(1a) Prove that every natural number N is congruent to the sum of its decimal digits mod 9.

PROOF: Let the decimal representation of N be \( n_d n_{d-1} \cdots n_1 n_0 \) so that \( N = \sum_{i=0}^{d} n_i \cdot 10^i \). We want to show that this sum is congruent mod 9 to \( N_9 := \sum_{i=0}^{d} n_i \). Now:

\[
N - N_9 = \sum_{i=0}^{d} n_i (10^i - 1)
\]

When \( i \geq 1 \), \( 10^i - 1 \) is a string of \( i \) 9's, so is clearly divisible by 9, and when \( i = 0 \), \( 10^i - 1 = 0 \) is also divisible by 9. Therefore \( N - N_9 \) is a sum of numbers which are each divisible by 9, so it follows that \( N - N_9 \) is itself divisible by 9, or equivalently \( N \equiv N_9 \mod 9 \) as desired.

(1b) Find a generalization to (a) for congruence mod 7 and mod 11.

SOLUTION: In part (a) we used the fact that \( 10^i \equiv 1 \mod 9 \) to establish congruence mod 9 of \( N \) and \( N_9 \). So if we want to find an analogous number \( N_7 \equiv N \mod 7 \), let us consider \( 10^i \mod 7 \). Calculating for \( i = 0, 1, \ldots \) we obtain the sequence 1, 3, 2, 6, 4, 5, 1, 3, \ldots Does this sequence start repeating at \( i = 6 \)? Yes, since \( 10^6 - 10^0 = 999999 = 7 \cdot 142857 \) so that in general \( 10^{n+6} - 10^n \equiv 10^n \cdot (10^6 - 1) \equiv 10^n \cdot (7 \cdot 142857) \) and hence the sequence of remainders mod 7 is periodic with period 6.

What we therefore conclude is that \( (n_0 \cdot 10^0) \equiv (n_0 \cdot 1) \mod 7 \), \( (n_1 \cdot 10^1) \equiv (n_1 \cdot 3) \mod 7 \), \( (n_2 \cdot 10^2) \equiv (n_2 \cdot 2) \mod 7 \), and so on, so that one possible choice for \( N_7 \) is given by:

\[
N_7 = (n_0 + n_6 + \ldots) + 3 \cdot (n_1 + n_7 + \ldots) + 2 \cdot (n_2 + n_8 + \ldots) + 6(n_3 + n_9 + \ldots) + 4 \cdot (n_4 + n_{10} + \ldots) + 5 \cdot (n_5 + n_{11} + \ldots)
\]

If we use a similar approach for finding \( N_{11} \) we find that \( 10^{n+2} - 10^n = 10^n \cdot (11 \cdot 9) \) and that the sequence of remainders \( 10^i \mod 11 \) is 1, 10, 1, 10, \ldots so that:

\[
N_{11} = (n_0 + n_2 + \ldots) + 10 \cdot (n_1 + n_3 + \ldots)
\]

Incidentally we could also consider \( N'_{11} := N_{11} - 11 \cdot (n_1 + n_3 + \ldots) = n_0 - n_1 + n_2 - n_3 + \ldots \) which is another number with the desired property which is also somewhat simpler to calculate.
(2a) Find all subgroups of $Q_8$.

SOLUTION: Each element of $Q_8$ generates a (cyclic) subgroup of $Q_8$, so in addition to $Q_8$ and $\{1\}$, we have subgroups generated by elements such as $i, j, k$, and $-1$. The subgroup generated by $i$ has elements $\{i, i^2 = -1, i^3 = (-1)i = -i, i^4 = (i^2)^2 = (-1)^2 = 1\}$ and similarly for the subgroups generated by $j$ and $k$. The subgroup generated by $i$ is the same subgroup generated by $-i$ and similarly for $j$ and $k$ as is easily checked. Finally the subgroup generated by $-1$ has just two elements: $\{1, -1\}$.

