

## Part A

### Question 1:

*How many bit strings of length 10 either begin with three 000s or end with two 00s.*

Let  $A$  be the set of all bit strings of length 10 that begin with three 000s, and let  $B$  be the set of all bit strings of length 10 that end with two 00s.  $|A| = 2^7 = 128$  and  $|B| = 2^8 = 256$ . We are looking for  $|A \cup B| = |A| + |B| - |A \cap B|$ .  $|A \cap B| = 2^5 = 32$ . Thus, our final answer is  $128 + 256 - 32 = 352$  bit strings.

### Question 2:

*Assuming that no one has more than 1,000,000 hairs on the head of any person and that the population of New York City was 8,008,278 in 2010, show that there had to be at least nine people in New York City in 2010 with the same number of hairs on their heads.*

We shall prove this with the pigeonhole principle. The holes are all of the possible number of hairs a person could have on their head. We make the assumption that no one can have more than 1,000,000 hairs on their head, so there are 1,000,001 holes, as a person could have anywhere between 0 and 1,000,000 hairs on their head. We also know that there are 8,008,278 pigeons, as there are 8,008,278 people in New York City. We now divide pigeons by holes, or  $8,008,278 / 1,000,001 = 8.0083$ . We take the ceiling of this number to get 9. By the pigeonhole principle, we know that there are at least 9 people who all have the same number of hairs on their heads.

### Question 3:

*Given the groups  $\mathbb{R}^*$  and  $\mathbb{Z}$ , let  $G = \mathbb{R}^* \times \mathbb{Z}$ . Define a binary operation  $\circ$  on  $G$  by  $(a, m) \circ (b, n) = (ab, m + n)$ . Show that  $G$  is a group under this operation.*

In order to show that  $G$  is a group, we must show that the operation defined is associative, that there is an identity element, and that for each element, there exists an inverse element.

We shall first show that the operation is associative. We define 3 elements,  $(a_1, a_2), (b_1, b_2), (c_1, c_2)$ , where  $a_1, b_1, c_1 \in \mathbb{R}^*$  and  $a_2, b_2, c_2 \in \mathbb{Z}$ .

$$((a_1, a_2) \circ (b_1, b_2)) \circ (c_1, c_2) = (a_1 b_1, a_2 + b_2) \circ (c_1, c_2) = (a_1 b_1 c_1, a_2 + b_2 + c_2) = (a_1, a_2) \circ (b_1 c_1, b_2 + c_2) = ((a_1, a_2) \circ ((b_1, b_2) \circ (c_1, c_2)))$$

We shall now show that there is an identity element. An identity element is a an element  $e \in G$  such that for any  $a \in G$ ,  $e \circ a = a \circ e = a$ . This element is  $(1, 0)$ . We must confirm this on both the right and the left.

For any element  $(a_1, a_2) \in G$ ,

$$(1, 0) \circ (a_1, a_2) = (1a_1, 0 + a_2) = (a_1, a_2) \text{ and } (a_1, a_2) \circ (1, 0) = (a_1 1, a_2 + 0) = (a_1, a_2).$$

Finally, we shall show that there exists an inverse element. An inverse element is that for each  $a \in G$ , there exists an element  $a^{-1}$  such that  $a \circ a^{-1} = a^{-1} \circ a = e$ . For our group, The inverse of any element  $(a_1, a_2)$  is the element  $(\frac{1}{a_1}, -a_2)$ . We must confirm this on both the left and the right.

For every element  $(a_1, a_2) \in G$ ,

$$\begin{aligned} (\frac{1}{a_1}, -a_2) \circ (a_1, a_2) &= (\frac{1}{a_1}a_1, -a_2 + a_2) = (1, 0) \text{ and} \\ (a_1, a_2) \circ (\frac{1}{a_1}, -a_2) &= (a_1 \frac{1}{a_1}, a_2 + (-a_2)) = (1, 0) \end{aligned}$$

This shows that there is an inverse for every element, and completes the proof.

## Part B

### Question 1:

*How many strings of 10 ternary digits (0, 1, or 2) are there that contain exactly two 0s, three 1s, and five 2s?*

There are 10 total places. We will place the two 0s first. This is 10 choose 2, which equals 45. We will then place the three 1s. This is 8 choose 3, which is 56. The remaining five spots will all be 2s. Thus, the number of strings is  $45 \times 56 = 2520$ .

### Question 2:

*Prove that if  $G$  has no proper nontrivial subgroups, then  $G$  is a cyclic group.*

We will use a constructive proof. We first suppose that  $G$  has no proper nontrivial subgroups. We will now take an element  $a \in G$  where  $a \neq e$ . By **Theorem 4.3** in the Judson text, we know that the set  $\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$  is a subgroup of  $G$  and is the smallest subgroup of  $G$  that contains  $a$ . We know that  $\langle a \rangle$  contains at least  $e$  and  $a$ , and thus it is not a trivial subgroup. We also know that  $G$  has no proper subgroups, so we know that  $\langle a \rangle = G$ . By the definition of cyclic groups,  $\langle a \rangle$  is a cyclic group. This completes the proof.

### Question 3:

*Prove or disprove: Every proper subgroup of a nonabelian group is nonabelian.*

I will disprove this by showing a counter example. Take the group  $S_3$  of order 6. From **Example 3.13** in the Judson text, we know that  $S_3$  is non-abelian.  $S_3 = \{id, (12), (13), (23), (123), (132)\}$ . Let us examine a subgroup generated by  $(12)$ .  $(12)(21) = id$ , so the subgroup is  $\{id, (12)\}$ . We know that its order is 2, and from **Corollary 6.12** in the Judson text we know that any group whose order  $p$  is a prime number is a cyclic group. We know from **Theorem 4.9** in the Judson textbook that every cyclic group is abelian. Thus, we have given an example of an abelian proper subgroup of a nonabelian group.