Solutions to MATH3411 Problems 93-101

93.

a) Here, $\alpha^3 = \alpha^2 + 1$, so

i	0	1	2	3	4	5	6	7
α^i	1	α	α^2	α^2+1	$\alpha^2+\alpha+1$	$\alpha+1$	$\alpha^2+\alpha$	1

We see that α is primitive in $GF(8) = \mathbb{Z}_2[x]/\langle x^3 + x^2 + 1\rangle$.

b) $M_1(x) = m(x) = x^3 + x^2 + 1$: it has α as root and is irreducible over $\mathbb{Z}_2$ ($m(0) = m(1) = 1$).

c) (i) The constructed BCH code C has error check matrix $H = (1\,\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6)$ and thus length $n = 7$, $m = 3$ check bits (labelled by $1\,\alpha, \alpha^2$) and $k = n - m = 4$ information bits. The information rate is then $R = \frac{k}{n} = \frac{4}{7}$.

(ii) The message $\mathbf{m} = 0101$ has information polynomial $I(x) = 0x^3 + 1x^4 + 0x^5 + 1x^6 = x^4 + x^6$.
Now, $I(x) = x^4 + x^6 = (x^3 + x^2 + 1)(x^3 + x^2 + 1) + x = (x^3 + x^2 + 1)M_1(x) + R(x)$
where $R(x) = 1$ is the check polynomial.
(Here, a good shortcut is to just calculate $R(\alpha) = I(\alpha) = \alpha^4 + \alpha^6 = 1$; then $R(x) = 1$.)
The codeword polynomial is then $C(x) = I(x) + R(x) = 1 + x^4 + x^6$,
so the encoded message is $\mathbf{c} = 1000101$.

(iii) The codeword polynomial of the received message $\mathbf{d} = 1011011$ is $C(x) = 1 + x^2 + x^3 + x^5 + x^6$.
Then

$$\begin{aligned} C(\alpha) &= 1 + \alpha^2 + \alpha^3 + \alpha^5 + \alpha^6 \\ &= 1 + \alpha^2 + (\alpha^2 + 1) + (\alpha + 1) + (\alpha^2 + \alpha) \\ &= 1 + \alpha^2 \\ &= \alpha^3 \end{aligned}$$

We see that there is an error in the position labelled by α^3 (the fourth coordinate).
Correcting this, we get the corrected message $\mathbf{c} = 101\mathbf{0}011$, so the decoded message is $\mathbf{m} = 0011$.

94.

a) Here, $\beta^4 = \beta^3 + 1$, so

$\beta^0 = 1$	$\beta^8 = \beta^3 + \beta^2 + \beta$
$\beta^1 = \beta$	$\beta^9 = \beta^2 + 1$
$\beta^2 = \beta^2$	$\beta^{10} = \beta^3 + \beta$
$\beta^3 = \beta^3$	$\beta^{11} = \beta^3 + \beta^2 + 1$
$\beta^4 = \beta^3 + 1$	$\beta^{12} = \beta + 1$
$\beta^5 = \beta^3 + \beta + 1$	$\beta^{13} = \beta^2 + \beta$
$\beta^6 = \beta^3 + \beta^2 + \beta + 1$	$\beta^{14} = \beta^3 + \beta^2$
$\beta^7 = \beta^2 + \beta + 1$	$\beta^{15} = 1$

We see that β is primitive in $GF(16) = \mathbb{Z}_2[x]/\langle x^4 + x^2 + 1\rangle$.

b) (i) The constructed BCH code C has error check matrix $H = (1\,\beta, \beta^2, \beta^3, \ldots, \beta^{14})$ and thus length $n = 15$, $m = 4$ check bits (labelled by $1\,\beta, \beta^2, \beta^3$) and $k = n - m = 11$ information bits.
The information rate is then $R = \frac{k}{n} = \frac{11}{15}$.

(ii) The message $\mathbf{m} = 10000111001$ has information polynomial $I(x) = x^4 + x^9 + x^{10} + x^{11} + x^{14}$.
We now use β's minimal polynomial $M_1(x) = x^4 + x^3 + 1$ as modulus to calculate :

$$\begin{aligned} I(x) &= x^4 + x^9 + x^{10} + x^{11} + x^{14} \\ &= (x^{10} + x^9 + x^8 + x^4 + x^3 + x^2 + x + 1)(x^4 + x^3 + 1) + (x^2 + x + 1) \\ &= (x^{10} + x^9 + x^8 + x^4 + x^3 + x^2 + x + 1)M_1(x) + R(x) \end{aligned}$$

where $R(x) = x^2 + x + 1$ is the check polynomial.
(Here, a good shortcut is to just calculate $R(\alpha) = I(\alpha) = \alpha^4 + \alpha^9 + \alpha^{10} + \alpha^{11} + \alpha^{14} = \alpha^2 + \alpha + 1$; then $R(x) = x^2 + x + 1$.)
The codeword polynomial is then $C(x) = I(x) + R(x) = 1 + x + x^2 + x^4 + x^9 + x^{10} + x^{11} + x^{14}$, so the encoded message is $\mathbf{c} = 111010000111001$.

(iii) The received message $\mathbf{d} = 000001111000110$ has codeword polynomial

$$D(x) = x^5 + x^6 + x^7 + x^8 + x^{12} + x^{13}$$

Then

$$\begin{aligned} S(\mathbf{d}) = D(\beta) &= \beta^5 + \beta^6 + \beta^7 + \beta^8 + \beta^{12} + \beta^{13} \\ &= (\beta^3 + \beta + 1) + (\beta^3 + \beta^2 + \beta + 1) + (\beta^2 + \beta + 1) + (\beta^3 + \beta^2 + \beta) + (\beta^2 + 1) + (\beta^2 + \beta) \\ &= \beta^3 + \beta^2 + \beta = \beta^8 \end{aligned}$$

We see that there is an error in the position labelled by β^8 (the ninth coordinate).
Correcting this, we get the corrected message $\mathbf{c} = 00000111\mathbf{0}000110$ and thus the decoded message $\mathbf{m} = 0111\mathbf{0}000110$.

