1. **Problem 1.** Let $U$ be the subspace of $(\mathbb{Z}_2)^8$ that is spanned by the following vectors:

$(1, 0, 1, 0, 1, 0, 1, 0)$
$(0, 0, 1, 1, 1, 0, 0, 0)$
$(1, 0, 1, 0, 0, 1, 1)$
$(1, 0, 0, 1, 0, 1, 1, 0)$
$(0, 0, 1, 0, 0, 1, 0, 1)$
$(1, 0, 0, 1, 1, 1, 0, 0)$
$(0, 1, 1, 0, 1, 1, 0, 1)$
$(0, 1, 0, 0, 1, 0, 0, 0)$

What is the dimension of $U$? Find a basis of $U$.

We accomplish this by putting the matrix

$$
\begin{bmatrix}
1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\
1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\
0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\
1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\
0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\
0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\
\end{bmatrix}
$$

in Row-Echelon form. The resulting non-zero rows give a basis (whence their number is the dimension).

Row-Echelon form for this matrix is:

$$
\begin{bmatrix}
1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\end{bmatrix}
$$

Thus the dimension of $U$ is 5, and a basis is

$\{(1, 0, 0, 1, 1, 1, 0), (0, 1, 0, 0, 1, 0, 0), (0, 0, 1, 0, 1, 0, 0), (0, 0, 0, 1, 1, 0, 0), (0, 0, 0, 0, 0, 0, 0, 0)\}$.

2. **Problem 2.** Which of the following are valid ISBN codes?

3. 0-387-12831-X
4. 0-444-73068-3
5. 1-85881-284-4

Recall that $a = (a_1, \ldots, a_n)$ is a valid ISBN number if

$$a_1 + 2a_2 + \cdots + 10a_{10} = 0 \pmod{11}.$$

Then remembering that $X$ stands for 10, it is a simple matter to check that
\[ 1(0) + 2(3) + 3(8) + 4(7) + 5(1) + 6(2) + 7(8) + 8(3) + 9(1) + 10(X) = 264 = 11(24) \equiv 0 \pmod{11}, \]

\[ 1(0) + 2(4) + 3(4) + 4(4) + 5(7) + 6(3) + 7(0) + 8(6) + 9(8) + 10(3) = 239 = 11(21) + 8 \not\equiv 0 \pmod{11}, \text{ and} \]

\[ 1(1) + 2(8) + 3(5) + 4(8) + 5(8) + 6(1) + 7(2) + 8(8) + 9(4) + 10(4) = 264 = 11(24) \equiv 0 \pmod{11}. \]

So the first and third are valid, while the second is not.

6. **Problem 3.**

(a) Encode the word “groovy” using the error-correcting (7,4) Hamming code. (First write the word in binary using ASCII code, then encode the result with the (7,4) Hamming Code).

The first step is to write “groovy” in binary using ASCII code. So g=1100111, r=1110010, etc. This yields the string “groovy”= 110011111011011111000100111. Then split this into pieces containing four bits apiece, yielding: 1100 1111 1100 1011 0111 1110 1110 1101 1110 0100, where we have added two zeros to the last term (in order that it might have length four). Now multiply each 4-tuple by the matrix \( G \) (considering the 4-tuples as column vectors) where

\[
G = \begin{bmatrix}
1 & 1 & 0 & 1 \\
1 & 0 & 1 & 1 \\
1 & 0 & 0 & 0 \\
0 & 1 & 1 & 1 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1
\end{bmatrix}.
\]

Thus

\[
G \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \end{bmatrix},
\]

\[
G \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 1 \end{bmatrix},
\]

\[
G \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \end{bmatrix},
\]

\[
G \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix},
\]

\[
G \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix},
\]

\[
G \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}.
\]
We concatenate the resulting vectors, obtaining the string
011110011111110110001100011111101111111011011001011001100.

