Assumptions

$\vdots$

$P_1 \vee P_2$

$\vdots$

Goal

Q

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.

Assumptions	Goal	Assumptions	Goal
$\vdots$	Q	$\vdots$	Q
P_1		P_2	
$\vdots$		$\vdots$	

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

$$P_1 \vee P_2$$

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.

$\binom{p}{m} = C^p_m = \dfrac{p!}{m!\,(p-m)!}$ for $0 \le m \le p$

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.

<u>RTP</u>: $(m = 0$ or $m = p) \Rightarrow \binom{p}{m} \equiv 1 \pmod{p}$

<u>Assume</u>: $m = 0$ or $m = p$

<u>RTP</u>: $\binom{p}{m} \equiv 1 \pmod{p}$

<u>Assume</u>: $m = 0$

Then $\binom{p}{m} = \binom{p}{0} = 1$

and we are done.

<u>Assume</u>: $m = p$

Then $\binom{p}{m} = \binom{p}{p} = 1$

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 and m be int.

Assume: ① p is prime

and ② $0 < m < p$

RTP: $\binom{p}{m} \equiv 0 \pmod{p}$; That is, $\binom{p}{m}$ is a multiple of p.

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

$$\binom{p}{m} = \frac{p!}{m!\,(p-m)!}$$

$\Rightarrow$

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

So $p \mid \binom{p}{m} \cdot \left[m!\,(p-m)!\right]$

By assumption $0 < m < p$

$m! = m \cdot (m-1) \ldots 2 \cdot 1$

and so $p \nmid m!$

and $p \nmid (p-m)!$

TBP:

$(p \mid a \cdot b \Rightarrow (p \mid a \vee p \mid b))$

$(p \mid a \cdot b \wedge p \nmid a \Rightarrow p \mid b)$

By TBP: $p \mid \binom{p}{m}$.

$\boxtimes$

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 m an integer $0 \leq m \leq p$.

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

Consider the cases:

1. $m = 0$ or $m = p$: Then $\binom{p}{m} = 1 \pmod{p}$
2. other: Then $\binom{p}{m} \equiv 0 \pmod{p}$

$\boxtimes$

Binomial Theorem

$$(m+n)^p = \sum_{k=0}^{p} \binom{p}{k} \cdot m^{p-k} \cdot n^k$$

$$= m^p + n^p + \sum_{k=1}^{p-1} \underbrace{\binom{p}{k}}_{\equiv\, 0 \pmod p} \cdot m^{p-k} \cdot n^k$$

$$\equiv m^p + n^p \pmod p$$

p prime

$$\left.\begin{aligned} a &\equiv a' \\ b &\equiv b' \end{aligned}\right\} \pmod m \Rightarrow \left\{\begin{aligned} a+b &\equiv a'+b' \\ a\cdot b &\equiv a'\cdot b' \end{aligned}\right. \pmod m$$

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:

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: Idea:

$$(m+i)^P = (m+\underbrace{1+1\cdots+1}_{i\text{ times}})^P \equiv (m+\underbrace{1+\cdots+1}_{i-1\text{ times}})^P + 1$$

$$\equiv (m+\underbrace{1+\cdots+1}_{i-2\text{ times}})^P + 1 + 1 \equiv \cdots \equiv (m+1)^P + \underbrace{1+\cdots+1}_{i-1\text{ times}} \equiv m^P + \underbrace{1+\cdots+1}_{i\text{ times}}$$

$$\equiv m^P + i \quad \boxtimes$$

Fermat's Little Theorem

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,

$p \mid (i^{p-1} - 1) \cdot i$ and if $p \nmid i$ $\Rightarrow$ $p \mid (i^{p-1} - 1)$

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 .

If $p \nmid i$

Then $\quad i^{p-1} \equiv 1 \pmod{p}$

$$i \cdot (i^{p-2}) \equiv 1 \pmod{p}$$

the reciprocal of i is a j such that $i \cdot j \equiv 1$

Every natural number i not a multiple of a prime number p has a *reciprocal* modulo p, namely $\mathrm{i}^{\mathrm{p}-2}$, as $\mathrm{i} \cdot (\mathrm{i}^{\mathrm{p}-2}) \equiv 1 \pmod{\mathrm{p}}$.

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

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

or, in symbols,

$$\boxed{\neg P}$$

A first proof strategy for negated goals and assumptions:

If possible, reexpress the negation in an *equivalent* form and use instead this other statement.

Logical equivalences

$$
\begin{array}{rcl}
\neg(\, P \implies Q \,) & \iff & P \wedge \neg Q \\
\neg(\, P \iff Q \,) & \iff & P \iff \neg Q \\
\neg\big(\forall x.\, P(x)\big) & \iff & \exists x.\, \neg P(x) \\
\neg(P \wedge Q) & \iff & (\neg P) \vee (\neg Q) \\
\neg\big(\exists x.\, P(x)\big) & \iff & \forall x.\, \neg P(x) \\
\neg(P \vee Q) & \iff & (\neg P) \wedge (\neg Q) \\
\neg(\neg P) & \iff & P \\
\neg P & \iff & (P \Rightarrow \mathbf{false})
\end{array}
$$

Theorem 37 *For all statements* P *and* Q,

$$(\mathrm{P} \implies \mathrm{Q}) \implies (\neg \mathrm{Q} \implies \neg \mathrm{P}) .$$

PROOF: Let P and Q be statements.

Assume: (2) $P \Rightarrow Q$

RTP: $\neg Q \Rightarrow \neg P$

Assume: (3) $\neg Q \Leftrightarrow (Q \Rightarrow \text{false})$

RTP: $\neg P \Leftrightarrow (P \Rightarrow \text{false})$

Assume (1) P

RTP: false.

By (1) and (2), we have (4) Q. By (4) and (3) we are done $\boxtimes$

Proof by contradiction

Amongst the equivalences for negation, we have postulated the somewhat controversial:

$$\neg\neg P \iff P$$

which is *classically* accepted.

In this light,

to prove P

one may equivalently

prove $\neg P \implies \mathbf{false}$;

that is,

assuming $\neg P$ leads to contradiction .

This technique is known as *proof by contradiction*.

The strategy for proof by contradiction:

To prove a goal P by contradiction is to prove the equivalent statement $\neg P \implies \mathbf{false}$

Proof pattern:

In order to prove

$$P$$

1. Write: We use proof by contradiction. So, suppose P is false.
2. Deduce a logical contradiction.
3. Write: This is a contradiction. Therefore, P must be true.

Scratch work:

Before using the strategy

Assumptions	Goal
	P
$\vdots$	

After using the strategy

Assumptions	Goal
	contradiction
$\vdots$	
$\neg P$	

Theorem 39 *For all statements* P *and* Q*,*

$$(\neg Q \implies \neg P) \implies (P \implies Q) \quad .$$

PROOF: Let P and Q be statements.

Assume: (1) $\neg Q \Rightarrow \neg P$

Assume: (2) P

By contradiction, assume: (3) $\neg Q$

By (3) and (1), we have (4) $\neg P$

(2) and (4) are a contradiction.

$\boxtimes$