بسم تعالی

حل تکلیف شماره ۱ کدگذاری کانال

1– Since m is not a prime, it can be factored as the product of two integers a and b,

$$m = a \cdot b$$

with $1 < a, b < m$. It is clear that both a and b are in the set $\{1, 2, \cdots, m-1\}$. It follows from the definition of modulo-m multiplication that

$$a \boxdot b = 0.$$

Since 0 is not an element in the set $\{1, 2, \cdots, m-1\}$, the set is not closed under the modulo-m multiplication and hence can not be a group.

2–

+	0	1	2	3	4	5	6	7	8	9	10
0	0	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10	0
2	2	3	4	5	6	7	8	9	10	0	1
3	3	4	5	6	7	8	9	10	0	1	2
4	4	5	6	7	8	9	10	0	1	2	3
5	5	6	7	8	9	10	0	1	2	3	4
6	6	7	8	9	10	0	1	2	3	4	5
7	7	8	9	10	0	1	2	3	4	5	6
8	8	9	10	0	1	2	3	4	5	6	7
9	9	10	0	1	2	3	4	5	6	7	8
10	10	0	1	2	3	4	5	6	7	8	9

×	0	1	2	3	4	5	6	7	8	9	10
0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10
2	0	2	4	6	8	10	1	3	5	7	9
3	0	3	6	9	1	4	7	10	2	5	8
4	0	4	8	1	5	9	2	6	10	3	7
5	0	5	10	4	9	3	8	2	7	1	6
6	0	6	1	7	2	8	3	9	4	10	5
7	0	7	3	10	6	2	9	5	1	8	4

8	0	8	5	2	10	7	4	1	9	6	3
9	0	9	7	5	3	1	10	8	6	4	2
10	0	10	9	8	7	6	5	4	3	2	1

	2	3	4	5	6	7	8	9	10
order	10	5	5	5	10	10	10	5	2

3– First we note that the set of sums of unit element contains the zero element 0. For any $1 \leq \ell < \lambda$,

$$\sum_{i=1}^{\ell} 1 + \sum_{i=1}^{\lambda-\ell} 1 = \sum_{i=1}^{\lambda} 1 = 0.$$

Hence every sum has an inverse with respect to the addition operation of the field $\mathrm{GF}(q)$. Since the sums are elements in $\mathrm{GF}(q)$, they must satisfy the associative and commutative laws with respect to the addition operation of $\mathrm{GF}(q)$. Therefore, the sums form a commutative group under the addition of $\mathrm{GF}(q)$.

Next we note that the sums contain the unit element 1 of $\mathrm{GF}(q)$. For each nonzero sum

$$\sum_{i=1}^{\ell} 1$$

with $1 \leq \ell < \lambda$, we want to show it has a multiplicative inverse with respect to the multiplication operation of $\mathrm{GF}(q)$. Since λ is prime, ℓ and λ are relatively prime and there exist two integers a and b such that

$$a \cdot \ell + b \cdot \lambda = 1, \tag{1}$$

where a and λ are also relatively prime. Dividing a by λ, we obtain

$$a = k\lambda + r \quad with \quad 0 \leq r < \lambda. \tag{2}$$

Since a and λ are relatively prime, $r \neq 0$. Hence

$$1 \leq r < \lambda$$

Combining (1) and (2), we have

$$\ell \cdot r = -(b + k\ell) \cdot \lambda + 1$$

Consider

$$\begin{aligned}
\sum_{i=1}^{\ell} 1 \cdot \sum_{i=1}^{r} 1 &= \sum_{i=1}^{\ell \cdot r} 1 = \sum_{i=1}^{-(b+k\ell)\cdot\lambda} +1 \\
&= (\sum_{i=1}^{\lambda} 1)(\sum_{i=1}^{-(b+k\ell)} 1) + 1 \\
&= 0 + 1 = 1.
\end{aligned}$$

Hence, every nonzero sum has an inverse with respect to the multiplication operation of GF(q). Since the nonzero sums are elements of GF(q), they obey the associative and commutative laws with respect to the multiplication of GF(q). Also the sums satisfy the distributive law. As a result, the sums form a field, a subfield of GF(q).

4–

By Theorem 2.22, S is a subspace if (i) for any $\mathbf{u}$ and $\mathbf{v}$ in S, $\mathbf{u}+\mathbf{v}$ is in S and (ii) for any c in F and $\mathbf{u}$ in S, $c\cdot\mathbf{u}$ is in S. The first condition is now given, we only have to show that the second condition is implied by the first condition for $F = GF(2)$. Let $\mathbf{u}$ be any element in S. It follows from the given condition that

$$\mathbf{u}+\mathbf{u}=\mathbf{0}$$

is also in S. Let c be an element in GF(2). Then, for any $\mathbf{u}$ in S,

$$c\cdot\mathbf{u}=\begin{cases}\mathbf{0} & for \quad c=0\\ \mathbf{u} & for \quad c=1\end{cases}$$

Clearly $c\cdot\mathbf{u}$ is also in S. Hence S is a subspace.

5–$G\times H^T = 0$ماتریس

6–

Let $\mathbf{u}$ and $\mathbf{v}$ be any two elements in $S_1\cap S_2$. It is clear the $\mathbf{u}$ and $\mathbf{v}$ are elements in S_1, and $\mathbf{u}$ and $\mathbf{v}$ are elements in S_2. Since S_1 and S_2 are subspaces,

$$\mathbf{u}+\mathbf{v}\in S_1$$

and

$$\mathbf{u}+\mathbf{v}\in S_2.$$

Hence,$\mathbf{u}+\mathbf{v}$ is in $S_1\cap S_2$. Now let $\mathbf{x}$ be any vector in $S_1\cap S_2$. Then $\mathbf{x}\in S_1$, and $\mathbf{x}\in S_2$. Again, since S_1 and S_2 are subspaces, for any c in the field F, $c\cdot\mathbf{x}$ is in S_1 and also in S_2. Hence $c\cdot\mathbf{v}$ is in the intersection, $S_1\cap S_2$. It follows from Theorem 2.22 that $S_1\cap S_2$ is a subspace.