(b) You receive the following message which was encoded with the error-correcting (7,4) Hamming Code. Assuming that at most one error occurred in each 7-bit group during transmission (ie, in the way I convinced the computer to print it out), what was the original message? (In English, not binary ... again use ASCII). Note that the message you receive should be in one continuous string, but I have included a line break so that you can read it.
11100001101111011001110101010000000100110101010101001100110101010001111010101011011001

First we split the message into pieces of length 7, yielding vectors:
1110000 1101111 0110011 1010101 0000000 1001101 0101010 1010101 0011001 1010101 0001111 0101010 1011010 1101001.

Next multiply the matrix
\[
H = \begin{bmatrix}
1 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 1 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 1 & 1 & 1 & 1
\end{bmatrix}
\]
by each of these vectors (as column vectors, of course). Suppose that \( x \) is one of our vectors of length 7, \( x = x_1x_2x_3x_4x_5x_6x_7 \). If
\[
H = \begin{bmatrix}
x_1 \\
x_2 \\
x_3 \\
x_4 \\
x_5 \\
x_6 \\
x_7
\end{bmatrix}
\]
is zero then we extract the 3rd, 5th, 6th and 7th entries (ie, the string of 4 bits which the sender encoded was $x_3x_5x_6x_7$. If the result of the multiplication is the $i$th entry of $H$, then we change the $i$th bit of $x$ before again extracting the 3rd, 5th, 6th and 7th entries. The result is 14 length 4 strings which we combine and decipher using ASCII code.

The calculations follow

$$
\begin{bmatrix}
1 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 1 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 1 & 1 & 1 & 1
\end{bmatrix}
\begin{bmatrix}
1 \\
1 \\
0 \\
0 \\
0 \\
0 \\
0
\end{bmatrix}
= 
\begin{bmatrix}
0 \\
0 \\
0 \\
0
\end{bmatrix}
$$

Here the 3rd, 5th, 6th and 7th bits are 1,0,0,0.

$$
\begin{bmatrix}
1 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 1 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 1 & 1 & 1 & 1
\end{bmatrix}
\begin{bmatrix}
1 \\
1 \\
0 \\
0 \\
0 \\
0 \\
0
\end{bmatrix}
= 
\begin{bmatrix}
1 \\
1 \\
0 \\
0
\end{bmatrix}
$$

Here the result of multiplication is the 3rd column of $H$ and so we change $(1,1,0,1,1,1,1)$ to $(1,1,1,1,1,1,1)$ before extracting the 3rd, 5th, 6th and 7th entries, 1,1,1,1.

$$
\begin{bmatrix}
1 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 1 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 1 & 1 & 1 & 1
\end{bmatrix}
\begin{bmatrix}
1 \\
1 \\
0 \\
0 \\
0 \\
0 \\
0
\end{bmatrix}
= 
\begin{bmatrix}
0 \\
0 \\
0 \\
0
\end{bmatrix}
$$

Here the 3rd, 5th, 6th, and 7th entries are 1,0,1,1.

$$
\begin{bmatrix}
1 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 1 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 1 & 1 & 1 & 1
\end{bmatrix}
\begin{bmatrix}
1 \\
1 \\
0 \\
0 \\
0 \\
0 \\
0
\end{bmatrix}
= 
\begin{bmatrix}
0 \\
0 \\
0 \\
0
\end{bmatrix}
$$

Here the 3rd, 5th, 6th, and 7th entries are 1,1,0,1

$$
\begin{bmatrix}
1 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 1 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 1 & 1 & 1 & 1
\end{bmatrix}
\begin{bmatrix}
0 \\
0 \\
0 \\
0 \\
0 \\
0 \\
0
\end{bmatrix}
= 
\begin{bmatrix}
0 \\
0 \\
0 \\
0
\end{bmatrix}
$$

Here the 3rd, 5th, 6th, and 7th entries are 0,0,0,0.
Here the result of the multiplication is the 7th row of $H$, so we change (1,0,0,1,1,0,1) to (1,0,0,1,1,0,0) and extract the 3rd, 5th, 6th, and 7th entries, 0,1,0,0.

Here the 3rd, 5th, 6th, and 7th entries are 1,0,0,1.

