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*,*

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

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

by simplification

The fact that the first part of Fermat's Little Theorem implies the second one will be proved later on .

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

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

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

P	Q	$P \Rightarrow Q$	$\neg P \vee Q$
T	F	F	
T	T	T	
F	T	T	
F	F	T	

W

$\longrightarrow$

false

$$\frac{\text{false}}{P}$$

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

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

PROOF: Let P and Q be statements.

Assume: (1) $P \Rightarrow Q$

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

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

Assume: (3) P

RTP: false

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

From (2) and (4) we have false.

∎

Proof by contradiction

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

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

which is *classically* accepted.

Assumptions

$\vdots$

$\neg P$

Goal

$P \iff \neg\neg P$

$\iff \cancel{(\neg P \Rightarrow \mathit{false})}$

false

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 $\neg P \implies \textbf{false}$;

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,

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

PROOF: Let P and Q be statements.

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

(2) P

RTP: Q equivalently, using proof by contradiction, assume (3) $\neg Q$. So, from (1) and (3) we have (4) $\neg P$. And (2) with (4) give a contradiction.

Therefore, Q holds.

$\boxtimes$

Proof by contrapositive

Corollary 40 *For all statements* P *and* Q*,*

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

Btw Using the above equivalence to prove an implication is known as *proof by contrapositive*.

Corollary 41 *For every positive irrational number* x*, the real number* $\sqrt{x}$ *is irrational.*

Lemma 42 *A positive real number* x *is rational iff*

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

PROOF: Let x be a positive real number.

($\Leftarrow$) Assume ($\dagger$). Let m_0 and n_0 be such that they are pos. int. with $x = m_0/n_0$ and $\neg(\exists$ prime $p.\ p \mid m_0 \wedge p \mid n_0)$.

Then $x = m_0/n_0$ and we are done.

($\Rightarrow$) Assume: $x = a_0/b_0$ for int. a_0 and b_0.

RTP: ($\dagger$)

We proceed by contradiction; that is,

assuming $\neg(\dagger)$ we will derive a contradiction.

$$\neg(\dagger) = \neg\left(\exists \text{ pos. int. } m,n.\ x = m/n \wedge \neg\left(\exists \text{ prime } p.\ p \mid m \wedge p \mid n\right)\right)$$

$$\Leftrightarrow \forall \text{ pos. int. } m,n.\ \neg\left(x = m/n \wedge \neg\left(\exists \text{ prime } p.\ p \mid m \wedge p \mid n\right)\right)$$

$$\Leftrightarrow \forall \text{ pos. int. } m,n.\ \neg\left(x = m/n\right) \vee \neg\neg\left(\exists \text{ prime } p.\ p \mid m \wedge p \mid n\right)$$

$$\Leftrightarrow \forall \text{ pos. int. } m,n.\ \neg\left(x = m/n\right) \vee \left(\exists \text{ prime } p.\ p \mid m \wedge p \mid n\right)$$

$$\Leftrightarrow \underbrace{\forall \text{ pos. int. } m,n.\ x = m/n \Rightarrow \exists \text{ prime } p.\ p \mid m \wedge p \mid n.}_{\text{Assumption.}}$$

$x = a_0/b_0 \quad a_0, b_0$ pos. int.

From the assumptions we have a prime p_0.
$a_0 = p_0 \cdot a_1$ and $b_0 = p_0 \cdot b_1$ for pos. int. a_1, b_1

Note: $x = a_0/b_0 = p_0 \cdot a_1 / p_0 \cdot b_1 = a_1/b_1$ (*)

From (*) and assumption we have a prime p_1.
$a_1 = p_1 \cdot a_2$ and $b_1 = p_1 \cdot b_2$ for pos. int. a_2 and b_2.

Note: $x = a_2/b_2, \dots$

Repeating the argument ℓ times.

$a_0 = p_0 \cdot a_1 = p_0 p_1 \cdot a_2 = p_0 \cdot p_1 p_2 \cdot a_3 = \dots = p_0 \cdot p_1 p_2 \cdots p_\ell \cdot a_{\ell+1}$

Take $\ell = a_0$. Then $a_0 \geq 2^{a_0}$ a contradiction. $\boxtimes$