Problem 1. Use mathematical induction to prove that

$$3 + 3 \cdot 4 + 3 \cdot 4^2 + ... + 3 \cdot 4^n = 4^{n+1} - 1$$

for all integers $n \geq 0$.

Proof. Using the steps of induction I show that this holds for the base case $n = 0$

$$4^{0+1} - 1 = 4 - 3 = 3$$

Now, I assume this holds for $n = k$, $k \geq 0$, that is

$$3 + 3 \cdot 4 + 3 \cdot 4^2 + ... + 3 \cdot 4^n = 4^{n+1} - 1$$

then I want to show this also holds for $n = k + 1$. Factoring the L.H.S of this equation

$$3 + 3 \cdot 4 + 3 \cdot 4^2 + ... + 3 \cdot 4^n + 3 \cdot 4^{n+1} = 4^{n+2} - 1$$

I get

$$3 + 4(3 + 4 \cdot 3 + ... + 4^{n-1} \cdot 3 + 4^n \cdot 3) = 4^{n+2} - 1$$

Doing algebraic manipulation I get

$$4 + 4(3 + 4 \cdot 3 + ... + 4^{n-1} \cdot 3 + 4^n \cdot 3) = 4^{n+2}$$

it follows that

$$1 + 1(3 + 4 \cdot 3 + ... + 4^{n-1} \cdot 3 + 4^n \cdot 3) = 4^{n+1}$$

and

$$3 + 3 \cdot 4 + ... + 3 \cdot 4^{n-1} + 3 \cdot 4^n = 4^{n+1} - 1$$

This shows that the identity still holds when $n = k + 1$, and the induction is completed. □

Problem 2. Solve the congruence

$$175x \equiv 234 \text{ mod}(603)$$

To find x, I can rewrite the problem as

$$175^{-1}175x \equiv 175^{-1}234 \text{ (mod } 603) \tag{1}$$

and to find 175^{-1}, I can use the extended euclidean algorithm to find s and t such that

$$175s + 603t \equiv 1 \text{ (mod } 603)$$

s_k	t_k	q_k		
0	1			
1	0	3	603	175
−3	1	2	525	156
7	−2	4	78	19
−31	9	9	76	18
286	−83	2	2	1
			2	
			0	

So, plugging s and t into the previous equation I get,

$$175(286) + 603(-83) \equiv 1 \pmod{603}$$

which means that

$$175^{-1} \equiv 286 (\text{mod } 603)$$

Finally, substituting the inverse into (1) I get

$$x \equiv 286 \cdot 234 \equiv 594 \pmod{603}$$

Problem 3. Approximate, in 4 decimal places, all the 6th roots of $-3 + 8i$.

Using De Moivre's theorem, I will use the fact

$$z^{\frac{1}{n}} = r^{\frac{1}{n}} \cdot \text{cis}\left(\frac{\theta}{n} + \frac{2k\pi}{n}\right)$$

to find the 6th roots of $-3 + 8i$ by substituting $r, n,$ and k with the corresponding values:

$$z = -3 + 8i$$

$$\theta = \pi - \tan^{-1}\left(\frac{8}{3}\right)$$

$$r = \sqrt{(-3)^2 + (-8)^2} = \sqrt{73}$$

$$n = 6$$

$$k = 0, 1, 2, ..., n - 1$$

Substituting these values, I get the roots to be

$$\begin{aligned}
z^{\frac{1}{6}} &= \sqrt[12]{73} \cdot \text{cis}\left(\frac{\pi - \tan^{-1}\left(\frac{8}{3}\right)}{6} + \frac{2 \cdot 0 \cdot \pi}{6}\right) \approx \quad 1.3565 + 0.4519i \\
z^{\frac{1}{6}} &= \sqrt[12]{73} \cdot \text{cis}\left(\frac{\pi - \tan^{-1}\left(\frac{8}{3}\right)}{6} + \frac{2 \cdot 1 \cdot \pi}{6}\right) \approx \quad 0.2869 + 1.4007i \\
z^{\frac{1}{6}} &= \sqrt[12]{73} \cdot \text{cis}\left(\frac{\pi - \tan^{-1}\left(\frac{8}{3}\right)}{6} + \frac{2 \cdot 2 \cdot \pi}{6}\right) \approx -1.0696 + 0.9488i \\
z^{\frac{1}{6}} &= \sqrt[12]{73} \cdot \text{cis}\left(\frac{\pi - \tan^{-1}\left(\frac{8}{3}\right)}{6} + \frac{2 \cdot 3 \cdot \pi}{6}\right) \approx -1.3565 - 0.4519i \\
z^{\frac{1}{6}} &= \sqrt[12]{73} \cdot \text{cis}\left(\frac{\pi - \tan^{-1}\left(\frac{8}{3}\right)}{6} + \frac{2 \cdot 4 \cdot \pi}{6}\right) \approx -0.2869 - 1.4007i \\
z^{\frac{1}{6}} &= \sqrt[12]{73} \cdot \text{cis}\left(\frac{\pi - \tan^{-1}\left(\frac{8}{3}\right)}{6} + \frac{2 \cdot 5 \cdot \pi}{6}\right) \approx \quad 1.0696 - 0.9488i
\end{aligned}$$

Problem 4. What are the primitive 15th roots of unity? Leave your answers in the form of ω^k for some appropriate complex number ω. Be sure to describe what ω represents.

The primitive 15th roots of unity are the roots of unity where $n = 15$, ω is a number such that $\omega^n = 1$ and $k = 1, 2, ..., n - 1$. When GCD(n,k) = 1, in other words, when k and n are relatively prime, ω^k is a root of unity. So, the 15th roots of unity are

$$\omega^2, \omega^4, \omega^7, \omega^8, \omega^{11}, \omega^{13}, \omega^{14}$$

Problem 5. How many fourth roots of the matrix

$$D = \begin{bmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{bmatrix}$$

are there? What are they? Leave the answers in the exact form.

There are 4 fourth roots to this matrix. Using De Moivre's theorem I can use the fact that

$$z^{\frac{1}{n}} = r^{\frac{1}{n}} \cdot \text{cis}\left(\frac{\theta}{n} + \frac{2k\pi}{n}\right) \tag{2}$$

to find the 4th roots of the complex number $z = -\frac{1}{2} + \frac{\sqrt{3}}{2}$ which is isomorphic to the matrix D. I can find the roots by substituting r, n and k into (1) where

$$\theta = \pi - \tan^{-1}\left(\frac{\frac{\sqrt{3}}{2}}{\frac{1}{2}}\right) = \pi - \tan^{-1}\left(\sqrt{3}\right) = \pi - \frac{\pi}{3} = \frac{2\pi}{3}$$

$$r = \sqrt{\left(-\frac{1}{2}\right)^2 + \left(\frac{\sqrt{3}}{2}\right)^2} = \sqrt{\frac{1}{4} + \frac{3}{4}} = \sqrt{1} = 1$$

$$n = 4$$

$$k = 0, 1, 2, 3$$

Substituting these values I get the roots to be

$$z^{\frac{1}{4}} = 1 \cdot \text{cis}\left(\frac{2\pi}{12} + \frac{2 \cdot 0 \cdot \pi}{4}\right)$$

$$z^{\frac{1}{4}} = 1 \cdot \text{cis}\left(\frac{2\pi}{12} + \frac{2 \cdot 1 \cdot \pi}{4}\right)$$

$$z^{\frac{1}{4}} = 1 \cdot \text{cis}\left(\frac{2\pi}{12} + \frac{2 \cdot 2 \cdot \pi}{4}\right)$$

$$z^{\frac{1}{4}} = 1 \cdot \text{cis}\left(\frac{2\pi}{12} + \frac{2 \cdot 3 \cdot \pi}{4}\right)$$

Problem 6. Define $\odot$ on $\mathbb{C}^*$ according to

$$(a + bi) \odot (c + di) = ac + bdi.$$

(a) Is $\odot$ well-defined? In other words, is $\mathbb{C}^*$ closed under $\odot$?

