Notation: $a \equiv b \pmod{m}$

use instead $a \equiv_m b$

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,

e.g $i^p \equiv_p i$

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[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.

$$(P \Rightarrow Q) \iff \neg P \vee Q$$

$$\neg(P \Rightarrow Q) \iff \neg(\neg P \vee Q)$$

$$\iff \neg\neg P \wedge \neg Q$$

$$\iff P \wedge \neg Q$$

Logical equivalences

$$\neg(P \implies Q) \iff P \wedge \neg Q$$

$$\neg(P \iff Q) \iff P \iff \neg Q$$

$$\neg(\forall x. P(x)) \iff \exists x. \neg P(x)$$

$$\neg(P \wedge Q) \iff (\neg P) \vee (\neg Q)$$

$$\neg(\exists x. P(x)) \iff \forall x. \neg P(x)$$

$$\neg(P \vee Q) \iff (\neg P) \wedge (\neg Q)$$

$$\neg(\neg P) \iff P$$

$$\neg P \iff (P \Rightarrow \textbf{false})$$

$\boxed{?}$ $(\neg Q \Rightarrow \neg P) \Rightarrow (P \Rightarrow Q)$?

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

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

PROOF: Let P and Q be statements.

Assume (1) $P \Rightarrow Q$

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

(2) $(Q \Rightarrow \text{false})$

Further assume $\neg Q$ holds

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

Further assume (3) P

RTP: false.

From (1) and (3) we have Q (4)

From (4) and (2) we have false, as required $\square$

$(P \Rightarrow Q) \Leftrightarrow (\neg Q \Rightarrow \neg P)$

$P \Leftrightarrow \neg\neg P$

$P \vee \neg P$

Classical Logic laws

not intuitionistically valid

Intuitionistic Logic laws

$(P \Rightarrow Q) \Rightarrow (\neg Q \Rightarrow \neg P)$

$P \Rightarrow \neg\neg P$

Proof by contradiction

The strategy for proof by contradiction:

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

Proof by contradiction

The strategy for proof by contradiction:

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

Proof pattern:

In order to prove

$$\mathrm{P}$$

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 38 *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

RTP Q

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

By (1) and (3), we have (4) $\neg P \Leftrightarrow (P \Rightarrow \text{false})$

By (2) and (4), we have false — hence a contradiction $\square$

$\Longleftrightarrow \exists$ po. int k and l. $x = k/l$.

Lemma 40 *A positive real number* x *is rational iff*

$\exists$ *positive integers* m, n :

$$x = m/n \land \neg(\exists \textit{ prime } p : p \mid m \land p \mid n) \qquad (\dagger)$$

PROOF: ($\Leftarrow$) Exercise.

($\Rightarrow$) Assume (1) ($\exists$ po. int k and l. $x = k/l$)

We assume ($\dagger$) is not the case; that is,

$\forall$ po. int m and n. $\neg(x = m/n) \lor (\exists$ prime p. $p \mid m \land p \mid n)$

$\Longleftrightarrow$

(2) $\forall$ po. int m and n. $x = m/n \Longrightarrow \exists$ prime p. $p \mid m \land p \mid n$

By (1), (3) $x = k_0/l_0$ for some po. int. k_0 and l_0.

By (2)

(4) $x = k_0/l_0 \Rightarrow \exists$ prime $p.$ $p | k_0 \wedge p | l_0$

By (3) and (4), (5) $\exists$ prime $p.$ $p | k_0 \wedge p | l_0$

That is, $k_0 = p_0 \cdot k_1$ for some integer k_1

and $l_0 = p_0 \cdot l_1$ for some integer l_1

and some prime p_0.

Note that $x = k_0/l_0 = \frac{p_0 \cdot k_1}{p_0 \cdot l_1} = k_1/l_1$ for int k_1 and l_1

By an analogous argument as above.

and $k_1 = p_1 \cdot k_2$ and $l_1 = p_1 \cdot l_2$ for some pos. int k_2 and l_2 and a prime p_1

In general

and $k_i = p_i \cdot k_{i+1}$ and $l_i = p_i \cdot l_{i+1}$ for some pos. int k_{i+1} and l_{i+1}, and a prime p_i

$$k_0 = p_0 \cdot k_1 = p_0 \cdot p_1 \cdot k_2 = p_0 \cdot p_1 \cdot p_2 \cdot k_3 = \dots$$
$$= p_0 \cdot p_1 \cdot p_2 \cdots p_{k_0} \cdot k' \geq 2^{k_0}$$ $\lightning$ contradiction $\square$