Here the 3rd, 5th, 6th, and 7th entries are 0,1,1,1.
Here the 3rd, 5th, 6th, and 7th entries are 0,0,1,0.

\[
\begin{bmatrix}
1 & 0 & 1 & 0 & 1 & 1 & 1 \\
0 & 1 & 1 & 0 & 1 & 1 & 1 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 \\
\end{bmatrix}
\begin{bmatrix}
0 \\
1 \\
0 \\
\end{bmatrix}
\begin{bmatrix}
0 \\
1 \\
0 \\
\end{bmatrix}
= 
\begin{bmatrix}
1 \\
0 \\
0 \\
\end{bmatrix}
\]

Here the 3rd, 5th, 6th, and 7th entries are 1,0,1,0.

\[
\begin{bmatrix}
1 & 0 & 1 & 0 & 1 & 1 & 1 \\
0 & 1 & 1 & 0 & 1 & 1 & 1 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 \\
\end{bmatrix}
\begin{bmatrix}
1 \\
1 \\
0 \\
\end{bmatrix}
\begin{bmatrix}
1 \\
0 \\
0 \\
\end{bmatrix}
= 
\begin{bmatrix}
0 \\
0 \\
0 \\
\end{bmatrix}
\]

Here the 3rd, 5th, 6th, and 7th entries are 0,0,0,1.

Collecting all of our extracted entries we obtain the string:

100011110110000010000101110110011110101100001

Splitting this into pieces of length 7 we obtain:

1000111 1101111 0100000 1000010 1101100 1110101 1100101 0100001

Then translating this using ASCII (1000111=G, 1101111=o, etc.) code we obtain the message:

Go Blue!

7. 9.A E.4

Find the orders of the nonzero elements of \( \mathbb{Z}_{11} \).

We can easily check that

\[
\begin{array}{c|c}
  a & 2^a \\
  \hline
  1 & 2 \\
  2 & 4 \\
  3 & 8 \\
  4 & 5 \\
  5 & 10 \\
  6 & 9 \\
  7 & 7 \\
  8 & 3 \\
  9 & 6 \\
  10 & 1 \\
\end{array}
\]

So the order of 2 is 10. Then 3 = 2^8 so by proposition 3 (page 137) the order of 3 = 2^8 is

\[
\frac{10}{(10,8)} = \frac{10}{2} = 5.
\]

The other orders are also easily calculated using this formula.
### 8. 9A E.5

Find the orders of the elements of $\mathbb{Z}_{13}$.

This problem is the same as the previous after one realizes that 2 is a primitive element.

<table>
<thead>
<tr>
<th>$a$</th>
<th>$2^a$</th>
<th>$10$ $(10, 5)$</th>
<th>order of $a$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$2^1$</td>
<td>$10$ $(10, 0)$</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>$2^2$</td>
<td>$10$ $(10, 1)$</td>
<td>10</td>
</tr>
<tr>
<td>3</td>
<td>$2^3$</td>
<td>$10$ $(10, 8)$</td>
<td>5</td>
</tr>
<tr>
<td>4</td>
<td>$2^4$</td>
<td>$10$ $(10, 2)$</td>
<td>5</td>
</tr>
<tr>
<td>5</td>
<td>$2^5$</td>
<td>$10$ $(10, 4)$</td>
<td>5</td>
</tr>
<tr>
<td>6</td>
<td>$2^6$</td>
<td>$10$ $(10, 1)$</td>
<td>10</td>
</tr>
<tr>
<td>7</td>
<td>$2^7$</td>
<td>$10$ $(10, 7)$</td>
<td>10</td>
</tr>
<tr>
<td>8</td>
<td>$2^8$</td>
<td>$10$ $(10, 3)$</td>
<td>10</td>
</tr>
<tr>
<td>9</td>
<td>$2^9$</td>
<td>$10$ $(10, 6)$</td>
<td>5</td>
</tr>
<tr>
<td>10</td>
<td>$2^{10}$</td>
<td>$10$ $(10, 5)$</td>
<td>2</td>
</tr>
</tbody>
</table>

So the order of 2 is 12. The remaining orders are then easily calculated.

