1 Task

$\Leftarrow$

Доказательство. $t \cdot k \equiv 1 mod n \Leftrightarrow kt = 1 + qn$

$k = k' \cdot d$

$n = n' \cdot d$

d – НОД(k, n)

Тогда из $kt = 1 + qn$ получаем $1 = k'dt - qn'd = (k't - qn')d$

В таком случае $d|1 \Rightarrow d = 1$ □

$\Rightarrow$

Доказательство. Пусть A – множество чисел, которые можно получить из k, n с помощью сложения и вычитания.

Тогда $r_1 = k - nq_1, r_2 = n - r_1 q_2, r_3 = r_1 - r_2 q_3, ...$

$r_1 \in A \Rightarrow r_2 \in A \Rightarrow r_3 \in A \Rightarrow ... \Rightarrow r_n \in A.$

А r_n как раз равно d.

Так как k и n взаимно просты, то $d = 1 = k\widetilde{k} + n\widetilde{n} \Rightarrow k\widetilde{k} = 1(mod n) \Rightarrow \exists t : kt = 1(mod n).$

□

2 Task

$17^{668} \equiv (-10)^{668} \equiv 10^{668}(mod 27).$

$10^{668} = 1 + 9...9$ (668 девяток) – делится на 9, но не делится на 27 (т.к. при делении на 9 остается 668 единиц, где сумма цифр не делится на 3).

Если вычесть 9 и оставить 667 девяток, то число также не будет делиться на 27. Значит, необходимо вычесть 18.

Таким образом, мы получим остаток от деления $1 + 18 =$ **19**.

3 Task

Методом пристального взгляда заметим, что $2^{3n} \equiv 8(mod 14)$. (То есть у нас тут получается циклическая группа порядка 3 остатков от деления на 14 чисел вида 2^n).

Заметим также, что $2^{21^{42069}} = 2^{3n}$, т.к. $21 \vdots 3$.

Таким образом, мы приходим к ответу **8**.

4 Task

4.1 Part

Сначала проверим на гомоморфизм: $\phi(a^{k_1}, a^{k_2}) \cdot \phi(a^{m_1}, a^{m_2}) =\rightarrow \phi(a^{m_1 * k_1}, a^{m_2 * k_2})$ – гомоморфизм.

Этот гомоморфизм биективен, т.к. каждому элементу (a^k, a^m) можно поставить в соответствие $a^(11k + m)$.

Значит, данные группы изоморфны.

4.2 Part

Данные группы не гомоморфны, т.к. биективное отображение из первой группы во вторую не сохраняет групповую операцию, а именно возникают проблемы с элементами вида $(a^6, a^16), (a^4, a^17)$ (изоморфизм сохраняет порядки элементов, а здесь этого, к сожалению, не наблюдается).

То есть данные группы **не изоморфны**

5 Task

Пусть ϕ – автоморфизм нашей группы. Если $\phi(1) = d \in Z$, то $\forall z \in Z \phi(z) = \phi(1 + ... + 1) = \phi(1) + ... + \phi(1) = dz$.

Таким образом, все автоморфизмы вида $\phi : G_1 \to G_2 : \phi(x) = dx$ нам подходят.

6 Task

Предположим, что $\phi(x_1) = \phi(x_2)$, т.е. $ax_1 = ax_2$.

Введем $t = x_1 - x_2$. Тогда $at = 0$. Значит, $|z||a$. По теореме Лагранжа порядок z также делит порядок группы G.

Т.к. a и $|G|$ взаимно просты, то $|t| = 1 \Rightarrow z = 1$ (нейтральный элемент), т.к. только нейтральный элемент может быть порядка 1. В таком случае мы получаем $x_1 = x_2$. Значит, отображение ϕ инъективно.

Т.к. ϕ – инъективное отображение множества в себя, то оно, очевидно, биективно.

7 Task

Т.к. $|G|$ = НОК длин непересекающихся циклов, то если НОК каких-то чисел равно 3, то среди этих чисел могут быть только 1 и 3.

Т.к. циклы длины 3 есть четные перестановки, то любое их произведение также будет четной перестановкой, откуда следует, что перестановки порядка 3 **не порождают** группу S_{33}.

8 Task

Стоит отметить, что для доказательства утверждения нам достаточно доказать, что $\forall a, b \in G_1 f(b)f(a) = f(a)f(b)$.

Итак, мы имеем $f(ab) = f(b)f(a)$ и $f(ba) = f(a)f(b)$.

$f(ab)f^{-1}(a) = f(b)f(a)f^{-1}(a)$

$f(ab)f^{-1}(a) = f(b)$

$f(ab)f(a^{-1}) = f(b)$

$f(a)f(ab)f^{-1}(a) = f(a)f(b) = f(ba)$

$f(ab) = f(ba) \Rightarrow$ данные группы изоморфны.

9 Task

Если $m, n \in H(G) \Rightarrow mn \in H(G)$

$P_{mn} = P_m P_n$

$P_n = P_m^{-1} P_{mn}$

Обозначим $q = mn$:

Если $m \in A(G), q \in H(G)$ и $m|q$, то $\frac{q}{m} \in H(G)$.

$x^{-n}y^{-n} = (yx)^{-n} \Rightarrow x^{1-n}y^{1-n} = (xy)^{1-n}$.
Если $n \in H(G) \Rightarrow 1 - n \in H(G)$
Аналогично доказываем, что $n - 1 \in H(G)$
Т.к. $1 - n \in H(G)$ и $n - 1 \in H(G)$, то группа G – абелева.

10 Task

Да, могут.

В качестве примера возьмем A – группу из множества рациональных многочленов с операцией сложения, а B – подгруппа, у которой свободный член – целое число. Тогда группа с множеством многочленов без свободного члена будет будет изоморфна A. Однако, в таком случае для элемента $1 \in B$ не будет элемента $b' \in B : 2b' = 1$. Значит, A и B неизоморфны.