MAT251 Proof by mathematical induction

Whenever it is desired to prove that an infinite sequence of statements contains only true statements, it is usually appropriate to use the method of mathematical induction. This method is a deductive (direct) method that has only two steps: BASIS and IMPLICATION. Unless both steps can be accomplished, the theorem is not proved.

To show \( P(n) \) (a statement form that depends on variable \( n \)), do:

1. **BASIS**: Establish \( P(m) \) is true for some initial value of \( m \) [This is usually easy.]
2. **IMPLICATION**: Prove \( P(k) \Rightarrow P(k+1) \) for any \( k \geq m \). [This is often not easy.]

Then by induction, we know \( P(n) \) is true for every \( n \geq m \).

**Principle of mathematical induction** The set \( \{ n \in \mathbb{P} : P(n) \text{ is true} \} = \mathbb{P} \) provided

- (B) \( P(1) \) is true and
- (I) \( P(k+1) \) is true whenever \( P(k) \) is true.

*****

**Theorem A** For any natural number \( n \geq 1 \), the value \( (n^3 - n) \) is divisible by 3.

- (B) Clearly \( 1^3 - 1 = 0 \) which is a multiple of 3.
- (I) Consider \( (k+1)^3 - (k+1) = k^3 + 3k^2 + 3k + 1 - k - 1 \) which = \( k^3 - k + 3k^2 + 3k \)

Now if \( k^3 - k \) is divisible by 3, then \( (k+1)^3 - (k+1) = 3q + 3k^2 + 3k = 3r \) for some \( r \); that is, \( (k+1)^3 - (k+1) \) is divisible by 3.

Then by induction we know the theorem is true for all \( n \geq 1 \).

*****

**Theorem B** If a set \( S \) has \( n \) elements, then the power set, \( \mathcal{P}(S) \), has \( 2^n \) elements, where \( n \geq 1 \).

- (B) Clearly a set \( S \) with only one element, \( S = \{a_1\} \), has 2 subsets: \( \emptyset \) and \( S \); that is, \( |\mathcal{P}(S)| = 2^1 \).
- (I) Given any set \( S \) with \( (k+1) \) elements, for some \( k \geq 1 \), we may represent by \( S_k \) the subset containing only the first \( k \) elements. Then \( S \) is the union of \( S_k \) with the subset containing only the last element; that is, \( S = \{a_1, a_2, a_3, ..., a_k\} \cup \{a_{k+1}\} = S_k \cup \{a_{k+1}\} \).

Now if \( |\mathcal{P}(S_k)| = 2^k \), where the element \( a_{k+1} \) is not contained in any of those subsets, then there are \( 2^k \) additional subsets formed by adjoining this element to each of those.

In total, there are \( 2^k + 2^k = 2^k(1+1) = 2^k(2) = 2^{k+1} \) subsets. That is, \( |\mathcal{P}(S)| = 2^{k+1} \).

Then by induction we know the theorem is true for all \( n \geq 1 \).

*****

**Theorem C** The sum of the first \( n \) cubes equals the square of half of \( n(n+1) \).

\[
\sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4}.
\]

- (B) Clearly, \( 1^3 = 1(1+1)^2/4 \).

- (I) Consider \( \sum_{i=1}^{k+1} i^3 = \sum_{i=1}^{k} i^3 + (k+1)^3 \), by definition of sum. Now if \( \sum_{i=1}^{k} i^3 = \frac{k^2(k+1)^2}{4} \), then

\[
\sum_{i=1}^{k+1} i^3 = \frac{k^2(k+1)^2}{4} + (k+1)^2(k+1)^2 = (k+1)^3 \left[ \frac{k^2}{4} + \frac{4(k+1)}{4} \right] = \frac{(k+1)^2(k+2)^2}{4}.
\]

Then by induction we know the theorem is true for all \( n \geq 1 \).

*****

**Theorem D** \( 2^n > 1 + 3n \) for \( n \geq 4 \).

- (B) Clearly \( 2^4 > 1 + 3(4) \) because \( 16 > 13 \).

- (I) If \( 2^k > 1 + 3k \) for some \( k \geq 4 \), then \( 2^{k+1} = 2^k(2) = 2^k + 2^k > 1 + 3k + 1 + 3k > 1 + 3k + 3k = 1 + 3(k+1) \); that is, \( 2^{k+1} > 1 + 3(k+1) \).