95.

a) Let α be a root of $q(x)$. Since $\alpha^5 = \alpha\alpha^4 = \alpha(\alpha^3 + \alpha^2 + \alpha + 1) = \alpha^4 + \alpha^3 + \alpha^2 + \alpha = 1$, we see that α is not primitive in F. Set $\gamma = \alpha + 1$. Then $\alpha = \gamma + 1$, so $q(\gamma + 1) = 0$:

$$\sum_{i=0}^{4} (\gamma + 1)^i \qquad \text{so} \qquad (\gamma^4 + 1) + (\gamma^3 + \gamma^2 + \gamma + 1) + (\gamma^2 + 1) + (\gamma + 1) + 1 = 0$$

and so $\gamma = \gamma^3 + 1$. Note that this is the same identity that β satisfies in Problem **95**, so we can re-use the power table and BCH construction from that problem. In particular,

$\gamma^0 = 1$	$\gamma^8 = \gamma^3 + \gamma^2 + \gamma$
$\gamma^1 = \gamma$	$\gamma^9 = \gamma^2 + 1$
$\gamma^2 = \gamma^2$	$\gamma^{10} = \gamma^3 + \gamma$
$\gamma^3 = \gamma^3$	$\gamma^{11} = \gamma^3 + \gamma^2 + 1$
$\gamma^4 = \gamma^3 + 1$	$\gamma^{12} = \gamma + 1$
$\gamma^5 = \gamma^3 + \gamma + 1$	$\gamma^{13} = \gamma^2 + \gamma$
$\gamma^6 = \gamma^3 + \gamma^2 + \gamma + 1$	$\gamma^{14} = \gamma^3 + \gamma^2$
$\gamma^7 = \gamma^2 + \gamma + 1$	$\gamma^{15} = 1$

Also, γ has minimal polynomial $M_1(x) = x^4 + x^3 + 1$.

b) The constructed BCH code C has error check matrix $H = (1\,\gamma, \gamma^2, \gamma^3, \ldots, \gamma^{14})$ and thus length $n = 15$, $m = 4$ check bits (labelled by $1\,\gamma, \gamma^2, \gamma^3$) and $k = n - m = 11$ information bits.
The information rate is then $R = \frac{k}{n} = \frac{11}{15}$.

(i) The message $\mathbf{m} = 10100111001$ has information polynomial $I(x) = x^4 + x^6 + x^9 + x^{10} + x^{11} + x^{14}$.
We now use β's minimal polynomial $M_1(x) = x^4 + x^3 + 1$ as modulus to calculate :

$$\begin{aligned} I(x) &= x^4 + x^6 + x^9 + x^{10} + x^{11} + x^{14} \\ &= (x^{10} + x^9 + x^8 + x^4 + x^3)(x^4 + x^3 + 1) + x^3 \\ &= (x^{10} + x^9 + x^8 + x^4 + x^3)M_1(x) + R(x) \end{aligned}$$

where $R(x) = x^3$ is the check polynomial.
(Here, a good shortcut is to just calculate $R(\alpha) = I(\alpha) = \alpha^4 + \alpha^6 + \alpha^9 + \alpha^{10} + \alpha^{11} + \alpha^{14} = \alpha^3$; then $R(x) = x^3$.)
The codeword polynomial is then $C(x) = I(x) + R(x) = x^3 + x^4 + x^6 + x^9 + x^{10} + x^{11} + x^{14}$, so the encoded message is $\mathbf{c} = 000110100111001$.

(ii) The received message $\mathbf{d} = 000101111000111$ has codeword polynomial

$$D(x) = x^3 + x^5 + x^6 + x^7 + x^8 + x^{12} + x^{13} + x^{14}$$

Then

$$\begin{aligned} S(\mathbf{d}) = D(\gamma) &= \gamma^3 + \gamma^5 + \gamma^6 + \gamma^7 + \gamma^8 + \gamma^{12} + \gamma^{13} + \gamma^{14} \\ &= \gamma^3 + (\gamma^3 + \gamma + 1) + (\gamma^3 + \gamma^2 + \gamma + 1) + (\gamma^2 + \gamma + 1) \\ &\quad + (\gamma^3 + \gamma^2 + \gamma) + (\gamma + 1) + (\gamma^2 + \gamma) + (\gamma^3 + \gamma^2) \\ &= \gamma^3 + \gamma^2 = \gamma^{14} \end{aligned}$$

We see that there is an error in the position labelled by γ^{14} (the fifteenth coordinate).
Correcting this, we get the corrected message $\mathbf{c} = 00010111100111\mathbf{0}$.
The decoded message is then $\mathbf{m} = 0111100111\mathbf{0}$.

96. Since

$$(\beta^3)^4 + (\beta^3)^3 + (\beta^3)^2 + \beta^3 + 1 = \beta^{12} + \beta^9 + \beta^6 + \beta^3 + 1 = (\beta + 1) + (\beta^2 + 1) + (\beta^3 + \beta^2 + \beta + 1) + \beta^3 + 1 = 0$$

we see that β^3 is a root of $M_3(x) = x^4 + x^3 + x^2 + x + 1$. This is an irreducible polynomial over $(Z)_2$: it has no roots ($M_3(0) = M_3(1) = 1 \neq 0$), so it has no linear factors, and it has no quadratic factors since $(x^2 + ax + 1)(x^2 + bx + 1) = x^4 + (a + b)x^3 + abx^2 + (a + b)x + 1$ cannot have all five terms. Thus, $M_3(x)$ is the minimal polynomial of β^3.
We can thus construct a double-error correcting code C over $GF(16) = \mathbb{Z}_2/\langle M_1(x)\rangle$ where $M_1(x) = x^4+x^3+1$ is the minimal polynomial for β; in particular, C has check matrix $H = \begin{pmatrix} 1 & \beta & \beta^2 & \cdots & \beta^{14} \\ 1 & \beta^3 & \beta^6 & \cdots & \beta^{42} \end{pmatrix}$.

