Question 1

A program for finding the multiplicative inverse can be found on page 9 named `inverse.m`. This program determines inverse of a where $1 \leq a \leq p-1$ by testing with every integer b in the range $[1, p-1]$ untill it finds one s.t $ab \equiv 1 \pmod{p}$.

But if we have that b is the inverse of a, then we already know that $p-b$ is the inverse of $p-a$. So we can find the inverses of a where $1 \leq a \leq \frac{p-1}{2}$ by testing and then assign the inverse of both a and $p-a$. This way we can speed up the procedure by a factor of 2. A program for this can be found on page 9 named `inverse2.m`.

Question 2

For the program `inverse.m`, we have to do at most $(p-1)^2$ multiplications, $(p-1)^2$ division by p and $(p-1)^2$ comparison(with 1), so in total at most $3(p-1)^2$ steps. Hence the compexity is p^2.

Question 3

A program for finding the row echelon form of a matrix can be found on page **??** named `rowechelon.m`. We run the program for the given matrices A_1 and A_2.

```
>> A1 = [ 0 1 7 2 10 ; 8 0 2 5 1 ; 2 1 2 5 5 ; 7 4 5 3 0];
>> rowechelon(11,A1)

ans =

     1     0     3     0     0
     0     1     7     0     0
     0     0     0     1     0
     0     0     0     0     1

>> rowechelon(19,A1)

ans =

     1     0     0     0    13
     0     1     0     0     6
     0     0     1     0     3
     0     0     0     1     1

>> A2 = [ 6 16 11 14 1 4 ; 7 9 1 1 21 0 ; 8 2 9 12 17 7 ; 2 19 2 19 7 12 ];
>> rowechelon(23,A1)

ans =

     1     0     0    19    14
     0     1     0    22    19
```

```
     0         0         1         7         2
     0         0         0         0         0
```

Easy to see that A_1 has rank 4 in both cases of $\pmod 1$1 and 19 whereas A_2 has rank 3. The rows of the row echelon form forms a basis for their row spaces. Hence bases for A_1 and A_2 can be given by

i Basis for $A_1 \pmod{11}$: $\{(1,0,3,0,0),(0,1,7,0,0),(0,0,0,1,0),(0,0,0,0,1)\}$

ii Basis for $A_1 \pmod{19}$: $\{(1,0,0,0,12),(0,1,0,0,6),(0,0,1,0,3),(0,0,0,0,1,1)\}$

iii Basis for $A_2 \pmod{23}$: $\{(1,0,0,19,24),(0,1,0,22,19),(0,0,1,7,2),(0,0,0,0,0)\}$

Question 4

A program to compute a basis for the kernel of a matrix can be found on page 11.

```
>> B1 = [ 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 ];
>> B2 = [ 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 ];
>> kerBasis(13,B1)

ans =

     7
     2
     1
     2
     1

>> kerBasis(17,B1)

ans =

  5x0 empty double matrix

>> kerBasis(23,B2)

ans =

     6
     6
     9
     9
     9
     1
```

So B_1 (mod 17) has trivial kernel. Where B_1 (mod 13) and B_2 (mod 23) has basis for the kernel $\{\begin{pmatrix}7\\2\\1\\2\\1\end{pmatrix}\}$ and $\{\begin{pmatrix}16\\16\\9\\9\\9\\1\end{pmatrix}\}$ respectively.

Question 5

For any matrix U, we have $dim(U) + dim(U^{\circ}) = \#(\text{rows of } U)$.

Question 6

```
>> A1 = [ 0 1 7 2 10 ; 8 0 2 5 1 ; 2 1 2 5 5 ; 7 4 5 3 0];
>> kerBasis(19,A1)

ans =

    13
     6
     3
     1
    18

>> X = kerBasis(19,A1)';
>> kerBasis(19,X)

ans =

    18     9     3    16
    18     0     0     0
     0    18     0     0
     0     0    18     0
     0     0     0    18

>> Y = kerBasis(19,X)';
>> rowechelon(19,Y)

ans =

     1     0     0     0    13
     0     1     0     0     6
     0     0     1     0     3
     0     0     0     1     1

>> rowechelon(19,A1)
```

```
ans =

     1     0     0     0    13
     0     1     0     0     6
     0     0     1     0     3
     0     0     0     1     1
```

We are given that U is the row space of matrix A_1. Now `kerBasis(19,A1)` produces a matrix which has it's columns as a basis for U°, let it's transpose be X. Similarly `kerBasis(19,X)` produces a matrix which has it's columns as a basis for $(U^{\circ})^{\circ}$, let it's transpose be Y. Now we can see that `rowechelon(19,Y)` and `rowechelon(19,A1)` give the same matrice, hence they have the same row space. So we can conclude that $U = (U^{\circ})^{\circ}$,

Question 7

Programs for computing bases for $U, W, U + W$ and $U \cap W$ can be found on page 12.

We have $dim(U) + dim(V) = dim(U + W) + dim(U \cap W)$.

