1. **[6 marks]** Show that whenever 25 girls and 25 boys are seated around a circular table there is always a person both of whose neighbors are boys.

   Ans: If three or more boys are sitting together anywhere, then clearly we are done. So, let us assume that the boys are seated in groups of 1 or 2. There are at least 13 such groups (from the pigeonhole principle). The 25 girls have to be seated in 13 slots that interleave the 13 groups of boys, such that at least one girl is seated in each slot. With 25 girls and 13 slots, there must at least be one slot with only one girl. Both the neighbors of this girl are boys.

2. **[3 marks]** Is the following statement true? Justify your answer.

   If $\alpha \rightarrow \beta$ is satisfiable and α is valid, then β is valid.

   Ans: Not true. Let p be an atomic proposition that can take both *true* and *false* values. $(p \vee \neg p) \rightarrow p$ is satisfiable (when p is *true*), and $(p \vee \neg p)$ is valid, but p is not valid.

3. **[8 marks]** The totient function $\varphi : \mathbb{Z}^{\geq 1} \rightarrow \mathbb{Z}^{\geq 0}$, sometimes called Euler's totient function (named after the Swiss mathematician Leonhard Euler), is defined as

   $$\varphi(n) = \mid \{k \ : \ 1 \leq k \leq n, \ k \text{ and } n \text{ have no common divisors}\} \mid$$

   For example, $\varphi(6) = 2$, because 1 and 5 have no common divisors with 6, whereas all the others (2, 3, 4, and 6) have a common divisor.

   Fermat-Euler's theorem states that for any a and n that are relatively prime, $a^{\varphi(n)} \equiv_n 1$.

   (a) **[4 marks]** Assuming Fermat-Euler's theorem, prove Fermat's little theorem. Recall the statement of Fermat's little theorem: let p be a prime, and let $a \in \mathbb{Z}_p$ where $a \neq 0$; then $a^{p-1} \equiv_p 1$.

   Ans: Note that for any prime p, $\varphi(p) = (p-1)$. From Fermat-Euler's theorem, we know that $a^{\varphi(p)} \equiv_p 1$. Thus, $a^{p-1} \equiv_p 1$, which proves Fermat's little theorem.

   (b) **[4 marks]** Assuming Fermat-Euler's theorem, prove that a^{-1} in $\mathbb{Z}_n$ is $a^{\varphi(n)-1} \bmod n$, for any $a \in \mathbb{Z}_n$ that is relatively prime to n.

   Ans: $a \cdot a^{\varphi(n)-1} = a^{\varphi(n)}$ which we know is $\equiv_n 1$ (from Fermat-Euler's theorem). Therefore, a^{-1} is $a^{\varphi(n)-1} \bmod n$.

4. **[6 marks]** Alice wishes to send a 3-bit message `011` to Bob, over a noisy channel that corrupts (flips) each transmitted bit independently as follows: the noisy channel flips `0` to `1` with probability p, and it flips `1` to `0` with probability q. To combat the possibility of her transmitted message differing from the received message, she adds a parity bit to the end of her message (so that the transmitted message is `0110`). Bob checks that he receives a message with an even number of ones, and if so interprets the first three received bits as the message that Alice wanted to send. Conditioned on receiving a message with an even number of ones, what is the probability that the message Bob received is the message that Alice sent?

   Ans: Let `AS` denote the message that Alice sent, and `BR` denote the message that Bob received. We need to compute $Pr[$`AS=BR` $\mid$ `BR` has even number of ones$]$.

   From the definition of conditional probability, we know that

$$Pr[\texttt{AS=BR} \mid \texttt{BR} \text{ has even number of ones}] =$$
$$Pr[\texttt{AS=BR} \text{ and } \texttt{BR} \text{ has even number of ones}] \;/\; Pr[\texttt{BR} \text{ has even number of ones}]$$

There is only one way in which "AS=BR" and "BR has even number of ones" is true – when BR is 0110. The probability of BR being 0110 (i.e., none of the bits being flipped) is $(1-p)^2(1-q)^2$.

What is Pr[BR has even number of ones]?

This happens when there are either 0 flips – only 1 such string possible, with probability $(1-p)^2(1-q)^2$, or when there are 4 flips – only one such string possible, with probability p^2q^2, or when there are 2 flips – 6 different strings possible: 0101 (with probability $(1-p)(1-q)qp$), 0011 (with probability $(1-p)q(1-q)p$), 1111 (with probability $p(1-q)^2p$), 0000 (with probability $(1-p)q^2(1-p)$), 1100 (with probability $p(1-q)q(1-p)$), 1010 (with probability $pq(1-q)(1-p)$).

Thus, Pr[AS=BR — BR has even number of ones] =

$$(1-p)^2(1-q)^2/((1-p)^2(1-q)^2 + p^2q^2 + 4(1-p)(1-q)qp + p^2(1-q)^2 + (1-p)^2q^2)$$

5. **[6 marks]** Suppose the numbers $1, 2, \ldots, 2n$ are written on a whiteboard, where n is an odd integer. Let us say we pick any two of the numbers, i and j, written on the board, write the number $|i-j|$ on the board, and erase i and j. We continue this process until only one integer is written on the board. Prove that this integer must be odd.

   Ans: Let us argue that the sum of all the numbers on the board is odd, always.

   It is true in the beginning: the sum is $(2n)(2n+1)/2$ which is same as $n(2n+1)$ which is odd.

   In each step, the sum (say, s) decreases by $(i+j)$ (because i and j are erased), and increases by $|i-j|$. If $i = j$, then s decreases by an even number ($2i$, or $2j$) and increases by 0. Therefore, it remains odd. If $i > j$, the s becomes $(s - i - j + i - j)$, which is $(s - 2j)$ and thus remains odd. Similarly, when $i < j$, the sum becomes $(s - 2i)$ and continues to remain odd.

   Therefore, the sum will continue to remain odd after each step. In particular, when only one integers remains, the sum, and therefore that integer, must be odd.

6. **[6 marks]** Let us call a logical proposition truth-preserving if the proposition is true under the all-true truth assignment.

   (a) **[4 marks]** Prove the following claim by structural induction on the form of the proposition:

   Any logical proposition that uses only the logical connectives $\vee$ and $\wedge$ is truth-preserving.

   Ans: The base case follows trivially. If the logical proposition is just a propositional variable/atom, then clearly the proposition is *true* when the variable is *true*.
   For the inductive step, the proposition can be made of two simpler propositions on which we assume that the claim holds. But then we can argue that *true* $\wedge$ *true* is *true*, and *true* $\vee$ *true* is also *true*.

   (b) **[2 marks]** Use the claim above to prove that the set $\{\wedge, \vee\}$ is not universal, i.e. there are propositions that cannot be expressed using only $\wedge$ and $\vee$.

   Ans: Clearly, there are propositions that are not truth-preserving. For example, $\neg p$ evaluates to *false* when p is true. But $\neg p$ cannot be expressed using only $\wedge$ and $\vee$ (and p). If it was expressible, then that proposition would be truth-preserving (from the claim above), and therefore cannot evaluate to *false* when p is *true*.