1 Define an equivalence relation on the Gaussian integers by:

$$\text{if } a, b \in \mathbb{Z}[i], \text{ then } a \equiv b \iff 3 \mid a - b.$$

How many equivalence classes are there? Here's one way of thinking about this problem: Think of it as a vector space over $\mathbb{Z}/3\mathbb{Z}$.

Solution The equivalence classes are as follows:

	$[0]$	$[1]$	$[2]$
$[0i]$	$[0]$	$[1]$	$[2]$
$[i]$	$[i]$	$[1+i]$	$[2+i]$
$[2i]$	$[2i]$	$[1+2i]$	$[2+2i]$

Indeed, consider $a + bi \in \mathbb{Z}[i]$ for $a, b \in \mathbb{Z}$. Then $a, b \in \{[0], [1], [2]\}$, which, allowing a and b to vary, give us all the possible equivalence classes.

These classes are also disjoint. Their differences have real parts among $[0], [1], [2]$ and imaginary parts among $[0], [1], [2]$ also, so 3 will not divide their differences.

---

2 Consider the following four matrices:

$$I_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad I_2 = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \qquad I_3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad I_4 = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix},$$

where $i = \sqrt{-1}$.

Let Q be the eight elements $\{\pm I_1, \pm I_2, \pm I_3, \pm I_4\}$ above. Show Q is a group under matrix multiplication. Relate Q to the quarternions.

Solution Closure:

It suffices to show that I_1, I_2, I_3, I_4 are closed under matrix multiplication, since multiplying with $-I_1, -I_2, -I_3, -I_4$ can only put a minus sign in front of the result, which is also in the set.

Notice that I_1 is the regular identity, so $I_j I_1 = I_1 I_j = I_j \in Q$ for any I_j. So, we only need the check multiplication with the other matrices.

$\cdot$	I_2	I_3	I_4
I_2	$-I_1$	I_4	$-I_3$
I_3	$-I_4$	$-I_1$	I_2
I_4	I_3	$-I_2$	$-I_1$

Identity:

As mentioned above, I_1 is the identity matrix and is the identity of the set.

Inverse:

Once again, we can just look at I_1, I_2, I_3, I_4, since the inverse of $-I_j$ will just be $-(I_j^{-1})$.

From the table above, it's easy to see that

$$I_1 I_1 = I_1 \qquad I_2(-I_2) = I_1 \qquad I_3(-I_3) = I_1 \qquad I_4(-I_4) = I_1.$$

so every element has an inverse.

Thus, Q is a group, and it is isomorphic to the quaternions, indeed, multiplication in Q corresponds to rotations by quaternions.

3 Label the vertices of a hexagon with the elements of $\mathbb{Z}/6\mathbb{Z}$ counter-clockwise. D_6 is the set of permutations $\sigma\colon \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$ so that the vertex labeled $\sigma(i)$ is always adjacent to the vertex labeled $\sigma(i+1)$ and the vertex labeled $\sigma(i-1)$. How many elements of D_6 are there? Find as many subgroups of D_6 as you can. In particular, find all elements of σ of order 2, i.e., $\sigma^2 = e$ and $\sigma \neq e$, so $\{e, \sigma\}$ is a subgroup with 2 elements, i.e., a subgroup of order 2. Can you find a subgroup with exactly 4 elements?

Solution $\sigma(1)$ has 6 options: $1, 2, 3, 4, 5, 6$. This restricts $\sigma(2)$ to either $\sigma(1) + 1$ or $\sigma(1) - 1 \pmod 6$, so we have 2 choices for $\sigma(2)$. Then $\sigma(0) = \sigma(6)$ has only 1 choice left. After this, all the elements have one choice remaining: the only spot next to to an adjacent element. Hence, we have $6 \cdot 2 = 12$ elements.

Notice that by the argument above, we see that any permutation is completely determined by the images of two adjacent elements.

We can write

$$D_6 = \{e, r, r^2, r^3, r^4, r^5, a, ra, r^2a, r^3a, r^4a, r^5a\},$$

where r is a rotation by $\pi/6$, and a is a horizontal flip. Notice that $r^6 = e$, $a^2 = 1$, and $ra = ar^5$.

Subgroups of order 2:

We can just try all the elements. After doing so, we find the following subgroups:

$$\{e, r^3\},\ \{e, a\},\ \{e, ra\},\ \{e, r^2a\},\ \{e, r^3a\},\ \{e, r^4a\},\ \{e, r^5a\}.$$

The first is a rotation by 180°, the second is a horizontal flip, and the rest corresponds to a horizontal flipping, and then a rotation.

Subgroup with 4 elements:

No, I cannot.

4** Given a group G, a subgroup H and an element $g \in G$, we can form a new set

$$gHg^{-1} := \left\{k \in G \mid \text{there is an } h \in H \text{ so that } k = ghg^{-1}\right\}.$$

Show gHg^{-1} is a subgroup of G.

