SECTION A

1. (a) In $\mathbf{R}[x]$ find polynomials $q(x)$ and $r(x)$ such that

$$x^6 + 2x^5 - 3x^4 + x^2 - x - 1 = q(x)(x^3 + 2x^2 + 1) + r(x)$$

where either $r(x) = 0$ or the degree of $r(x)$ is less than that of $x^3 - 1$.

(b) In $\mathbf{R}[x]$, divide $f(x) = x^5 - 2x^4 + 2x^3 + x - 1$ by $x - 3$ and show that the remainder is $f(3)$.

(c) In the field of complex numbers, find the nearest Gaussian integer to $\dfrac{11 - 4i}{5 + i}$.

Hence or otherwise find Gaussian integers

$$a + bi, c + di (a, b, c, d \in \mathbf{Z})$$

such that $11 - 4i = (5 + i)(a + bi) + (c + di)$ where $c^2 + d^2 < 26$. [9 marks]

2. (a) Decide, giving reasons, in which of the following cases S is a subring of R, where

(i) $S = \{ 3a + ib : a, b \in \mathbf{Z} \}, R = \{ a + ib : a, b \in \mathbf{Z} \}$ (the Gaussian integers).

(ii) $S = \{ a + 3ib : a, b \in \mathbf{Z} \}, R = \{ a + ib : a, b \in \mathbf{Z} \}$ (the Gaussian integers).

(iii) $S = \{ f(x^3) : f \in \mathbf{Z}[x] \}, R = \mathbf{Z}[x]$

(b) Decide, giving reasons, in which of the following cases I is an ideal of R, where

(i) $I = \{ 3n + 1 : n \in \mathbf{Z} \}, R = \mathbf{Z}$

(ii) $I = \{ 3n : n \in \mathbf{Z} \}, R = \mathbf{Z}$

(iii) $I = \{ f : f \in \mathbf{Z}[x], f(0) = 1 \}, R = \mathbf{Z}[x]$

(iv) $I = \{ f : f \in \mathbf{Z}[x], f(0) = 0 \}, R = \mathbf{Z}[x]$ [9 marks]

3. (a) Express each of the following elements as a product of irreducibles in the given ring

(i) 13 in $\mathbf{Z}$.

(ii) 2 in $\{ a + ib : a, b \in \mathbf{Z} \}$ (the Gaussian integers).

(iii) 6 in $\mathbf{Z}$.

(iv) 6 in $\{ a + ib : a, b \in \mathbf{Z} \}$ the Gaussian integers

(b) Express the polynomial $x^2 + x + 1$ as a product of irreducible polynomials in each of the following rings

(i) $\mathbf{Z}[x]$.

(ii) $\mathbf{Z}_2[x]$.

(iii) $\mathbf{Z}_7[x]$. [9 marks]

4. Prove that $x^2 + 1$ is irreducible over $\mathbf{F}_3$. Find two other distinct irreducible polynomials of degree 2 over $\mathbf{F}_3$. By considering the ring $\mathbf{F}_3[x]$ subject to the side condition $x^2 + 1 = 0$ write down a multiplication table for $\mathbf{F}_9$ and show that the non-zero elements of $\mathbf{F}_9$ form a cyclic group under multiplication. [9 marks]

5. Show that the affine plane over $\mathbf{F}_3$ has 9 points and 12 lines, and that the affine plane over $\mathbf{F}_2$ has 4 points and 6 lines. Show that there is a Steiner system $S(2, 3, 12)$.

Dr Rayner has taught a first year class for twelve years. Each year he tells exactly three jokes; he never repeats the same pair of jokes (in any order) in any one year. Find the smallest number of jokes he must know. [9 marks]

6. Consider the following words in $\mathbf{F}_2^6$: 110110, 011011, 101101, 000000. Show that they form a group code which can detect three errors and correct one. Decide whether or not this code is cyclic. In each of the following cases, find the distance of w from each of the four code words, and indicate whether there is a nearest one.

(a) $w = 110101$.

(b) $w = 111111$.

(c) $w = 111100$. [10 marks]

SECTION B

7. (a) Say what is meant by an euclidean domain.

