Question 1

(a)

Prove that one root of $x^3 + px^2 + qx + r = 0$ is negative of another root if and only if $r = pq$.

Proof. Let the roots be $\alpha, -\alpha, \beta$. Using Vieta's formulas:

1. Sum of roots: $\alpha + (-\alpha) + \beta = -p \Rightarrow \beta = -p$
2. Sum of product of roots two at a time: $\alpha(-\alpha) + \alpha\beta + (-\alpha)\beta = q \Rightarrow -\alpha^2 = q$
3. Product of roots: $\alpha(-\alpha)\beta = -r \Rightarrow -\alpha^2\beta = -r \Rightarrow q(-p) = -r$ (since $-\alpha^2 = q$ and $\beta = -p$)

Thus, $r = pq$.

Conversely, if $r = pq$, assume roots are α, β, γ. Then:

$$\begin{aligned} \alpha + \beta + \gamma &= -p \\ \alpha\beta + \beta\gamma + \gamma\alpha &= q \\ \alpha\beta\gamma &= -r = -pq \end{aligned}$$

Assume $\gamma = -\beta$, then:

$$\begin{aligned} \alpha &= -p \text{ (from sum)} \\ -\beta^2 &= q \text{ (from sum of products)} \\ \alpha\beta\gamma &= -p \cdot \beta \cdot (-\beta) = p\beta^2 = -pq \Rightarrow \beta^2 = -q \end{aligned}$$

Thus, one root is negative of another. □

(b)

Solve $x^4 - 2x^3 - 21x^2 + 22x + 40 = 0$, whose roots are in arithmetical progression.

Let the roots be $a-3d, a-d, a+d, a+3d$ (arithmetic progression with common difference $2d$).

Sum of roots:

$$(a - 3d) + (a - d) + (a + d) + (a + 3d) = 4a = 2 \Rightarrow a = 0.5$$

Sum of product of roots two at a time:

$$6a^2 - 10d^2 = -21$$

Substitute $a = 0.5$:

$$6(0.25) - 10d^2 = -21 \Rightarrow 1.5 - 10d^2 = -21 \Rightarrow d^2 = 2.25 \Rightarrow d = \pm 1.5$$

Thus, roots are:

$$x = -4, -1, 2, 5$$

(c)

Find all the integral roots of $x^5 + 2x^4 + 4x^3 - 8x^2 - 32 = 0$.

Possible integer roots are factors of 32: $\pm1, \pm2, \pm4, \pm8, \pm16, \pm32$.

Testing:

$$\begin{aligned}
x = 2 &: 32 + 32 + 32 - 32 - 32 = 32 \neq 0 \\
x = -2 &: -32 + 32 - 32 - 32 - 32 = -96 \neq 0 \\
x = 1 &: 1 + 2 + 4 - 8 - 32 = -33 \neq 0 \\
x = -1 &: -1 + 2 - 4 - 8 - 32 = -43 \neq 0 \\
x = 4 &: 1024 + 512 + 256 - 128 - 32 = 1632 \neq 0
\end{aligned}$$

None of these work. The equation has no simple integer roots.

Conclusion: There are no integral roots for this polynomial.

Question 2

(a)

Find the polar representation of $z = \sin a + i(1 + \cos a)$.

Magnitude:

$$|z| = \sqrt{\sin^2 a + (1 + \cos a)^2} = \sqrt{2 + 2\cos a} = 2\cos(a/2)$$

Argument:

$$\arg z = \tan^{-1}\left(\frac{1 + \cos a}{\sin a}\right) = \frac{\pi}{2} - \frac{a}{2}$$

Polar Form: $z = 2\cos(a/2)e^{i\left(\frac{\pi}{2} - \frac{a}{2}\right)}$

(b)

Find $|z|$ and $\arg z$ for

$$z = \frac{(2\sqrt{3} + 2i)^8}{(1 - i)^6} + \frac{(1 + i)^6}{(2\sqrt{3} - 2i)^8}$$

