Spot the mistake

Claim

A positive integers \( l, m, n \).

\((m | l \land n | l) \Rightarrow m = n\)

Argument

Let \( l, m, n \) be positive integers.

Assume: (1) \( \exists \text{ int } i. \ l = m \cdot i \) and (2) \( \exists \text{ int } i. \ l = n \cdot i \)

From (1) we have (3) \( l = m \cdot i \) for \( i \) an integer that is positive because both \( l \) and \( m \) are. From (2) we have (4) \( l = n \cdot i \). Therefore, from (3) and (4), \( m \cdot i = n \cdot i \); and, as \( i \) is positive, \( m = n \).
The core of the argument gives a proof of

\( \forall \text{positive integers } l, m, n. \)

\( (\exists \text{int } i. \ l = m \cdot i) \land (\forall \text{int } j. \ l = n \cdot j) \)

\( \Rightarrow m = n \)
Disjunction

Disjunctive statements are of the form

\[ P \lor Q \]

or, in other words,

either \( P, Q \), or both hold

or, in symbols,

\[ P \lor Q \]
The main proof strategy for disjunction:

To prove a goal of the form \( P \lor Q \), you may

1. try to prove \( P \) (if you succeed, then you are done); or
2. try to prove \( Q \) (if you succeed, then you are done); otherwise
3. break your proof into cases; proving, in each case, either \( P \) or \( Q \).
Proposition 25  For all integers $n$, either $n^2 \equiv 0 \pmod{4}$ or $n^2 \equiv 1 \pmod{4}$.

**Proof:** Let $n$ be an arbitrary integer.

RTP: $n^2 \equiv 0 \pmod{4}$ or $n^2 \equiv 1 \pmod{4}$

(1) Let's show $n^2 \equiv 0 \pmod{4}$ ×

(2) Let's show $n^2 \equiv 1 \pmod{4}$ ×

Consider the following case (i) $n$ even; (ii) $n$ odd

**Case (i):** Assume $n$ even. Then $n = 2k$ for some int. $k$.

So $n^2 = 4k^2$ and therefore $n^2 \equiv 0 \pmod{4}$.

**Case (ii):** Assume $n$ odd. Then $n = 2k+1$ for an int. $k$.

So $n^2 = (2k+1)^2 = 4k^2 + 4k + 1$ and therefore

$n^2 \equiv 1 \pmod{4}$. 

The use of disjunction:

To use a disjunctive assumption

\[ P_1 \lor P_2 \]

to establish a goal \( Q \), consider the following two cases in turn: (i) assume \( P_1 \) to establish \( Q \), and (ii) assume \( P_2 \) to establish \( Q \).
Scratch work:

Before using the strategy

<table>
<thead>
<tr>
<th>Assumptions</th>
<th>Goal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q</td>
<td></td>
</tr>
<tr>
<td>:</td>
<td></td>
</tr>
<tr>
<td>( P_1 \lor P_2 )</td>
<td></td>
</tr>
</tbody>
</table>

After using the strategy

\[ \begin{array}{c|c|c}
\text{Assumptions} & \text{Goal} & \text{Assumptions} \\
\hline
Q & : & Q \\
: & : & : \\
\text{P}_1 & & \text{P}_2 \\
\end{array} \]
Proof pattern:
In order to prove $Q$ from some assumptions amongst which there is

\[ P_1 \lor P_2 \]

write: We prove the following two cases in turn: (i) that assuming $P_1$, we have $Q$; and (ii) that assuming $P_2$, we have $Q$. Case (i): Assume $P_1$. and provide a proof of $Q$ from it and the other assumptions. Case (ii): Assume $P_2$. and provide a proof of $Q$ from it and the other assumptions.
\( \forall n \in \mathbb{N} \\quad (n \text{ even } \lor n \text{ odd}) \quad \Rightarrow \quad (n^2 \equiv 0 \pmod{4} \lor n^2 \equiv 1 \pmod{4}) \)
A little arithmetic

\[ \binom{p}{m} = \frac{p!}{m! (p-m)!} \]

**Lemma 27** For all positive integers \( p \) and natural numbers \( m \), if \( m = 0 \) or \( m = p \) then \( \binom{p}{m} \equiv 1 \) (mod \( p \)).

