A proof strategy

To prove

$$\forall x. \exists! y. P(x, y) ,$$

for an arbitrary $x$ construct the unique witness and name it, say as $f(x)$, showing that

$$P(x, f(x))$$

and

$$\forall y. P(x, y) \implies y = f(x)$$

hold.
Disjunctions

- How to *prove* them as goals.
- How to *use* them as assumptions.
Disjunction

Disjunctive statements are of the form

\[ P \text{ or } Q \]

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 integer.

Let's see if (1) holds.

Let's see if (2) holds.

Case $n$ is even; that is, $n = 2i$ for an int $i$.

Then $n^2 = (2i)^2 = 4i^2$ and so we have (1)

Case $n$ is odd; that is, $n = 2i+1$ for an int $i$. 

— 106 —
Then \( n^2 = (2i+1)^2 = 4(i^2 + i) + 1 \) so (2) holds.

\[ a = b \land b = c \Rightarrow a = c \]
\[ a = b \land p = q \Rightarrow a + p = b + q \]
\[ a = b \Rightarrow ac = bc \]

\[
\begin{align*}
4x & \equiv 0 \pmod{4} \\
4(i^2+i) & \equiv 0 \pmod{4} \\
4(i^2+i) + 1 & \equiv 0 + 1 \equiv 1 \pmod{4}
\end{align*}
\]
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

Assumptions          Goal
                     Q
                     \vdots
                     P_1 \lor P_2

After using the strategy

Assumptions | Goal | Assumptions | Goal
                     Q
                     \vdots
                     P_1  | \vdots
                     P_2
**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.
A little arithmetic

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 pos. int.
Let $m$ be a nat. number.

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

Assume: $m=0$

Then $\binom{p}{m} = \binom{p}{0} = 1$
and we are done.

Assume: $m=p$

Goal $\binom{p}{m} = \binom{p}{p} = 1 \pmod{p}$ so we are done.

\[ \binom{p}{m} = C_p^m = \frac{p!}{m! (p-m)!} \]
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: Let $p$ be a prime.
Let $m$ be an int. s.t. $0 < m < p$.

RTP: $\binom{p}{m} = \frac{p!}{m! (p-m)!}$ is a multiple of $p$.

\[
\binom{p}{m} = p \cdot \left[ \frac{(p-1)!}{m! (p-m)!} \right] \text{ and we wish to show that } \left[ \frac{(p-1)!}{m! (p-m)!} \right] \text{ is an integer.}
\]
\( l_p(m) = p \cdot \left[ \frac{(p-1)!}{m! \cdot (p-m)!} \right] \)

**Amendment**

Know \( m! \cdot (p-m)! \) divides \( p \cdot (p-1)! \)

Can it be that \( m! \cdot (p-m)! \) divide \( p \)?

**Note** that \( m < p, \ m - 1 < p, \ldots \)

So every factor of \( m! \) is below \( p \).

Also \( p - m < p, \ p - m - 1 < p, \ldots \)

So every factor of \( (p-m)! \) is below \( p \).
If \( m!(p-m)! = 1 \) then \( \frac{(p-1)!}{m!(p-m)!} \) is an integer.

Otherwise, \( p \) is not a prime factor of \( m!(p-m)! \) and

Therefore, \( m!(p-m)! \nmid p \) and so \( m!(p-m)! \mid (p-1)! \).
Proposition 29 \textit{For all prime numbers }p\textit{ and integers }0 \leq m \leq p, \textit{either }\binom{p}{m} \equiv 0 \pmod{p} \textit{ or }\binom{p}{m} \equiv 1 \pmod{p}.

\textbf{Proof:}

Consider cases:
- \( m = 0 \)
- \( m = p \)
- \( 0 < m < p \)
NB: \[ \exists \text{ predicate} \]
\[ a \equiv b \pmod{m} \quad \text{is either true or false!} \]

\[ \not\exists \]

\[ (5 \mod 2) = 1 \]
\[ \exists \text{ operation} \]

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

Let \(p\) be a prime.

\[
(m+n)^p = \sum_{i=0}^{p} \binom{p}{i} m^i n^{p-i}
\]

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

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

because \[ (p) \equiv 0 \pmod{p} \]

for all \( 0 \leq i < p \)
\[(m+n)^p \equiv m^p + n^p\]

\[(m+1)^p \equiv m^p + 1\]

\[m^p = \underbrace{(1+1+\cdots+1)}_{m \text{ times}}^p \equiv \underbrace{(1+\cdots+1)}_{m-1 \text{ times}}^p + 1\]

\[\equiv \underbrace{(1+\cdots+1)}_{m-2 \text{ times}}^p + 2 \equiv \underbrace{(1+\cdots+1)}_{m-k \text{ times}}^p + k\]

\[m^p \equiv m \quad \text{mod} \ p \quad \text{prime} \quad \text{(when } k = m)\]

Fermat's Little Theorem