<table>
<thead>
<tr>
<th>$a$</th>
<th>$2^a$</th>
<th>$10$ $(10, 7)$</th>
<th>order of $a$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$2^1$</td>
<td>$12$ $(12, 0)$</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>$2^2$</td>
<td>$12$ $(12, 1)$</td>
<td>12</td>
</tr>
<tr>
<td>3</td>
<td>$2^3$</td>
<td>$12$ $(12, 3)$</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>$2^4$</td>
<td>$12$ $(12, 2)$</td>
<td>6</td>
</tr>
<tr>
<td>5</td>
<td>$2^5$</td>
<td>$12$ $(12, 5)$</td>
<td>4</td>
</tr>
<tr>
<td>6</td>
<td>$2^6$</td>
<td>$12$ $(12, 5)$</td>
<td>12</td>
</tr>
<tr>
<td>7</td>
<td>$2^7$</td>
<td>$12$ $(12, 11)$</td>
<td>12</td>
</tr>
<tr>
<td>8</td>
<td>$2^8$</td>
<td>$12$ $(12, 3)$</td>
<td>4</td>
</tr>
<tr>
<td>9</td>
<td>$2^9$</td>
<td>$12$ $(12, 5)$</td>
<td>3</td>
</tr>
<tr>
<td>10</td>
<td>$2^{10}$</td>
<td>$12$ $(12, 10)$</td>
<td>6</td>
</tr>
<tr>
<td>11</td>
<td>$2^11$</td>
<td>$12$ $(12, 7)$</td>
<td>12</td>
</tr>
<tr>
<td>12</td>
<td>$2^{12}$</td>
<td>$12$ $(12, 9)$</td>
<td>2</td>
</tr>
</tbody>
</table>

### 9. 9A E.8

Let $r$ and $s$ be relatively prime numbers $\geq 2$ and suppose the order of $a$ modulo $r$ is $d$, and the order of $a$ modulo $s$ is $e$. Let $m = rs$. Show that the order of $a$ modulo $m$ is the least common multiple of $d$ and $e$.

Let $L = [e, d]$. Then we are required to show that $a^L \equiv 1 \pmod{m}$ and that if $a^j \equiv 1 \pmod{m}$, then $L \leq j$.

Write that $L = db = ec$. Then

$$a^L = a^{db} = (a^d)^b \equiv 1 \pmod{r}, \text{ and}$$

$$a^L = a^{ec} = (a^e)^c \equiv 1 \pmod{s}.$$
We conclude that
\[ a^L = 1 + \lambda r \]
\[ a^L = 1 + \gamma s \]
for some \( \lambda, \gamma \in \mathbb{Z} \). Thus \( \lambda r + 1 = \gamma s + 1 \), or \( \lambda r = \gamma s \). This implies that \( r \mid \gamma s \) and because \((r, s) = 1\), we know that \( r \mid \gamma \) (we proved long ago that if \((r, s) = 1 \) and \( r \mid s \theta \), then \( r \mid \theta \)). So \( \gamma = \theta r \) for some \( \theta \in \mathbb{Z} \). Thus \( a^L = 1 + \gamma s = 1 + \theta rs = 1 + \theta m \equiv 1 \pmod{m} \). This shows that \( a^L \equiv 1 \pmod{m} \).

Suppose then that there exists \( j \) such that \( a^j \equiv 1 \pmod{m} \). This implies that \( a^j = 1 + \lambda rs \).

Rewriting this relationship we find that
\[ a^j = 1 + (\lambda s)r \]
\[ a^j = 1 + (\lambda r)s \]
and hence by proposition 2 (page 137), both \( d \) and \( e \) divide \( j \). But \( L \) is the least common multiple of \( d \) and \( e \), so \( L \leq j \). This completes the proof.