Convert to polar form:

$$\begin{aligned}
2\sqrt{3} + 2i &= 4e^{i\pi/6} \\
1 - i &= \sqrt{2}e^{-i\pi/4} \\
1 + i &= \sqrt{2}e^{i\pi/4} \\
2\sqrt{3} - 2i &= 4e^{-i\pi/6}
\end{aligned}$$

Compute:

$$(2\sqrt{3}+2i)^8 = 4^8 e^{i8\pi/6} = 65536e^{i4\pi/3}$$
$$(1-i)^6 = 8e^{-i3\pi/2} = 8e^{i\pi/2}$$
$$(1+i)^6 = 8e^{i3\pi/2} = 8e^{-i\pi/2}$$
$$(2\sqrt{3}-2i)^8 = 65536e^{-i4\pi/3} = 65536e^{i2\pi/3}$$

Thus:

$$z = \frac{65536e^{i4\pi/3}}{8e^{i\pi/2}} + \frac{8e^{-i\pi/2}}{65536e^{i2\pi/3}} = 8192e^{i5\pi/6} + \frac{1}{8192}e^{-i7\pi/6}$$

But $e^{-i7\pi/6} = e^{i5\pi/6}$, so:

$$z = \left(8192 + \frac{1}{8192}\right)e^{i5\pi/6}$$

Magnitude: $|z| = 8192 + \frac{1}{8192}$
Argument: $\arg z = \frac{5\pi}{6}$

(c)

Find the geometric image for $|z+1+i| < 3$ and $0 < \arg z < \frac{\pi}{6}$.

1. $|z+1+i| < 3$: All points inside a circle centered at $-1-i$ with radius 3.

2. $0 < \arg z < \pi/6$: All points in the complex plane with argument between 0 and $\pi/6$.

Geometric Image: The intersection is a sector of the circle centered at $-1-i$ with radius 3, bounded by the angles 0 and $\pi/6$ from the positive real axis.

Question 3

(a)(i)

Prove that $\epsilon_j\epsilon_k \in U_n$ for all j, k.

Proof. $\epsilon_j = e^{2\pi ij/n}$, $\epsilon_k = e^{2\pi ik/n}$. Then:

$$\epsilon_j\epsilon_k = e^{2\pi i(j+k)/n}$$

Since $j+k \mod n$ is in $\{0, \dots, n-1\}$, $\epsilon_j\epsilon_k$ is also an n-th root of unity. □

(a)(ii)

Prove that $\epsilon_j^{-1} \in U_n$.

Proof.

$$\epsilon_j^{-1} = e^{-2\pi ij/n} = e^{2\pi i(n-j)/n} = \epsilon_{n-j} \in U_n$$

□

(b)

Show that $a^2 = 3k$ or $a^2 = 3k + 1$ for some integer k.

Proof. Any integer a is congruent to $0, 1,$ or $2 \mod 3$:

- If $a \equiv 0 \mod 3$, then $a^2 \equiv 0 \mod 3 \Rightarrow a^2 = 3k$
- If $a \equiv 1 \mod 3$, then $a^2 \equiv 1 \mod 3 \Rightarrow a^2 = 3k + 1$
- If $a \equiv 2 \mod 3$, then $a^2 \equiv 4 \equiv 1 \mod 3 \Rightarrow a^2 = 3k + 1$

□

(c)(i)

Prove $\gcd(n, n + 1) = 1$.

Proof. Let $d = \gcd(n, n + 1)$. Then d divides $(n + 1) - n = 1$, so $d = 1$.
Find x, y: By Bezout's identity, $n(-1) + (n + 1)(1) = 1$. □

(c)(ii)

Prove $\gcd(a, b) = 1$ given $\gcd(a, c) = 1$ and b divides c.