(b) Show that for any field $\mathbf{F}$, $\mathbf{F}[x]$ is an euclidean domain.

(c) Let $f = x^6 + x^4 - x^3 + x^2 + 1$ and $g = x^4 + x^2 + 1$.

Calculate q and r such that $f = gq + r$ and the degree of r is less than four.

(d) Prove that any common divisor of g and r is a divisor of f, and also that any common divisor of f and g is a divisor of r.

(e) Repeat the calculation in (c) with g and r in the place of f and g. Hence find the highest common factor h (say) of f and g and find two polynomials u and v such that $h = fu + gv$. [15 marks]

8. Show that $x^4 + 1$ is divisible by $x^2 + x + 2$ over $\mathbf{F}_3$, and hence or otherwise express $x^8 - 1$ as a product of irreducible factors over $\mathbf{F}_3$.

Show that $x^4 + x^3 + x + 2$ is a divisor of $x^8 + 2$ over $\mathbf{F}_3$, and considering the ideal generated by this polynomial in $\mathbf{F}_3[x]/(x^8 - 1)\mathbf{F}_3[x]$ show that

$$G = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 \\ 0 & 1 & 2 & 0 \\ 1 & 0 & 1 & 2 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

generates a cyclic code $\mathcal{A}$ of length 8. Show that $\mathcal{A}$ has 81 words, and find a a parity check matrix H for $\mathcal{A}$. Verify that the ranks of the matrices G and H are both four, and that $HG = 0$. [15 marks]

9. Let

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

By solving the linear equations

$$H \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{pmatrix} = 0,$$

or otherwise, find a generator matrix for a code $\mathcal{C}$ with parity check matrix H. Show that $\mathcal{C}$ has sixteen words, and can correct one error.

Draw up a table of syndromes and coset leaders for $\mathcal{C}$, and where possible correct any errors in the following words: 1111010, 1000100, 1110001 and 1110000. [15 marks]

10. Show that the affine plane over $\mathbf{F}_4$ has 16 points and 20 lines. Draw up a schedule for an experiment in which all possible combinations of four varieties of wheat and four types of fertiliser are compared by four experimental farms over a period of five years. Each year, each farm tests all four varieties of wheat and all four kinds of fertiliser in different combinations on four experimental plots. Each pair of possible combinations of one variety of wheat and one kind of fertiliser is tested once and once only during the experiment. [15 marks]

11. Say what is meant by a quadratic residue code.

Make a list of the irreducible polynomials of degree one and of degree three over $\mathbf{F}_2$, and calculate their product.

Find a generator matrix and a parity check matrix for a cyclic code $\mathcal{C}$ of length seven generated by one of the irreducible polynomials of degree three over $\mathbf{F}_2$.

Show that the equation $x^2 = 2$ has two roots in $\mathbf{F}_7$.

Show that $\mathcal{C}$ is a quadratic residue code, and hence find its minimum distance. [15 marks]

Solutions

1. (a)

				1	0	−3	5			
1	2	0	1	1	2	−3	0	1	−1	−1
				1	2	0	1			
						−3	−1	1	−1	
							5	1	2	−1
							5	10	0	5
								−9	2	−6

Thus, quotient $= x^3 - 3x + 5$, remainder $= -9x^2 + 2x - 6$.

(b)

		1	1	5	12	37	
1	−3	1	−2	2	−3	1	−1
		1	−3				
			1	2			
			1	−3			
				5	−3		
				5	−15		
					12	1	
					12	−36	
						37	−1
						37	−111
							110

Hence quotient $= x^4 + x^3 + 5x^2 + 12x + 37$, remainder $= 110$.
Also $f(3) = 3^5 - 2.3^4 + 2.3^3 - 3.3^2 + 3 - 1 = 110$.

(c) $\frac{11-4i}{5+i} = \frac{(11-4i)(5-i)}{(5+i)(5-i)} = \frac{59-31i}{26} = 2 + \frac{7}{26} - (1 + \frac{5}{26})i$.
Nearest Gaußian integer is $2 - i$, so use this as the quotient $c + id$, thus $11 - 4i = (5 + i)(2 - i) + e + if$, whence $e = 0$ and $f = 1$.