a. The message $\mathbf{m} = 1011011$ has information polynomial $I(x) = x^8 + x^{10} + x^{11} + x^{13} + x^{14}$.
We reduce $I(x)$ modulo $M(x) = M_1(x)M_3(x) = (x^4+x^3+1)(x^4+x^3+x^2+x+1) = x^8+x^4+x^2+x+1$:

$$\begin{aligned} I(x) &= x^8 + x^{10} + x^{11} + x^{13} + x^{14} \\ &= (x^6 + x^5 + x^3 + x)(x^8 + x^4 + x^2 + x + 1) + (x^7 + x^5 + x^4 + x^2 + x) \\ &= (x^6 + x^5 + x^3 + x)M(x) + R(x) \end{aligned}$$

where $R(x) = x^7 + x^5 + x^4 + x^2 + x$ is the check polynomial.
The codeword polynomial is then $C(x) = I(x)+R(x) = x+x^2+x^4+x^5+x^7+x^8+x^{10}+x^{11}+x^{13}+x^{14}$, so the encoded message is $\mathbf{c} = 011011011011011$.

b. The received message $\mathbf{d} = 111011000110001$ has codeword polynomial

$$D(x) = 1 + x + x^2 + x^4 + x^5 + x^9 + x^{10} + x^{14}$$

Then

$$\begin{aligned}
S(\mathbf{d}) = \begin{pmatrix} D(\beta) \\ D(\beta^3) \end{pmatrix} &= \begin{pmatrix} 1 + \beta + \beta^2 + \beta^4 + \beta^5 + \beta^9 + \beta^{10} + \beta^{14} \\ 1 + \beta^3 + \beta^6 + \beta^{12} + \beta^{15} + \beta^{27} + \beta^{30} + \beta^{42} \end{pmatrix} \\
&= \begin{pmatrix} 1 + \beta + \beta^2 + \beta^4 + \beta^5 + \beta^9 + \beta^{10} + \beta^{14} \\ 1 + \beta^3 + \beta^6 + \beta^{12} + 1 + \beta^{12} + 1 + \beta^{12} \end{pmatrix} \\
&= \begin{pmatrix} 1 + \beta + \beta^2 + \beta^4 + \beta^5 + \beta^9 + \beta^{10} + \beta^{14} \\ 1 + \beta^3 + \beta^6 + \beta^{12} \end{pmatrix} \\
&= \begin{pmatrix} 1 + \beta + \beta^2 + (\beta^3+1) + (\beta^3+\beta+1) + (\beta^2+1) + (\beta^3+\beta) + (\beta^3+\beta^2) \\ 1 + \beta^3 + (\beta^3+\beta^2+\beta+1) + (\beta+1) \end{pmatrix} \\
&= \begin{pmatrix} \beta^2 + \beta \\ 1 + \beta^2 \end{pmatrix} = \begin{pmatrix} \beta^{13} \\ \beta^9 \end{pmatrix}
\end{aligned}$$

Since $D(\beta) \neq 0$, there is at least one error.
Since $D(\beta)^3 = (\beta^{-2})^3 = \beta^{-6} = \beta^9 = D(\beta^3)$, there is only one error, given by $D(\beta) = \beta^{13}$ (the 14th position). Correcting this, we get the corrected message $\mathbf{c} = 1110110001100\mathbf{1}1$.
The decoded message is then $\mathbf{m} = 110001100\mathbf{1}1$.

c. The received message $\mathbf{d} = 111011000110101$ has codeword polynomial

$$D(x) = 1 + x + x^2 + x^4 + x^5 + x^9 + x^{10} + x^{12} + x^{14}$$

Then

$$\begin{aligned}
S(\mathbf{d}) = \begin{pmatrix} D(\beta) \\ D(\beta^3) \end{pmatrix} &= \begin{pmatrix} 1 + \beta + \beta^2 + \beta^4 + \beta^5 + \beta^9 + \beta^{10} + \beta^{12} + \beta^{14} \\ 1 + \beta^3 + \beta^6 + \beta^{12} + \beta^{15} + \beta^{27} + \beta^{30} + \beta^{36} + \beta^{42} \end{pmatrix} \\
&= \begin{pmatrix} 1 + \beta + \beta^2 + \beta^4 + \beta^5 + \beta^9 + \beta^{10} + \beta^{12} + \beta^{14} \\ 1 + \beta^3 + \beta^6 + \beta^{12} + 1 + \beta^{12} + 1 + \beta^6 + \beta^{12} \end{pmatrix} \\
&= \begin{pmatrix} 1 + \beta + \beta^2 + \beta^4 + \beta^5 + \beta^9 + \beta^{10} + \beta^{12} + \beta^{14} \\ 1 + \beta^3 + \beta^{12} \end{pmatrix} \\
&= \begin{pmatrix} 1 + \beta + \beta^2 + (\beta^3+1) + (\beta^3+\beta+1) + (\beta^2+1) + (\beta^3+\beta) + (\beta+1) + (\beta^3+\beta^2) \\ 1 + \beta^3 + (\beta+1) \end{pmatrix} \\
&= \begin{pmatrix} \beta^2 + 1 \\ \beta^3 + \beta \end{pmatrix} = \begin{pmatrix} \beta^9 \\ \beta^{10} \end{pmatrix}
\end{aligned}$$

Since $D(\beta) \neq 0$, there is at least one error.
Since $D(\beta)^3 = (\beta^9)^3 = \beta^{27} = \beta^{12} \neq D(\beta^3)$, there are two errors, say in positions β^j and β^ℓ, respectively. Writing $S(\mathbf{d}) = \begin{pmatrix} S_1 \\ S_3 \end{pmatrix} = \begin{pmatrix} \beta^j + \beta^\ell \\ \beta^{3j} + \beta^{3\ell} \end{pmatrix}$, we have that

$$S_1^3 = (\beta^j + \beta^\ell)^3 = \beta^{3j} + \beta^{3\ell} + 3\beta^j\beta^\ell(\beta^j + \beta^\ell) = S_3 + \beta^j\beta^\ell S_1$$

so $\beta^j\beta^\ell = S_1^2 + \frac{S_3}{S_1}$. Therefore, β^j and β^ℓ are the roots of the polynomial

$$x^2 + (\beta^j + \beta^\ell)x + \beta^j\beta^\ell = x^2 + S_1 x + (S_1^2 + \frac{S_3}{S_1}) = x^2 + \beta^9 x + (\beta^{18} + \frac{\beta^{10}}{\beta^9}) = x^2 + \beta^9 x + \beta^3 + \beta$$