Solution By definition, it is clear that $gHg^{-1} \subseteq G$.

Closure:

Let $k_1, k_2 \in gHg^{-1}$. Then there exist $h_1, h_2 \in H$ such that $k_1 = gh_1g^{-1}$ and $k_2 = gh_2g^{-1}$.

Then $k_1k_2 = gh_1g^{-1}gh_2g^{-1} = gh_1eh_2g^{-1} = g(h_1h_2)g^{-1}$. Since H is a subgroup, $h_1h_2 \in H$, which means that $k_1k_2 \in gHg^{-1}$, so the set is closed under the group operation.

Associativity:

Associativity is inherited from G, since we use the same operations on elements of $gHg^{-1} \subseteq G$.

Identity:

Notice that $geg^{-1} = gg^{-1} = e$ is an element of gHg^{-1}. Since e was the identity in G, it is still the identity in gHg^{-1}.

Inverse:

Given $ghg^{-1} \in gHg^{-1}$, its inverse is $gh^{-1}g^{-1}$, which exists since h is an element of G.

$$ghg^{-1}gh^{-1}g^{-1} = ghh^{-1}g^{-1} = gg^{-1} = e$$
$$gh^{-1}g^{-1}ghg^{-1} = gh^{-1}hg^{-1} = gg^{-1} = e.$$

Hence, gHg^{-1} is a subgroup of G.

5** Suppose H and H' are subgroups of a group G. Define a relation $H \sim H'$ if there is a $g \in G$ so that $H' = gHg^{-1}$. Show $\sim$ is an equivalence relation. We say H and H' are conjugate in G if $H \sim H'$.

Solution Reflexivity:

We can take $g = e = e^{-1}$. Then it is easy to see that

$$eHe^{-1} = eHe = H,$$

since eHe^{-1} is created by taking an element $h \in H$, and then multiplying on the left by e and on the right by e^{-1}, which gives us h back.

Thus, $H \sim H$.

Symmetry:

Let $H \sim H'$, with $H' = gHg^{-1}$ for some $g \in G$. If we replace g with g^{-1}, we see that $g^{-1}H'(g^{-1})^{-1} = g^{-1}H'g$. We'll show that this set is precisely H.

Let $h \in H$. Then by definition, $ghg^{-1} \in H'$. Again by definition, $g^{-1}H'g \ni g^{-1}(ghg^{-1})g = h$, so $H \subseteq g^{-1}H'g$.

Let $k \in g^{-1}H'g$. Then there exists $h' \in H'$ such that $k = g^{-1}h'g$. Since $H' = gHg^{-1}$, there exists $h \in H$ such that $h' = ghg^{-1}$, so $k = g^{-1}(ghg^{-1})g = h \in H$, so $g^{-1}H'g \subseteq H$.

Thus, by double inclusion, $H = g'H'g$, so $H' \sim H$.

Transitivity:

Let $A \sim B$ and $B \sim C$. By definition, there exists $g, h \in G$ such that

$$B = gAg^{-1} \quad \text{and} \quad C = hBh^{-1}.$$

We'll show that

$$C = hgA(hg)^{-1}.$$

Let $c \in C$.

Since $C = hBh^{-1}$, there exists $b \in B$ such that $c = hbh^{-1}$. Similarly, since $B = gAg^{-1}$, there exists $a \in A$ such that $b = gag^{-1}$. Substituting,

$$c = h(gag^{-1})h^{-1} = hgag^{-1}h^{-1} = hga(hg)^{-1} \in hgA(hg)^{-1}.$$

Let $k \in hgA(hg)^{-1}$. Then there exists $a \in A$ such that $k = hgag^{-1}h^{-1}$. Since $B = gAg^{-1}$, there exists $b \in B$ such that $b = gag^{-1}$. Similarly, there exists $c \in C$ such that $c = hbh^{-1}$. Substituting,

$$k = h(gag^{-1})h^{-1} = hbh^{-1} = c \in C.$$

Thus, $C = hgA(hg)^{-1}$, by double inclusion.

Since G is a group, $hg \in G$, so $A \sim C$. Thus, transitivity holds.

Since the three axioms hold, $\sim$ is an equivalence relation.

6 Which of the subgroups of order 2 that you found in problem 3 are conjugate?

Solution These were the subgroups:

$$\{e, r^3\},\ \{e, a\},\ \{e, ra\},\ \{e, r^2a\},\ \{e, r^3a\},\ \{e, r^4a\},\ \{e, r^5a\}.$$

It suffices to just check the non-identity element in each subgroup.

