Data Structures and Algorithms
Review of Proofs
September 01, 2015

The *unique factorization theorem* states that every positive number can be uniquely represented as a product of primes. More formally, it can be stated as follows.

> Given any integer $n > 1$, there exist a positive integer k, distinct prime numbers $p_1, p_2, \ldots, p_k$, and positive integers $e_1, e_2, \ldots, e_k$ such that
>
> $$n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_k^{e_k}$$
>
> and any other expression of n as a product of primes is identical to this except, perhaps, for the order in which the factors are written.

Example. Prove that $\sqrt{2}$ is irrational using the unique factorization theorem.

Solution. Assume for the purpose of contradiction that $\sqrt{2}$ is rational. Then there are numbers a and b ($b \neq 0$) such that

$$\sqrt{2} = \frac{a}{b}$$

Squaring both sides of the above equation gives

$$\begin{aligned} 2 &= \frac{a^2}{b^2} \\ a^2 &= 2b^2 \end{aligned}$$

Let $S(m)$ be the sum of the number of times each prime factor occurs in the unique factorization of m. Note that $S(a^2)$ and $S(b^2)$ is even. Why? Because the number of times that each prime factor appears in the prime factorization of a^2 and b^2 is exactly twice the number of times that it appears in the prime factorization of a and b. Then, $S(2b^2)$ must be odd. This is a contradiction as $S(a^2)$ is even and the prime factorization of a positive integer is unique.

Example. Prove or disprove that the sum of two irrational numbers is irrational.

Solution. The above statement is false. Consider the two irrational numbers, $\sqrt{2}$ and $-\sqrt{2}$. Their sum is $0 = 0/1$, a rational number.

Example. Show that there exist irrational numbers x and y such that x^y is rational.

Solution. We know that $\sqrt{2}$ is an irrational number. Consider $\sqrt{2}^{\sqrt{2}}$.

Case I: $\sqrt{2}^{\sqrt{2}}$ is rational.
In this case we are done by setting $x = y = \sqrt{2}$.

Case II: $\sqrt{2}^{\sqrt{2}}$ is irrational.
In this case, let $x = \sqrt{2}^{\sqrt{2}}$ and let $y = \sqrt{2}$. Then, $x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = (\sqrt{2})^2 = 2$, which is an integer and hence rational.

Example. Prove that, for any positive integer n, if $x_1, x_2, \ldots, x_n$ are n distinct real numbers, then no matter how the parenthesis are inserted into their product, the number of multiplications used to compute the product is $n-1$.

Solution. Let $P(n)$ be the property that "If $x_1, x_2, \ldots, x_n$ are n distinct real numbers, then no matter how the parentheses are inserted into their product, the number of multiplications used to compute the product is $n-1$".
Base Case: $P(1)$ is true, since x_1 is computed using 0 multiplications.
Induction Hypothesis: Assume that $P(j)$ is true for all j such that $1 \leq j \leq k$.
Induction Step: We want to prove $P(k+1)$. Consider the product of $k+1$ distinct factors, $x_1, x_2, \ldots, x_{k+1}$. When parentheses are inserted in order to compute the product of factors, some multiplication must be the final one. Consider the two terms, of this final multiplication. Each one is a product of at most k factors. Suppose the first and the second term in the final multiplication contain f_k and s_k factors. Clearly, $1 \leq f_k, s_k \leq k$. Thus, by induction hypothesis, the number of multiplications to obtain the first term of the final multiplication is $f_k - 1$ and the number of multiplications to obtain the second term of the final multiplication is $s_k - 1$. It follows that the number of multiplications to compute the product of $x_1, x_2, \ldots, x_k, x_{k+1}$ is

$$(f_k - 1) + (s_k - 1) + 1 = f_k + s_k - 1 = k + 1 - 1 = k$$

Example. Prove that every graph with n vertices and m edges has at least $n - m$ connected components.

Solution. We will prove this claim by doing induction on m.
Base Case: $m = 0$. A graph with n vertices and no edges has n connected components as each vertex itself is a connected component. Hence the claim is true for $m = 0$.
Induction Hypothesis: Assume that for some $k \geq 0$, every graph with n vertices and k edges has at least $n - k$ connected components.
Induction Step: We want to prove that a graph, G, with n vertices and $k+1$ edges has at least $n-(k+1) = n-k-1$ connected components. Consider a subgraph G' of G obtained by removing any arbitrary edge, say $\{u, v\}$, from G. The graph G' has n vertices and k edges. By induction hypothesis, G' has at least $n - k$ connected components. Now add $\{u, v\}$ to G' to obtain the graph G. We consider the following two cases.

Case I: u and v belong to the same connected component of G'. In this case, adding the edge $\{u, v\}$ to G' is not going to change any connected components of G'. Hence, in this case the number of connected components of G is the same as the number of connected components of G' which is at least $n - k > n - k - 1$.
CaseII: u and v belong to different connected components of G'. In this case, the two connected components containing u and v become one connected component in G. All other connected components in G' remain unchanged. Thus, G has one less connected component than G'. Hence, G has at least $n - k - 1$ connected components.

Example. Prove that every connected graph with n vertices has at least $n - 1$ edges.

Solution. We will prove the contrapositive, i.e., a graph G with $m \leq n - 2$ edges is disconnected. From the result of the previous problem, we know that the number of components of G is at least

$$n - m \geq n - (n - 2) = 2$$

which means that G is disconnected. This proves the claim.

One could also have proved the above claim directly by observing that a connected graph has exactly one connected component. Hence, $1 \geq n - m$. Rearranging the terms gives us $m \geq n - 1$.

Example. Prove that every tree with at least two vertices has at least two leaves and deleting a leaf from an n-vertex tree produces a tree with $n - 1$ vertices.

Solution. A connected graph with at least two vertices has an edge. In an acyclic graph, an endpoint of a maximal non-trivial path (a path that is not contained in a longer path) has no neighbors other than its only neighbor on the path. Hence, the endpoints of such a path are leaves.

Let v be a leaf of a tree T and let $T' = T - v$. A vertex of degree 1 belongs to no path connecting two vertices other than v. Hence, for any two vertices $u, w \in V(T')$, every path from u to w in T is also in T'. Hence T' is connected. Since deleting a vertex cannot create a cycle, T' is also acyclic. Thus, T' is a tree with $n - 1$ vertices.

Example. Prove that if G is a tree on n vertices then G is connected and has $n - 1$ edges.

Solution. We can prove this by induction on n. The property is clearly true for $n = 1$ as G has 0 edges. Assume that any tree with k vertices, for some $k \geq 1$, has $k - 1$ edges. We want to prove that a tree G with $k + 1$ vertices has k edges. Let v be a leaf in G, which we know exists as G is a tree with at least two vertices. Thus $G' = G - \{v\}$ is connected. By induction hypothesis, G' has $k - 1$ edges. Since $deg(v) = 1$, G has k edges.