10. 9A E.10
Find the order of \( 2^{10} \pmod{77} \).
Notice that \( 77=7(11) \). Now \( 2^{10} \pmod{7} \) is 2, and the order of 2 modulo 7 is easily seen to be 3. By Fermat’s theorem, \( 2^{10} \pmod{11} = 1 \). So the order of \( 2^{10} \pmod{11} = 1 \). Thus by problem E.8, the order of \( 2^{10} \pmod{77} = 3 \).

11. 9A E.16
Show that if \( n \) is a number not divisible by 41, and \( n \) has order 2 modulo 41, then \( n = 40 + 41k \) for some integer \( k \).
If \( n \) has order 2 modulo 41 then \( n^2 \equiv 1 \pmod{41} \), or \( n^2 - 1 = 41r \) for some \( r \in \mathbb{Z} \). Thus \((n - 1)(n + 1) = 41r \) and because 41 is prime, either 41 \mid \((n - 1)\) or 41 \mid \((n + 1)\). If 41 \mid \((n - 1)\) then \( n - 1 \equiv 0 \pmod{41} \), so that \( n \equiv 1 \pmod{41} \), whence \( n \) would have order 1. This is a contradiction, and we conclude that 41 \mid \((n + 1)\). This implies that \( 41k' = n - 1 \) for some \( k' \in \mathbb{Z} \). Rewriting this equality yields, \( 41k' = 41(k' - 1) + 41 = n + 1 \), and if we write \( k = k' - 1 \) then \( 41k + 40 = n \) as required.

12. 9B E.3
Find the inverse of \([2]\) in \( \mathbb{Z}_p \) where \( p = 11; 13; 17 \); by Fermat’s theorem. Verify your answer by some other method.
By Fermat’s theorem,
\[ 2^{10} \equiv 1 \pmod{11}, \]
\[ 2^{12} \equiv 1 \pmod{13}, \]
\[ 2^{16} \equiv 1 \pmod{17}. \]
Thus
\[ 2(2^{9}) \equiv 1 \pmod{11}, \]
\[ 2(2^{11}) \equiv 1 \pmod{13}, \]
\[ 2(2^{15}) \equiv 1 \pmod{17}, \]
giving inverses \( 2^9, 2^{11}, \) and \( 2^{15} \) for \( p = 11, 13, \) and 17 respectively.
We know from question 9.A E.4, that \( 2^9 \equiv 6 \pmod{11}, \) and \( 2(6) \) is clearly 1 in \( \mathbb{Z}_{11} \).
It is similarly easy to check modulo 13 and 17. We find that \( 2^{11} \equiv 7 \pmod{13}, \) and \( 2(7) \) is clearly 1 in \( \mathbb{Z}_{13} \). Likewise, \( 2^{15} \equiv 9 \pmod{17}, \) and \( 2(9) \) is clearly 1 in \( \mathbb{Z}_{17} \).

13. 9B E.7
Prove that if \( P \) is prime, then for any number \( a \), divisible by \( p \) or not, \( a^p \equiv a \pmod{p} \).
If \( p \mid a \), then \( a^p \) and \( a \) are both congruent to zero modulo \( p \), so it is clear that \( a^p \equiv a \pmod{p} \).
If \( p \nmid a \), then we know that \( a^{p-1} \equiv 1 \pmod{p} \), by Fermat’s theorem. Multiplying both sides by \( a \) we find that \( a^p \equiv a \pmod{p} \) as required.
14. 9B E.11

Show that $n^{13} - n$ is divisible by 2, 3, 5, 7, and 13 for all $n$. Let $p$ be a prime. If $p$ divides $n$ then $p$ also divides $n^{13} - n$ so we may assume that $p$ does not divide $n$. Then by Fermat’s theorem, $n^{p-1} \equiv 1 \pmod{p}$. Because 1, 2, 4, 6, and 12 divide 12, by raising both sides of $n^{p-1} \equiv 1 \pmod{p}$ to the appropriate power (ie, 12, 6, 3, 2, and 1 respectively), we find that $n^{12} \equiv 1 \pmod{p}$. Multiplying through by $n$ yields $n^{13} \equiv n \pmod{p}$ so that $p$ divides $n^{13} - n$ as required.