takes be a constant $C$. Checking if $\text{mod}(ab)$ equals 1 takes one step. For each $a$ we have $(p-1)$ values of $b$ to check. Storing the inverse takes one step. Hence for each $a$ we use $(C+1)(p-1)+1$ steps. We have $(p-1)$ values for $a$ so the overall complexity is $O((p-1)((C+1)(p-1)+1)) = O(p^2)$.

## Question 3

- $A_1$ (mod 11)
  - Row Echelon Form = $\begin{pmatrix} 1 & 0 & 3 & 0 & 0 \\ 0 & 1 & 7 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$

- Rank = 4
- Basis = $\left\{ \begin{pmatrix}1\\0\\3\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\7\\0\\0\end{pmatrix}, \begin{pmatrix}0\\0\\0\\1\\0\end{pmatrix}, \begin{pmatrix}0\\0\\0\\0\\1\end{pmatrix} \right\}$

- $A_1 \pmod{19}$
  - Row Echelon Form = $\begin{pmatrix}1&0&0&0&13\\0&1&0&0&6\\0&0&1&0&3\\0&0&0&1&1\end{pmatrix}$
  - Rank = 4
  - Basis = $\left\{ \begin{pmatrix}1\\0\\0\\0\\13\end{pmatrix}, \begin{pmatrix}0\\1\\0\\0\\6\end{pmatrix}, \begin{pmatrix}0\\0\\1\\0\\3\end{pmatrix}, \begin{pmatrix}0\\0\\0\\1\\1\end{pmatrix} \right\}$

- $A_2 \pmod{23}$
  - Row Echelon Form = $\begin{pmatrix}1&0&0&9&11&9\\0&1&0&10&5&5\\0&0&1&9&14&7\\0&0&0&0&0&0\end{pmatrix}$
  - Rank = 3
  - Basis = $\left\{ \begin{pmatrix}1\\0\\0\\9\\11\\9\end{pmatrix}, \begin{pmatrix}0\\1\\0\\10\\5\\5\end{pmatrix}, \begin{pmatrix}0\\0\\1\\9\\14\\7\end{pmatrix} \right\}$

## Question 4

**Algorithm**. Since the original matrix and the $REF$ matrix have the same row space, they have the same kernel.

Let $S = \{l(1), \ldots, l(r)\}$ and $T = [n] \setminus S$. Expanding out $A\mathbf{x} = 0$, for each $l(i) \in S$ we have

$$x_{l(i)} = -\sum_{j \in T} A_{ij} x_j$$

On the RHS, we let one of the $x_j$ equal -1 and all the others equal 0, which determines the $x_{l(i)}$. Doing this for each $x_j$ on the RHS yields $n-r$ vectors which are clearly linearly independent. Since the rank is $r$, the dimension of the kernel is $n-r$, and so they form a basis.

**Bases**

- $B_1$ (mod 13): Kernel basis $= \left\{ \begin{pmatrix} 6 \\ 11 \\ 12 \\ 11 \\ -1 \end{pmatrix} \right\}$
- $B_1$ (mod 17): Kernel basis $= \{\mathbf{0}\}$
- $B_2$ (mod 23): Kernel basis $= \left\{ \begin{pmatrix} 17 \\ 17 \\ 14 \\ 14 \\ 14 \\ -1 \end{pmatrix} \right\}$

## Question 5

$$\dim U + \dim U^\circ = n$$

## Question 6

We use the program from Q4 to find the kernel of $A_1$, which is $U^\circ$

$$U^\circ = \left\{ \begin{pmatrix} 13 \\ 6 \\ 3 \\ 1 \\ -1 \end{pmatrix} \right\}$$

We form a matrix $A_1^\circ$ whose rows are the kernel basis vectors and reduce it to $REF$

$$A_1^\circ = \begin{pmatrix} 13 & 6 & 3 & 1 & -1 \end{pmatrix} \ REF = \begin{pmatrix} 1 & 18 & 9 & 3 & 16 \end{pmatrix}$$

We find the kernel of $A_1^\circ$ and write it in matrix form. Reducing $A_1^{\circ\circ}$ to $REF$ gives a basis for $(U^\circ)^\circ$

$$A_1^{\circ\circ} = \begin{pmatrix} 18 & -1 & 0 & 0 & 0 \\ 9 & 0 & -1 & 0 & 0 \\ 3 & 0 & 0 & -1 & 0 \\ 16 & 0 & 0 & 0 & -1 \end{pmatrix} REF = \begin{pmatrix} 1 & 0 & 0 & 0 & 13 \\ 0 & 1 & 0 & 0 & 6 \\ 0 & 0 & 1 & 0 & 3 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

So we have

$$(U^\circ)^\circ = \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 13 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 6 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 3 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} \right\}$$

which is clearly the same as $U$. Hence $(U^\circ)^\circ = U$.

