Задание 8 (на 06.04).

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

(а) если $\mathbf{BPTime}(f(n)) = \mathbf{BPTime}(g(n))$, то $\mathbf{BPTime}(f(h(n))) = \mathbf{BPTime}(g(h(n)))$, где f, g, h — конструктивные по времени, $f(n), g(n) \geq \log n$, $h(n) \geq n$ — возрастающая функция;

(б) $\mathbf{DTime}(f(n)) \subseteq \mathbf{BPTime}(f(n)) \subseteq \mathbf{DTime}(2^{O(f(n))})$;

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

$\boxed{\textbf{CC 46.}}$ $\mathbf{BPL}_H$ — это класс языков, для которых существует вероятностная машина Тьюринга M, которая использует логарифмическую память, останавливается с вероятностью 1, и для всех x выполняется, что $\Pr[M(x) = L(x)] \geq \frac{2}{3}$. Покажите, что $\mathbf{BPL}_H \subseteq \mathbf{P}$.

$\boxed{\textbf{CC 47.}}$ Докажите, что $\mathbf{BPP} = \mathbf{BPP}^{\mathbf{BPP}}$.

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

$\boxed{\textbf{CC 10.}}$ 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 $\mathbf{EXP}$, схемная сложность которого не меньше $\frac{2^n}{10n}$.

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

$\boxed{\textbf{CC 37.}}$ (подсказка: представьте формулу, как дерево и найдите "среднюю" вершину) Покажите, что язык можно разрешить булевой формулой размера s тогда и только тогда, когда этот язык можно разрешить булевой схемой глубина $O(\log(s))$.

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