To show that all subgroups of $Q_8$ are cyclic, let us consider the subgroups containing pairs of elements of $Q_8$. $-1$ and 1 lie in the subgroup generated by $i$ or $-i$, so that the subgroups generated by the pairs $(i, 1), (i, -1), (-i, 1),$ and $(-i, -1)$ are all equal to the subgroup generated by just $i$, and similarly for $j$ and $k$. So we need only consider a subgroup containing $i$ and $j$. Such a subgroup must contain $ij = k$, as well as $ji = -k$ and all powers of $i$ and $j$; but these elements exhaust $Q_8$ so that the only subgroup containing $(i, j)$ is $Q_8$ itself, and similarly for other pairs such as $(j, k)$ and $(i, k)$.

Thus the six subgroups of $Q_8$ are the trivial subgroup, the cyclic subgroups generated by $-1, i, j, k$, and $Q_8$ itself.

(2b) Find $Z(Q_8)$.

SOLUTION: The identity element is always contained in the center of a group, so we wish to know if any other elements of $Q_8$ lie in the center. $i$ cannot lie in the center since $ij = k$ but $ji = -k$, and similarly for $-i$ and $\pm j, \pm k$. So we only need to determine if $-1 \in Z(Q_8)$ to determine $Z(Q_8)$. Now $-1 = i^2$ so that it commutes with $i$ because of associativity: $(-1)*i = (i*i)*i = i*(i*i) = i*(-1)$. Likewise, since $j^2 = k^2 = -1$ we see that $-1$ commutes with $i, j,$ and $k$ and hence with all of $Q_8$, so the center of $Q_8$ is $Z(Q_8) = \{1, -1\}$. 

2
(3) Determine all homomorphisms from $\mathbb{Z}/4\mathbb{Z}$ to $Q_8$.

SOLUTION: Since $\mathbb{Z}/4\mathbb{Z}$ is generated by the single element $x := 1 + 4\mathbb{Z}$, to specify a homomorphism $h : \mathbb{Z}/4\mathbb{Z} \to Q_8$ we need only specify $h(x)$. $h$ preserves multiplication, so since $x^4 = 0 + 4\mathbb{Z}$ is the identity element of $\mathbb{Z}/4\mathbb{Z}$, $h(x)^4$ must equal $h(x^4) = h(0 + 4\mathbb{Z}) = 1$ in $Q_8$. But all 8 elements of $Q_8$ have the property that raising them to the fourth power is equal to 1, so $h(x)$ can be any element of $Q_8$, hence there are 8 total homomorphisms from $\mathbb{Z}/4\mathbb{Z}$ to $Q_8$.

Note that the homomorphisms determined by $h_1(x) = i$ and $h_2(x) = -i$ are distinct, even though their images coincide in $Q_8$. The two are considered to be different homomorphisms because they send the same element to different images; it does not matter that the set of images coincides.
(4a) Find all subgroups of $D_8$, the symmetries of a square.

SOLUTION: Consider the square as a subset of $\mathbb{R}^2$, aligned with the coordinate axes. We first describe the different elements of $D_8$, then determine how these fit into subgroups. First, there is a rotation clockwise by $\frac{\pi}{2}$ (call it $s$), and repeating it we get rotations by $\pi$ ($s^2$), $\frac{3\pi}{2}$ ($s^3$) and rotation by 0 or $2\pi$ ($s^4$) which is just the identity element of $D_8$. Clearly the set of these forms a subgroup of $D_8$, and within this subgroup we have the further subgroup of rotation by 0 and $\pi$, which is therefore another subgroup of $D_8$ as well. We also have symmetries determined by reflections in an axis of the square; there are four axes of the square, so this gives our other four elements of $D_8$ (call them $s_x, s_y, s_{x+y}$ and $s_{x-y}$ where $s_w$ is the reflection across the line $w = 0$; i.e. $s_x$ is the reflection across the y-axis and so forth). Applying a reflection twice gives the identity element, so each of these reflections gives rise to yet another cyclic subgroup of $D_8$.

