1. By evaluating $f(0), f(1)$ and $f(2)$ we see that $f(x)$ has no roots in $\mathbf{Z}/3\mathbf{Z}$ and thus is irreducible.

(i) The size of $\mathbf{F}$ is $3^3 = 27$ and the size of $\mathbf{F}^*$ is 26. The possible orders are the divisors of $|\mathbf{F}^*| = 26$, that is, 1, 2, 13 and 26.

(ii) If 2 were a square in $\mathbf{F}$, its square root would be of order 4, which is not possible.

(iii) If $2x^2 = a^2$ then $2 = (a/x)^2$, contradicting the result of (ii) above.

(iv) The elements of order 13 which are not 1 are precisely the squares in $\mathbf{F}$ because the order of a square is a divisor of 13 and so is either 1 or 13. In this case we have $(x+2)^2 = x^2 + x + 1$.

2. The easiest way to show N is multiplicative is to note that $N(r) = |r|^2 = r\bar{r}$ so that

$$N(rs) = rs\overline{rs} = r\bar{r}s\bar{s} = N(r)N(s).$$

It is also acceptable to compute explicitly in terms of the real and imaginary parts.

The units in $\mathbf{Z}[i]$ are those elements u with $N(u) = 1$ i.e. $\pm 1, \pm i$.

If $N(r)$ is a prime in $\mathbf{N}$ and $r = st$ then $N(r) = N(s)N(t)$ so either $N(s)$ or $N(t)$ must be 1 and hence either s or t is a unit. Hence r is irreducible.

(i) $N(3) = 9$ so if there is a factorisation $3 = rs$ into two irreducibles then $N(r) = N(s) = 3$. However $a^2 + b^2 = 3$ has no integer solutions so 3 is irreducible.

(ii) $N(5) = 25$ so if there is a factorisation $5 = rs$ into two irreducibles then $N(r) = N(s) = 5$. The possibilities are $2 \pm i$ (up to associates). Trial dividing we find that $5 = (2+i)(2-i)$. (Any other factorisation which is the same up to associates is acceptable.)

(iii) $N(1 + 4i) = 17$ so $1 + 4i$ is irreducible.

(iv) $N(3 + 5i) = 34$ so possible irreducible factors have norms 17 or 2. Trial dividing we find

$$3 + 5i = (1 - 4i)(-1 + i)$$

(or similar up to associates).

(v) $N(7 - i) = 50$ so possible irreducible factors have norms $2, 5$, or 25. The elements of norm 2 are $1 \pm i$, those of norm 5 are $2 \pm i$ (up to associates). Trial dividing we obtain

$$7 - i = (1 + i)(2 - i)^2.$$

From the above 3 is irreducible but $N(3) = 9$ is not prime in $\mathbf{Z}$. (Any other prime of the form $4k+3$ is also acceptable, provided they show it is irreducible!)

3.

a) Clearly $\sqrt{2}$ is a root of x^2-2 which is irreducible in $\mathbf{Z}[x]$ because 2 is not a perfect square. Hence, by Gauss's lemma, x^2-2 is irreducible in $\mathbf{Q}[x]$ and so is the minimal polynomial of $\sqrt{2}$.

Let $\alpha=\sqrt{2}+\sqrt{7}$. Then $\alpha^2=9+2\sqrt{14}$ so

$$(\alpha^2-9)^2=56 \quad \text{or, equivalently,} \quad \alpha^4-18\alpha^2+25=0.$$

Let $f(x)=x^4-18x^2+25$. We show this is irreducible in $\mathbf{Z}[x]$ and thence by Gauss's lemma in $\mathbf{Q}[x]$. The only possible linear factors in $\mathbf{Z}[x]$ are $x\pm 1$ and $x\pm 5$ but we easily see that none of $\pm1, \pm5$ are roots. Since the coefficient of x^3 vanishes the possible factorisations into quadratics are

$$(x^2+ax\pm 5)(x^2-ax\pm 5) \quad \text{or} \quad (x^2+ax\pm 1)(x^2-ax\pm 25).$$

Comparing coefficients of x^2 we have

$$-18=-a^2\pm 10 \quad \text{or} \quad -18=-a^2\pm 26$$

none of which have solutions in $\mathbf{Z}$ because none of $8, 28, -8$ and 44 are perfect squares. hence $f(x)$ is irreducible and so is the minimal polynomial.

b) We have $\alpha(\alpha^2-9)=(\sqrt{2}+\sqrt{7})2\sqrt{14}=4\sqrt{7}+14\sqrt{2}$. Hence

$$\alpha(\alpha^2-9)-4\alpha=10\sqrt{2}$$

or, equivalently,

$$\sqrt{2}=\frac{1}{10}\Big(\alpha(\alpha^2-9)-4\alpha\Big)\in\mathbf{Q}[\alpha].$$

(i) Since the minimal polynomial of $\sqrt{2}$ has degree 2 we have $[\mathbf{Q}[\sqrt{2}]:\mathbf{Q}]=2$.

