1 Задание 3

1.1 Задача 1

Докажите: НОД(k, n) = 1 $\leftrightarrow \exists t : t \cdot k \equiv 1 mod n$

$\leftarrow$: пусть d – общий делитель k и n и известно, что $tk \equiv 1 mod n$. Тогда $tk = nm + 1, tk - mn = 1$, следовательно $d = 1$, то есть единственный общий делитель 1, то есть числа взаимно простые.

$\rightarrow$: Пусть НОД(k, n) = 1. Рассмотрим вычеты, кратые $[k]_n$, из множество $(k, n) = \{z : xk + yn, x, y \in \mathbb{Z}\}$ = НОД(k, n)$\mathbb{Z} = \mathbb{Z}$, значит $\exists x : kx = 1 - ny$, что и требовалось доказать.

1.2 Задача 2

Вычислите 17^{668} mod 27

$17^{668} = 17^{4\cdot 167} = (17^4)^{167} = 10^{167} = |10^6 \text{ mod } 27 = 1| = 10^5 \cdot (1)^27 = 10^5 = 19$

Ответ: 19.

1.3 Задача 3

Вычислите $2^{21^{42069}}$ mod 14

$$2^{3+1} \equiv 2 \text{ mod } 14 \rightarrowtail 2^{3+1} \cdot 2^3 \equiv 2 \text{ mod } 14$$

Тогда получаем:

$$2^{3n+1} \equiv 2 \text{ mod } 14$$

$$2^{3n} \equiv 8 \text{ mod } 14 \rightarrowtail 2^{21^{42069}} \equiv 8 \text{ mod } 14$$

Ответ: 8

1.4 Задача 4

Изоморфны ли группы:

1. $C_{13} \times C_{13}$ и C_{169}
2. $C_7 \times C_{15}$ и $C_5 \times C_{21}$

1. В группе $C_{13} \times C_{13}$ порядки всех элементов не превосходят 13, а в группе C_{169} есть элемент порядка 169. Изоморфизм сохраняет порядки элементов, поэтому группы неиозоморфны.

2. Воспользуемся Китайской теоремой об остатках: $C_7 \times C_{15} = C_7 \times C_3 \times C_5$, $C_5 \times C_{21} = C_5 \times C_3 \times C_7$, откуда получим, что $C_7 \times C_3 \times C_5 = C_5 \times C_3 \times C_7$ с точностью до перестановок.

Ответ: 1) Нет 2) Да

1.4.1 Задача 7

Порождают ли перестановки порядка 3 группу S_{33}?

Порядок перестановки – это НОК длин циклов в цикловом разложении. Т.к. $3 = 3 \cdot 1$, то циклы либо длины 1, либо длины 3. Циклы длины 3 – чётные перестановки (т.к. любая четная перестановка является произведением циклов длины 3). Поэтому их произведение – чётная перестановка $\rightarrow$ они образуют подгруппу четных перестановок.

Ответ: Нет.