Proof. Since $\gcd(a, c) = 1$ and b divides c, any common divisor of a and b must also divide c. But $\gcd(a, c) = 1$, so $\gcd(a, b) = 1$. □

Question 4

(a)

Prove $a \equiv b \pmod{n}$ given $ac \equiv bc \pmod{n}$ and $\gcd(c, n) = 1$.

Proof. $ac \equiv bc \pmod{n} \Rightarrow n$ divides $c(a - b)$.
Since $\gcd(c, n) = 1$, n must divide $a - b$, so $a \equiv b \pmod{n}$. □

(b)

Solve $7x \equiv 8 \pmod{11}$.
Find the inverse of 7 modulo 11. $7 \times 8 = 56 \equiv 1 \pmod{11}$, so $7^{-1} \equiv 8 \pmod{11}$.
Multiply both sides by 8:

$$x \equiv 64 \equiv 9 \pmod{11}$$

(c)

Solve:

$$2x + 3y \equiv 1 \pmod{6}$$
$$x + 3y \equiv 5 \pmod{6}$$

Subtract the second equation from the first:

$$x \equiv -4 \equiv 2 \pmod{6}$$

Substitute $x = 2$ into the second equation:

$$2 + 3y \equiv 5 \pmod{6} \Rightarrow 3y \equiv 3 \pmod{6} \Rightarrow y \equiv 1 \pmod{2}$$

Solution: $x \equiv 2 \pmod{6}$, $y \equiv 1 \pmod{2}$.

Question 5

(a)

Show G (2×2 real matrices with non-zero determinant) is a non-abelian group.

Proof.

- **Closure:** Product of two matrices with non-zero determinant has non-zero determinant.
- **Associativity:** Matrix multiplication is associative.
- **Identity:** Identity matrix I is in G.
- **Inverse:** Every matrix in G has an inverse in G.

Non-abelian: Example:

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

$$AB = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \neq BA = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$$

□

(b)

Show that left-right cancellation implies abelian.

Proof. Assume $xy = zx \Rightarrow y = z$. Let $z = y$, then $xy = yx$ for all x, y, so G is abelian.
Example: S_3 is non-abelian and doesn't satisfy the condition. □

(c)

Show $G = \{1, 5, 7, 11\}$ is a group under multiplication modulo 12.

Proof. Cayley table:

$\times$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

- **Closure:** All products are in G.
- **Associativity:** Inherited from integers.
- **Identity:** 1 is the identity.
- **Inverses:** Each element is its own inverse.

$\square$

Question 6

(a)

Show $H_n = \{nx | x \in \mathbb{Z}\}$ is a subgroup of $\mathbb{Z}$, and $H_2 \cup H_3$ is not.

Proof. For H_n:

- **Closure:** $nx + ny = n(x + y) \in H_n$
- **Identity:** $0 = n \cdot 0 \in H_n$
- **Inverse:** $-nx = n(-x) \in H_n$

For $H_2 \cup H_3$:

$$2 \in H_2, 3 \in H_3, \text{ but } 2 + 3 = 5 \notin H_2 \cup H_3$$

Thus, not closed under addition. $\square$

(b)

Show $|aba^{-1}| = |b|$.

Proof. Let $|b| = n$. Then:

$$(aba^{-1})^n = ab^n a^{-1} = aea^{-1} = e$$

If $m < n$, $(aba^{-1})^m = ab^m a^{-1} \neq e$. Thus, $|aba^{-1}| = n$. $\square$

(c)

Show $\mathbb{Z}_n$ is cyclic, find generators, describe subgroups of $\mathbb{Z}_{40}$.

- **Cyclic:** Generated by 1.
- **Generators:** Integers k with $\gcd(k, n) = 1$. For $n = 40$, $\phi(40) = 16$.
- **Subgroups:** For each divisor d of 40, there is a subgroup $\langle d \rangle$:

$$1, 2, 4, 5, 8, 10, 20, 40$$