Next we consider subgroups containing 2 reflections or a reflection and a rotation. By labelling the four vertices of a square and taking all possible symmetries generated by $s$ (or $s^3$) and a reflection $r_w$, we obtain all of $D_8$. However, there are only four symmetries generated by $s^2$ and $r_w$ for any $w$, so we obtain two new subgroups of $D_8$ in this way: $\{e, s^2, r_x, r_y\}$ and $\{e, s^2, r_{x+y}, r_{x-y}\}$. Taking pairs of reflections yields one of these two new subgroups (for the pairs $(r_x, r_y)$ and $(r_{x+y}, r_{x-y})$) or all of $D_8$ (all other pairs).

Finally, we note that any triple of distinct nonidentity elements falls into one of four categories. Firstly, it contains 3 rotations, in which case it is the rotation subgroup again. Secondly it may contain 2 rotations and a reflection, in which case it must be $D_8$ since it contains either $s$ or $s^3$ and a reflection, which was seen earlier to generate all of $D_8$. Thirdly it may contain 1 rotation and 2 reflections, in which case the rotation is $s^2$ and it is one of the two subgroups $\{e, s^2, r_x, r_y\}$ or $\{e, s^2, r_{x+y}, r_{x-y}\}$ or the rotation is $s$ or $s^3$ which together with any reflection again gives all of $D_8$. The final option is that it contains 3 distinct reflections, in which case it must contain a pair of reflections generating all of $D_8$. Thus triples of distinct elements do not give rise to any new subgroups and hence we have found all subgroups of $D_8$.

Thus there are 10 subgroups of $D_8$: the trivial subgroup, the six cyclic subgroups $\{e, s, s^2, s^3\}, \{e, s^2\}, \{e, r_x\}, \{e, r_y\}, \{e, r_{x+y}\}$, and $\{e, r_{x-y}\}$, the two subgroups $\{e, s^2, r_x, r_y\}$ and $\{e, s^2, r_{x+y}, r_{x-y}\}$, and $D_8$.

(4b) Show that $D_8$ is not isomorphic to $Q_8$.

Based on (2) and (4a), there are several ways to show this. One way is to consider subgroups; in (2) we showed there are exactly six subgroups of $Q_8$ and in (4a) we showed there are ten subgroups of $D_8$, so the two groups cannot be isomorphic. Another way is to count the orders of elements; any isomorphism must preserve orders. In $Q_8$ we saw there was one element of order 1, one element of order 2, and 6 elements of order 4, whereas in $D_8$ we saw that there are one element of order 1, five elements of order 2, and two elements of order 4; thus the two groups cannot be isomorphic.
Let \( H(\mathbb{R}) \) be the subgroup of \( GL_3(\mathbb{R}) \) consisting of all matrices of the form:

\[
\begin{pmatrix}
  1 & x & z \\
  0 & 1 & y \\
  0 & 0 & 1
\end{pmatrix}
\]

\( x, y, z \in \mathbb{R} \)

(5a) Show \( (Z(H(\mathbb{R}))), \cdot) \cong (\mathbb{R}, +) \).

**PROOF:** Let \( m = \begin{pmatrix} 1 & X & Z \\ 0 & 1 & Y \\ 0 & 0 & 1 \end{pmatrix} \in Z(H(\mathbb{R})) \) and let \( h \) be the matrix given above with \( x, y, z \) arbitrary. Then:

\[
h \cdot m = \begin{pmatrix} 1 & x + X & z + Z + xY \\ 0 & 1 & y + Y \\ 0 & 0 & 1 \end{pmatrix}, \quad m \cdot h = \begin{pmatrix} 1 & x + X & z + yX + yZ \\ 0 & 1 & y + Y \\ 0 & 0 & 1 \end{pmatrix}
\]

