Problem 1

Give the addition, multiplication and power table of GF(7)!
Solve the following equation over GF(7)
$6x+3=6$

Solution:

Let's write down the addition and multiplication table of GF(7)

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

*	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Let's write down the power table of all the elements of GF(7)

α^i in GF(7):

$\alpha \setminus i$	1	2	3	4	5	6	7
1	1	1	1	1	1	1	1
2	2	4	1	2	4	1	2
3	3	2	6	4	5	1	3
4	4	2	1	4	2	1	4
5	5	4	6	2	3	1	5
6	6	1	6	1	6	1	6
7	0	0	0	0	0	0	0

so the primitive elements are 3 and 5

$$6x+3=6 \qquad \left|-3 := +\left(3_+^{-1}\right)\right. \quad \text{the additive inverse element}$$

$$6x+3+\left(3_+^{-1}\right)=6+\left(3_+^{-1}\right) \qquad \left|\left(3_+^{-1}\right)=4\right.$$

$$6x=6+4 \qquad |\,6+4 \bmod 7$$

$$6x=3 \qquad |:6 := \cdot\left(6_\bullet^{-1}\right) \quad \text{the multiplicative inverse element}$$

$$\left(6_\bullet^{-1}\right)\cdot 6x=\left(6_\bullet^{-1}\right)\cdot 3$$

Using the multiplicative table, find the inverse element

n	1	2	3	4	5	6	7
$6\cdot n$	6	12	18	24	30	36	42
$6\cdot n \bmod 7$	6	5	4	3	2	1	0

$$\left(6_{\bullet}^{-1}\right)\cdot 6x = \left(6_{\bullet}^{-1}\right)\cdot 3 \qquad \left|\left(6_{\bullet}^{-1}\right)=6\right.$$

$$x = 6\cdot 3 \qquad |\, 6\cdot 3 \bmod 7 = 4$$

$$x = 4$$

verification:

$$6x+3=6 \qquad |\, x \leftarrow 4$$

$$6\cdot 4+3 \stackrel{?}{=} 6$$

$$6\cdot 4 \bmod 7 + 3 = 3+3 = 6 \equiv 6$$

Problem 2

Give the addition, multiplication and power table of GF(7)!
Determine the value of the following determinant over GF(5)

$$\det\begin{bmatrix} 2 & 1 & 2 \\ 1 & 3 & 2 \\ 1 & 0 & 1 \end{bmatrix} = ?$$

Solution:

$$\det\begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} = a\cdot\det\begin{bmatrix} e & f \\ h & i \end{bmatrix} - b\cdot\det\begin{bmatrix} d & f \\ g & i \end{bmatrix} + c\cdot\det\begin{bmatrix} d & e \\ g & h \end{bmatrix} =$$

$$= aei - afh - \left(bdi - bfg\right) + cdh - ceg$$

Consequently

$$\det\begin{bmatrix} 2 & 1 & 2 \\ 1 & 3 & 2 \\ 1 & 0 & 1 \end{bmatrix} = 2\cdot 3\cdot 1 - 2\cdot 0\cdot 2 - \left(1\cdot 1\cdot 1 - 1\cdot 1\cdot 2\right) + 2\cdot 1\cdot 0 - 2\cdot 1\cdot 3$$

Using the multiplication table over *GF(5)*:

*	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$$\det\begin{bmatrix} 2 & 1 & 2 \\ 1 & 3 & 2 \\ 1 & 0 & 1 \end{bmatrix} = 1 - 0 - \left(1-2\right) + 0 - 1 =$$

$$= 1 \qquad -\left(1+3\right) \qquad +4 =$$

$$= 1 \qquad +1 \qquad +4 = 1$$

Problem 3

Give the addition, multiplication and power table of GF(11)!

Solve the following equation over GF(11)

$7x-4=2$

Solution

$7x-4 = 2 \qquad \backslash +4$

$7x \quad = 6 \qquad \backslash :7$ which is equivalent to $\cdot 7^{-1}$

$x=4$

Problem 4

Given an RS code capable to correct every two error over GF(7), generated by the largest primitive element of the field.

a) Give the code parameters!
b) Construct the generator matrix!
c) Construct the parity check matrix!

