Problem 1: finding a bi-partite matching
Let $G=(U,V,E)$ be a bi-partite graph with $|U|=|V|=n$. We saw in class an algorithm based on Polynomial Identity Testing (PIT) that decides in poly-time whether $G$ contains a bi-partite matching or not.

Design a revised algorithm that finds a bi-partite matching whenever one exists.

Problem 2: ZPP = RP $\cap$ co-RP
Recall that RP is the set of languages with a one-sided error for yes instances, and co-RP is the set of languages with a one-sided error for no instances.

ZPP is the class of languages for which there exists randomized algorithms that always find the correct solution, and their expected running time is poly(n). That is, for ZPP the uncertainty is only in how much time they take to terminate, but it is guaranteed that when they terminate the answer must be correct.

Prove that $ZPP = RP \cap co-RP$.

(a) Let $L$ be a language in ZPP. This means that there exists a randomized algorithm $A$ which runs in expected time $T(n) = poly(n)$ that always outputs the correct answer. Prove that if we “early terminate” the algorithm after $100T(n)$ steps (say) if it did not terminate already, then we get an algorithm in $RP \cap co-RP$.

(b) Let $L$ be a language in $RP \cap co-RP$. This means that there exist two randomized algorithms deciding it, one in RP and the other in co-RP. Show how to combine them to get a ZPP algorithm.

Problem 3: lower bounds
Prove that PSPACE does not have poly-size boolean circuits.

Concretely: for every $k \geq 1$ there exists a language $L_k \subset \{0,1\}^*$ that satisfies two properties:
(a) $L_k$ can be decided in PSPACE
(b) There exists $n_0 = n_0(k)$, such that for all $n > n_0$ the language $L_k \cap \{0,1\}^n$ cannot be computed by boolean circuits of size $n^k$.

Hint: first, show that the number of all circuits of size $n^k$ is $exp(n^{k+1})$. Then, use a diagonalization argument to design a language that cannot be computed by any of them. Finally, show that this language that you designed can be decided in PSPACE.