Задание 1 (на 24.02).

CC 10. Докажите, что:

а) что число n простое тогда и только тогда, когда для каждого простого делителя q числа $n-1$ существует $a \in 2, 3, \ldots, n-1$ при котором $a^{n-1} = 1 \; mod \; n$, а $a^{\frac{n-1}{q}} \neq 1 \; mod \; n$;

б) язык простых чисел лежит в **NP**.

CC 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 co**C** $= \{L \mid \overline{L} \in \mathbf{C}\}$, где $\overline{L}$ — дополнение языка.

CC 12. Покажите, что:

а) **P** $\subseteq$ **NP** $\cap$ co**NP**;

б) **NP** $\subseteq$ **EXP**.

CC 13. Покажите, что если **P** $=$ **NP**, то **EXP** $=$ **NEXP**.

CC 14. Докажите, что язык GNI (пар неизоморфных подграфов) лежит в $\mathbf{P}^{\mathbf{NP}}$.

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

CC 16. (подсказка: вспомните прошлый семестр) Докажите, что **P** $\neq$ **EXP**.