Notice that since $ra = ar^5$, we have

$$r^n a = r^{n-1} a r^5.$$

We can then rewrite the subgroups as

$$\{e, r^3\},\ \{e, a\},\ \{e, ar^5\},\ \{e, rar^5\},\ \{e, r^2ar^5\},\ \{e, r^3ar^5\},\ \{e, r^4ar^5\}.$$

Then notice that $(r^n)^{-1} = r^{6-n}$, which gives

$$\{e, r^3\},\ \{e, a\},\ \{e, ar^{-1}\},\ \{e, rar^{-1}\},\ \{e, r^2ar^{-1}\},\ \{e, r^3ar^{-1}\},\ \{e, r^4ar^{-1}\}.$$

So, we see that $\{e, a\} \sim \{e, rar^{-1}\}$.

---

7 Consider the vertices of a cube. They are the eight points (a, b, c) so that a, b, c are zero or one. Consider two vertices as connected if the vertices different in exactly one position, e.g., $(1, 1, 0)$ is connected to $(0, 1, 0), (1, 0, 0), (1, 1, 1)$. Let V be the set of vertices and consider a permutation $\sigma\colon V \to V$ so that $v_1, v_2 \in V$ are connected if and only if $\sigma(v_1), \sigma(v_2)$ are connected. Such a permutation is called a symmetry of the cube; these symmetries form a group G. What is $|G|$?

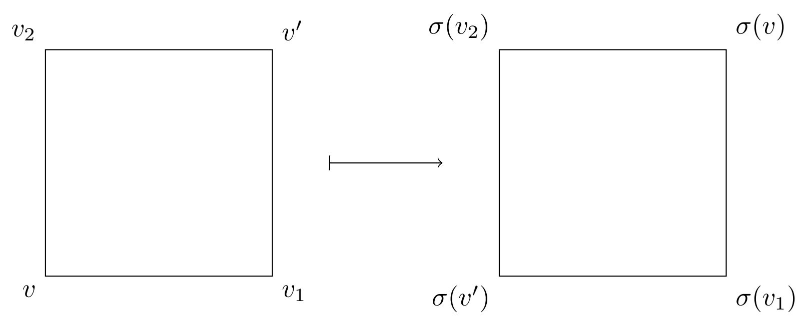
Solution Let $\sigma \in G$.

There are 8 possibilities for $\sigma(v)$, since we can place it anywhere. A symmetry must then map the connected vertices of v to connected vertices of $\sigma(v)$.

There are 3 vertices v_1, v_2, v_3 connected to v, since we can only change 1 of the 3 coordinates of v. Similarly, there are 3 vertices connected to $\sigma(v)$.

$\sigma(v_1)$ hence has 3 choices, which leaves 2 connected vertices remaining, so there are 2 choices for $\sigma(v_2)$. Afterwards, $\sigma(v_3)$ only has 1 choice.

Notice that given 2 vertices whose coordinates differ in 2 places (i.e., vertices lying on the same side), there are 2 vertices connected to both of them.



v is one of the vertices connected to both v_1 and v_2, which means that the other vertex connected to both v_1 and v_2 is v'. Since $\sigma(v)$ is connected to $\sigma(v_1)$ and $\sigma(v_2)$, we see that $\sigma(v')$ only has 1 choice remaining.

In general, sides map to sides.

We can repeat the argument to see that the remaining vertices have exactly 1 choice each, so

$$|G| = 8 \cdot 3 \cdot 2 = 48.$$

8 Compute $(\mathbb{Z}/8\mathbb{Z})^\times$. Find a different group isomorphic to it. Can you do the same for $(\mathbb{Z}/2^n\mathbb{Z})^\times$ if $n = 4, 5$? If n is any integer at least 3?

Solution The integers coprime to 8 in $\mathbb{Z}/8\mathbb{Z}$ are given by $1, 3, 5, 7$. Even numbers share a factor of 2 with 8, so they are not coprime with 8

The multiplication table is as follows (each number represents an equivalence class, for simplicity):

$\times$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

The group is isomorphic to permutations of the set $\{0, 1, 2, 3\}$ with the maps $\sigma_i(n) = n + [i]_4$ for $i = 0, \ldots, 3$, i.e., the permutations which preserve the order of the elements modulo 4, with function composition.

This is a group: $(\sigma_i \circ \sigma_j)(n) = (n + [j]_4) + [i]_4 = n + [i+j]_4$, which is another order-preserving permutation. Its identity is σ_0, which is the do-nothing permutation. The inverse of σ_i is then $\sigma_{(4-i)}$, so this is a group.

We can then take φ so that $\varphi(\sigma_i) = 2[i]_4 + 1$, which is clearly a bijection. We'll now show that it's a homomorphism between the two groups.