We find these roots by trial and error:

$$\begin{aligned}
1^2 + \beta^9 1 + \beta^3 + \beta &= 1 + \beta^2 + 1 + \beta^3 + \beta = \beta^3 + \beta^2 + \beta \neq 0\\
\beta^2 + \beta^9\beta + \beta^3 + \beta &= \beta^2 + (\beta^2 + 1) + \beta^3 + \beta = \beta^3 + \beta + 1 \neq 0\\
(\beta^2)^2 + \beta^9\beta^2 + \beta^3 + \beta &= (\beta^3 + 1) + (\beta^3 + \beta^2 + 1) + \beta^3 + \beta = \beta^3 + \beta^2 \neq 0\\
(\beta^3)^2 + \beta^9\beta^3 + \beta^3 + \beta &= (\beta^3 + \beta^2 + \beta + 1) + (\beta + 1) + \beta^3 + \beta = \beta^2 + \beta \neq 0\\
(\beta^4)^2 + \beta^9\beta^4 + \beta^3 + \beta &= (\beta^3 + \beta^2 + \beta) + (\beta^2 + \beta) + \beta^3 + \beta = \beta \neq 0\\
(\beta^5)^2 + \beta^9\beta^5 + \beta^3 + \beta &= (\beta^3 + \beta) + (\beta^3 + \beta^2) + \beta^3 + \beta = \beta^3 + \beta^2 \neq 0\\
(\beta^6)^2 + \beta^9\beta^6 + \beta^3 + \beta &= (\beta + 1) + 1 + \beta^3 + \beta = \beta^3 \neq 0\\
(\beta^7)^2 + \beta^9\beta^7 + \beta^3 + \beta &= (\beta^3 + \beta^2) + \beta + \beta^3 + \beta = \beta^2 \neq 0\\
(\beta^8)^2 + \beta^9\beta^8 + \beta^3 + \beta &= \beta + 1 \neq 0\\
(\beta^9)^2 + \beta^9\beta^9 + \beta^3 + \beta &= \beta^3 + \beta \neq 0\\
(\beta^{10})^2 + \beta^9\beta^{10} + \beta^3 + \beta &= (\beta^3 + \beta + 1) + (\beta^3 + 1) + \beta^3 + \beta = \beta^3 \neq 0\\
(\beta^{11})^2 + \beta^9\beta^{11} + \beta^3 + \beta &= (\beta^2 + \beta + 1) + (\beta^3 + \beta + 1) + \beta^3 + \beta = \beta^2 + \beta \neq 0\\
(\beta^{12})^2 + \beta^9\beta^{12} + \beta^3 + \beta &= (\beta^2 + 1) + (\beta^3 + \beta^2 + \beta + 1) + \beta^3 + \beta = 0
\end{aligned}$$

We have found one of the roots, namely β^{12}. The other one is then

$$S_1 - \beta^{12} = \beta^9 - \beta^{12} = (\beta^2 + 1) - (\beta + 1) = \beta^2 + \beta = \beta^{13}$$

The errors are then in the positions labelled by β^{12} and β^{13} (the 13th and 14th coordinates). Correcting this, we get the corrected message $\mathbf{c} = 111011000110\mathbf{01}1$.
The decoded message is then $\mathbf{m} = 11000110\mathbf{01}1$.

d. The received message $\mathbf{d} = 110010000011001$ has codeword polynomial

$$D(x) = 1 + x + x^4 + x^{10} + x^{11} + x^{14}$$

Then

$$\begin{aligned}
S(\mathbf{d}) = \begin{pmatrix} D(\beta) \\ D(\beta^3) \end{pmatrix} &= \begin{pmatrix} 1 + \beta + \beta^4 + \beta^{10} + \beta^{11} + \beta^{14} \\ 1 + \beta^3 + \beta^{12} + \beta^{30} + \beta^{33} + \beta^{42} \end{pmatrix}\\
&= \begin{pmatrix} 1 + \beta + \beta^4 + \beta^{10} + \beta^{11} + \beta^{14} \\ 1 + \beta^3 + \beta^{12} + 1 + \beta^3 + \beta^{12} \end{pmatrix}\\
&= \begin{pmatrix} 1 + \beta + (\beta^3 + 1) + (\beta^3 + \beta) + (\beta^3 + \beta^2 + 1) + (\beta 3 + \beta^2) \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}
\end{aligned}$$

Since $S(\mathbf{d}) = \mathbf{0}$, there are no errors, so the decoded message is $\mathbf{m} = 10000011001$.

97. Let β be a root of $M_1(x) = x^4 + x + 1$. Then, $\beta^4 = \beta + 1$, so

$\beta^0 = 1$	$\beta^8 = \beta^2 + 1$
$\beta^1 = \beta$	$\beta^9 = \beta^3 + \beta$
$\beta^2 = \beta^2$	$\beta^{10} = \beta^2 + \beta + 1$
$\beta^3 = \beta^3$	$\beta^{11} = \beta^3 + \beta^2 + \beta$
$\beta^4 = \beta + 1$	$\beta^{12} = \beta^3 + \beta^2 + \beta + 1$
$\beta^5 = \beta^2 + \beta$	$\beta^{13} = \beta^3 + \beta^2 + 1$
$\beta^6 = \beta^3 + \beta^2$	$\beta^{14} = \beta^3 + 1$
$\beta^7 = \beta^3 + \beta + 1$	$\beta^{15} = 1$

We construct a double-error correcting code C over $GF(16) = \mathbb{Z}_2/\langle M_1(x)\rangle$ where $M_1(x) = x^4 + x + 1$ is the minimal polynomial for β; in particular, C has check matrix $H = \begin{pmatrix} 1 & \beta & \beta^2 & \cdots & \beta^{14} \\ 1 & \beta^3 & \beta^6 & \cdots & \beta^{42} \end{pmatrix}$.
Since β^3 is a root of $M_3(x) = x^4 + x^3 + x^2 + x + 1$ and $M_3(x)$ is irreducible, we see that $M_3(x)$ is the minimal polynomial of β^3.