If these are to be equal, then \( xY = yX \) for \( x, y \) arbitrary, hence \( X = Y = 0 \) and \( Z(H(\mathbb{R})) \) consists of all matrices of the form:

\[
h_Z := \begin{pmatrix} 1 & 0 & Z \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad Z \in \mathbb{R}
\]

Now consider the map from \((\mathbb{R}, +)\) to \((Z(H(\mathbb{R}))), \cdot)\) given by \( r \mapsto h_r \). This is a group homomorphism since it is easy to check that \( h_r \cdot h_s = h_{r+s} \cdot h_r \). Furthermore \( h_r = h_s \) iff \( r = s \), so this map is 1-1 and onto, hence is a group isomorphism.

(5b) Find all finite subgroups of \( H(\mathbb{R}) \).

**SOLUTION:** Any element of a finite group has finite order, so let us start our search by finding all elements of finite order in \( H(\mathbb{R}) \); i.e. those elements \( g \in H(\mathbb{R}) \) such that \( g^k = Id_3 \) for some positive integer \( k \). Consider a generic element \( g \in H(\mathbb{R}) \):

\[
g = \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}
\]

Now we will show by induction that:

\[
g^k = \begin{pmatrix} 1 & kx + (\frac{k}{2})xy & kz + (\frac{k}{2})xy \\ 0 & 1 & ky \\ 0 & 0 & 1 \end{pmatrix}
\]
This is clearly true for $k = 1$. Now if it is true for $k - 1$, then:

$$g^k = g \cdot g^{k-1} = \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & (k-1)x & (k-1)z + \binom{k-1}{2}xy \\ 0 & 1 & (k-1)y \\ 0 & 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & x + (k-1)x & (k-1)z + \binom{k-1}{2}xy + z + (k-1)xy + z \\ 0 & 1 & (k-1)y \\ 0 & 0 & 1 \end{pmatrix}$$

(1)

$$= \begin{pmatrix} 1 & kx & kz + \binom{k}{2}xy \\ 0 & 1 & ky \\ 0 & 0 & 1 \end{pmatrix}$$

(2)

(2) simplifies to (3) upon realizing that $(k - 1) = \binom{k-1}{1}$ and then applying the binomial identity $\binom{k-1}{1} + \binom{k-1}{2} = \binom{k}{2}$.

Now that we know what the powers of $g$ look like, let us set $g^k = Id_3$. This means that $kx = ky = kz + \binom{k}{2}xy = 0$. Since $k \neq 0$ by assumption, we must have $x = y = z = 0$ and thus $g = Id_3$. Thus $Id_3$ is the only element of finite order in $H(\mathbb{R})$ and hence the trivial subgroup is the only finite subgroup of $H(\mathbb{R})$. 
(6) Now consider $H(\mathbb{Z}/2\mathbb{Z})$, the same set of matrices as in (5), but defined over $\mathbb{Z}/2\mathbb{Z}$ instead of $\mathbb{R}$. Note that $H(\mathbb{Z}/2\mathbb{Z})$ has 8 elements. Is $H(\mathbb{Z}/2\mathbb{Z})$ isomorphic to either $Q_8$ or $D_8$?

SOLUTION: Since we are working with matrices whose entries are elements of $\mathbb{Z}/2\mathbb{Z}$, not $\mathbb{Z}$, remember that all matrix multiplications are done mod 2, i.e. multiply the two matrices as usual, then replace each entry with its remainder when divided by 2.

Considering the orders of elements in $H(\mathbb{Z}/2\mathbb{Z})$ we can immediately conclude $H(\mathbb{Z}/2\mathbb{Z}) \cong Q_8$ since it has one element of order 1, five elements of order 2, and two elements of order 4:

- **Order = 1**:\[
\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}
\]

- **Order = 2**:\[
\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}
\]

- **Order = 4**:\[
\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}
\]

Even though these numbers of elements of each order coincide with the numbers for $D_8$, in general this is not enough to conclude that the two groups are isomorphic. Instead, let us try to set construct an isomorphism $I: D_8 \to H(\mathbb{Z}/2\mathbb{Z})$.