**Method**. To check if two subspaces are equal we write both as matrices and reduce both to $REF$. By the uniqueness[1] of $REF$ they are equal iff they have the same $REF$.

## Question 7

**Program**. To compute a basis for a row space we use gaussian elimination on its corresponding matrix.

The **Sum** function finds a basis for $U+W$. It starts by concatenating the matrices $A$ and $B$ together (so that $A$ is on top of $B$). The row space of this matrix spans $U+W$. It puts this matrix into $REF$ which achieves linear independence.

The **Inter** function finds a basis for $U \cap W$. We use the second relation from the text, $U \cap W = (U^\circ + W^\circ)^\circ$. It is implemented using the kernel function from Q4 and the Sum function.

- Modulo 11 with $U$ the row space of $A_1$ and $W$ the row space of $B_1$

$$U = \left\{ \begin{pmatrix}1\\0\\3\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\7\\0\\0\end{pmatrix}, \begin{pmatrix}0\\0\\0\\1\\0\end{pmatrix}, \begin{pmatrix}0\\0\\0\\0\\1\end{pmatrix} \right\} \quad W = \left\{ \begin{pmatrix}1\\0\\0\\2\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\\3\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\\4\\0\end{pmatrix}, \begin{pmatrix}0\\0\\0\\0\\1\end{pmatrix} \right\}$$

$$U + W = \mathrm{GF}(11)^5 \qquad U \cap W = \left\{ \begin{pmatrix}1\\0\\3\\3\\0\end{pmatrix}, \begin{pmatrix}0\\1\\7\\9\\0\end{pmatrix}, \begin{pmatrix}0\\0\\0\\0\\1\end{pmatrix} \right\}$$

- Modulo 19 with $U$ the row space of $A_3$ and $W$ the kernel of $A_3$

$$U = \left\{ \begin{pmatrix}1\\0\\0\\0\\0\\6\\1\end{pmatrix}, \begin{pmatrix}0\\1\\0\\0\\0\\3\\14\end{pmatrix}, \begin{pmatrix}0\\0\\1\\0\\0\\16\\9\end{pmatrix}, \begin{pmatrix}0\\0\\0\\1\\0\\0\\8\end{pmatrix}, \begin{pmatrix}0\\0\\0\\0\\1\\17\\6\end{pmatrix} \right\} \quad V = \left\{ \begin{pmatrix}1\\0\\9\\18\\6\\1\\12\end{pmatrix}, \begin{pmatrix}0\\1\\0\\2\\0\\4\\14\end{pmatrix} \right\}$$

$$U + W = \mathrm{GF}(19)^7 \qquad U \cap W = \{\mathbf{0}\}$$

- Modulo 23 with $U$ the row space of $A_3$ and $W$ the kernel of $A_3$

$$U = \left\{ \begin{pmatrix} 1\\0\\0\\0\\0\\8\\22 \end{pmatrix}, \begin{pmatrix} 0\\1\\0\\0\\0\\3\\18 \end{pmatrix}, \begin{pmatrix} 0\\0\\1\\0\\0\\21\\6 \end{pmatrix}, \begin{pmatrix} 0\\0\\0\\1\\0\\4\\0 \end{pmatrix}, \begin{pmatrix} 0\\0\\0\\0\\1\\5\\8 \end{pmatrix} \right\} \quad W = \left\{ \begin{pmatrix} 1\\0\\17\\8\\15\\21\\8 \end{pmatrix}, \begin{pmatrix} 0\\1\\0\\3\\0\\5\\17 \end{pmatrix} \right\}$$

$$U + W = \left\{ \begin{pmatrix} 1\\0\\0\\0\\0\\0\\12 \end{pmatrix}, \begin{pmatrix} 0\\1\\0\\0\\0\\0\\20 \end{pmatrix}, \begin{pmatrix} 0\\0\\1\\0\\0\\0\\20 \end{pmatrix}, \begin{pmatrix} 0\\0\\0\\1\\0\\0\\18 \end{pmatrix}, \begin{pmatrix} 0\\0\\0\\0\\1\\0\\19 \end{pmatrix}, \begin{pmatrix} 0\\0\\0\\0\\0\\1\\7 \end{pmatrix} \right\}$$

$$U \cap W = \left\{ \begin{pmatrix} 1\\17\\17\\13\\15\\14\\21 \end{pmatrix} \right\}$$

We see that in each case we have

$$\dim (U + W) = \dim U + \dim W - \dim (U \cap W)$$

## Question 8

**Feature**. In the last part of Q7, the intersection of the row space and the kernel is not trivial. Working over the real numbers, let $y$ be an element in both the kernel and the row space. We must have $y \cdot y = 0$ so $y = \mathbf{0}$. Hence their intersection is always $\{\mathbf{0}\}$ over the real numbers.

