1. Группа G (допустим, для простоты, по умножению) называется *циклической*, если все её элементы являются степенями некоторого элемента $g \in G$. Такой элемент g называется *образующей* группы G.

Докажите, что все циклические группы порядка n изоморфны.

2. Пусть группа G порядка n является циклической. Найдите количество элементов группы G, каждый из которых является образующей этой группы.

3. Перестановка элементов группы G, являющаяся изоморфизмом, называется *автоморфизмом*.

Докажите, что при любом автоморфизме циклической группы G образующая этой группы переходит в образующую.

4. Множество всех автоморфизмов группы G обозначается $\operatorname{Aut} G$. Докажите, что $\operatorname{Aut} G$ является группой.

5. Опишите группу $\operatorname{Aut} \mathbb{Z}_n$, понимая $\mathbb{Z}_n$ как группу по сложению.

6. Пусть $n \in \mathbb{N}$, $n \geqslant 2$, $e \in \mathbb{Z}$, $(e, \varphi(n)) = 1$. Докажите, что отображение

$$\operatorname{Enc}_e(a) = a^e \pmod n$$

является автоморфизмом группы $\mathbb{Z}_n^*$.

Замечание: Это отображение играет ключевую роль в криптосистеме RSA.

7. Пусть p — простое число. Опишите группу $\operatorname{Aut} \mathbb{Z}_p^*$.

Указание: Воспользуйтесь тем фактом, что группа $\mathbb{Z}_p^*$ — циклическая.