We start by mapping the elements of order 4 in $D_8$ to the elements of order 4 in $H(\mathbb{Z}/2\mathbb{Z})$, say:

\[
I(s) = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \quad I(s^3) = I(s)^3 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}
\]

Since $I$ is a homomorphism, $I(s^2) = I(s)^2 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. Now consider $I(r_x)$;

Since $r_x^2 = e$ and $r_x$ is not in the subgroup of $D_8$ generated by $s$, we only need $I(r_x)^2 = Id_3$, so we can send it to any of the four remaining matrices, say

\[
I(r_x) = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}
\]

In $D_8$, $r_x \cdot s = r_{x+y}$, so $I(r_{x+y})$ must equal $I(r_x) \cdot I(s) = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$. Likewise,

\[
s \cdot r_x = r_{x-y} \text{ so } I(r_{x-y}) = I(s) \cdot I(r_x) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \text{ and finally } r_x \cdot s^2 = r_y
\]
so \( I(r_y) = I(r_x) \cdot I(s^2) = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \). Thus \( I \) at least maps distinct elements of \( D_8 \) to distinct elements of \( H(\mathbb{Z}/2\mathbb{Z}) \) and furthermore \( I \) preserves the orders of these elements. To conclude that \( I \) is an isomorphism, we just have to check that products of pairs of elements of \( D_8 \) are mapped to the corresponding products in \( H(\mathbb{Z}/2\mathbb{Z}) \). It remains to check that if we have \( d_1 \) and \( d_2 \) in \( D_8 \) that \( I(d_1) \cdot I(d_2) = I(d_1 \cdot d_2) \) to verify that \( I \) is indeed a homomorphism; combined with the fact that \( I \) is injective will show that it is an isomorphism. Checking these products is easily done, with a little thought one can save much time by realizing that it is not necessary to check all 64 pairs of elements.

Once you know a little more about group theory, this problem is even easier since it is well-known that, up to isomorphism, there are only two groups of order 8 which are not commutative; \( Q_8 \) and \( D_8 \), so \( H(\mathbb{Z}/2\mathbb{Z}) \) itself being noncommutative must be isomorphic to one of the two; the count of orders of elements we did earlier, along with the fact that it is noncommutative, would then be sufficient to conclude that \( H(\mathbb{Z}/2\mathbb{Z}) \) is indeed isomorphic to \( D_8 \). In the absence of knowing (or proving) that there are only two noncommutative groups of order 8, this shorter proof is invalid as it does not show why knowing the orders of elements of \( H(\mathbb{Z}/2\mathbb{Z}) \) is sufficient for determining that it is isomorphic to \( D_8 \).

If the isomorphism \( I \) described above still seems a bit cloudy, it has a natural geometrical picture which clearly establishes the isomorphism. Consider a square labelled as follows:

\[
\begin{array}{ccc}
& (0,0,1) & \\
\langle 1,1,1 \rangle & \langle 1,0,1 \rangle & (0,1,1) \\
\langle 0,1,1 \rangle & & \\
\end{array}
\]

Now consider the matrix \( I(s) \) defined earlier as acting on these vectors and reduce the results \( \mod 2 \), then \( I(s) \) has the effect of rotating this square clockwise by \( \frac{\pi}{2} \) (i.e. \( I(s) \ast (0,0,1) = (0,1,1) \)), and so the image of the vector label of the top edge under \( I(s) \) is the vector label of the right edge, and so on around the square). Similarly, the matrix \( I(r_x) \), when acting on these vectors switches the vectors on the left and right, but fixes the top and bottom vectors which is exactly the action of the reflection \( r_x \) on this square and we have a visual proof of the isomorphism between \( D_8 \) and \( H(\mathbb{Z}/2\mathbb{Z}) \).

8