**References**

[1] https://en.wikipedia.org/wiki/Row_echelon_form

### Program In.m for Question 1

```
function I = In(p)

I = zeros(p-1,1);
for a = 1:p-1
    for b = 1:p-1
        if mod(a*b,p)==1
            I(a) = b;
            %fprintf('%2g & %2g \\\\ \n',a ,b);
            break
        end
    end
end
```

### Program REF.m for Question 3

```
function [Mp,l] = REF(M,p)

Mp = mod(M,p);
m = size(Mp,1);%rows
n = size(Mp,2);%columns
I = In(p);%Inverses
l = zeros(1,m);

for i = 1:m
    for j = 1:n %Reorders rows
        if all(Mp(i:m,j) == 0) %checks if the column j from row i to m is zero
            continue
        else
```

```
            l(i) = j; %constructs vector l, the array of pivot columns
            for k = i:m
                if Mp(k,j) ~= 0 %finds a non-zero entry
                    Mp([i,k],:) = Mp([k,i],:); % swaps rows k and i
                    break
                end
            end
            break
        end
    end
    if l(i) == 0 %checks if process has finished
        break
    end
    Mp(i,:) = mod(I(Mp(i,l(i)))*Mp(i,:),p); %makes leading entry 1
    for h = i+1:m
        Mp(h,:) = mod(-1*Mp(h,l(i))*Mp(i,:)+Mp(h,:),p); %cancels out rows below leading entry
    end
end
for i = 2:m %cancels out rows above leading entry
    if l(i) ~= 0
        for k = 1:i-1
            Mp(k,:) = mod(-1*Mp(k,l(i))*Mp(i,:)+Mp(k,:),p);
        end
    else
        continue
    end
end
```

**Program** rk.m **for Question 3**

```
function rank = rk(M,p)
M = REF(M,p);
rank = 0;
for i = 1:size(M,1)
    if ~all(M(i,:) == 0)
        rank = rank +1;
    end
end
```

**Program** Ker.m **for Question 4**

```
function Uo = Ker(M,p)

[Mp,l] = REF(M,p);
r = rk(Mp,p);
m = size(Mp,1);%rows
n = size(Mp,2);%columns

g = []; %array of non-pivot columns
for j = 1:n
    if ~ismember(j,l)
        g = [g,j];
    end
end

L = [];%array of pivot columns without zeros
for h = l
    if h ~=0
        L = [L,h];
    end
end

Mpt = zeros(r,n);%last n-r rows of zeros removed off
    Mp Matrix
```

```
for i = 1:m
    if any(Mp(i,:))
        Mpt(i,:) = Mp(i,:);
    end
end

Uo = zeros(n-r,n);
h=1;%counter
for i = g
     x = zeros(1,n);
     for j = g
          x(j) = 0;
     end
     x(i) = -1;
     x(L) = Mpt(:,i);
     Uo(h,:) = x;
     h = h+1;
end
```

**Program** Sum.m **for Question 7**

```
function S = Sum(V,W,p)
D = [V;W];
S = REF(D,p);
```

**Program** Inter.m **for Question 7**

```
function I = Inter(V,W,p)
Vo = Ker(V,p);
Wo = Ker(W,p);
Intero = Sum(Wo,Vo,p);
I = REF(Ker(Intero,p),p);
```

**Program** DM.m **to display matrix**

```
function DM(M)
m = size(M,1);%rows
n = size(M,2);%columns
fprintf('$\\begin{pmatrix} \n')
for i = 1:m
    for j = 1:n
        if j == n
            fprintf('%3g \\\\ \n', M(i,j));
        else
            fprintf('%3g &', M(i,j))
        end
    end
end
fprintf('\\end{pmatrix} $\n')
```

**Program** DB.m **to display basis**

```
function DB(M)
m = size(M,1);%rows
n = size(M,2);%columns
for i = 1:m
    fprintf('\\begin{pmatrix}')
    for j = 1:n
        fprintf('%3g \\\\', M(i,j))
    end
    fprintf('\\end{pmatrix} \n')
end
```