2. (a) i. $1_R \notin S$, not a subring.

ii. S is a subring because S is closed under $\pm$ and $\times$ $1_R = 1+0i \in S$. $(a_1 + 3ib_1) \pm (a_2 + 3ib_2) = (a_1 \pm a_2) + 3(b_1 \pm b_2)i$ and $(a_1 + 3ib_1) \times (a_2 + 3ib_2) = (a_1a_2 - 9b_1b_2) + 3(a_1b_2 + a_2b_1)$

iii. S is a subring. S is closed under $\pm$ and $\times$
$1_R = 1 + 0x^3 + \ldots \in S$.

$\sum a_i x^{3i} \pm \sum b_i x^{3i} = \sum (a_i \pm b_i) x^{3i} \in S$
$\sum a_i x^{3i} . \sum b_i x^{3i} = \sum \sum (a_i b_j) x^{3(i+j)} \in S$

(b) i. No $1 \in I$, but $1 + 1 \notin I$

ii. Yes Closed under $\pm$
$3n_1 \pm 3n_2 = 3(n_1 \pm n_2)$ and $\forall r \in \mathbf{Z} 3nr \in I$

iii. No $0 \notin I$

iv. Yes $f(0) = 0, g(0) = 0 \Longrightarrow f \pm g|_0 = 0$ and $rf|_0 = r(0)f(0) = r(0).0 = 0$.

.

3. (a) (i) 13 (ii) $(1 + i)(1 - i)$ (iii) 2×3 (iv) $3(1 + i)(1 - i)$

(b) (i) $x^2 + x + 1$ (ii) $x^2 + x + 1$ (since $f(0) = f(1) = 1$ there are no roots in $\mathbf{Z}_2$. (iii)$(x - 2)(x - 4)$ (since $f(2) = f(4) = 0$).

4.

$\mathbf{F}_3$	0	1	2
$x^2 + 1$	1	2	2

$x^2 + 1$ has no linear factor. The other ireducible polynomials are $x^2 + x - 1$ and $x^2 - x - 1$. The other polynomials of degree 2 are reducible $x^2, x^2 + x, x^2 - x, x^2 - 1, x^2 + x + 1 = (x + 1)^2, x^2 + x + 1 = (x - 1)^2$.

In the quotient ring, denote the image of x by i, so that $i^2 = -1$.

$\times$	1	-1	i	$i+1$	$i-1$	$-i$	$-i+1$	$-i-1$
1	1	-1	i	$i+1$	$i-1$	$-i$	$-i+1$	$-i-1$
-1	-1	1	$-i$	$-i-1$	$-i+1$	i	$i-1$	$i+1$
i	i	$-i$	-1	$-1+i$	$-i-1$	1	$1+i$	$1-i$
$i+1$	$i+1$	$-i-1$	$i-1$	$-i$	1	$1-i$	-1	i
$i-1$	$i-1$	$-i+1$	$-1-i$	1	i	$1+i$	$-i$	-1
$-i$	$-i$	i	1	$1-i$	$i+1$	-1	$-1-i$	$-1+i$
$-i+1$	$-i+1$	$i-1$	$1+i$	-1	$-i$	$-1-i$	i	1
$-i-1$	$-i-1$	$i+1$	$1-i$	i	-1	$i-1$	1	$-i$

The orders of the elements may be found from the multiplication table. The order of 1 is 1, of -1 is 2, of i is 4, and of $1 + i$ is 8 (no further calculation needed). The group has order 8 and so is cyclic, generated by $1 + i$.

5. The points are pairs (a, b), where $a = 0, 1, -1$ and $b = 0, 1, -1$. There are nine possiblities. There are lines of the form $y = mx + c$ (three

possibilities for each of m and c, so nine altogether) and of the form $x = a$ (three possibilities). Regarding the twelve lines as varieties in a combinatorial design, these are triples, any two points lie on a unique line. Thus we have an $S(2, 3, 12)$. Now assume the jokes are distinct and distinguishable. Any two jokes occur in only one year of the twelve (and with a minimal set of minimal jokes, must occur in one year), so we have an $S(2, 3, 12)$. There are therefore nine jokes.

