Задание 10 (на 20.04).

CC 53. Докажите, что язык булевых формул с ровно одним выполняющим набором (USAT):

(а) **co-NP**-трудным;

(б) лежит в $\mathbf{P}^{\mathbf{NP}}$.

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

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 $\mathtt{QNR} \in \mathbf{IP}$.

CC 48. Докажите, что $\mathbf{BPP/poly} \subseteq \mathbf{P/poly}$ (**BPP/poly** — класс языков, которые разрешаются вероятностными (есть специальные гейты, куда подаются случайные биты) схемами полиномиального размера).

CC 49. Покажите, что:

(в) если граф представляет собой шахматную доску с выбитыми клетками (вершины — клетки, ребра соединяют соседние клетки), то существует полиномиальный алгоритм, который считает число полных паросочетаний (подсказка: иногда вес ребра удобно взять комплексным).

CC 51. Существует вариант класса **MA** с односторонней ошибкой. $L \in \mathbf{MA}_1$, если существует такая полиномиальная вероятностная машина V и полином p, что если $x \in L$, то найдется такая строка $y \in \{0,1\}^{p(n)}$, что $\Pr[V(x,y) = 1] = 1$, а если $x \notin L$, то для любой строки $y \in \{0,1\}^{p(n)}$ выполняется $\Pr[V(x,y) = 1] < \frac{1}{3}$. Покажите, что $\mathbf{MA} = \mathbf{MA}_1$.

CC 52. Покажите, что $\mathbf{MA} \subseteq \Sigma_2^P$.