Задание 13 (на 06.05).

CC 60. Докажите, что $\mathbf{MAM} = \mathbf{AM}$ (и $\mathbf{MAM}_1 = \mathbf{AM}_1$, данный факт можно использовать в задаче 57).

CC 61. Покажите, что $\mathbf{AM} \subseteq \Pi_2$.

CC 62. Пусть есть оракул, который считает перманент матрицы $n \times n$ над полем $\mathbb{F}$ верно для доли матриц $1 - \frac{1}{3n}$. Пусть $|\mathbb{F}| > 3n$). Докажите, что используя этот оракул можно построить вероятностный полиномиальный по времени алгоритм, который для каждой матрицы с большой вероятностью находит ее перманент.

CC 63. Докажите, что если $\mathbf{NP} \subseteq \mathbf{PCP}(o(\log n), 1)$, то $\mathbf{P} = \mathbf{NP}$.

CC 64. Докажите, что:

(а) если GI — **NP**-полный язык, то **co-NP** $\subseteq$ **AM**;

(б) если GI — **NP**-полный язык, то $\Sigma_2 \subseteq \mathbf{MAM}$.

(в) если GI — **NP**-полный язык, то $\mathbf{PH} = \Sigma_2 \cap \Pi_2$

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 $a^{\frac{n-1}{q}} \not\equiv 1 \pmod{n}$;

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 $\frac{2^n}{10n}$.

CC 33. Докажите, что задача CircuitEval **P**-полная.

CC 44. Покажите, что:

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

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.

CC 54. Докажите, что:

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

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

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.

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

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