6. Let $a = 110110$, $b = 011011$, $c = 101101$, $d = 000000$. Then $a + b = c$, $b + c = a$,$c + a = b$ and $a + b + c = d = 0$. The set is closed under $+$. It is a linear space code over $\mathbf{F}_2$.

   The minimum weight of a code word is three. The code can detect two errors and correct one. The code is cyclic because if the last symbol is moved to the first place a becomes b, b becomes c, and c becomes a. (And if you must, d becomes d.) For 110101, distance to a is 2, to b is 4, to c is 2, to d is 4. For 111111, distance to a is 2, to b is 2, to c is 2, to d is 6. For 111100, distance to a is 2, to b is 4, to c is 2, to d is 4.

7. An E.D. is an I.D. R with a function $e\colon R \setminus 0 \to \mathbf{N}$ such that (i) $e(xy) \geq e(x)(x \neq 0, y \neq 0)$ (ii) $\forall x, y(y \neq 0)\exists q, r$ such that $x = yq + r$ and either $r = 0$ or $e(r) < e(y)$. $\mathbf{F}[x]$ with $e =$ degree satisfies (i) because $e(fg) = e(f) + e(g) \geq e(f)$ and satisfies (ii) because q and r may be found by synthetic division. (c) By inspection $f = gx^2 + (-x^3 + 1)$.(*They might set out formal synthetic division, which is easy to write but long to type!*). If d divides g and r then d divides $gq + r = f$. If d divides both f and g then d divides $f - gq = r$. (d) repeating the calculation, division of $x^4 + x^2 + 1$ by $-x^3 + 1$ gives $x^4 + x^2 + 1 = -x(-x^3 + 1) + x^2 + x + 1$. Next division of $-x^3 + 1$ by $x^2 + x + 1$ is as follows

			-1	1		
1	1	1	-1	0	0	1
			-1	-1	-1	
				1	1	1
				1	1	1

   so that $-x^3 + 1 = (-x + 1)(x^2 + x + 1)$ It is now clear that the hcf is $x^2 + x + 1$. Also $x^2 + x + 1 = x^4 + x^2 + 1 + x(-x^3 + 1) = g + x(f - gx^2) = xf + (1 - x^3)g$ as required.

8.

			1	2	2		
1	1	2	1	0	0	0	1
			1	1	2		
				2	1	0	
				2	2	1	
					2	2	1
					2	2	1

Thus $x^4+1=(x^2+x+2)(x^2+2x+2)$. Over $\mathbf{F}_3$ these factors are irreducible:

x	0	1	2
x^2+x+2	2	1	2
x^2+2x+2	2	2	1

They have no zeros, and hence no linear factors. $x^8-1=(x^4+1)(x^4-1)=(x^4+1)(x^2+1)(x+1)(x+2)$. Again x^2+1 is irreducible. $x^4+x^3+x+2=(x^2+1)(x^2+x+2)$, so we have a divisor of x^8-1. x^4+x^3+x+2 generates a cyclic code of length eight, with matrix G. The column space has a basis of four elements, hence the code has $3^4=81$ words. The parity check matrix H will be generated by the polynomial $(x^2-1)(x^2+2x+2)=x^4+2x^3+x^2+x+1$. Thus it is

$$\begin{pmatrix} 1 & 2 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 2 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 2 & 1 & 1 & 1 \end{pmatrix}$$

Rank G is four, from the first four rows, and rank H is four from the last four columns, and

$$HG=\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

9.

$$H\mathbf{x}=0 \iff \begin{matrix}\rho_2-\rho_1\\ \rho_3-\rho_1\end{matrix} \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \end{pmatrix}\mathbf{x}=0$$

$$\iff \rho_3-\rho_2 \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}\mathbf{x}=0$$

$$\Longleftrightarrow \rho_1 - \rho_3 \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix} \mathbf{x} = 0.$$

Hence

$$\begin{pmatrix} x_1 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{pmatrix} = \begin{pmatrix} x_5 + x_6 + x_7 \\ x_4 + x_5 + x_7 \\ x_4 + x_5 + x_6 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{pmatrix} = x_4 \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + x_5 \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + x_6 \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} + x_7 \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

Hence

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

Dimension=4. Number of words $= 2^4 = 16$. Minimum weight is three (for example, enumerate the elements).