(b) Is $\odot$ associative? If you think it is, prove it. If you do not thing so, explain, or provide a counterexample.

(c) Find, if possible, an element e such that $e \odot z = z$ for any $z \in \mathbb{C}^*$. Or, explain why such an element does not exist.

(d) Based on the identity element you found in (c), find the inverse of a typical element z in $\mathbb{C}^*$. Does the inverse always exist?

(e) Is $\langle \mathbb{C}^*, \odot \rangle$ a group? Explain.

(a) $\mathbb{C}^*$ is not closed under $\odot$ because there are two elements in $\mathbb{C}^*$ I can use with the $\odot$ operator to get an element which is not in $\mathbb{C}^*$. For example, $0 + 1i \odot 1 + 0i = 0 + 0i$ and $0 + 0i \notin \mathbb{C}^*$. Therefore $\odot$ is not well-defined

(b) $\odot$ is associative. To show that $\odot$ is associative, I let $A = a + bi, B = c + di, C = e + fi$ where $A, B, C \in \mathbb{C}^*$ and will show that

$$(A \odot B) \odot C = A \odot (B \odot C)$$

Since,

$$(A \odot B) \odot C = ac + bdi \odot C = ace + bdfi$$

and

$$A \odot (B \odot C) = A \odot (ce + dfi) = cea + dfbi$$

because real numbers under multiplication are known to be commutative it follows that $(A \odot B) \odot C = A \odot (B \odot C)$. Therefore $\odot$ is associative.

(c) The element $e \in \mathbb{C}^*$ such that $e \odot z = z$ exists. This can be shown by rewriting $e \odot z = z$ as

$$e_1 + e_2 i \odot z_1 + z_2 i = e_1 z_1 + e_2 z_2 = z_1 + z_2 i$$

it is clear that $e_1 + e_2 i$ must equal $1 + 1i$ which is in $\mathbb{C}^*$. Therefore $e = 1 + 1i$.

(d) The inverse is the element A^{-1} such that $A \odot A^{-1} = e$. In this case, an inverse does not always exist. I can show this by rewriting $A \odot A^{-1} = e$ to be

$$a + bi \odot a' + b'i = aa' + bb'i = 1 + 1i = e$$

It would follow that a' would be the multiplicative inverse of a and b' would be the multiplicative inverse of b leaving the inverse to be $A^{-1} = \frac{1}{a} + \frac{1}{b}i$. But this is not always the case because either a or b could be equal to zero which there is no multiplicative inverse of. Therefore the inverse does not always exist.

(e) $\langle \mathbb{C}^*, \odot \rangle$ is not a group because it is not closed under $\odot$ and every element in $\langle \mathbb{C}^*, \odot \rangle$ does not necessarily have an inverse.

Problem 7. Let $S = \mathbb{R} - \{-1\}$. In other words, S is the set of all real numbers except -1. Define a binary operation $*$ on S by

$$a * b = a + b + ab.$$

Show that $\langle S, * \rangle$ is a group, as follows:

(a) Establish closure using a proof by contradiction.

(b) Show that $*$ is associative

(c) Find the identity element

(d) Find the inverse of a. Be sure to show that it is an element of S.

(e) What is your conclusion about $\langle S, * \rangle$?

(a) Suppose that S was not closed under $*$. Then there is an $a * b = -1$ because $a * b = a + b + ab$ is closed under $\mathbb{R}$ because multiplication and addition is closed. So the only element that would make S not closed is -1 because $-1 \in \mathbb{R}$ and $-1 \notin \mathbb{R} - \{-1\}$. Furthermore, if

$$a * b = a + b + ab = -1$$

Then when I solve for a I get,

$$a + ab = -1 - b$$
$$a(1 + b) = -1 - b$$

$$a = \frac{-1-b}{1+b} = \frac{-(1+b)}{(1+b)} = -1$$

Since a must be equal to -1, and $-1 \notin \mathbb{R} - \{-1\}$, this forms a contradiction with the assumption that $a \in \mathbb{R} - \{-1\}$. Therefore S must be closed.

