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

$$P \underset{\text{or}}{\vee} Q$$

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.

Hint n. $n^2 \equiv 0 \pmod 4$ or $n^2 \equiv 1 \pmod 4$)

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. Every int n is either (1) even or (2) odd. Consider case (1) and (2)

Case (1) n even, i.e. $n = 2k$ for integer k.

$$n^2 = (2k)^2 = 4k^2 \quad \therefore n^2 \equiv 0 \pmod 4$$

Case (2) n odd, i.e. $n = 2k+1$ for int. k.

$$n^2 = (2k+1)^2 = 4k^2 + 2k + 2k + 1$$

$$= 4(k^2 + k) + 1$$

$$\therefore n^2 \equiv 1 \pmod 4$$

$\boxtimes$

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	$\Vert$		Q
$\vdots$		$\Vert$	$\vdots$	
P_1		$\Vert$	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.

$\binom{p}{m} = \frac{p!}{(p-m)!\, m!}$ ${}^{p}C_m \quad C^{p}_{m}$

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, m be integers, p +ve.

Case (1) $m=0$ $\quad \binom{p}{0} = \frac{p!}{p!\,0!} = 1 \equiv 1 \pmod p$

Case (2) $m = p$ $\quad \binom{p}{p} = \frac{p!}{(p-p)!\,p!} = 1$

$\equiv 1 \pmod p$

using

$x \equiv x \pmod p$

$\boxed{X}$

Euclid prime p & $p \mid x \cdot y \Rightarrow p \mid x$ or $p \mid y$

Lemma 28 *For all integers* p *and* m, *if* p *is prime and* $0 < m < p$ *then* $\binom{p}{m} \equiv 0 \pmod{p}$.

WRITE THIS OUT PROPERLY!

PROOF: Let p, m be integers, p prime with $0 < m < p$.

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

an integer?

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

$\therefore\ p \mid$ rhs

impossible

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

$\therefore\ p \mid \binom{p}{m}$. ∎

Euclid prime $\Rightarrow p \mid \underbrace{x_1 \cdots x_m}_{\text{int}} \Rightarrow p \mid x_i$ for i, $1 \leq i \leq m$.

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: By cases. Case (1) $m = 0$ or p. Case (2) $0 < m < p$

by Prop 27

by Prop 28.

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, n be nat. nos. and p a prime.

$$(m+n)^p = \sum_{i=0}^{p} \binom{p}{i} m^i n^{(p-i)} \quad \text{(Binomial Thm)}$$

$$= m^p + n^p + \sum_{i=1}^{(p-1)} \binom{p}{i} m^i n^{(p-i)}$$

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

$$\therefore (m+n)^p \equiv m^p + n^p \pmod{p}$$

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:

$$(m+i)^p = (m + \overbrace{1 + \cdots + 1}^{i \text{ times}})^p$$

$$\equiv (m + \underbrace{1 + \cdots + 1}_{i-1})^p + 1$$

$$\vdots$$

$$\equiv m^p + i \, .$$

Via Euclid's thm: For p prime and integers x, y,
$p \mid x \cdot y \Rightarrow p \mid x$ or $p \mid y$.

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

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

Via 'drop out' lemma, so Euclid's thm.

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

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

Via Euclid's thm: By 1., $p \mid i^p - i$, i.e. $p \mid i \cdot (i^{p-1} - 1)$ ...

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 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

$$\boxed{\text{not } P}$$

or, in other words,

$$\boxed{P \text{ is not the case}}$$

or

$$\boxed{P \text{ is absurd}}$$

or

$$\boxed{P \text{ leads to contradiction}}$$

in symbols:
$P \Rightarrow \text{false}$

or, in symbols,

$$\boxed{\neg P}$$