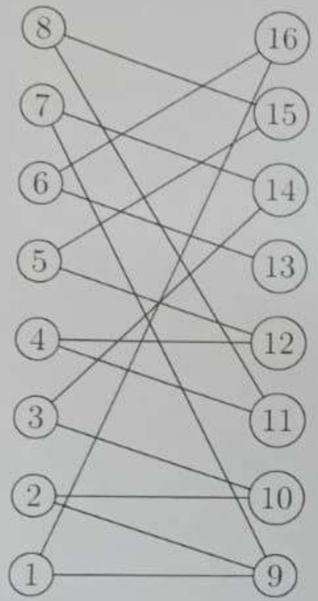
Regular Version (50 marks)

1. **Matching in Bipartite Graph (4 marks).** Prove that the following graph has a perfect matching. You can either do this by explicitly providing the perfect matching,[1] or invoke one of the results we proved in class to conclude that the graph has a perfect matching.



2. **52 numbers in a set (5 marks).** Consider any set of 52 integers. Prove that there exist two distinct numbers x, y in this set such that either $x + y$ or $x - y$ is divisible by 100. Does this claim hold true if we had only 51 numbers in the set?

3. **Issues due to mid-semester course withdrawals (7 marks)** There are $3n$ students registered in COL202 course. The course has a project component, and students have formed groups of 3 each for the project. However, midway through the semester, n students are picked by the institute, uniformly at random (without replacement), for a *higher mission*, and as a result, they don't need to participate in any course-related activities. If a project group has at least one out of the three members left, then the group must complete the project.[2]

   (a) (2 points) What is the expected number of projects that the instructor needs to grade at the end of the semester?

   (b) (2 points) What is the expected number of groups with exactly one group member?

[1] This is the perfect opportunity to use your fancy highlighter :)

[2] A bit unfair for groups with exactly one member left, but not much can be done in this scenario.

(c) (3 points) Suppose, instead of picking n uniformly random students from the class, the institute picked each student with probability $1/3$. Show that the probability that the instructor needs to grade all n projects at the end of the semester is bounded by 2^{-cn} for some constant c.

4. **Random Graphs (8 marks)** Let $0 < p < 1$. Consider the following process for sampling random (undirected) graphs on n vertices: for any distinct vertices $u, v \in V$, $\{u, v\}$ is added to the edge set with probability p, independently. This is called the Erdös-Renyi model, or $G(n, p)$ model. We are interested in how the properties of graphs evolve as a function of p.

   Prove that there exists a constant $c > 0$ such that if $p = (c \log n)/n$, then the resulting graph is connected with probability at least $1 - 1/n$.

5. **~~Question 6:~~ 2-vertex-connected graphs (8 marks)** Let $G = (V, E)$ be an undirected graph. We say that G is *special 2-vertex-connected* if G is 2-vertex-connected, but if any edge of G is removed, then G is no longer 2-vertex-connected.

   1. (2 marks) Construct two non-isomorphic graphs with 6 vertices such that they are special 2-vertex-connected.
   2. (6 marks) Prove that there exists a constant $c > 0$ such that any special 2-vertex-connected graph on n vertices has at most cn edges.

6. **Permutations on Trees. (8 marks)**

   Let $T = (V, E)$ be a tree on n vertices. Consider any permutation $\sigma : V \to V$ such that for all distinct vertices u, v, $\{u, v\} \in E$ if and only if $\{\sigma(u), \sigma(v)\} \in E$. As a result, even after applying this permutation, you get back the exact same graph.

   Prove that one of the following properties must hold:

   - there exists a $v \in V$ such that $\sigma(v) = v$. $\sigma(u) = v$ and $\sigma(v) = u$
   - there exists an edge $\{u, v\} \in E$ such that $\cancel{\{\sigma(u), \sigma(v)\} \in E}$.

7. **Roots of Multivariate Polynomials (8 marks)** Let q be a prime. In class, we proved that any degree-d, univariate polynomial $f(x) \in \mathbb{Z}_q[x]$ has at most d roots. As a result, for any non-zero polynomial $f(x)$ of degree d, if we sample a uniformly random $y \leftarrow \mathbb{Z}_q$, then $\Pr[f(y) = 0] \leq d/q$.

   For multivariate polynomials, the number of roots can be large, even if the degree is bounded. For instance, consider the polynomial $g(x_1, x_2) = x_1 x_2$. For this polynomial, there are $2q - 1$ roots. However, if we sample $y_1 \leftarrow \mathbb{Z}_q, y_2 \leftarrow \mathbb{Z}_q$, then $\Pr[g(y_1, y_2) = 0] \leq 2/q$. You will prove this formally below.

An n-variate polynomial with coefficients from $\mathbb{Z}_q$ is of the form

$$g(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{k} c_i \cdot x_1^{\alpha_{i,1}} \cdot x_2^{\alpha_{i,2}} \cdot \ldots \cdot x_n^{\alpha_{i,n}}.$$

Here, each $c_i \in \mathbb{Z}_q$, and each $\alpha_{i,j} \in \mathbb{N} \cup \{0\}$. The degree of the polynomial is $\max_{i \in [k]} \sum_{j=1}^{n} \alpha_{i,j}$.

As an example, consider the polynomial $g(x_1, x_2, x_3, x_4) = 4x_1^2 + 2x_1x_3^4 + 3x_4^3 + 7$. This polynomial has degree 5.

1. (2 marks) How many tuples $(y_1, y_2, y_3) \in \mathbb{Z}_q^3$ satisfy $x_1x_2x_3 = 0$? Give brief explanation for your answer.
2. (6 marks) Prove that for any degree d, non-zero, n-variate polynomial $g(x_1, x_2, \ldots, x_n)$ with coefficients from $\mathbb{Z}_q$, if $y_1, y_2, \ldots, y_n$ are sampled uniformly at random from $\mathbb{Z}_q$, then $\Pr[g(y_1, y_2, \ldots, y_n) = 0] \leq d/q$.