a. The message $\mathbf{m} = 1011011$ has information polynomial $I(x) = x^8 + x^{10} + x^{11} + x^{13} + x^{14}$.
We reduce $I(x)$ modulo $M(x) = M_1(x)M_3(x) = (x^4+x+1)(x^4+x^3+x^2+x+1) = x^8+x^7+x^6+x^4+1$:

$$\begin{aligned} I(x) &= x^8 + x^{10} + x^{11} + x^{13} + x^{14} \\ &= (x^6 + x^4 + x^2 + x)(x^8 + x^7 + x^6 + x^4 + 1) + (x^7 + x^5 + x^4 + x^2 + x) \\ &= (x^6 + x^4 + x^2 + x)M(x) + R(x) \end{aligned}$$

where $R(x) = x^7 + x^5 + x^4 + x^2 + x$ is the check polynomial.
The codeword polynomial is then $C(x) = I(x)+R(x) = x+x^2+x^4+x^5+x^7+x^8+x^{10}+x^{11}+x^{13}+x^{14}$, so the encoded message is $\mathbf{c} = 011011011011011$.

b. The received message $\mathbf{d} = 011110001101001$ has codeword polynomial

$$D(x) = x + x^2 + x^3 + x^4 + x^8 + x^9 + x^{11} + x^{14}$$

Then

$$\begin{aligned} S(\mathbf{d}) = \begin{pmatrix} D(\beta) \\ D(\beta^3) \end{pmatrix} &= \begin{pmatrix} \beta + \beta^2 + \beta^3 + \beta^4 + \beta^8 + \beta^9 + \beta^{11} + \beta^{14} \\ \beta^3 + \beta^6 + \beta^9 + \beta^{12} + \beta^{24} + \beta^{27} + \beta^{33} + \beta^{42} \end{pmatrix} \\ &= \begin{pmatrix} \beta + \beta^2 + \beta^3 + \beta^4 + \beta^8 + \beta^9 + \beta^{11} + \beta^{14} \\ \beta^3 + \beta^6 + \beta^9 + \beta^{12} + \beta^9 + \beta^{12} + \beta^3 + \beta^{12} \end{pmatrix} \\ &= \begin{pmatrix} \beta + \beta^2 + \beta^3 + \beta^4 + \beta^8 + \beta^9 + \beta^{11} + \beta^{14} \\ \beta^6 + \beta^{12} \end{pmatrix} \\ &= \begin{pmatrix} \beta + \beta^2 + \beta^3 + (\beta + 1) + (\beta^2 + 1) + (\beta^3 + \beta) + (\beta^3 + \beta^2 + \beta) + (\beta^3 + 1) \\ (\beta^3 + \beta^2) + (\beta^3 + \beta^2 + \beta + 1) \end{pmatrix} \\ &= \begin{pmatrix} \beta^2 + 1 \\ \beta + 1 \end{pmatrix} \\ &= \begin{pmatrix} \beta^8 \\ \beta^4 \end{pmatrix} \end{aligned}$$

Since $D(\beta) \neq 0$, there is at least one error. Since $D(\beta)^3 = (\beta^8)^3 = \beta^{24} = \beta^9 \neq D(\beta^3)$, there are two errors, say in positions β^j and β^ℓ, respectively. Writing $S(\mathbf{d}) = \begin{pmatrix} S_1 \\ S_3 \end{pmatrix}$, we have, as in Problem 96**c.**, that β^j and β^ℓ are the roots of the polynomial

$$x^2 + (\beta^j + \beta^\ell)x + \beta^j\beta^\ell x^2 + S_1 x + (S_1^2 + \frac{S_3}{S_1}) = x^2 + \beta^8 x + (\beta^{16} + \frac{\beta^4}{\beta^8}) = x^2 + \beta^8 x + \beta^3 + \beta^2$$

We find these roots by trial and error:

$$\begin{aligned}
1^2 + \beta^8 1 + \beta^3 + \beta^2 &= 1 + \beta^2 + 1 + \beta^3 + \beta^2 = \beta^3 \neq 0 \\
\beta^2 + \beta^8\beta + \beta^3 + \beta^2 &= \beta^2 + (\beta^3 + \beta) + \beta^3 + \beta^2 = \beta \neq 0 \\
(\beta^2)^2 + \beta^8\beta^2 + \beta^3 + \beta^2 &= (\beta + 1) + (\beta^2 + \beta + 1) + \beta^3 + \beta^2 = \beta^3 \neq 0 \\
(\beta^3)^2 + \beta^8\beta^3 + \beta^3 + \beta^2 &= (\beta^3 + \beta^2) + (\beta^3 + \beta^2 + \beta) + \beta^3 + \beta^2 = \beta^3 + \beta^2 + \beta \neq 0 \\
(\beta^4)^2 + \beta^8\beta^4 + \beta^3 + \beta^2 &= (\beta^2 + 1) + (\beta^3 + \beta^2 + \beta + 1) + \beta^3 + \beta^2 = \beta^2 + \beta \neq 0 \\
(\beta^5)^2 + \beta^8\beta^5 + \beta^3 + \beta^2 &= (\beta^2 + \beta + 1) + (\beta^3 + \beta^2 + 1) + \beta^3 + \beta^2 = \beta^2 + \beta \neq 0 \\
(\beta^6)^2 + \beta^8\beta^6 + \beta^3 + \beta^2 &= (\beta^3 + \beta^2 + \beta + 1) + (\beta^3 + 1) + \beta^3 + \beta^2 = \beta^3 + \beta \neq 0 \\
(\beta^7)^2 + \beta^8\beta^7 + \beta^3 + \beta^2 &= (\beta^3 + 1) + 1 + \beta^3 + \beta^2 = \beta^2 \neq 0 \\
(\beta^8)^2 + \beta^8\beta^8 + \beta^3 + \beta^2 &= \beta^3 + \beta^2 = \beta^2 \neq 0 \\
(\beta^9)^2 + \beta^8\beta^9 + \beta^3 + \beta^2 &= \beta^3 + \beta^2 + \beta^3 + \beta^2 = 0
\end{aligned}$$

We have found one of the roots, namely β^9. The other one is then

$$S_1 - \beta^9 = \beta^8 - \beta^9 = (\beta^2 + 1) - (\beta^3 + \beta)) = \beta^3 + \beta^2 + \beta + 1 = \beta^{12}$$

The errors are then in the positions labelled by β^9 and β^{12} (the 10th and 13th coordinates).
Correcting this, we get the corrected message $\mathbf{c} = 011110001\mathbf{0}01\mathbf{1}01$.
The decoded message is then $\mathbf{m} = 1\mathbf{0}01\mathbf{1}01$.