Notice that given $2i + 1$ and $2j + 1$ in $(\mathbb{Z}/8\mathbb{Z})^\times$,

$$(2[i]_4 + 1) \times (2[j]_4 + 1) = 4[ij]_4 + 2[i]_4 + 2[j]_4 + 1 = 2[i + j]_4 + 1.$$

Thus,

$$\varphi(\sigma_i \circ \sigma_j) = 2[i + j]_4 + 1 = (2[i]_4 + 1) \times (2[j]_4 + 1),$$

so φ is an isomorphism between the two groups.

For $(\mathbb{Z}/2^n\mathbb{Z})^\times$ for $n \geq 3$, we first prove the following lemma by induction: The order of 5 is 2^{n-1}.

Base step:

For $n = 3$, we had $5^2 \equiv 1 \mod 8$, so the base step holds.

Inductive step:

Assume that the order of 5 in $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is 2^{n-1}. We want to prove that its order in $(\mathbb{Z}/2^{n+1}\mathbb{Z})^\times$ is 2^n.

By definition, we know that

$$5^{2^{n-1}} = 1 + k \cdot 2^n,$$

for some odd k. Squaring both sides,

$$\begin{aligned} 5^{2^n} &= 1 + k \cdot 2^{n+1} + k^2 \cdot 2^{2n} \\ &= 1 + 2^{n+1}k(1 + k^2 2^{n-1}). \end{aligned}$$

k is odd, $k^2 2^{n-1}$ is even, so $1 + k^2 2^{n-1}$ is odd, which means that 2^{n+1} contains all the factors of 2. Thus, for ℓ odd,

$$5^{2^n} = 1 + \ell \cdot 2^{n+1} \equiv 1 \mod 2^{n+1},$$

so 5 has order 2^n, and the inductive step holds.

By induction, 5 has order 2^{n-1} in $(\mathbb{Z}/2^n\mathbb{Z})^\times$.

Hence, we can break the group up into $\langle 5 \rangle$ and $(\mathbb{Z}/2^n\mathbb{Z})^\times \setminus \langle 5 \rangle$. $\langle 5 \rangle$ then has 2^{n-1} elements, and there are 2^{n-1} remaining elements. Let g be an element not in $\langle 5 \rangle$. Then we can form a bijection from the two sets as follows:

$$\langle 5 \rangle \ni 5^x \longmapsto g5^x \in (\mathbb{Z}/2^n\mathbb{Z})^\times \setminus \langle 5 \rangle := g\langle 5 \rangle.$$

Indeed, $g5^x$ is not in $\langle 5 \rangle$ because $\langle 5 \rangle$ is a subgroup, which would imply that $g = g5^x(5^x)^{-1} \in \langle 5 \rangle$.

Our claim is $(\mathbb{Z}/2^n\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-1}\mathbb{Z}$.

Notice that we can identify $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-1}\mathbb{Z}$ with $(-1)^s 5^n$, for $s \in \{0, 1\}$ and $n \in \{0, 1, \ldots, n-1\}$. This is injective: if $(-1)^a 5^b = (-1)^{a'} 5^{b'}$, then

$$5^{2b} = 5^{2b'} \implies 5^{2(b-b')} = 1 \implies b = b'.$$

Since their signs are the same, we must have that $a = a'$ also, since a and a' are either 0 or 1. By definition, this identification is also surjective.

Define φ as follows: Write an element in $(\mathbb{Z}/2^n\mathbb{Z})^\times$ as $g^0 5^n$ or $g5^n$, and then set

$$\varphi(g^s 5^n) = (-1)^s 5^n \sim (s, n) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-1}\mathbb{Z}.$$

By the same argument above, this map is bijective. It suffices to show that φ is a homomorphism.

$$\varphi(g^s 5^n \cdot g^t 5^m) = \varphi(g^{(s+t)} 5^{(n+m)}) = (s + t, n + m) = (s, n) + (t, m).$$

Thus, φ is an isomorphism, so

$$(\mathbb{Z}/2^n\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-1}\mathbb{Z}.$$

---

9 Find the smallest positive integer x satisfying the congruences

$$x \equiv 3 \mod 11, \quad x \equiv 2 \mod 12, \quad \text{and} \quad x \equiv 3 \mod 13.$$

Solution By the division algorithm, x must satisfy the following relations, for some $a, b, c \in \mathbb{Z}$:

$$\begin{aligned} x &= 11a + 3 \\ x &= 12b + 2 \\ x &= 13c + 3. \end{aligned}$$

Notice that

$$\begin{aligned} 3 &\equiv x \mod 13 \\ &\equiv 11a + 3 \\ &\equiv -2a + 3 \\ \implies 2a &\equiv 0 \mod 13. \end{aligned}$$

The smallest positive value of a which satisfies the above is 13, which gives $x = 146$. Then by the division algorithm, we see that

$$\begin{aligned} 146 &= 12 \cdot 12 + 2 \\ 146 &= 13 \cdot 11 + 3, \end{aligned}$$

so $x = 146$ is the smallest positive integer satisfying the congruences.