1. Show that if $\text{NP} \subseteq \text{BPP}$ then $\text{NP} = \text{RP}$.

2. (Multiplicative Chernoff Bound). Let $X_1, \ldots, X_n$ be independent random variables taking values over $[0,1]$. Let $X = \sum_i X_i$. Show that

   (a) For $r \in (-\infty, \ln 2]$, prove that $\mathbb{E}[e^{rX}] \leq e^{r\mathbb{E}[X]+r^2\mathbb{E}[X]}$, where you may use without proof that $1 + x \leq e^x \leq 1 + x + x^2$ for such $r$.

   (b) Explain how the above used the independence of the $X_i$.

   (c) Apply Markov’s inequality ($\Pr[Y \geq a] \leq \mathbb{E}[Y]/a$) to $e^{rX}$, and optimize over $r$, to conclude that

   i. For $0 \leq \epsilon \leq \ln 4$, $\Pr[X \geq (1 + \epsilon)\mathbb{E}[X]] \leq e^{-\epsilon^2\mathbb{E}[X]/4}$
   ii. For $\epsilon \geq \ln 4$, $\Pr[X \geq (1 + \epsilon)\mathbb{E}[X]] \leq 2^{-\epsilon\mathbb{E}[X]/2}$
   iii. For $0 \leq \epsilon \leq 1$, $\Pr[X \leq (1 - \epsilon)\mathbb{E}[X]] \leq e^{-\epsilon^2\mathbb{E}[X]/4}$
   iv. (Additive Chernoff Bound) For $\epsilon \geq 0$, $\Pr[|X - \mathbb{E}[X]| \geq \epsilon \cdot n] \leq 2e^{-\epsilon^2n/4}$

   Note that the additive Chernoff bound suffices for BPP amplification, but the multiplicative bound is in general stronger and sometimes needed (e.g. consider $\mathbb{E}[X] = \lg n$ and the resulting bound for $\Pr[X \geq 2\mathbb{E}[X]]$).

3. (Arora-Barak Problem 6.5) Show that for every constant $c \geq 1$ there is a language in PH that requires circuits of size $\Omega(n^c)$.

4. Show that $\text{TIME} \left(2^{n^{O(\log n)}} \right) \not\subseteq \text{P/poly}$.
Some hints.

3. Where have we seen languages that require large circuits? How can I debate you to prove (to a verifier) that I am computing such a language? What if there are multiple such languages? Obtain such a language in $\Sigma^4\mathcal{P}$.

4. Use the proof of the circuit size hierarchy theorem, and ideas similar to those arising in problem 3. When does asymptotic behavior kick in?