**Proof:** Let \( p \) be a positive integer and \( m \) a natural number.

Assume: \( m = 0 \lor m = p \)

\[ \Rightarrow \binom{p}{m} \equiv 1 \pmod{p} \]

Assume \( m = 0 \)

Then \( \binom{p}{m} = 1 \)

Hence we are done

Assume \( m = p \)

Then \( \binom{p}{m} = 1 \)

Hence we are done \( \Box \)
Lemma 28  For all integers $p$ and $m$, if $p$ is prime and $0 < m < p$ then $\binom{p}{m} \equiv 0 \pmod{p}$.

**Proof:**

\[
\binom{p}{m} = \frac{p!}{m!(p-m)!} = p \cdot \left[ \frac{(p-1)!}{m!(p-m)!} \right]
\]

Is it an integer?

\[
m! \cdot (p-m)! \cdot \binom{p}{m} = p \cdot (p-1)!
\]
Proposition 29  For all prime numbers $p$ and integers $0 \leq m \leq p$, either \[ \binom{p}{m} \equiv 0 \pmod{p} \] or \[ \binom{p}{m} \equiv 1 \pmod{p}. \]

**Proof:** Let $p$ be a prime and $m$ an integer such that $0 \leq m \leq p$.

**Case 1:** $m = 0$ or $m = p$

Then we have shown \( \binom{p}{m} \equiv 1 \pmod{p} \) and we are done.

**Case 2:** $0 < m < p$

Then we have shown \( \binom{p}{m} \equiv 0 \pmod{p} \) and we are done.
A little more arithmetic

Corollary 33 (The Freshman’s Dream)  For all natural numbers \( m, n \) and primes \( p \),

\[
(m + n)^p \equiv m^p + n^p \pmod{p}.
\]

Proof: Let \( m \) and \( n \) be natural numbers, and let \( p \) be a prime.

RTP: \((m+n)^p - (m^p + n^p)\) is a multiple of \( p \)

\[
\sum_{i=0}^{p} \binom{p}{i} m^i n^{p-i} - m^p - n^p = \sum_{i=1}^{p-1} \binom{p}{i} m^i n^{p-i}
\]

Since \( \binom{p}{i} \equiv 0 \pmod{p} \) \( \forall 1 \leq i \leq p-1 \). Then

\[
0 \pmod{p}.
\]
Corollary 34 (The Dropout Lemma) \textit{For all natural numbers} \(m\) \textit{and primes} \(p\),

\[(m + 1)^p \equiv m^p + 1 \pmod{p} .\]

Proposition 35 (The Many Dropout Lemma) \textit{For all natural numbers} \(m\) \textit{and} \(i\), \textit{and primes} \(p\),

\[(m + i)^p \equiv m^p + i \pmod{p} .\]

PROOF: 

\[(m + i)^p \quad \text{either} \quad i \geq 0 \quad (m + i)^p \equiv m^p = m^p + i\]

\[
\text{Or,} \quad (m + i)^p = (m + (i - i + 1))^p \quad \\
\quad \equiv (m + i - 1)^p + 1 \pmod{p} \quad \\
i > 1 \quad \equiv (m + i - 2)^p + 2 \pmod{p}
\]
The Many Dropout Lemma (Proposition 35) gives the first part of the following very important theorem as a corollary.

**Theorem 36 (Fermat’s Little Theorem)** For all natural numbers \(i\) and primes \(p\),

1. \(i^p \equiv i \pmod{p}\), and

2. \(i^{p-1} \equiv 1 \pmod{p}\) whenever \(i\) is not a multiple of \(p\).

The fact that the first part of Fermat’s Little Theorem implies the second one will be proved later on.
Btw

1. Fermat’s Little Theorem has applications to:
   (a) primality testing\(^a\),
   (b) the verification of floating-point algorithms, and
   (c) cryptographic security.

\(^a\)For instance, to establish that a positive integer \(m\) is not prime one may proceed to find an integer \(i\) such that \(i^m \not\equiv i \pmod{m}\).