

Задание 1 (на 24.02).

СС 10. Докажите, что:

- а) что число n простое тогда и только тогда, когда для каждого простого делителя q числа $n - 1$ существует $a \in 2, 3, \dots, n - 1$ при котором $a^{n-1} = 1 \pmod n$, а $a^{\frac{n-1}{q}} \neq 1 \pmod n$;
- б) язык простых чисел лежит в **NP**.

СС 11. Докажите **NP**-полноту следующих задач:

- а) на вход подается пара графов (G_1, G_2) , необходимо определить, изоморфен ли граф G_2 подграфу графа G_1 (подсказка для одного из решений, вершины графа G_1 кодируют подстановку для группы переменных из булевой формулы);
- б) на вход подается граф G_1 и число $k \leq |G|$, необходимо определить, есть ли в графе G клика размера k ;
- в) на вход подается граф G_1 и число $k \leq |G|$, необходимо определить, существует такое ли $V \subseteq G$, что $|V| \leq k$ и все ребра графа G инцидентны хотя бы одной вершине из множества V .

EXP — класс языков, разрешимых на ДМТ за время $2^{\text{poly}(n)}$. **NEXP** — класс языков, разрешимых на НМТ за время $2^{\text{poly}(n)}$.

Пусть **C** — класс языков, тогда $\text{coC} = \{L \mid \bar{L} \in \text{C}\}$, где \bar{L} — дополнение языка.

СС 12. Покажите, что:

- а) $\text{P} \subseteq \text{NP} \cap \text{coNP}$;
- б) $\text{NP} \subseteq \text{EXP}$.

СС 13. Покажите, что если $\text{P} = \text{NP}$, то $\text{EXP} = \text{NEXP}$.

СС 14. Докажите, что язык *GNI* (пар неизоморфных подграфов) лежит в P^{NP} .

СС 15. Пусть существует **NP**-полный унарный язык (все слова которого, состоят только из одного символа). Докажите, что $\text{P} = \text{NP}$.

СС 16. (подсказка: вспомните прошлый семестр) Докажите, что $\text{P} \neq \text{EXP}$.