Задание 9

$\boxed{\mathbf{46.}}$ Пусть ZPP — это класс языков, которые принимаются вероятностной машиной Тьюринга без ошибки, математическое ожидание времени работы которых полиномиально. а) Докажите, что $L \in$ ZPP тогда и только тогда, когда существует полиномиальная по времени вероятностная машина Тьюринга M, которая выдает $\{0, 1, ?\}$, что для всех $x \in \{0,1\}^*$ с вероятностью 1, $M(x) \in \{L(x), ?\}$ и $\Pr[M(x) = ?] \leq \frac{1}{2}$. б) Докажите, что $\mathrm{ZPP} = \mathrm{RP} \cap \mathrm{coRP}$.

$\boxed{\mathbf{47.}}$ Докажите, что если $\mathrm{NP} \subseteq \mathrm{BPP}$, то $\mathrm{NP} = \mathrm{RP}$.

$\boxed{\mathbf{48.}}$ BPL — это класс языков, для которых существует вероятностная машина Тьюринга M, которая использует логарифмическую память, останавливается при всех последовательностях случайных битов и для всех x выполняется, что $\Pr[M(x) = L(x)] \geq \frac{2}{3}$. Покажите, что $\mathrm{BPL} \subseteq \mathrm{P}$.

---

23. а) Докажите, 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 $a^{n-1} = 1 \bmod n$, а $a^{\frac{n-1}{q}} \neq 1 \bmod n$. б) Докажите, что язык простых чисел лежит в NP.

42. Покажите, что существует такой оракул A и язык $L \in NP^A$, что L не сводится по Тьюрингу к $3SAT$, даже если сведение может использовать оракул A.

43. Докажите, что если $\mathrm{P} = \mathrm{NP}$, то существует язык из EXP, схемная сложность которого не меньше $2^n/(10n)$.

45. Назовем машину Тьюринга забывчивой, если положение ее головок в каждый момент времени не зависит от входа, а зависит только от длины входа. Докажите, что для конструктивной по времени функции T любой язык из класса $\mathrm{DTime}[T(n)]$ решается на двухленточной забывчивой машине Тьюринга за время б) $O(T(n) \log T(n))$; в) Докажите, что любой язык из класса $\mathrm{NTime}[T(n)]$ сводится к SAT, причем вход длины n сводится ко входу длины $O(T(n) \log T(n))$ и сведение использует $poly(\log(n))$ памяти.