1 a. $deg f(x) = k \Rightarrow f(x)$ has at most k roots

b. If a has order three, then $a^3 = 1$
$\Rightarrow a$ is a root of $x^3 - 1$
$\Rightarrow$ there are at most 3 elements of order 3.

c. $\mathbb{Z}_{23}$ is a field because 23 is prime

d. $a \in \mathbb{Z}_{23}^*$, $|a|$ divides $|\mathbb{Z}_{23}^*| = 22$
$\Rightarrow |a| \in \{1, 2, 11, 22\}$

e. $|a| = 2 \Rightarrow a$ satisfies $x^2 - 1 = 0 \Rightarrow$ at most 2 elements of order 2

(f) order 1 : one element

order 2 : at most two elements

order 11 : at most eleven elements

$\Rightarrow$ at most 14 elements of order < 22.

(g) $\mathbb{Z}_{23}^*$ has 22 elements, at most 14 elements have order < 22

$\Rightarrow$ At least 8 elements have order 22. This implies that $\mathbb{Z}_{23}^*$ is cyclic.

h. $2^{11} \bmod 23 = 1$ $\quad 2^2 \bmod 23 = 4$

$3^{11} \bmod 23 = 1$ $\quad 3^2 \bmod 23 = 9$

$4^{11} \bmod 23 = 1$ $\quad 4^2 \bmod 23 = 16$

$5^{11} \bmod 23 = 22$ $\quad 5^2 \bmod 23 = 2$

Hence $|5| \neq 2$, $|5| \neq 11$, $\Rightarrow |5| = 22$

$\Rightarrow \mathbb{Z}_{23}^* = \langle 5 \rangle$

other generators: 7, 10, 11, 14, 15, 17, 19, 20, 21

in total there are 10 generators

[Since $\mathbb{Z}_{23}^* \sim \mathbb{Z}_{22}$ under $\mathbb{Z}_{22} = \langle a \rangle \Leftrightarrow \gcd(a, 22) = 1$

$\Leftrightarrow a \in \{1, 3, 5, 7, 9, 13, 15, 17, 19, 21\}$]

2. a. 8 triangles $\Rightarrow$ 24 edges, each edge is counted twice $\Rightarrow$ 12 edges $\Rightarrow$ 6 pairs of opposite edges

b. 24 vertices, each vertex is counted four times $\Rightarrow$ 6 vertices $\Rightarrow$ 3 pairs of opposite vertices

c. Orbit-Stabilizer theorem:

$|G| = |Stab_G(s)| \cdot |Orb_G(s)|$

Let s be one of the faces, then

$|Stab_G(s)| = 3$ $|Orb_G(s)| = 8 \Rightarrow |G| = 24$

(d) 4 pairs of opposite faces

2 rotations: $120°, 240°$

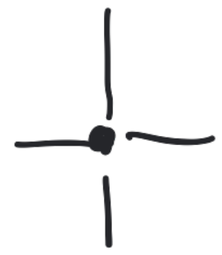
$\Rightarrow$ 8 rotations

6 pairs of opposite edges

1 rotation: $180°$

$\Rightarrow$ 6 rotations

3 pairs of opposite vertices



3 rotations: $90°, 180°, 270°$

$\Rightarrow$ 9 rotations

$\Rightarrow$ 1 identity

total: $8+6+9+1 = 24 = |G|$

(e) Algebraic approach

Opposite faces: 120°, 240°, both are of order 3, two faces are invariant, corresponds to permutation of faces in disjoint cycle form:
(a)(b)(cde)(fgh)

Opposite edges 180° ⇒ order 2, no face invariant:
(ab)(cd)(ef)(gh)

Opposite vertices: 90°, 180°, 270°
90°, 270° have order 4: (abcd)(efgh)
180° has order 2: (ab)(cd)(ef)(gh)

Geometric approach

Opposite faces two faces are invariant, the three adjacent faces are permuted cyclically, so:

(a)(bcd)(e)(fgh)

Opposite edges, no faces invariant

for instance (15)(26)(37)(48)

Opposite vertices: the four faces joining one of the vertices are permuted cyclically

(1234)(5678) for 90°

(13)(24)(57)(68) for 180°

(1432)(5876) for 270°

(f) Opposite faces:
(a)(b)(cde)(fgh) each cycle can be colored independently

$|fix(120°)| = |fix(240°)| = 2^4$

4 pairs in total $4.2.2^4 = 2^7 = 128$

Opposite edges
(ab)(cd)(ef)(gh) $|fix(180°)| = 2^4$

6 pairs, in total $6.2^4 = 96$

Opposite vertices
90°, 270° (abcd)(efgh) $|fix(90°)| = |fix(270°)| = 4$

180° (ab)(cd)(ef)(gh) $|fix(180°)| = 2^4 = 16$

3 pairs: in total $3.(4+4+16) = 72$

$$|\mathrm{fix}(\mathrm{identity})| = 2^8 = 256$$

(g) $$\sum_{g \in G} |\mathrm{fix}(g)| = 128 + 16 + 72 + 256 = 552$$

$$\#\text{orbits} = \frac{\sum_{g \in G} |\mathrm{fix}(g)|}{|G|} = \frac{552}{24} = 23$$

