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 \( Q \).
For all integers \( n \), either \( n^2 \equiv 0 \pmod{4} \) or \( n^2 \equiv 1 \pmod{4} \).

**Proof:** Let \( n \) be an integer. Every integer is either (1) even or (2) odd. Consider case (1) and (2).

**Case (1):** \( n \) even, i.e., \( n = 2k \) for integer \( k \).

\[
\begin{align*}
    n^2 &= (2k)^2 = 4k^2 \\
    &\equiv 0 \pmod{4}
\end{align*}
\]

**Case (2):** \( n \) odd, i.e., \( n = 2k + 1 \) for integer \( k \).

\[
\begin{align*}
    n^2 &= (2k + 1)^2 = 4k^2 + 4k + 1 \\
     &\equiv 1 \pmod{4}
\end{align*}
\]

Thus, \( n^2 \equiv 0 \pmod{4} \) or \( n^2 \equiv 1 \pmod{4} \).
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>
<th>Assumptions</th>
<th>Goal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q</td>
<td></td>
<td>Q</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P₁ ∨ P₂</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**After using the strategy**

<table>
<thead>
<tr>
<th>Assumptions</th>
<th>Goal</th>
<th>Assumptions</th>
<th>Goal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P₁</td>
<td></td>
<td>P₂</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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.
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 $p, m$ be integers, $p$ positive.

Case (1) $m = 0$ \hspace{3cm} \binom{p}{0} \equiv \frac{p!}{p! \cdot 0!} = 1 \equiv 1 \pmod{p}$

Case (2) $m = p$ \hspace{3cm} \binom{p}{p} = \frac{p!}{(p-p)! \cdot p!} = 1 \equiv 1 \pmod{p}$

$x \equiv x \pmod{p}$
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 $p, m$ be integers, $p$ prime with $0 < m < p$.

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

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

impossible

By Euclid's Lemma, $p \mid \binom{p}{m}$ or $p \mid (p-m)! \cdot m!$.

$\therefore p \mid \binom{p}{m}$. \( \square \)
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: By cases. Case (1) $m = 0$ or $p$. Case (2) $0 < m < p$

\[
\begin{align*}
\text{by Prop 27} & \quad \text{by Prop 28.}
\end{align*}
\]
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 \( m, n \) be not necessarily and \( p \) a prime.

\[
(m + n)^p = \sum_{i=0}^{p} \binom{p}{i} m^i n^{p-i} \quad (\text{Binomial Theorem}).
\]

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

\[
= m^p + n^p + k \cdot p \quad \text{where } k \text{ is an integer}.
\]

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

$$(m + i)^p = (m + 1 + \ldots + 1)^p$$

$$(m + 1 + \ldots + 1)^p \equiv (m + 1 + \ldots + 1)^p + i$$

$$(m + 1 + \ldots + 1)^p \equiv m^p + i.$$
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, 
   (b) the verification of floating-point algorithms, and 
   (c) cryptographic security.

\[ i^m \not\equiv i \pmod{m} \]

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

Negations are statements of the form

\[
\text{not } P
\]

or, in other words,

\[
P \text{ is not the case}
\]

or

\[
P \text{ is absurd}
\]

or

\[
P \text{ leads to contradiction}
\]

or, in symbols,

\[
\neg P
\]