- Modulo 11 with U the row space of $A1$ and W the row space of $B1$.

```
>> A1 = [ 0 1 7 2 10 ; 8 0 2 5 1 ; 2 1 2 5 5 ; 7 4 5 3 0];
>> B1 = [ 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 ];
>> Basis(11,A1)

ans =

     5     4     0     0
     1     0     0     0
     0     1     0     0
     0     0     1     0
     0     0     0     1

>> Basis(11,B1)

ans =

     4     9     6     0
     1     0     0     0
     0     1     0     0
     0     0     1     0
     0     0     0     1

>> sumBasis(11,A1,B1)

ans =

     1     0     0     0     0
```

```
     0     1     0     0     0
     0     0     1     0     0
     0     0     0     1     0
     0     0     0     0     1

>> intBasis(11,A1,B1)

ans =

     7     8     0
     5     6     0
     1     0     0
     0     1     0
     0     0     1
```

- Modulo 19 with U the row space of $A3$ and W the kernel of $A3$.

```
>> A3 = [ 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 ];
>> kerBasis(19,A3)

ans =

    13    18
    16     5
     3    10
     0    11
     2    13
     1     0
     0     1
>> kerA3 = (kerBasis(19,A3))';

>> Basis(19,A3)

ans =

    10     1    13    18     7
     0    17     0    15     5
     1     0     0     0     0
     0     1     0     0     0
     0     0     1     0     0
     0     0     0     1     0
     0     0     0     0     1

>> Basis(19,kerA3)
```

```
ans =

    13    18
    16     5
     3    10
     0    11
     2    13
     1     0
     0     1

>> sumBasis(19,A3,kerA3)

ans =

     1     0     0     0     0     0     0
     0     1     0     0     0     0     0
     0     0     1     0     0     0     0
     0     0     0     1     0     0     0
     0     0     0     0     1     0     0
     0     0     0     0     0     1     0
     0     0     0     0     0     0     1

>> intBasis(19,A3,kerA3)

ans =

   70 empty double matrix
```

- Modulo 23 with U the row space of $A3$ and W the kernel of $A3$.

```
>> A3 = [ 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 ];
>> kerBasis(23,A3)

ans =

    15     1
    20     5
     2    17
    19     0
    18    15
     1     0
     0     1

>> kerA3 = (kerBasis(23,A3))';

>> Basis(23,A3)
```

```
ans =

     6    15     8     2    15
     0    20     0    18     6
     1     0     0     0     0
     0     1     0     0     0
     0     0     1     0     0
     0     0     0     1     0
     0     0     0     0     1

>> Basis(23,kerA3)

ans =

    15     1
    20     5
     2    17
    19     0
    18    15
     1     0
     0     1

>> sumBasis(23,A3,kerA3)

ans =

     6     6    10     8     9     2
     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

>> intBasis(23,A3,kerA3)

ans =

    11
     3
     3
     5
     4
    16
     1
```

Question 8

If we had the field of real numbers instead of $GF(23)$, then $U \cap W$ would be the empty space. Becasue $\forall (x, y) \in (U, W)$, we have $x.y = 0$, so if there exists $v \in U \cap W$, we must have $v.v = 0$. But that's possible if and only if $v = 0$, hence $U \cap W = 0$. This is not the case when we work over $GF(23)$ as it's not a ordered field, so the inner product doesn't define a norm. The last example in Question 7 gives a contradiction for that.

Program for Question 1

```
(i) function [I] = inverse (p)
for i=1:p-1
    for j=1:p-1
        if mod(i*j,p) == 1
            I(i) = j;
            break
        else
            j = j+1;
        end
    end
end
end

(ii) function [I] = inverse2 (p)

for i=1:(p-1)/2
    for j=1:p-1
        if mod(i*j,p) == 1
            I(i) = j;
            I(p-i) = p-j;
            break
        else
            j = j+1;
        end
    end
end

end
```

Program for Question 3

```
function [A,l] = rowechelon(p,A)

I = inverse(p);
A = mod(A,p);
[m,n]=size(A);
l = zeros(1,0);
L = 1;

for i = 1:n
    for j = L:m
        if A(j,i) ~= 0
            A(j,:) = mod( A(j,:).*I(A(j,i)) ,p);

            storeMe = A(j,:); % store row v of A
            A(j,:) = A(L,:); % copy row u of A into row v of A
            A(L,:) = storeMe; % copy the stored row into row u of A

            for k = 1:m
                if k == L
                    A=A;
                else
                A(k,:) = mod( A(k,:) - A(k,i).*A(L,:) ,p);
                end
            end
            l(L) = i;
            L = L+1;

            break

        end
    end
end

end
```

Program for Question 4

```
function [C] = kerBasis(p,A)

[m,n]=size(A);
[A,l] = rowechelon(p,A);
r = length(l);
q = setdiff(1:n,l);

C = zeros(n,n-r);
for i = 1:n-r
     for k = 1:r
        C(l(k),i) = mod(-A(k,q(i)),p);
     end
        C(q(i),i) = 1;
end

end
```

Program for Question 7

```
(i) Basis.m
function [U] = Basis(p,A)

C = kerBasis(p,A);
U = kerBasis(p,C.');

end

(ii) sumBasis.m
function [Z] = sumBasis(p,A,B)

U = Basis(p,A);
W = Basis(p,B);

Y = union(U.',W.','rows');
Z = Basis(p,Y);

end

(iii) intBasis.m
function [R] = intBasis(p,A,B)

C = kerBasis(p,A);
D = kerBasis(p,B);

Q = sumBasis(p,C.',D.');
R = kerBasis(p,Q.');

end
```