The use of disjunction:

To use a disjunctive assumption

$$P_1 \lor P_2$$

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		Q
$\vdots$		$\vdots$	
P_1		P_2	

Proof pattern:

In order to prove Q from some assumptions amongst which there is

$$P_1 \lor P_2$$

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.

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:

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:

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:

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:

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*,*

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.

Logical equivalences

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