1. **Leaves in a tree**

A *leaf* in a tree is a vertex with degree 1.

(a) Prove that every tree on $n \geq 2$ vertices has at least two leaves.

(b) What is the maximum number of leaves in a tree with $n \geq 3$ vertices?

**Solution:**

(a) We give a direct proof. Consider the longest path \(\{v_0, v_1\}, \{v_1, v_2\}, \ldots, \{v_{k-1}, v_k\}\) between two vertices \(x = v_0\) and \(y = v_k\) in the tree (here the length of a path is how many edges it uses, and if there are multiple longest paths then we just pick one of them). We claim that \(x\) and \(y\) must be leaves. Suppose the contrary that \(x\) is not a leaf, so it has degree at least two. This means \(x\) is adjacent to another vertex \(z\) different from \(v_1\). Observe that \(z\) cannot appear in the path from \(x\) to \(y\) that we are considering, for otherwise there would be a cycle in the tree. Therefore, we can add the edge \(\{z, x\}\) to our path to obtain a longer path in the tree, contradicting our earlier choice of the longest path. Thus, we conclude that \(x\) is a leaf. By the same argument, we conclude \(y\) is also a leaf.

The case when a tree has only two leaves is called the *path graph*, which is the graph on \(V = \{1, 2, \ldots, n\}\) with edges \(E = \{\{1, 2\}, \{2, 3\}, \ldots, \{n-1, n\}\}\).

(b) We claim the maximum number of leaves is \(n - 1\). This is achieved when there is one vertex that is connected to all other vertices (this is called the *star graph*).

We now show that a tree on \(n \geq 3\) vertices cannot have \(n\) leaves. Suppose the contrary that there is a tree on \(n \geq 3\) vertices such that all its \(n\) vertices are leaves. Pick an arbitrary vertex \(x\), and let \(y\) be its unique neighbor. Since \(x\) and \(y\) both have degree 1, the vertices \(x, y\) form a connected component separate from the rest of the tree, contradicting the fact that a tree is connected.

2. **Edge-disjoint paths in hypercube**

Prove that between any two distinct vertices \(x, y\) in the \(n\)-dimensional hypercube graph, there are at least \(n\) edge-disjoint paths from \(x\) to \(y\) (i.e., no two paths share an edge, though they may share vertices).

**Solution:** We use induction on \(n \geq 1\). The base case \(n = 1\) holds because in this case the graph only has two vertices \(V = \{0, 1\}\), and there is 1 path connecting them. Assume the claim holds for the \((n-1)\)-dimensional hypercube. Let \(x = x_1x_2\ldots x_n\) and \(y = y_1y_2\ldots y_n\) be distinct vertices in the \(n\)-dimensional hypercube; we want to show there are at least \(n\) edge-disjoint paths from \(x\) to \(y\). To do that, we consider two cases:

1. **Suppose \(x_i = y_i\) for some index \(i \in \{1, \ldots, n\}\).** Without loss of generality (and for ease of explanation), we may assume \(i = 1\), because the hypercube is symmetric with respect to the indices. Moreover, by interchanging the bits 0 and 1 if necessary, we may also assume \(x_1 = y_1 = 0\). This means \(x\) and \(y\) both lie in the 0-subcube, where recall the 0-subcube (respectively, the 1-subcube) is the \((n-1)\)-dimensional hypercube with vertices labeled 0\(z\) (respectively, 1\(z\)) for \(z \in \{0, 1\}^{n-1}\).

   Applying the inductive hypothesis, we know there are at least \(n - 1\) edge-disjoint paths from \(x\) to \(y\), and moreover, these paths all lie within the 0-subcube. Clearly these \(n - 1\) paths will still be edge-disjoint in the original \(n\)-dimensional hypercube. We have an additional path from \(x\) to \(y\) that goes through the
1-subcube as follows: go from \( x \) to \( x' \), then from \( x' \) to \( y' \) following any path in the 1-subcube, and finally go from \( y' \) back to \( y \). Here \( x' = 1x_2 \ldots x_n \) and \( y = 1y_2 \ldots y_n \) are the corresponding points of \( x \) and \( y \) in the 1-subcube. Since this last path does not use any edges in the 0-subcube, this path is edge-disjoint to the \( n-1 \) paths that we have found. Therefore, we conclude that there are at least \( n \) edge-disjoint paths from \( x \) to \( y \).

2. Suppose \( x_i \neq y_i \) for all \( i \in \{1, \ldots, n\} \). This means \( x \) and \( y \) are two opposite vertices in the hypercube, and without loss of generality, we may assume \( x = 00 \ldots 0 \) and \( y = 11 \ldots 1 \). We explicitly exhibit \( n \) paths \( P_1, \ldots, P_n \) from \( x \) to \( y \), and we claim they are edge-disjoint.

For \( i \in \{1, \ldots, n\} \), the \( i \)-th path \( P_i \) is defined as follows: start from the vertex \( x \) (which is all zeros), flip the \( i \)-th bit to a 1, then keep flipping the bits one by one moving rightward from position \( i+1 \) to \( n \), then from position 1 moving rightward to \( i-1 \). For example, the path \( P_1 \) is given by

\[
000 \ldots 0 \rightarrow 100 \ldots 0 \rightarrow 110 \ldots 0 \rightarrow 111 \ldots 0 \rightarrow \cdots \rightarrow 111 \ldots 1
\]

while the path \( P_2 \) is given by

\[
000 \ldots 0 \rightarrow 010 \ldots 0 \rightarrow 011 \ldots 0 \rightarrow \cdots \rightarrow 011 \ldots 1 \rightarrow 111 \ldots 1
\]

Note that the paths \( P_1, \ldots, P_n \) don’t share vertices other than \( x = 00 \ldots 0 \) and \( y = 11 \ldots 1 \), so in particular they must be edge-disjoint.

3. Baby Fermat

Assume that \( a \) does have a multiplicative inverse \( \pmod{m} \). Let us prove that its multiplicative inverse can be written as \( a^k \pmod{m} \) for some \( k \geq 0 \).

- Consider the sequence \( a, a^2, a^3, \ldots \pmod{m} \). Prove that this sequence has repetitions.
  
  **Solution:** There are only \( m \) possible values \( \pmod{m} \), and so after the \( m \)-th term we should see repetitions.

- Assuming that \( a^i \equiv a^j \pmod{m} \), where \( i > j \), what can you say about \( a^{i-j} \pmod{m} \)?
  
  **Solution:** If we multiply both sides by \( (a^*)^j \), where \( a^* \) is the multiplicative inverse, we get \( a^{i-j} \equiv 1 \pmod{m} \).

- Prove that the multiplicative inverse can be written as \( a^k \pmod{m} \). What is \( k \) in terms of \( i \) and \( j \)?
  
  **Solution:** We can rewrite \( a^{i-j} \equiv 1 \pmod{m} \) as \( a^{i-j-1}a \equiv 1 \pmod{m} \). Therefore \( a^{i-j-1} \) is the multiplicative inverse of \( a \pmod{m} \).