- You have to discuss the running time of your algorithms. Always try to give algorithm with best possible running time.
- You are required to give proofs of correctness whenever needed.
- You may use any of the following known NP-complete problems to show that a given problem is NP-complete: 3-SAT, INDEPENDENT-SET, VERTEX-COVER, SUBSET-SUM, 3-COLORING, 3D-MATCHING, SET-COVER, CLIQUE.
- **Use of unfair means will be severely penalized.**

There are 3 questions for a total of 50 points.

---

(20) 1. Consider the following problem:

F-SAT: Given a boolean formula in CNF form such that (i) each clause has exactly 3 terms and (ii) each variable appears in at most 3 clauses (including in negated form), determine if the formula is satisfiable.

Answer the following questions with respect to the above problem under the assumptions (i) $\mathbf{P} = \mathbf{NP}$, and (ii) $\mathbf{P} \neq \mathbf{NP}$. Give reasons.

(a) Is F-SAT $\in \mathbf{NP}$?

(b) Is F-SAT **NP**-complete?

(c) Is F-SAT **NP**-hard?

(d) Is F-SAT $\in \mathbf{P}$?

(15) 2. For integers $r, s, r < s$, $s\ (mod\ r)$ is the remainder when dividing s by r. For integers r, s, t, we say that $r \equiv s\ (mod\ t)$ if $r = k \cdot t + s$ for some integer k. For example, $11 \equiv 4\ (mod\ 7)$, $22 \equiv 1\ (mod\ 7)$ etc.

(**RSA**) The RSA public key cryptosystem for private communication can be described in the following manner: Suppose alice wants to send a secret message to Bob. Bob picks two large (1024 bits) prime numbers p and q. Let $N = p \cdot q$. He picks two other numbers $e, d < (p-1)(q-1)$ such that $e \cdot d \equiv 1\ (mod\ (p-1)(q-1))$. Bob makes N and e public (e.g., posts these numbers on his blog) while keeping d secret. Alice who wants to send a message $M \in \{0, ..., N-1\}$ to Bob computes $C \leftarrow M^e\ (mod\ N)$ and sends C to Bob. Bob decrypts it using $M \leftarrow C^d\ (mod\ N) (= M^{ed}\ (mod\ N) = M)$.

Show that if $\mathbf{P} = \mathbf{NP}$, then RSA is *broken*. By broken we mean that an adversary who can see C will always be able to know the secret message M that Alice sends to Bob even without knowing Bob's secret d. You may assume the following:

1. Given $x, p, x < p$, it is easy to find $y < p$ such that $x \cdot y \equiv 1\ (mod\ p)$.
2. It is easy to determine if a given number is prime.

3. (*MAKESPAN problem*) Consider the following problem:

   3-MAKESPAN: Given n jobs with integer durations $d_1, ..., d_n$ and an integer D, determine if these jobs can be scheduled on 3 machines such that the maximum finishing time of any job is $\leq D$.

(10) (a) Show that 3-MAKESPAN is **NP**-complete.

Now consider the optimization version of the problem.

MIN-3-MAKESPAN: Given n jobs with duration $d_1, ..., d_n$, determine a schedule of these n jobs on 3 machines that minimizes the maximum finishing time of any job.

The optimization version of a problem is usually harder than the decision version. The next question asks you to show this formally.

(5) (b) Show that MIN-3-MAKESPAN is **NP**-hard.