98. Here, $\alpha^4 = \alpha + 1$, so we can just use the power table from Problem 97, replacing β by α. Then

$$\begin{aligned}
R(\alpha) &= 1 + \alpha + \alpha^2 + \alpha^4 + \alpha^8 + \alpha^9 + \alpha^{11} + \alpha^{14} \\
&= 1 + \alpha + \alpha^2 + (\alpha + 1) + (\alpha^2 + 1) + (\alpha^3 + \alpha) + (\alpha^3 + \alpha^2 + \alpha) + (\alpha^3 + 1) \\
&= \alpha^2 + \alpha^3 = \alpha^6 \\
R(\alpha^3) &= 1 + \alpha^3 + \alpha^6 + \alpha^{12} + \alpha^{24} + \alpha^{27} + \alpha^{33} + \alpha^{42} \\
&= 1 + \alpha^3 + \alpha^6 + \alpha^{12} + \alpha^9 + \alpha^{12} + \alpha^3 + \alpha^{12} \\
&= 1 + \alpha^6 + \alpha^9 + \alpha^{12} \\
&= 1 + (\alpha^3 + \alpha^2) + (\alpha^3 + \alpha) + (\alpha^3 + \alpha^2 + \alpha + 1) = \alpha^3
\end{aligned}$$

Since $R(\alpha) \neq 0$, there is at least one error. Since $R(\alpha)^3 = (\alpha^6)^3 = \alpha^{18} = \alpha^3 \neq R(\alpha^3)$, there is just a single error, say in position α^j, respectively. Then $R(x) = C(x) + x^j$, so $\alpha^j = R(\alpha) - C(\alpha) = R(\alpha) = \alpha^6$.
We see that there is an error in the x^6 term.
Correcting this, we get the polynomial $C(x) = 1 + x + x^2 + x^4 + x^6 + x^8 + x^9 + x^{11} + x^{14}$.

99.

a. The minimal polynomials of β and β^3 are $M_1(x) = x^4 + x^3 + 1$ and $M_3(x) = x^4 + x^3 + x^2 + x + 1$ (from Problem 96). Since β^5 is a root of the irreducible polynomial $M_5(x) = x^2 + x + 1$, we see that $M_5(x)$ is the minimal polynomial of β^5. Since 1, 3, and 5 are in separate cyclotomic sets, the polynomials $M_1(x)$, $M_3(x)$, $M_5(x)$ have no roots in common, so their lowest common multiple is just their product:

$$M(x) = M_1(x)M_3(x)M_5(x) = (x^4+x^3+1)(x^4+x^3+x^2+x+1)(x^2+x+1) = x^{10}+x^9+x^8+x^6+x^5+x^2+1$$

The degree of this polynomial is $m = 10$, so there are $k = n - m = 15 - 10 = 5$ information bits. The information rate is then $R = \frac{k}{n} = \frac{5}{15} = \frac{1}{3}$.

b. The received message $\mathbf{d} = 110000100001001$ has codeword polynomial

$$D(x) = 1 + x + x^6 + x^{11} + x^{14}$$

Then

$$\begin{aligned}
S_1 &= D(\beta) &&= 1 + \beta + \beta^6 + \beta^{11} + \beta^{14} \\
&&&= 1 + \beta + (\beta^3 + \beta^2 + \beta + 1) + (\beta^3 + \beta^2 + 1) + (\beta^3 + \beta^2) = \beta^3 + \beta^2 + 1 = \beta^{11} \\
S_2 &= D(\beta^2) &&= D(\beta)^2 = \beta^{22} = \beta^7 \\
S_3 &= D(\beta^3) &&= 1 + \beta^3 + \beta^{18} + \beta^{33} + \beta^{42} = 1 + \beta^3 + \beta^3 + \beta^3 + \beta^{12} = 1 + \beta^3 + (\beta + 1) = \beta^{10} \\
S_4 &= (S_2)^2 &&= \beta^{14} \\
S_5 &= D(\beta^5) &&= 1 + \beta^5 + \beta^{30} + \beta^{55} + \beta^{70} = 1 + \beta^5 + 1 + \beta^{10} + \beta^{10} = \beta^5 \\
S_6 &= (S_3)^2 &&= \beta^{20} = \beta^5
\end{aligned}$$

Then

$$\begin{aligned}
\mathbf{S} = \begin{pmatrix} S_1 & S_2 & S_3 \\ S_2 & S_3 & S_4 \\ S_3 & S_4 & S_5 \end{pmatrix} &= \begin{pmatrix} \beta^{11} & \beta^7 & \beta^{10} \\ \beta^7 & \beta^{10} & \beta^{14} \\ \beta^{10} & \beta^{14} & \beta^5 \end{pmatrix} \to \begin{pmatrix} \beta^{11} & \beta^7 & \beta^{10} \\ \beta^7 - \beta^{11}\beta^{11} & \beta^{10} - \beta^7\beta^{11} & \beta^{14} - \beta^{10}\beta^{11} \\ \beta^{10} - \beta^{11}\beta^{14} & \beta^{14} - \beta^7\beta^{14} & \beta^5 - \beta^{10}\beta^{14} \end{pmatrix} \\
&= \begin{pmatrix} \beta^{11} & \beta^7 & \beta^{10} \\ 0 & \beta^{10} - \beta^3 & \beta^{14} - \beta^6 \\ 0 & \beta^{14} - \beta^6 & \beta^5 - \beta^9 \end{pmatrix} = \begin{pmatrix} \beta^{11} & \beta^7 & \beta^{10} \\ 0 & \beta & \beta^{12} \\ 0 & \beta^{12} & \beta^8 \end{pmatrix} \\
&\to \begin{pmatrix} \beta^{11} & \beta^7 & \beta^{10} \\ 0 & \beta & \beta^{12} \\ 0 & \beta^{12} - \beta\beta^{11} & \beta^8 - \beta^{12}\beta^{11} \end{pmatrix} = \begin{pmatrix} \beta^{11} & \beta^7 & \beta^{10} \\ 0 & \beta & \beta^{12} \\ 0 & 0 & 0 \end{pmatrix}
\end{aligned}$$