(b) To show that $*$ is associative, I will show that $(a * b) * c = a * (b * c)$, where $a, b, c \in S$

$$(a * b) * c = (a + b + ab) * c = (a + b + ab) + c + (a + b + ab)c = a + b + c + ab + ac + bc + abc$$

and

$$a*(b*c) = a*(b+c+bc) = a+(b+c+bc)+a(b+c+bc) = (a+b+c+bc)+(ab+ac+abc) = a+b+c+ab+ac+bc+abc$$

This shows that $(a * b) * c = a * (b * c)$.

(c) The identity element $e \in S$ is the element such that $e * a = a$. That is,

$$e * a = e + a + ea$$

If I let $e = 0$ it becomes clear that

$$0 * a = 0 + a + 0a = a$$

this shows that $e = 0$ is the identity.

(d) The inverse of an element a, denoted a^{-1} is an element in S such that $a * a^{-1} = e$. To find the inverse, I rewrite $a * a^{-1} = e$ as

$$a * a^{-1} = a + a^{-1} + aa^{-1} = 0$$

Now, subtracting a on both sides I get

$$a^{-1} + aa^{-1} = -a$$

Simplifiying, I get

$$a^{-1}(1 + a) = -a$$

and dividing by $(1 + a)$ on both sides I get

$$a^{-1} = \frac{-a}{(1+a)}$$

Now to show that $a^{-1} \neq -1$, I will show $a^{-1} = -1$ cannot be true. If $a^{-1} = -1$, then

$$a^{-1} = \frac{-a}{(1+a)} = -1$$

it follows that

$$-a = -1(1 + a) = (-1 - a)$$

and

$$0 = -1$$

Which is false. This shows that $a^{-1} \neq -1$. Since every element in $\mathbb{R} - \{-1\}$ has an inverse not equal to -1, this shows that every element in $\mathbb{R} - \{-1\}$ has an inverse.

(e) $\mathbb{R} - \{-1\}$ is a group under $*$ because it satisfies the properties of, closure, associativity, every element having and inverse and $*$ has an identity.

Problem 8. Conisder the binary operation $*$ on the set of matrices

$$T = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \,\middle|\, a \in \mathbb{R},\ b \in \mathbb{Z} \right\}$$

defined as

$$\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} * \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix} = \begin{bmatrix} ac & 0 \\ 0 & b+d \end{bmatrix}.$$

Show that $\langle T, * \rangle$ is a group.

To show that $\langle T, * \rangle$ is associative I will show that $(A * B) * C = A * (B * C)$ where $A, B, C \in T$. Since,

$$(A * B) * C = \begin{bmatrix} ac & 0 \\ 0 & b+d \end{bmatrix} * \begin{bmatrix} e & 0 \\ 0 & f \end{bmatrix} = \begin{bmatrix} ace & 0 \\ 0 & b+d+f \end{bmatrix}$$

and

$$A * (B * C) = A * \begin{bmatrix} ce & 0 \\ 0 & d+f \end{bmatrix} = \begin{bmatrix} cea & 0 \\ 0 & d+f+b \end{bmatrix}$$

Since addition is associative in $\mathbb{Z}$ and multiplication is associative in $\mathbb{R}$ it is clear that

$$\begin{bmatrix} ace & 0 \\ 0 & b+d+f \end{bmatrix} = \begin{bmatrix} cea & 0 \\ 0 & d+f+b \end{bmatrix}$$

Therefore $(A * B) * C = A * (B * C)$. This shows that $*$ is associative.