3 a. $x^2+a_1x+a_0$ no roots $x=0 \Rightarrow a_0=1$

$x=1 \Rightarrow a_1=1$

only irreducible polynomial of degree 2:

x^2+x+1

b. $x^3+a_2x^2+a_1x+a_0$ no roots

$x=0 \Rightarrow a_0=1$ $x=1 \Rightarrow 1+a_2+a_1+1 \neq 0$

$\Rightarrow a_2+a_1 \neq 0 \Rightarrow a_1=1, a_2=0$

or $a_1=0, a_2=1$

$\Rightarrow$ irreducible polynomials of degree 3:

x^3+x^2+1 and x^3+x+1

(c) A polynomial of degree can be factorised:

degrees: • 1-1-1-1-1

• 2-1-1-1

• 2-2-1

• 3-1-1

• 3-2

(d) If the polynomial has no roots, then the only factorisation is 3-2

So: $(x^3+x^2+1)(x^2+x+1) = x^5+x+1$

and $(x^3+x+1)(x^2+x+1) = x^5+x^4+1$

(e) $p(x) \neq x^5 + x^4 + 1$

$p(x) \neq x^5 + x + 1$

so $p(x)$ is not a 3-2 product

$p(0) = 1$ $p(1) = 1 \Longrightarrow p(x)$ has no roots

$\Rightarrow p(x)$ cannot be one of the other factorisations

$\Rightarrow p(x)$ is irreducible

(f) $\overline{F} : \mathbb{Z}_2[x] / \langle p(x) \rangle = \{ a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 + \langle p(x) \rangle : a_i \in \mathbb{Z}_2 \}$

$\Rightarrow \overline{F}$ has $2^5 = 32$ elements

(g) $(x+\langle x^5+x^3+1\rangle)(x^4+x^2+\langle x^5+x^3+1\rangle)$

$= x^5+x^3+\langle x^5+x^3+1\rangle$

$= -1+\langle x^5+x^3+1\rangle$

$= 1+\langle x^5+x^3+1\rangle$

$(x^5+x^3+\langle x^5+x^3+1\rangle = 1+\langle x^5+x^3+1\rangle)$

4 (a) As $n = 119$, $p = 7$ and $q = 17$.

Hence $r = \varphi(n) = 6 \cdot 16 = 96$. 1

So in order to compute $M = C^d \pmod n$ we need $d = e^{-1}$ (in $\mathbb{Z}_{96}$). As $e = 35$:

$$\begin{pmatrix} 96 & 1 & 0 \\ 35 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 26 & 1 & -2 \\ 35 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 26 & 1 & -2 \\ 9 & -1 & 3 \end{pmatrix}$$

$$\sim \begin{pmatrix} 8 & 3 & -8 \\ 9 & -1 & 3 \end{pmatrix} \sim \begin{pmatrix} 8 & 3 & -8 \\ 1 & -4 & 11 \end{pmatrix}$$

$\Rightarrow 1 = -4 \cdot 96 + 11 \cdot 35$

$\Rightarrow 35^{-1} = 11 \pmod{96}$, so $d = 11$. 2

Now as $C = 5$, we need to compute $5^{11} \pmod{119}$. To that end, note that $11 = 2^3 + 2^1 + 2^0$. Compute mod 119:

$5^{2^0} = 5$

$5^{2^1} = (5)^2 = 25$

$5^{2^2} = (25)^2 = 625 = 30$

$5^{2^3} = (30)^2 = 900 = 67$.

$\Rightarrow M = 5^{2^0} \cdot 5^{2^1} \cdot 5^{2^3} = 5 \cdot 25 \cdot 67$

$= 6 \cdot 67 = 45$ ∎ 2

4 | b) If $\gcd(M,n) > 1$, because $n = p \cdot q$ with primes p and q, we know that either $p \mid M$ or $q \mid M$. 1

In that case, also either $p \mid C = M^e$ or $q \mid C = M^e$. 1

That means that Eve can compute $\gcd(C,n) = p$ (or q), and this is just one application of the Euclidean alg., hence efficient. 2

After that, Eve can compute $r = (p-1)(q-1)$, and $d = e^{-1}(\mathbb{Z}_r)$.

And finally, can compute $M = C^d \pmod n$.

All steps are computationally efficient (just like for Alice), since Eve knows p (or q) ∎ 1