DISTJUNCTIONS

• 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:

(1) $n^2 \equiv 0 \pmod{4}$ \times

(2) $n^2 \equiv 1 \pmod{4}$ \times
Proposition 25  For all integers \( n \), either \( n^2 \equiv 0 \) (mod 4) or \( n^2 \equiv 1 \) (mod 4).

PROOF: Let \( n \) be an integer.

CASE 1 \( n \) is even; i.e. \( n = 2i \) for some int \( i \)

Then \( n^2 = 4i^2 \) and hence \( n^2 \equiv 0 \) (mod 4)

CASE 2 \( n \) is odd; i.e. \( n = 2i+1 \) for some int \( i \)

Then \( n^2 = (2i+1)^2 = 4(i^2+i) + 1 \)

and hence \( n^2 \equiv 1 \) (mod 4).
Thus either \( n^2 \equiv 0 \pmod{4} \) or \( n^2 \equiv 1 \pmod{4} \)

as required.
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 \hspace{1cm} Goal
\vdots
P_1 \lor P_2

After using the strategy

Assumptions \hspace{1cm} Goal \hspace{1cm} Assumptions \hspace{1cm} Goal
\vdots
P_1 \hspace{4cm} \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 positive integer and let $m$ be a natural number.

Assume $m = 0$ or $m = p$

RTP: $\binom{p}{m} = \frac{p!}{m!(p-m)!} \equiv 1 \pmod{p}$
Assume \( m = 0 \)

\[
\text{RIP } (\mathbf{0}) \equiv 1 \mod p
\]

\[\vdash\]

1 and we are done.

Assume \( m = p \)

\[
\text{RIP } (\mathbf{p}) \equiv 1 \mod p
\]

\[\vdash\]

1 and 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: Let $p$ be a prime number and let $m$ be a positive integer below $p$.

RTP: \( \binom{p}{m} \equiv 0 \pmod{p} \).

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

So \( \binom{p}{m} \equiv 0 \pmod{p} \iff \frac{(p-1)!}{m! (p-m)!} \) is a not. number.
We know that
\[ p \cdot \frac{(p-1)!}{m! (p-m)!} \] is a natural number.

Hence:
1. \( m! (p-m)! \) divides \( p(p-1)! \)

Since \( p \) is a prime and \( m < p \) and \( p-m < p \).
2. \( m! (p-m)! \) and \( p \) have only 1 as a common factor

From (1) and (2), \( m! (p-m)! \) should divide \( p(p-1)! \).
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 let $m$ be a natural number ranging from 0 to $p$.

**Case 1** $m = 0$. Then $\binom{p}{m} \equiv 1 \pmod{p}$

**Case 2** $m = p$. Then $\binom{p}{m} \equiv 1 \pmod{p}$

**Case 3** $0 < m < p$. Then $\binom{p}{m} \equiv 0 \pmod{p}$

Hence, either $\binom{p}{m} \equiv 0 \pmod{p}$ or $\binom{p}{m} \equiv 1 \pmod{p}$ as required.