1. Sketch the subgroup lattice for $\mathbf{Z}_{20}$. For each subgroup, list all the elements and indicate all possible generators of the subgroup.

Positive divisors of 20 : 1, 2, 5, 4, 10, 20

Possible generators underlined.

Recall $\langle k_1 \rangle = \langle k_2 \rangle \iff \gcd(k_1, m) = \gcd(k_2, m)$:)

$$\begin{tikzcd}
 & \langle 1 \rangle = \mathbb{Z}_{20} \arrow[dl, dash] \arrow[dr, dash] & \\
\langle 2 \rangle = 2\mathbb{Z}_{20} \arrow[d, dash] \arrow[drr, dash] & & \langle 5 \rangle = 5\mathbb{Z}_{20} \arrow[d, dash] \\
\langle 4 \rangle = 4\mathbb{Z}_{20} \arrow[dr, dash] & & \langle 10 \rangle = 10\mathbb{Z}_{20} \arrow[dl, dash] \\
 & \langle 0 \rangle = 0\mathbb{Z}_{20} &
\end{tikzcd}$$

$\langle 1 \rangle = \mathbb{Z}_{20} = \{0, \underline{1}, 2, \underline{3}, 4, 5, 6, \underline{7}, 8, \underline{9}, 10, \underline{11}, 12, \underline{13}, 14, 15, 16, \underline{17}, 18, \underline{19}\}$

$\langle 2 \rangle = 2\mathbb{Z}_{20} = \{0, \underline{2}, 4, \underline{6}, 8, \underline{10}, 12, \underline{14}, 16, \underline{18}\}$

$\langle 5 \rangle = 5\mathbb{Z}_{20} = \{0, \underline{5}, 10, \underline{15}\}$

$\langle 4 \rangle = 4\mathbb{Z}_{20} = \{0, \underline{4}, \underline{8}, \underline{12}, \underline{16}\}$

$\langle 10 \rangle = 10\mathbb{Z}_{20} = \{0, \underline{10}\}$

$\langle 0 \rangle = 0\mathbb{Z}_{20} = \{0\}$

2. Suppose G is a group and $a \in G$ such that $|a| = 13$. Prove there exists $b \in G$ such that $a = b^9$

$9 \cdot 3 = 27 = 2 \cdot 13 + 1 \equiv 1 \bmod 13$, so let $b = a^3$

Then $b^9 = (a^3)^9 = a^{27} = a^{2 \cdot 13 + 1} = (\underbrace{a^{13}}_{e})^2 \cdot a = a$

3. Suppose $\alpha = (4,3,7,8,9)(1,3,7,5,2)(2,7,6)$ is a permutation in cycle notation.

(a) Express α as a product of disjoint cycles.

(b) Find the order of α. Explain.

(c) Find the parity of α. Explain.

(d) Simplify α^{659}

(a) $\alpha = (1,7,6)(2,5)(3,8,9,4)$

(b) By Ruffini's theorem $|\alpha| = \mathrm{lcm}(\underbrace{3,2,4}_{\text{orders of cycles}}) = 12$ (lengths)

(c) Discriminant = sum of $\underbrace{\text{sizes}}_{\text{lengths} - 1}$ of cycles $= 2+1+3 = 6$, so α is even

(d) lemma: If G is a group, $a \in G$, $|a| = m$, and $n \equiv r \bmod m$, then $a^n = a^r$

Pf: Since $\exists q \in \mathbb{Z}$ $n - r = qm$, $n = r + qm$, so

$a^n = a^{r+qm} = (a^m)^q \cdot a^r = e^q a^r = a^r$ ☺

Since disjoint cycles commute $\alpha^{659} = (1,7,6)^{659}(2,5)^{659}(3,8,9,4)^{659}$.

Since $659 \equiv 3 \bmod 4$, $2 \bmod 3$, $1 \bmod 2$

$\alpha^{659} = (1,7,6)^2(2,5)(3,8,9,4)^3 = (1,7,6)^{-1}(2,5)(3,8,9,4)^{-1}$

$= (1,6,7)(2,5)(3,4,9,8)$

4. Prove that $5\mathbf{Z}/40\mathbf{Z}$ is isomorphic to $\mathbf{Z}_8$

Define $f: \mathbb{Z} \to 5\mathbb{Z}/40\mathbb{Z}$ by $f(x) = 5x + 40\mathbb{Z}$

Then f is a surjective hom with $\ker f = 8\mathbb{Z}$

Pf: (i) $f(x+y) = 5(x+y) + 40\mathbb{Z} = 5x + 40\mathbb{Z} + 5y + 40\mathbb{Z} = f(x) + f(y)$

