DISJUNCTIONS

- How to PROVE them as goals.

&

- How to USE them as assumptions.

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* $\mathrm{n}^2 \equiv 0 \pmod 4$ *or* $\mathrm{n}^2 \equiv 1 \pmod 4$.

PROOF:

(1) $n^2 \overset{?}{\equiv} 0 \pmod 4$ ✗

(2) $n^2 \overset{?}{\equiv} 1 \pmod 4$ ✗

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.

<u>CASE 1</u> n is even; i.e. $n = 2i$ for some int i

Then $n^2 = 4i^2$ and hence $n^2 \equiv 0 \pmod 4$

<u>CASE 2</u> 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 $n^2 \equiv 1 \pmod 4$.

Thus

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

as required. $\boxtimes$

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

$$P_1 \lor P_2$$

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: $\binom{p}{m} \stackrel{\text{def}}{=} \dfrac{p!}{m!(p-m)!} \equiv 1 \pmod{p}$

Assume $n = 0$

RTP $\binom{p}{0} \equiv 1 \pmod{p}$

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

Assume $n = p$

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

$\binom{p}{p} = 1$ and we are done

$\boxtimes$

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 $\binom{p}{m} \equiv 0 \pmod{p} \iff \dfrac{(p-1)!}{m!\,(p-m)!}$ is a nat. 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 $(p-1)!$ $\boxtimes$

Proposition 29 *For all prime numbers* p *and integers* $0 \le m \le p$, *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.

<u>CASE 1</u> $m = 0$. Then $\binom{p}{m} \equiv 1 \pmod{p}$

<u>CASE 2</u> $m = p$. Then $\binom{p}{m} \equiv 1 \pmod{p}$

<u>CASE 3</u> $0 < m < p$. 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. $\boxtimes$