This matrix has rank 2, so there are just two errors, say in positions β^j and β^ℓ, respectively. as in Problem 96**c.**, β^j and β^ℓ are the roots of the polynomial

$$x^2 + (\beta^j + \beta^\ell)x + \beta^j\beta^\ell x^2 + S_1 x + (S_1^2 + \frac{S_3}{S_1}) = x^2 + \beta^{11}x + (\beta^{22} + \frac{\beta^{10}}{\beta^{11}}) = x^2 + \beta^{11}x + \beta^3 + \beta + 1$$

We find these roots by trial and error:

$$\begin{aligned}
1^2 + \beta^{11}1 + \beta^3 + \beta + 1 &= 1 + \beta^2 + 1 + \beta^3 + \beta + 1 = \beta^3 + \beta^2 + \beta \neq 0 \\
\beta^2 + \beta^{11}\beta + \beta^3 + \beta + 1 &= \beta^2 + (\beta + 1) + \beta^3 + \beta + 1 = \beta^3 + \beta^2 \neq 0 \\
(\beta^2)^2 + \beta^{11}\beta^2 + \beta^3 + \beta + 1 &= (\beta^3 + 1) + (\beta^2 + \beta) + \beta^3 + \beta + 1 = \beta^2 \neq 0 \\
(\beta^3)^2 + \beta^{11}\beta^3 + \beta^3 + \beta + 1 &= (\beta^3 + \beta^2 + \beta + 1) + (\beta^3 + \beta^2) + \beta^3 + \beta + 1 = \beta^3 \neq 0 \\
(\beta^4)^2 + \beta^{11}\beta^4 + \beta^3 + \beta + 1 &= (\beta^3 + \beta^2 + \beta) + 1 + \beta^3 + \beta + 1 = \beta^2 \neq 0 \\
(\beta^5)^2 + \beta^{11}\beta^5 + \beta^3 + \beta + 1 &= (\beta^3 + \beta) + \beta + \beta^3 + \beta + 1 = \beta + 1 \neq 0 \\
(\beta^6)^2 + \beta^{11}\beta^6 + \beta^3 + \beta + 1 &= (\beta + 1) + \beta^2 + \beta^3 + \beta + 1 = \beta^3 + \beta^2 \neq 0 \\
(\beta^7)^2 + \beta^{11}\beta^7 + \beta^3 + \beta + 1 &= (\beta^3 + \beta^2) + \beta^3 + \beta^3 + \beta + 1 = \beta^3 + \beta^2 + \beta + 1 \neq 0 \\
(\beta^8)^2 + \beta^{11}\beta^8 + \beta^3 + \beta + 1 &= \beta + \beta^3 + 1 + \beta^3 + \beta + 1 = 0
\end{aligned}$$

We have found one of the roots, namely β^8. The other one is then

$$S_1 - \beta^8 = \beta^{11} - \beta^8 = (\beta^3 + \beta^2 + 1) - (\beta^3 + \beta^2 + \beta) = \beta + 1 = \beta^{12}$$

The errors are then in the positions labelled by β^8 and β^{12} (the 9th and 13th coordinates).
Correcting this, we get the corrected message $\mathbf{c} = 11000010\mathbf{1}001\mathbf{1}01$.
The decoded message is then $\mathbf{m} = 01\mathbf{1}01$.

c. The received message $\mathbf{d} = 101010010010101$ has codeword polynomial

$$D(x) = 1 + x^2 + x^4 + x^7 + x^{10} + x^{12} + x^{14}$$

Then

$$\begin{aligned}
S_1 &= D(\beta) &&= 1 + \beta^2 + \beta^4 + \beta^7 + \beta^{10} + \beta^{12} + \beta^{14} \\
& &&= 1 + \beta^2 + (\beta^3 + 1) + (\beta^2 + \beta + 1) + (\beta^3 + \beta) + (\beta + 1) + (\beta^3 + \beta^2) \\
& &&= \beta^3 + \beta^2 + \beta = \beta^8 \\
S_2 &= D(\beta^2) &&= D(\beta)^2 = \beta^{16} = \beta \\
S_3 &= D(\beta^3) &&= 1 + \beta^6 + \beta^{12} + \beta^{21} + \beta^{30} + \beta^{36} + \beta^{42} \\
& &&= \beta^6 \\
S_4 &= (S_2)^2 &&= \beta^2 \\
S_5 &= D(\beta^5) &&= 1 + \beta^{10} + \beta^{20} + \beta^{35} + \beta^{50} + \beta^{60} + \beta^{70} \\
& &&= 1 + \beta^{10} + \beta^5 + \beta^5 + \beta^5 + 1 + \beta^{10} \\
& &&= \beta^5 \\
S_6 &= (S_3)^2 &&= \beta^{12}
\end{aligned}$$

Assuming that there are 3 errors, we need to solve the equation in Theorem 7.1 of the notes:

$$\begin{pmatrix} S_1 & S_2 & S_3 \\ S_2 & S_3 & S_4 \\ S_3 & S_4 & S_5 \end{pmatrix} \begin{pmatrix} \sigma_3 \\ \sigma_2 \\ \sigma_1 \end{pmatrix} = \begin{pmatrix} S_4 \\ S_5 \\ S_6 \end{pmatrix}$$

$$\left(\begin{array}{ccc|c} S_1 & S_2 & S_3 & S_4 \\ S_2 & S_3 & S_4 & S_5 \\ S_3 & S_4 & S_5 & S_6 \end{array}\right) = \left(\begin{array}{ccc|c} \beta^8 & \beta & \beta^6 & \beta^2 \\ \beta & \beta^6 & \beta^2 & \beta^5 \\ \beta^6 & \beta^2 & \beta^5 & \beta^{12} \end{array}\right) \to \left(\begin{array}{ccc|c} 1 & \beta^5 & \beta & \beta^4 \\ \beta^8 & \beta & \beta^6 & \beta^2 \\ \beta^6 & \beta^2 & \beta^5 & \beta^{12} \end{array}\right)$$

