Spot the mistake

Claim

$\forall$ positive integers l, m, n.

$$(m \mid l \wedge n \mid l) \Rightarrow m = n$$

Argument

Let l, m, n be positive integers.

Assume: (1) $\exists$ int i. $l = m \cdot i$ and (2) $\exists$ 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

$\forall$ positive integers l, m, n.

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

$$\Rightarrow m = n$$

Disjunction

Disjunctive statements are of the form

$$\boxed{P \text{ or } Q}$$

or, in other words,

$$\boxed{\text{either } P, Q, \text{ or both hold}}$$

or, in symbols,

$$\boxed{P \vee Q}$$

The main proof strategy for disjunction:

To prove a goal of the form

$$P \vee Q$$

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
$n \equiv 1 \pmod 4$. ☒

Assumptions

$P_1 \vee P_2$ — use?

Goal

Q

The use of disjunction:

To use a disjunctive assumption

$$P_1 \vee P_2$$

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

Assumptions	Goal
	Q
$\vdots$	
$P_1 \vee P_2$	

After using the strategy

Assumptions	Goal	Assumptions	Goal
	Q		Q
$\vdots$		$\vdots$	
P_1		P_2	

Proof pattern:

In order to prove Q from some assumptions amongst which there is

$$P_1 \vee P_2$$

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.

$$\forall\, \text{int. } n$$

$$(n \text{ even} \vee n \text{ odd})$$

$$\Rightarrow$$

$$(n^2 \equiv 0 \pmod 4 \vee n^2 \equiv 1 \pmod 4)$$

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* $\binom{p}{m} \equiv 1 \pmod{p}$.

PROOF: Let p be a positive integer and m a natural number.

Assume: $m = 0 \vee m = p$

RTP: $\binom{p}{m} \equiv 1 \pmod{p}$

Assume $m = 0$

Then $\binom{p}{m} = 1$

Hence we are done

Assume $m = p$

Then $\binom{p}{m} = 1$

Hence we are done ☒

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 ?

$$m!\,(p-m)!\,\binom{p}{m} = p \cdot (p-1)!$$

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 $\binom{p}{i} \equiv 0 \pmod{p}$ $\forall 1 \le i \le p-1$ Then $\sim \equiv 0 \pmod{p}$ ☒

Corollary 34 (The Dropout Lemma) *For all natural numbers* m *and primes* p*,*

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

Proposition 35 (The Many Dropout Lemma) *For all natural numbers* m *and* i*, and primes* p*,*

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

PROOF:

Idea

For ms by induction

$(m+i)^p$ either $i=0$ $(m+i)^p = m^p = m^p + i$

otw. $(m+i)^p = (m+(i-1)+1)^p$

$\equiv (m+i-1)^p + 1 \pmod{p}$

$i > 1$ $\equiv (m+i-2)^p + 2 \pmod{p}$

The Many Dropout Lemma (Proposition 35) gives the fist part of the following very important theorem as a corollary.

Instantiate the many dropout lemma for m=0.

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

1. $i^p \equiv i \pmod{p}$*, and*

"$i^p - i = p \cdot k$ for some int. k"

$(i^{p-1} - 1) \cdot i$

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

$\Downarrow$ $i \cdot (i^{p-2}) \equiv 1 \pmod{p}$

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 $\mathfrak{m}$ is not prime one may proceed to find an integer $\mathfrak{i}$ such that $\mathfrak{i}^{\mathfrak{m}} \not\equiv \mathfrak{i} \pmod{\mathfrak{m}}$.