CSC236H Tutorial 2

Sample Solutions

1. Use induction to prove that $3^{2n} - 1$ is divisible by 8, for all $n \in \mathbb{N}$.

   Solution: Let $P(n)$ denote the assertion that $3^{2n} - 1$ is divisible by 8.

   Base Case: Let $k = 0$.
   Then $3^{2k} - 1 = 3^0 - 1 = 0$. Since 0 is divisible by any natural number, including 8, we can conclude that $P(0)$ is true.

   Induction Step: Let $k \in \mathbb{N}$. Suppose $P(k)$ is true, i.e., $3^{2k} - 1$ is divisible by 8. **[IH]**
   WTP: $P(k+1)$ holds, i.e., $3^{2(k+1)} - 1$ is divisible by 8.

$$\begin{aligned} 3^{2(k+1)} - 1 &= 3^{2k+2} - 1 \\ &= 3^{2k}3^2 - 1 \\ &= (3^{2k} - 1 + 1)3^2 - 1 && \text{\# added and subtracted 1} \\ &= (3^{2k} - 1)3^2 + 3^2 - 1 && \text{\# distributed } 3^2 \text{ over } (3^{2k} - 1 + 1) \end{aligned}$$

   By IH, $3^{2k} - 1$ is divisible by 8, so there must exists $j \in \mathbb{N}$ such that $3^{2k} - 1 = 8j$. Then we have

$$\begin{aligned} 3^{2(k+1)} - 1 &= 8j \times 3^2 + 9 - 1 \\ &= 8(9j + 1) \end{aligned}$$

   Therefore, $3^{2(k+1)} - 1$ is divisible by 8, and so $P(k+1)$ holds.

2. Assume $x \in \mathbb{R}$ and $(x + \frac{1}{x}) \in \mathbb{Z}$. Use induction to prove that for all $n \in \mathbb{N}$

$$(x^n + \frac{1}{x^n}) \in \mathbb{Z}.$$

   Solution: Let $P(n)$ denote the assertion that $x^n + \frac{1}{x^n}$ is an integer.

   Base Case: Let $k = 0$.
   Then $x^n + \frac{1}{x^n} = x^0 + \frac{1}{x^0} = 1 + 1 = 2$. Therefore, $P(0)$ holds.

   Notice that in the problem statement, $P(1)$ is given as an assumption.

   Induction Step: Let $k \in \mathbb{N}$ and $k \geq 2$. Suppose for all $j \in \mathbb{N}$, $0 \leq j < k$, $P(j)$ is true, i.e., $x^j + \frac{1}{x^j}$ is an integer. **[IH]**
   (Note that we need to include the condition $k \geq 2$ in the IH because in the inductive step we go to

$k-2$.)
WTP: $P(k)$ holds, i.e., $x^k + \frac{1}{x^k}$ is an integer.

By IH, we know that $x + \frac{1}{x}$ and $x^{k-1} + \frac{1}{x^{k-1}}$ are both integers. Since integer numbers are closed under multiplication, $(x + \frac{1}{x})(x^{k-1} + \frac{1}{x^{k-1}})$ is also an integer.

$$\begin{aligned}(x + \frac{1}{x})(x^{k-1} + \frac{1}{x^{k-1}}) &= x^k + \frac{1}{x^{k-2}} + x^{k-2} + \frac{1}{x^k} \\ &= (x^{k-2} + \frac{1}{x^{k-2}}) + (x^k + \frac{1}{x^k})\end{aligned}$$

Since $(x + \frac{1}{x})(x^{k-1} + \frac{1}{x^{k-1}})$ is an integer, we have $(x^{k-2} + \frac{1}{x^{k-2}}) + (x^k + \frac{1}{x^k}) \in \mathbb{Z}$.

On the other hand, by IH, we know that $(x^{k-2} + \frac{1}{x^{k-2}}) \in \mathbb{Z}$. Therefore, $(x^k + \frac{1}{x^k})$ must also be an integer.

3. Prove using the Principle of Well Ordering that every positive integer greater than one can be factored as a product of primes.

Solution:

Let $P(n)$ denote the assertion *"n admits a prime factorization"*. Let us assume that not all integers greater than one can be factored as a product of primes, i.e., there exists $n \in \mathbb{N}$ such that $P(n)$ does not hold. Let C be the set of all integers greater than one that cannot be factored as a product of primes. By assumption, S is not empty. By the Principle of Well Ordering S has a smallest element. Let m be this element. m cannot be prime because a prime number by itself is considered the product, of length one, of primes. Since m isn't prime, it must be the product of two integers, a and b, where $1 < a$, $1 < b$. Since both a and b are smaller than m they cannot belong to S and hence they each admit a prime factorization. Let $p_1 P_2 ... p_u$ be the prime factorization of a and $q_1 q_2 ... q_v$ be the prime factorization of b. Therefore $m = p_1 P_2 ... p_u q_1 q_2 ... q_v$ which contradicts the claim that m is in S. Our assumption that S is not empty must therefore be false. It follows that $\forall n \in \mathbb{N}$, $P(n)$ holds.