$$\to \left(\begin{array}{ccc|c} 1 & \beta^5 & \beta & \beta^4 \\ 0 & \beta-\beta^{13} & \beta^6-\beta^9 & \beta^2-\beta^{12} \\ 0 & \beta^2-\beta^{11} & \beta^5-\beta^7 & \beta^{12}-\beta^{10} \end{array}\right) = \left(\begin{array}{ccc|c} 1 & \beta^5 & \beta & \beta^4 \\ 0 & \beta^2 & \beta^{10} & \beta^7 \\ 0 & \beta^4 & \beta^{14} & \beta^4 \end{array}\right)$$

$$\to \left(\begin{array}{ccc|c} 1 & \beta^5 & \beta & \beta^4 \\ 0 & 1 & \beta^8 & \beta^5 \\ 0 & \beta^4 & \beta^{14} & \beta^4 \end{array}\right) \to \left(\begin{array}{ccc|c} 1 & 0 & \beta-\beta^{13} & \beta^4-\beta^{10} \\ 0 & 1 & \beta^8 & \beta^5 \\ 0 & 0 & \beta^{14}-\beta^{12} & \beta^4-\beta^9 \end{array}\right) = \left(\begin{array}{ccc|c} 1 & 0 & \beta^2 & \beta^{12} \\ 0 & 1 & \beta^8 & \beta^5 \\ 0 & 0 & \beta^6 & \beta^{14} \end{array}\right)$$

$$\to \left(\begin{array}{ccc|c} 1 & 0 & \beta^2 & \beta^{12} \\ 0 & 1 & \beta^8 & \beta^5 \\ 0 & 0 & 1 & \beta^8 \end{array}\right) \to \left(\begin{array}{ccc|c} 1 & 0 & 0 & \beta^{12}-\beta^{10} \\ 0 & 1 & 0 & \beta^5-\beta \\ 0 & 0 & 1 & \beta^8 \end{array}\right) = \left(\begin{array}{ccc|c} 1 & 0 & 0 & \beta^4 \\ 0 & 1 & 0 & \beta^4 \\ 0 & 0 & 1 & \beta^8 \end{array}\right)$$

Therefore, $\sigma_1 = \beta^8$ and $\sigma_2 = \sigma_3 = \beta^4$. The three errors are given by the roots of the polynomial

$$z^3 + \sigma_1 z^2 + \sigma_2 z + \sigma_3 = z^3 + \beta^8 z^2 + \beta^4 z + \beta^4$$

We find these roots by trial and error:

$$\begin{aligned}
1^3 + \beta^8 1^2 + \beta^4 1 + \beta^4 &= \beta^8 \neq 0 \\
\beta^3 + \beta^8\beta^2 + \beta^4\beta + \beta^4 &= \beta^3 + \beta^{10} + \beta^5 + \beta^4 = 0 \\
(\beta^2)^3 + \beta^8(\beta^2)^2 + \beta^4\beta^2 + \beta^4 &= \beta^6 + \beta^{12} + \beta^6 + \beta^4 = \beta^{10} \neq 0 \\
(\beta^3)^3 + \beta^8(\beta^3)^2 + \beta^4\beta^3 + \beta^4 &= \beta^9 + \beta^{14} + \beta^7 + \beta^4 = \beta + 1 \neq 0 \\
(\beta^4)^3 + \beta^8(\beta^4)^2 + \beta^4\beta^4 + \beta^4 &= \beta^9 \neq 0 \\
(\beta^5)^3 + \beta^8(\beta^5)^2 + \beta^4\beta^5 + \beta^4 &= 1 + \beta^3 + \beta^9 + \beta^4 = \beta^9 \neq 0 \\
(\beta^6)^3 + \beta^8(\beta^6)^2 + \beta^4\beta^6 + \beta^4 &= \beta^3 + \beta^5 + \beta^{10} + \beta^4 \neq 0
\end{aligned}$$

We have found two roots, namely $\beta = \beta^1$ and β^6. The third root is then the constant term β^4 divided by these: $\frac{\beta^4}{\beta\beta^6} = \beta^{12}$. The errors are thus in positions 1, 6, and 12 (the 2nd, 7th, and 13th coordinate positions). The corrected message is then $\mathbf{c} = 1\mathbf{1}11010\mathbf{1}10010\mathbf{0}01$.

The decoded message is then $\mathbf{m} = 10\mathbf{0}01$.

100.

a.

$$\begin{aligned}
K_1 &= \{1, 5, 25, \ldots \pmod{24}\} = \{1, 5\} \\
K_2 &= \{2, 10, \ldots \pmod{24}\} = \{2, 10\} \\
K_3 &= \{3, 15, \ldots \pmod{24}\} = \{3, 15\} \\
K_4 &= \{4, 20, \ldots \pmod{24}\} = \{4, 20\} \\
K_6 &= \{6, 30, \ldots \pmod{24}\} = \{6\} \\
K_7 &= \{7, 35, \ldots \pmod{24}\} = \{7, 11\} \\
K_8 &= \{8, 40, \ldots \pmod{24}\} = \{8, 16\} \\
K_9 &= \{9, 45, \ldots \pmod{24}\} = \{9, 21\} \\
K_{12} &= \{12, 60, \ldots \pmod{24}\} = \{12\} \\
K_{13} &= \{13, 65, \ldots \pmod{24}\} = \{13, 17\} \\
K_{14} &= \{14, 70, \ldots \pmod{24}\} = \{14, 22\} \\
K_{18} &= \{18, 90, \ldots \pmod{24}\} = \{18\} \\
K_{19} &= \{19, 90, \ldots \pmod{24}\} = \{19, 23\}
\end{aligned}$$

b. There are 9 possible BCH codes based on $GF(25)$. The table below lists the number of information bits k and the maximum error correcting capability t for each one:

k	20	16	15	11	9	8	4	3	1
t	1	2	3	4	5	6	8	9	11

101.

a. $x^7 + 1 = (x + 1)(x^3 + x + 1)(x^3 + x^2 + 1)$

b. $h(x) = x^4 + x^2 + x + 1.$

c.

$$G = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} \qquad H = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

d. A basis for C is

$$\{1101000, \quad 0110100, \quad 0011010, \quad 0001101\}$$