10. Points are of the form (a, b) where a, b have four distinnct values each, thus sixteen altogether. Lines $y = mx + c$ four values for m and also for c, sixteen of this type and four more lines $x = a$. Multiplication table for $\mathbf{F}_4$, regarded as $\mathbf{F}_2[x]/(x^2 + x + 1)\mathbf{F}_2[x]$, writing ω for the image of x is

	1	ω	$1+\omega$
1	1	ω	$1+\omega$
ω	ω	$1+\omega$	1
$1+\omega$	$1+\omega$	1	ω

Incidence matrix arranged by parallels is

$$
\begin{array}{cccccccccccccccc}
1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0
\end{array}
$$

where the columns correspond to the points $(0,0)$,$(0,1)$,$(0,\omega)$,$(0,\omega+1)$,$(1,0)$,$(1,1)$, $(1,\omega)$,$(1,\omega+1)$,$(\omega,0)$,$(\omega,1)$, (ω,ω),$(\omega,\omega+1)$,$(\omega+1,0)$, $(\omega+1,1)$,$(\omega+1,\omega)$,$(\omega+1,\omega+1)$, and the rows to the lines $x=0$,$x=1$,$x=\omega$,$x=\omega+1$, $y=0$,$y=1$,$y=\omega$,$y=\omega+1$, $y=x$,$y=x+1$,$y=x+\omega$,$y=x+\omega+1$, $y=\omega x$,$y=\omega x+1$, $y=\omega x+\omega$,$y=\omega x+\omega+1$, $y=(\omega+1)x$,$y=(\omega+1)x+1$,$y=(\omega+1)x+\omega$, $y=(\omega+1)x+\omega+1$. The first four rows of the matrix correspond to the four expermintal farms in the first year, the next four to the same farms in the second year, and so on. The first four columns corerespond to the first variety of wheat with the four types of fertiliser in order, the next four to the second variety, and so on. The matrix then gives the schedule required.

11. $x, x+1, x^3+x^2+1, x^3+x+1$. Note that all other irreducible polynomials of degree three are divisors of $x^{3^2}-x(=x^8-x)$. Now $x(x+1)(x^3+$

$x^2+1)(x^3+x+1) = (x^2+x)(x^6+x^5+x^4+x^3+x^2+x+1) = x^8 - x.$
$x^7 - 1 = (x+1)(x^3+x^2+1)(x^3+x+1)$

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

(for x^3+x+1).

Parity check matrix comes from the factor $(x+1)(x^3+x^2+1) = x^4+x^2+x+1$, and is

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

In $\mathbf{Z}_7$

x	0	1	2	3	4	5	6
x^2-2	5	6	2	0	0	2	6

. Hence $x^2 = 1 \iff x = 3$ or $x = 4$.
2 is a quadratic residue mod 7. The other squares mod 7 are 0,1,4.

The multiplicative group of $\mathbf{Z}_7$ is cyclic of order 6 with $\{1, 2, 4\}$ as the subgroup of quadratic residues, and it is generated under multiplication by 3 (for example).

Let α be a primitive 7^{th} root of unity over $\mathbf{F}_2$, where α lies in $\mathbf{F}_8$ and α is a zero of either x^3+x^2+1 or of x^3+x+1. We may suppose it is the first of these. The polynomial $(x-\alpha)(x-\alpha^2)(x-\alpha^4)$ is unchanged under automorphisms of $\mathbf{F}_8$ fixing $\mathbf{F}_2$ (the group of these being generated by $x \mapsto x^2$), and hence has coefficients in $\mathbf{F}_2$. In fact it has to be x^3+x^2+1, which is irreducible over $\mathbf{F}_2$ and has α as a zero. The cyclic code generated by x^3+x^2+1 is therefore a quadratic residue code $\mathcal{C}$. Because the minimum weight of a quadratic residue code is not less than the square root of its length, the minimum weight of $\mathcal{C}$ is $\geq \sqrt{7}$, i.e strictly greater than 2, so at least 3. But there are words of length 3, which is therefore the mimimum distance of this linear space code.