(ii) Since the minimal polynomial of $\alpha=\sqrt{2}+\sqrt{7}$ has degree 4 we have $[\mathbf{Q}[\alpha]:\mathbf{Q}]=4$.

(iii) By the above $[\mathbf{Q}[\alpha]:\mathbf{Q}[\sqrt{2}]]=[\mathbf{Q}[\alpha]:\mathbf{Q}]/[\mathbf{Q}[\sqrt{2}]:\mathbf{Q}]=2$.

If $\sqrt{7}\in Q[\sqrt{2}]$ then $\alpha\in\mathbf{Q}[\sqrt{2}]$ and $[\mathbf{Q}[\alpha]:\mathbf{Q}[\sqrt{2}]]=1$. Since this is not the case $\sqrt{7}\notin Q[\sqrt{2}]$.

4. If $\deg g(x) < \deg f(x)$ then $g(x)$ has no common factors with the irreducible polynomial $f(x)$. Hence $\gcd(f(x), g(x)) = 1$. We can find the gcd by using the Euclidean algorithm and then (Bézout's theorem) we can find $a(x), b(x) \in \mathbf{Q}[x]$ with

$$a(x)f(x) + b(x)g(x) = 1.$$

Reducing modulo $\langle f(x) \rangle$ the above equation becomes

$$b(x)g(x) = 1$$

in $\mathbf{Q}[x]/\langle f(x) \rangle$ so that the class of $b(x)$ is a multiplicative inverse for that of $g(x)$.

To find the multiplicative inverses we carry out the Euclidean algorithm:

(i)

$$x^3 + x + 1 = (x^2 - x + 2)(x + 1) - 1$$

Thus

$$\begin{aligned} \gcd(f(x), g(x)) &= -1 \\ &= f(x) - (x^2 - x + 2)g(x). \end{aligned}$$

So $a(x) = -1$ and the required multiplicative inverse is

$$b(x) = x^2 - x + 2.$$

(ii)

$$\begin{aligned} x^3 + 4x + 2 &= (x + 4)(x^2 + 1) + (-x - 2) \\ x^2 + 1 &= (-x + 2)(-x - 2) + 5 \end{aligned}$$

So

$$\begin{aligned} \gcd(f(x), g(x)) &= 5 \\ &= g(x) + (x - 2)\left(f(x) - (x + 4)g(x)\right) \\ &= (x - 2)f(x) - (x^2 + 2x - 9)g(x) \end{aligned}$$

So $a(x) = \frac{1}{5}(x - 2)$ and the required multiplicative inverse is

$$b(x) = \frac{1}{5}(-x^2 + 2x - 9).$$

5. There are $5^2 = 25$ points in $(\mathbf{Z}/5\mathbf{Z})^2$ and 5 points on any line.

(i) There are $25 \times 24/2 = 300$ distinct pairs of points in $(\mathbf{Z}/5\mathbf{Z})^2$ and $5 \times 4/2 = 10$ pairs of points on each line. Since there is a unique line through any pair of distinct points the number of lines in $(\mathbf{Z}/5\mathbf{Z})^2$ is $300/10 = 30$.

The number of lines through a point x is given by the number of other points divided by the number of other points on any line through x i.e. there are $24/4 = 6$ lines through a given point.

(ii) Both sets of parameters can be obtained by taking as blocks the subsets of $(\mathbf{Z}/5\mathbf{Z})^2$ given by points on each line (there are 5 points on each line so each block has size 5 as required). Each point lies on 6 lines and each pair of points lies on 1 line. This gives the required 1-design and 2-design, respectively.

(iii) The first set of parameters can be obtained by taking as blocks the subsets of lines through each point (there are 6 lines through each point so each block has size 6). Each line passes through 5 points giving a 1-$(30, 6, 5)$-design.

The second set of parameters can be obtained by taking as blocks the subsets of parallel lines. There are 5 lines in each block and each line lies in exactly one block giving a 1-$(30, 5, 1)$-design.

6. a) Label the seven varieties by the points in the projective plane $\mathbf{P}^2(\mathbf{Z}/2\mathbf{Z})$ and the seven locations by the lines in $\mathbf{P}^2(\mathbf{Z}/2\mathbf{Z})$. The three varieties grown in a location are those corresponding to the three points on the line corresponding to the location.

Since any two points lie on a line, any two varieties are planted together in one location.

The incidence matrix of the schedule is therefore the same as that of points and lines in $\mathbf{P}^2(\mathbf{Z}/2\mathbf{Z})$:

	$[1:0:0]$	$[0:1:0]$	$[0:0:1]$	$[1:1:0]$	$[1:0:1]$	$[0:1:1]$	$[1:1:1]$
$x=0$	0	1	1	0	0	1	0
$y=0$	1	0	1	0	1	0	0
$z=0$	1	1	0	1	0	0	0
$x+y=0$	0	0	1	1	0	0	1
$x+z=0$	0	1	0	0	1	0	1
$y+z=0$	1	0	0	0	0	1	1
$x+y+z=0$	0	0	0	1	1	1	0

b) A 2-(v,k,r)-design consists of an underlying set X and a set $\mathbf{B}$ of subsets of X (the blocks of the design) each of which has size k and with the property that each pair of elements of X occurs in precisely r of the blocks of the design.

