1. A language $L \subseteq \{0, 1\}^*$ is sparse if there is a polynomial $p(n)$ such that $|L \cap \{0, 1\}^n| \leq p(n)$ for every $n$. Show that every sparse language is in P/poly.

2. Prove that $\text{PSPACE} \neq \text{uniformNC}^1$.

3. Prove that if there is a polynomial time oracle TM that takes two CNF’s $\phi_1$ and $\phi_2$ and outputs their satisfiability using only one oracle query to SAT, then $P = NP$.

4. A function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ naturally corresponds to a bipartite graph on $2n$ vertices. This graph is called $k$-Ramsey if there do not exist $A, B \subseteq \{0, 1\}^n$ with $|A| = |B| = k$, and $b \in \{0, 1\}$, with $f(x, y) = b$ for all $x \in S, y \in T$.
   
   (a) Prove that with probability at least $\frac{1}{2}$ a random function defines a $O(n)$-Ramsey graph.
   
   (b) Show that if $f$ has an AC circuit of size $s$, and depth $d$, then it is not $2^{\Omega(n/\log^2(s))}$-Ramsey.

5. Let $p \in [0,1/2]$ and $q \in [0,1]$, $c > 5$ and $t > 1$. Suppose that a Boolean function $f : \{0,1\}^n \to \{0,1\}$ is computed by an AC circuit of size $S$ and depth at most $d \leq \frac{\log q}{(tc + \log \log S)}$. Select a random restriction $\rho$ with parameters
   
   $\Pr[*] = q, \Pr[1] = (1 - q)p, \Pr[0] = (1 - q)(1 - p)$.

   Prove that
   
   $\Pr[\text{dt}(f|_\rho) \geq \log(S)/c] \leq S^{1-t}$.

6. Below is a few facts/problems related to finite fields.

   (a) Let $p$ be prime. Let $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$ along with operations addition and multiplication mod $p$. Every integer can be treated as an element of $\mathbb{F}_p$ (by taking the remainder after dividing by $p$). All of $\mathbb{F}_p$ forms a group under addition. The nonzero elements of $\mathbb{F}_p$, denoted $\mathbb{F}_p^*$ form a group under multiplication. Both groups are commutative.

   (b) For each $a \in \mathbb{F}_p$, we have $a^p = a$, and if $a \neq 0$, then $a^{p-1} = 1$.

   (c) Following the Razborov-Smolensky proof strategy from the lecture notes, show that PARITY and MAJORITY do not have polynomial size $AC_0(MOD_3)$ circuits. Here in addition to the usual gates of AC circuits, we all MOD_3 gates, which have unbounded fan-in, and output 0 iff the number of 1s on the input wires is divisible by 3.

   (d) Where does the above proof fail if we replace MOD_3 with MOD_6?