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.

^aFor 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

or, in other words,

P is not the case

not P

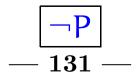
or

P is absurd

or

P leads to contradiction

or, in symbols,



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

PQ P=1Q T F T T F T \sqrt{FT} T

ZPVQ

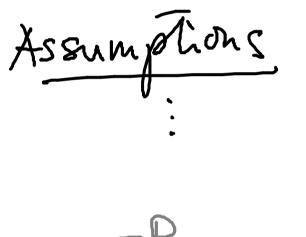
Theorem 37 For all statements P and Q,

Proof by contradiction

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

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

which is *classically* accepted.



Good P(=>72P (=>)(7P=)file)

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 $\neg P \implies false;$

that is,

assuming ¬ P leads to contradiction.

This technique is known as *proof by contradiction*.

The strategy for proof by contradiction:

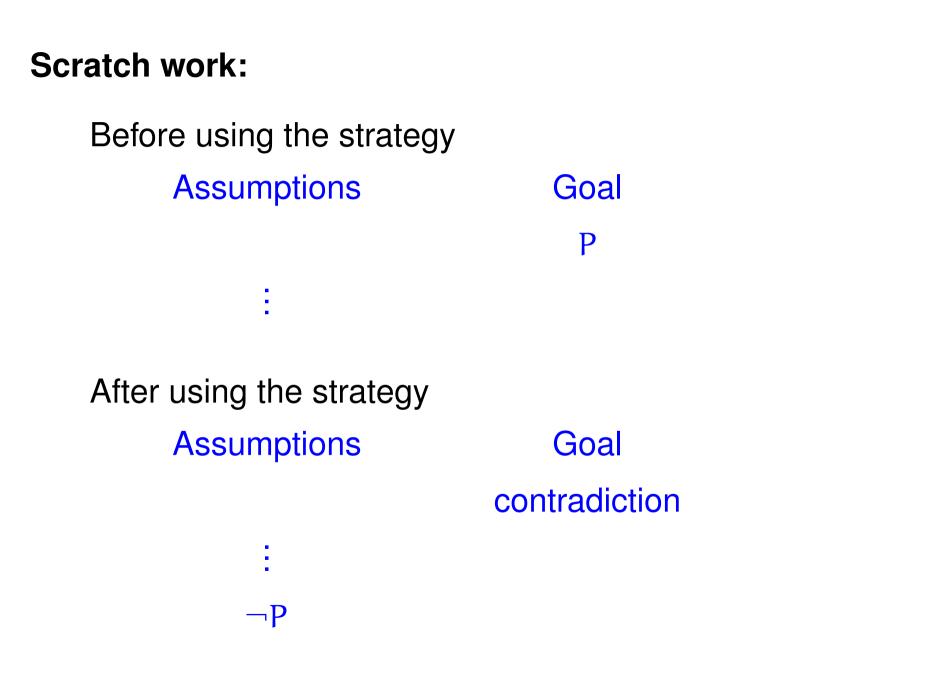
To prove a goal P by contradiction is to prove the equivalent statement $\neg P \implies false$

Proof pattern:

In order to prove

Ρ

- 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.



Theorem 39 For all statements P and Q,

Proof by contrapositive

Corollary 40 For all statements P and Q,

$$(\mathsf{P} \implies \mathsf{Q}) \iff (\neg \mathsf{Q} \implies \neg \mathsf{P})$$

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

Fron The assuptions we have a prime po. ao=po.a1 and bo=po.b. for po. int. a, ibn $Noto: x = a_0/b_0 = \frac{k_0 \cdot k_1}{p_0 \cdot b_1} = a_1/b_1(*)$ Fron (*1 and a semption ne have a prime pr. al=pr.az and by=pr.bz for pro. ut. az ad bz. $Note: x = \frac{a^2}{b^2} - - -$ Repting the orpn wit l times. Qu= po.Q1 = pop1. Q2 = po. p1 p2. Q3 = --- = po. p1 p2-- pe. Qet1 Take $l = q_0$. Then $q_0 \ge 2^{q_0}$ a contradiction.