Solution:

a) $t=2=\left\lfloor \frac{d_{\min}-1}{2} \right\rfloor \rightarrow d_{\min}=5, \alpha=5$, Since RS codes are MDS, $d_{\min}-1=n-k$

and we know that for RS codes $n=q-1$. From this, the parameters are:

$n=6, k=2, C(6,2)$

b) since $\mathbf{G}_{k\times n}=\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ \alpha_0 & \alpha_1 & \alpha_2 & \cdots & \alpha_{n-1} \\ \alpha_0^2 & \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_{n-1}^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha_0^{k-1} & \alpha_1^{k-1} & \alpha_2^{k-1} & \cdots & \alpha_{n-1}^{k-1} \end{pmatrix}, \alpha_i \in GF(q)\backslash\{0\}, i=0\ldots n-1$

Specially we can generate all the elements of *GF(q)* with the different powers of the primitive element we can use it to simplify the rule of constructing the generator matrix:

$$\mathbf{G}_{k\times n}=\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha^1 & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2\cdot(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{k-1} & \alpha^{(k-1)\cdot 2} & \cdots & \alpha^{(k-1)\cdot(n-1)} \end{pmatrix}$$

$$\mathbf{G}=\begin{pmatrix} 1\,1\,1\,1\,1\,1 \\ 1\,5\,4\,6\,2\,3 \end{pmatrix}$$

c) since $\mathbf{H}=\begin{bmatrix}1 & \alpha^1 & \alpha^2 & \cdots & \alpha^{n-1}\\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(n-1)}\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ 1 & \alpha^{n-k} & \alpha^{2(n-k)} & \cdots & \alpha^{(n-1)(n-k)}\end{bmatrix}$, α is a primitive element of $GF(q)$

$$\mathbf{H}=\begin{pmatrix}1\,5\,4\,6\,2\,3\\ 1\,4\,2\,1\,4\,2\\ 1\,6\,1\,6\,1\,6\\ 1\,2\,4\,1\,2\,4\end{pmatrix}$$

Problem 5

Given a $C(6,3)$ RS code which is generated by the largest primitive element of the field.

a) construct the generator matrix!

b) construct the parity check matrix!

c) How many error can be corrected with this code?

Solution:

the code is over $GF(7)$ so $\alpha=5$

a) $\mathbf{G}=\begin{pmatrix}1 & 1 & 1 & 1 & 1 & 1\\ 1 & 5 & 4 & 6 & 2 & 3\\ 1 & 4 & 2 & 1 & 4 & 2\end{pmatrix}$ and

b) $\mathbf{H}=\begin{pmatrix}1 & 5 & 4 & 6 & 2 & 3\\ 1 & 4 & 2 & 1 & 4 & 2\\ 1 & 6 & 1 & 6 & 1 & 6\end{pmatrix}$.

c) the RS codes are MDS codes, so $d_{\min}=n-k-1=4$, thus it can detect every 3 and correct every single error

Problem 6

We design an RS code over GF(11), which we want to correct every 3 errors using the largest possible message length.

a) Give code parameters n,k !

b) Construct the parity check matrix !

Solution:

From t=3, it follows that $t=\left\lfloor\frac{d_{\min}-1}{2}\right\rfloor$, $\quad d_{\min}=7$.

Since RS codes are MDS codes, thus $d_{\min}=n-k+1$.

Since we use GF(11), and the code is RS thus n=q-1=10, from this k=4.
H has n-k=6 rows and n columns.
H is in general:

$$\mathbf{H}=\begin{bmatrix}1 & \alpha^1 & \alpha^2 & \cdots & \alpha^{n-1}\\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(n-1)}\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ 1 & \alpha^{n-k} & \alpha^{2(n-k)} & \cdots & \alpha^{(n-1)(n-k)}\end{bmatrix},$$

if we choose α=2 as a primitive element

$$\mathbf{H}=\begin{bmatrix}1&2&4&8&5&10&9&7&3&6\\1&4&5&9&3&1&4&5&9&3\\1&8&9&6&4&10&3&2&5&7\\1&5&3&4&9&1&5&2&4&9\\1&10&1&10&1&10&1&10&1&10\\1&9&4&3&5&1&9&4&3&5\end{bmatrix},$$

with α=6 $\mathbf{H}=\begin{bmatrix}1&6&3&7&9&10&5&8&4&2\\1&3&9&5&4&1&3&9&5&4\\1&7&5&2&3&10&4&6&9&8\\1&9&4&3&5&1&9&4&3&5\\1&10&1&10&1&10&1&10&1&10\\1&5&3&4&9&1&5&3&4&9\end{bmatrix},$

with α=7 $\mathbf{H}=\begin{bmatrix}1&7&5&2&3&10&4&6&9&8\\1&5&3&4&9&1&5&3&4&9\\1&2&4&8&5&10&9&7&3&6\\1&3&9&5&4&1&3&9&5&4\\1&10&1&10&1&10&1&10&1&10\\1&4&5&9&3&1&4&5&9&3\end{bmatrix},$

and with α=8 $\mathbf{H}=\begin{bmatrix}1&8&3&6&4&10&3&2&5&7\\1&9&4&3&5&1&9&4&3&5\\1&6&3&7&9&10&5&8&4&2\\1&4&5&9&3&1&4&5&9&3\\1&10&1&10&1&10&1&10&1&10\\1&3&9&5&4&1&3&9&5&4\end{bmatrix}.$