The numerical constraints for a 2-design are

$$(k-1) \mid (v-1)r \quad \text{and} \quad k(k-1) \mid v(v-1)r$$

When $k=3$ and $r=1$ these yield

$$2 \mid (v-1) \quad \text{and} \quad 6 \mid v(v-1).$$

Hence $v = 2\ell+1$ where $(2\ell+1)2\ell = 6m$. So $\ell = 3n$ or $\ell = 3n+1$. The first case yields $v = 6n+1$ and the second $v = 6n+3$.

7. a) The irreducible degree 2 polynomial in $(\mathbf{Z}/2\mathbf{Z})[x]$ is x^2+x+1 (it is easy to check it has no roots). The three irreducible degree 4 polynomials in $(\mathbf{Z}/2\mathbf{Z})[x]$ are

$$x^4+x^3+x^2+x+1, \quad x^4+x+1 \quad \text{and} \quad x^4+x^3+1.$$

Again, it is easy to check they have no roots. Since there is only one irreducible degree 2 polynomial and none of these is its square (which is x^4+x^2+1) they must be irreducible.

The theory of factorisations of $x^{p^n}-x$ in $(\mathbf{Z}/p\mathbf{Z})[x]$ tells us that the factors of $x^{16}+x$ in $(\mathbf{Z}/2\mathbf{Z})[x]$ are the irreducible polynomials in $(\mathbf{Z}/2\mathbf{Z})[x]$ of degrees dividing 16, and that each occurs once in the factorisation. Hence

$$x^{15}+1=(x+1)(x^2+x+1)(x^4+x^3+x^2+x+1)(x^4+x+1)(x^4+x^3+1).$$

b) If $g(x)=(x+1)(x^4+x+1)$ then $g(x)h(x)=x^{15}+1$ where

$$\begin{aligned} h(x) &= (x^2+x+1)(x^4+x^3+x^2+x+1)(x^4+x^3+1) \\ &= x^{10}+x^9+x^8+x^6+x^5+x^2+1. \end{aligned}$$

The first row of the check matrix is the coefficients of $h(x)$ in descending order starting with that of the highest power x^{10} and followed by 4 zeros (to make 15 entries). The next row is the cyclic shift of this right by one place and so on. So the matrix is

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

There are no zero columns and no two columns are the same so the code has weight ≥ 3.

c) Each cyclic code of length 15 is generated by a factor of $x^{15}+1$. The dimension of the code is 15 less the degree of the factor. Simple combinatorics yields: there is one cyclic code of each dimension in $\{0,1,2,3,12,13,14,15\}$ and three of each dimension in $\{4,5,6,7,8,9,10,11\}$.

8. a) The *minimum distance* of a code C in $(\mathbf{Z}/2\mathbf{Z})^n$ is

$$\min\{d(x,x') : x \neq x' \in C\}$$

where $x = (x_1, x_2, \ldots, x_n)$, $x' = (x'_1, x'_2, \ldots, x'_n)$ and the distance

$$d(x,x') = |\{i : x_i \neq x'_i\}|.$$

The *weight* of a word $x = (x_1, x_2, \ldots, x_n)$ is $w(x) = |\{x_i \neq 0\}|$, and the *weight* of the code C is

$$\min\{w(x) : x \in C\}.$$

It follows that $d(x,x') = w(x - x') = w(x + x')$ and so the minimum distance and the weight are the same.

b)

(i) Suppose x is a word of weight 1 and that x_i is the non-zero entry. Then Mx^T is the ith column of M. If this column is not identically zero then $x \notin C$.

(ii) Suppose x is a word of weight 2 and that x_i and x_j are the non-zero entries. Then Mx^T is the sum, equivalently the difference, of the ith and jth columns of M. If these columns are not the same then $x \notin C$.

(iii) Suppose x is a word of weight 3 and that x_i, x_j and x_k are the non-zero entries. Then Mx^T is the sum of the ith, jth and kth columns of M. If the sum of these columns is not zero then $x \notin C$.

(iv) Clearly M has no identically zero columns and no two columns are the same. Each column has either 1 or 3 non-zero entries. The sum of any two of the first, or last, four columns has two non-zero entries. Hence adding any other column gives a non-zero result. Thus C has weight ≥ 4.

An example of a word in the code with weight 4 is 11101000. Thus C has weight exactly 4.

The code C detects $4 - 1 = 3$ errors and corrects $\lfloor (4-1)/2 \rfloor = 1$ error.