Note that there are two problems of 4 marks – the first one is copied from Tutorial 9, which you will need to solve and submit along with the tutorial 10 submission this week.

1. **[4 marks]** Recall the key generation protocol of RSA. Prove that:
   (a) **[2 marks]** the number e that is chosen will always be odd.
   (b) **[2 marks]** the number d that is chosen will always be odd.

2. Recall the lemma that we had proved while proving the correctness of RSA.

   Suppose e, d, p, q, n are all as specified in the RSA key generation protocol – that is, $n = pq$ for primes p and q, and $ed \equiv_{(p-1)(q-1)} 1$. Let $m \in \mathbb{Z}_n$ be any message. Then

   $$m' := [(m^e \bmod n)^d \bmod n]$$

   satisfies both $m' \equiv_p m$ and $m' \equiv_q m$.

   We had proved only the first part (i.e., $m' \equiv_p m$) in the class. Prove the second part, i.e. $m' \equiv_q m$.

3. In a computer science class, there are 10 students who have previously written a program in C, and 18 students who have previously written a program in Python. What can you say about the number of students who have previously written a program in one of the two languages?

4. I gave a piece of paper to my friend (who was going to visit my place) with my WiFi password written on it: *W1F1p@ssw0rd101*. Due to my poor handwriting, however, it was not clear whether the 1's were actually the digit 1, or the letter small L, or the letter capital I (i.e, each instance of 1 could actually be any of these three possibilities). The 0's were also not clear whether they were actually 0 or the letter capital O. How many different passwords will my friend have to try, in order to exhaust all the possibilities that my poor handwriting has led to?

5. Determine how many k-bit strings have exactly three ones, using the idea of dividing the set of bitsrings on the position of the third one.

6. A string over Σ is a sequence of elements of a set Σ, i.e. a string x over Σ satisfies $x \in \Sigma^n$ for some length $n \geq 0$. How many strings of length n over the alphabet $\Sigma = \{A, B, \ldots, Z, \text{␣}\}$ are there? How many contain exactly two "words" (that is, contain exactly one space, where the space does not come in the first or the last position)?

7. Let $n \geq 1$ be an integer, and let P_n denote the set of palindromes of length n, over some alphabet Σ. Define a bijection $f : P_n \to \Sigma^k$ (for some k that you choose). Prove that f is a bijection, and use this bijection to give a formuula for $|P_n|$, for arbitrary $n \in \mathbb{Z}^{\geq 1}$.

8. How many one-to-one functions $f : \{1, 2, 3, 4, 5\} \to \{1, 2, 3, 4, 5\}$ are there?

9. How many bijections $f : \{1, 2, 3, 4, 5\} \to \{1, 2, 3, 4, 5\}$ are there?

10. How many different ways can you arrange the letters of the following words?
    (a) `PASCAL`

(b) `CHARLESBABBAGE`

(c) `PEERTOPEERSYSTEM`

11. At a party attended by $n \geq 2$ people, some pairs of people shake hands. Show that two people shook the same number of hands.

12. In any list of n numbers, there is either a number divisible by n, or two whose difference is divisible by n.

13. **[4 marks]** Take any sequence of n numbers. Prove that there is a consecutive subsequence of these numbers whose sum is divisible by n.

14. Prove that in any group of 6 people, either 3 of them are mutually acquainted, or 3 of them are mutually unacquainted.

15. How many 42-bit strings have exactly 16 ones?

16. How many different integers have exactly 10 prime factors that comes from the set of the first 20 prime numbers?

17. Conside rthe equation $a + b + c = 202$. How many solutions are there where a, b, and c are all non-negative integers?

18. Prove that $k \cdot \binom{n}{k} = n \cdot \binom{n-1}{k-1}$.

19. Prove that $\binom{n}{m}\binom{m}{k} = \binom{n}{k}\binom{n-k}{m-k}$.

20. Use the Binomial Theorem to prove that

$$\Sigma_{k=0}^{n}(-1)^k \cdot \binom{n}{k} = 0.$$