(ii) Surjective: $f(1) = 5 + 40\mathbb{Z}$ generates $5\mathbb{Z}/40\mathbb{Z}$

(ii) $x \in \ker f \iff f(x) = 40\mathbb{Z} \iff 5x \in 40\mathbb{Z} \iff$
$\exists k \;\; 5x = 40k \iff \exists k \;\; x = 8k \iff x \in 8\mathbb{Z}$

By the 1^{st} isomorphism theorem $\mathbb{Z}/8\mathbb{Z} \cong 5\mathbb{Z}/40\mathbb{Z}$

Alternative: Let $i: 5\mathbb{Z} \to \mathbb{Z}$ be the natural inclusion $(i(x) = x)$

and $\pi: \mathbb{Z} \to \mathbb{Z}_8$ the natural projection $(\pi(x) = x \bmod 8 = x + 8\mathbb{Z})$

Define $f: 5\mathbb{Z} \to \mathbb{Z}_8$ $\quad f = \pi \circ i$

Since $f(5) = 5 \bmod 8$ is a generator of $\mathbb{Z}_8$ $(\gcd(5,8) = 1)$

f is surjective.

Since $\ker f = 40\mathbb{Z}$ $(5x \in 8\mathbb{Z} \iff x \in 40\mathbb{Z})$,

by the 1^{st} isomorphism theorem $5\mathbb{Z}/40\mathbb{Z} \cong \mathbb{Z}_8$

5. Solve the following system of two congruence equations

$2x \equiv 5 \bmod 13$ $\qquad$ $$4x \equiv 10 \bmod 13$$

$2x \equiv 3 \bmod 11$ $\qquad$ $$6x \equiv 9 \bmod 11$$

Hint: first separately solve each congruence for x

(i) $2 \cdot 7 = 13 + 1$, so $x = 5 \cdot 7 = 13 \cdot 2 + 9 = 9 \bmod 13$

$2 \cdot 6 = 11 + 1$, so $x = 3 \cdot 6 = 11 + 7 = 7 \bmod 11$

(ii) $\exists y \in \mathbb{Z}$ $\quad x = 9 + 13y$, so $9 + 13y \equiv 7 \bmod 11$,

$2y \equiv -2 \bmod 11$, i.e. $y \equiv -1 \bmod 11$, i.e. $\exists z$ $\quad y = -1 + 11z$

so $x = 9 + 13(-1 + 11z) = -4 + 143z$,

so $x \equiv -4 \bmod 143 \equiv 139 \bmod 143$

Alternate (ii): Chinese remainder formula: $x \equiv a_1 b_1 M_1 + a_2 b_2 M_2$

where $M = m_1 m_2 = 143$, $M_i = M / m_i$, $M_i b_i \equiv 1 \bmod m_i$

i	m_i	M_i	b_i	a_i	$a_i b_i M_i \bmod M$
1	13	11	6	9	$594 = 22 \bmod 143$
2	11	$\underbrace{13}_{2 \bmod 11}$	6	7	117

$6 \cdot 11 = 5 \cdot 13 + 1$

$2 \cdot 6 = 11 + 1$

Sum: $x \equiv 139 \bmod 143$

6. (a) How many group homomorphisms are there from $\mathbf{Z}$ to $\mathbf{Z}_9 \times \mathbf{Z}_{25}$? Explain.

(b) How many of these are surjective? Explain.

(c) How many of these are injective? Explain.

(a) If $f: \mathbb{Z} \to \mathbb{Z}_9 \times \mathbb{Z}_{25}$ is a group hom., $f(k) = f(k \cdot 1) = k f(1)$

so f is uniquely determined by $f(1)$,

so $|\mathrm{Hom}[\mathbb{Z}, \mathbb{Z}_9 \times \mathbb{Z}_{25}]| = 9 \cdot 25 = 225$

(b) For f to be surjective $f(1)$ must be a generator of $\mathbb{Z}_9 \times \mathbb{Z}_{25}$

so a unit in $\mathbb{Z}_9 \times \mathbb{Z}_{25}$, so $f(1) = [i, j]$ where $i \in U(9)$, $j \in U(25)$

Euler totients: $\varphi(9) = 9 - 3 = 6$, $\phi(25) = 25 - 5 = 20$

So $6 \cdot 20 = 120$ surjective homs.

(c) By the pigeonhole principle, none are injective,

because $\mathbb{Z}$ is infinite and $\mathbb{Z}_9 \times \mathbb{Z}_{25}$ is finite.