To show that $\langle T, * \rangle$ has an identity element, I will show that there is an element, $e \in T$, such that $A * e = A$. It follows that

$$A * e = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} * e = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} * \begin{bmatrix} e_1 & 0 \\ 0 & e_2 \end{bmatrix} = \begin{bmatrix} ae_1 & 0 \\ 0 & b+e_2 \end{bmatrix} = A.$$

Since,

$$\begin{bmatrix} ae_1 & 0 \\ 0 & b+e_2 \end{bmatrix} = A$$

If I let $e_1 = 1$ and $e_2 = 0$, then

$$\begin{bmatrix} 1a & 0 \\ 0 & b+0 \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} = A$$

Since $e_1 \in \mathbb{R}$ and $e_2 \in \mathbb{Z}$, the identity element is

$$e = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

To show that $\langle T, * \rangle$ has an inverse for all elements in T, I show that for all $A \in T$ that there is an $A^{-1} \in T$ such that $A * A^{-1} = e$. This can be rewritten as

$$A * A^{-1} = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} * \begin{bmatrix} a_1^{-1} & 0 \\ 0 & a_2^{-1} \end{bmatrix} = \begin{bmatrix} aa_1^{-1} & 0 \\ 0 & b+a_2^{-1} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}.$$

So, I need to find a_1^{-1} and a_2^{-1} such that $aa_1^{-1} = 1$ and $b + a_2^{-1} = 0$. Solving for a_1^{-1}, I get $a_1^{-1} = \frac{1}{a}$ and solving for a_2^{-1}, I get $a_2^{-1} = -b$. Since $\frac{1}{a} \in \mathbb{R}^*$ because $a \in \mathbb{R}^*$ and $-b \in \mathbb{Z}$ because $b \in \mathbb{Z}$, the inverse must exist for all elements in T as

$$A^{-1} = \begin{bmatrix} \frac{1}{a} & 0 \\ 0 & -b \end{bmatrix}.$$

Since $\langle T, * \rangle$ satasfies all properties of a group, $\langle T, * \rangle$ is a group.

Problem 9. Let $\langle G, * \rangle$ be a group, and $a, b, c \in G$. Solve the equation $a * x * b = c$ for x.

Since $a, b, c \in G$, G is closed, and a and b have left and right inverses, by left multiplying the L.H.S by a^{-1} and right multiplying by b^{-1} I get

$$a^{-1}a * x * bb^{-1} = a^{-1}cb^{-1}$$

Therefore $x = a^{-1}cb^{-1}$

Problem 10. Let $\langle G, * \rangle$ be a group. Use induction to show that, for any integer $n \geq 2$, and for any n elements $a_1, a_2, ..., a_n$ from G,

$$(a_1 * a_2 * ... * a_n)' = a_n' * a_{n-1}' * ... * a_1'$$

Proof. Using the steps of mathematical induction, I show that this holds for the base case $n = 2$. That is I need to show that

$$(a_1 * a_2)' = a_2' * a_1'$$

Since $\langle G, * \rangle$ is a group, it is closed, $*$ is associative, and each element has an inverse. If I multiply both sides by $(a_1 * a_2)$, I get

$$e = a_2' * a_1' * (a_1 * a_2)$$

Using the associative property, I get

$$e = a_2' * (a_1' * a_2 * a_1) = a_2' * (e * a_2) = a_2' * a_2 = e$$

This shows that $(a_1 * a_2)' = a_2' * a_1'$.

Now, I assume this holds for n, that is I want to show that

$$(a_1 * a_2 * ... * a_n)' = a_n' * a_{n-1}' ... * a_1'$$

and I want to show that this holds for $n + 1$. That is,

$$(a_1 * a_2 * ... * a_n * a_{n+1})' = a_{n+1}' * a_n' * ... * a_1'.$$

It follows from the IHOP, associativity, and inverse multiplication that

$$e = (a_1 * a_2 * ... * a_{n+1}) * a_{n+1}' * a_n' * ... * a_1'$$

it then follows that

$$e = (a_1 * a_2 * ... * a_n * a_{n+1} * a_{n+1}') * a_n' * ... * a_1' = (a_1 * a_2 * ... * a_n) * a_n' * ... * a_1'$$

Finally, when multiplying by the inverse of $(a_1 * a_2 * ... * a_n)$ on both sides I get

$$(a_1 * a_2 * ... * a_n)' = a_1' * a_2' * ...a_n'.$$

This shows that the identity still holds whith $n + 1$, and the induction is completed. ☐