Задание 12 (на 27.04).

$\boxed{\textbf{CC 56.}}$

(а) Постройте граф со следующими выделенными вершинами: T, t_1, t_2, r, со следующим свойством: в любой правильной раскраске графа в три цвета вершина r покрашена в тот же цвет, что и T, тогда и только тогда, когда хотя бы одна из вершин t_1, t_2 покрашена в тот же цвет, что и T.

(б) Постройте граф со следующими выделенными вершинами: T, t_1, t_2, t_3, r, со следующим свойством: в любой правильной раскраске графа в три цвета вершина r покрашена в тот же цвет, что и T, тогда и только тогда, когда хотя бы одна из вершин t_1, t_2, t_3 покрашена в тот же цвет, что и T.

(в) (подсказка: создайте в графе треугольник с вершинами: $True, False, Base$) Докажите, что язык графов, которые можно раскрасить в три цвета, **NP**-полон.

$\boxed{\textbf{CC 57.}}$ Покажите, что $\mathbf{AM} = \mathbf{AM}_1$

$\boxed{\textbf{CC 58.}}$ Докажите, что:

(а) $\mathbf{P} = \mathbf{PCP}(0, \log(n))$;

(б) $\mathbf{NP} = \mathbf{PCP}(0, \mathrm{poly}(n))$.

$\boxed{\textbf{CC 59.}}$ Покажите, что если $\mathbf{PSPACE} \subseteq \mathbf{P/poly}$, то $\mathbf{PSPACE} = \mathbf{MA}$ (подсказака: используйте $\mathbf{IP} = \mathbf{PSPACE}$).

$\boxed{\textbf{CC 10.}}$ 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 $a^{n-1} \equiv 1 \pmod n$, а $a^{\frac{n-1}{q}} \not\equiv 1 \pmod n$;

$\boxed{\textbf{CC 26.}}$ (подсказка: $\mathbf{NEXP}^{\mathbf{NP}} vs. \mathbf{NEXP}$) Докажите, что если $\mathbf{P} = \mathbf{NP}$, то существует язык из **EXP**, схемная сложность которого не меньше $\frac{2^n}{10n}$.

$\boxed{\textbf{CC 33.}}$ Докажите, что задача `CircuitEval` **P**-полная.

$\boxed{\textbf{CC 43.}}$ (подсказка: понизьте ошибку) Докажите, что $\mathbf{MA} \subseteq \mathbf{AM}$.

$\boxed{\textbf{CC 44.}}$ Покажите, что:

(в) $\mathbf{BPP} \subseteq \mathbf{BPTime}(n^{\log n}) \subsetneq \mathbf{BPTime}(2^n)$.

$\boxed{\textbf{CC 45.}}$ Определим язык

$$\mathtt{QNR} = \{(y, m) \mid y \text{ не является квадратичным вычетом по модулю } m\}.$$

Докажите, что $\mathtt{QNR} \in \mathbf{IP}$.

Определим класс **UP**. $L \in \mathbf{UP}$, если существует такая недетерминированная машина Тьюринга M, что для любого x выполнено: $M(x) = L(x)$ и существует не более одной подсказки, которая принимается машиной M.

$\boxed{\textbf{CC 54.}}$ Докажите, что:

(а) язык простых чисел лежит в классе **UP**;

(б) если $\mathtt{USAT} \in \mathbf{UP}$, то $\mathbf{NP} = \mathbf{co\text{-}NP}$.

$\boxed{\textbf{CC 55.}}$ Покажите, что существует такой оракул A и язык $L \in \mathbf{NP}^A$, что L не сводится по Тьюрингу к `3SAT`, даже если сведение может использовать оракул A.