Then by induction we know the theorem is true for all \( n \geq 4 \).
1. Explain why \( n^5 - n \) is a multiple of 10 for all \( n \in \mathbb{P} \).
Example 1 showed that \( n^5 - n \) is always a multiple of 5 for \( n \in \mathbb{P} \).
And by cases we can see that \( n^5 - n \) is always a multiple of 2.
[If \( n \) is odd then \( n^5 \) is odd so \( n^5 - n \) is even  If \( n \) is even then \( n^5 \) is even so \( n^5 - n \) is even.]
Hence \( n^5 - n \) is a multiple of 5 and 2; that is, a multiple of 10.

2. Write a loop that corresponds to the proof that \( \sum_{i=1}^{n} i = \frac{n(n + 1)}{2} \) in Example 2 (b).

```plaintext
n := 1
while 1 \leq n do
    if \( \sum_{i=1}^{n} i = \frac{n(n + 1)}{2} \) then
        n := n + 1
```

3. a) Show that “\( n^5 - n + 1 \) is a multiple of 5” is an invariant of the loop in Figure 1.
If \( (n^5 - n + 1) \) is a multiple of 5 for some \( k \in \mathbb{P} \), then \( (k+1)^5 - (k+1) + 1 \)
\( = (k^5 - k + 1) + 5(k^4 + 2k^3 + 2k^2 + k) \), so \( (k+1)^5 - (k+1) + 1 \) is also a multiple of 5.

b) Is \( n^5 - n + 1 \) a multiple of 5 for all \( n \in \mathbb{P} \) with \( n \leq 37 \) or \( n \leq 100 \)?
No, the basis fails. Example 1 shows that \( n^5 - n + 1 \) is always 1 more than a multiple of 5.

4. a) Show that \( n^3 - n \) is a multiple of 6 for all \( n \in \mathbb{P} \).
Clearly, \( n^3 - n \) is a multiple of 2 by the argument in Exercise 1.
Proof by mathematical induction will show that \( p(n) \): “\( n^3 - n \) is a multiple of 3” is true for all \( n \):
(B) We see that \( 1^3 - 1 = 0 = 3 \cdot 0 \), so \( P(1) \) is true.
(I) If \( p(k) \) is true then \( (k+1)^3 - (k+1) = k^3 + 3k^2 + 3k + 1 - k - 1 = (k^3 - k) + 3k^2 + 3k \)
\( = 3(k + 1) + 3(2k + 1) \), which is a multiple of 3. That is, \( p(k) \) implies \( p(k+1) \).
So \( n^3 - n \) is a multiple of 3, and it is a multiple of 2; hence it is a multiple of 6.

b) Use part a) above to prove all numbers of the form \( 8^n - 2^n \) are divisible by 6.
We see that \( 8^n - 2^n = (2^n)^3 - (2^n) \) must be a multiple of 6 because \( 2^n \) is a positive integer.

5. Prove \( p(n): \sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6} \) for \( n \in \mathbb{P} \).
(B) Clearly \( \sum_{i=1}^{1} i^2 = 1^2 = \frac{1 \cdot 2 \cdot 3}{6} = \frac{2(2^2 + 1)}{6} \), so \( p(1) \) is true.
(I) If \( p(k) \) is true then \( \sum_{i=1}^{k+1} i^2 \) can be split into \( \sum_{i=1}^{k} i^2 + (k+1)^2 \),
which by a bit of algebra becomes \( (k+1)^2 + \left(\frac{k(2k+1)}{6}\right)^2 = \frac{(k+1)(2k^2 + 7k + 6)}{6} \)
and a bit more algebra gives \( \frac{(k+1)(2k+1)}{6} = \frac{(k+1)(k+2)(2k+3)}{6} \).
That means \( p(k) \) implies \( p(k+1) \). So \( p(n) \) is true for all \( n \in \mathbb{P} \).
6. Prove $4 + 10 + 16 + \cdots + (6n - 2) = n(3n + 1)$ for all $n \in \mathbb{P}$.

We proceed by induction where $p(n) : \sum_{i=1}^{n} (6i - 2) = n(3n + 1)$ for all $n \in \mathbb{P}$.

(B) Clearly $\sum_{i=1}^{1} (6i - 2) = (6 - 2) = 4 = 1(3 \cdot 1 + 1)$ so $p(1)$ is true.

(I) If $p(k)$ is true then $\sum_{i=1}^{k+1} (6i - 2) = \left( \sum_{i=1}^{k} (6i - 2) \right) + (6(k+1) - 2) = (k(3k + 1)) + (6k + 4)$. 

which by a bit of algebra becomes $3k^2 + 7k + 4 = (k + 1)(3k + 4) = (k + 1)(3(k + 1) + 1)$. This means $p(k)$ implies $p(k+1)$. So $p(n)$ is true for all $n \in \mathbb{P}$. 