Unique existence

The notation

$$\exists!\, x.\, P(x)$$

stands for

the *unique existence* of an x for which the property $P(x)$ holds .

That is,

$$\exists x.\, P(x) \;\wedge\; \underbrace{\Big(\forall y.\, \forall z.\, \big(P(y) \wedge P(z)\big) \implies y = z\Big)}_{\text{Uniqueness}}$$

Disjunction

Disjunctive statements are of the form

$$\boxed{P \text{ or } Q}$$

or, in other words,

$$\boxed{\text{either } P,\ Q, \text{ or both hold}}$$

or, in symbols,

$$\boxed{P \vee Q}$$

The main proof strategy for disjunction:

To prove a goal of the form

$$P \vee Q$$

you may

1. try to prove P (if you succeed, then you are done); or
2. try to prove Q (if you succeed, then you are done); otherwise
3. break your proof into cases; proving, in each case, either P or Q.

Proposition 25 *For all integers* n*, either* $n^2 \equiv 0 \pmod 4$ *or* $n^2 \equiv 1 \pmod 4$*.*

PROOF: $\forall \text{int}\, n.\, [n^2 \equiv 0 \pmod 4] \vee [n^2 \equiv 1 \pmod 4]$

Assume arbitrary int. n.

Try to show: $n^2 \equiv 0 \pmod 4$ ✗

Try to show: $n^2 \equiv 1 \pmod 4$ ✗

We consider two cases:

(1) n even and (2) n is odd.

Case (1) $n = 2k$ for some k

$$n^2 = 4k^2 \equiv 0 \pmod 4 \quad \checkmark$$

Case (2) $n = 2l+1$ for some l

$$n^2 = (2l+1)^2 = 4l^2 + 4l + 1$$

$$= 4(l^2+l) + 1 \equiv 1 \pmod 4$$

$\boxtimes$

Assumptions

$\vdots$ $P_1 \vee P_2$

$\vdots$

Goals

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.

Assume	Goal	Assume	Goal
$\vdots$ P_1	Q	$\vdots$ P_2	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

$$P_1 \vee P_2$$

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.

$\binom{p}{m} = \frac{p!}{m!(p-m)!} \in \mathbb{N}$

notations: C^p_m

${}^pC_m$

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: $\forall$ pos. int p. $\forall$ nat. m.

$$(m=0 \vee m=p) \Rightarrow \binom{p}{m} \equiv 1 \pmod{p}$$

Assume p arbitrary pos. int. and m arbitrary natural number.

Assume: $(m=0 \vee m=p)$

RTP: $\binom{p}{m} \equiv 1 \pmod{p}$

We proceed by cases.

(1) Assume $m=0$.

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

(2) Assume $m=p$

Then $\binom{p}{m} = \binom{p}{p} = 1 \equiv 1 \pmod{p}$ $\boxtimes$

<u>NB</u>

$\equiv$ is a predicate and $n \equiv n \pmod{k}$ for all n and k

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: Assume p integer and m integer.

Assume p is prime and $0 < m < p$.

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

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

$\binom{p}{m} = p \cdot k$ and we are done. k ✗

We need show k is an integer!

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

$$m! = m \cdot (m-1) \cdot \cdots 1$$

So

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

need to argue/show that $p \mid \binom{p}{m}$

p prime and $p \nmid m!\,(p-m)! \Rightarrow p \mid \binom{p}{m}$

Euclid's Theorem.

Proposition 29 *For all prime numbers* p *and integers* $0 \le m \le p$, *either* $\binom{p}{m} \equiv 0 \pmod{p}$ *or* $\binom{p}{m} \equiv 1 \pmod{p}$.

PROOF: Let p be a prime and m be an integer between 0 and p.

<u>RTP</u>: $\binom{p}{m} \equiv 0 \pmod{p} \vee \binom{p}{m} \equiv 1 \pmod{p}$

(1) <u>Case $m = 0$</u>: $\binom{p}{m} \equiv 1 \pmod{p}$ by Prop 27

(2) <u>Case $0 < m < p$</u>: $\binom{p}{m} \equiv 0 \pmod{p}$ by Lemma 28

(3) <u>Case $m = p$</u>: $\binom{p}{m} \equiv 1 \pmod{p}$ by Prop 27.

$\boxtimes$

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: Let m, n be nat. Let p prime.

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

$$= m^p + n^p + \sum_{i=1}^{p-1} \binom{p}{i} m^i n^{p-i}$$

$\forall\, i=1,\dots,p-1 \,.\quad \binom{p}{i} \equiv 0 \pmod{p}$

$$\Rightarrow \binom{p}{i} m^i n^{p-i}$$

$$\equiv 0 \cdot m^i \cdot n^{p-i}$$

$$\equiv 0 \pmod{p}$$

$$\Rightarrow \sum_{i=1}^{p-1} \binom{p}{i} m^i n^{p-i} \equiv 0 \pmod{p}$$

<u>Lemma</u>

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

$\boxtimes$

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:

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

$$= ((m+1+1\cdots+1)+1)^p$$

$$(m+\overbrace{1+\cdots+1}^{i})^p$$

$$\equiv (m+\underbrace{1+\cdots+1}_{i-1})^p+1$$

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

$$\vdots$$

$$\equiv (m+\underbrace{1+\cdots+1}_{i-(i-1)})^p+\underbrace{1+\cdots+1}_{i-1}$$

$$\equiv m^p+\overbrace{1+\cdots+1}^{i} = m^p+i$$

$\boxtimes$

Formally one proceeds by induction!

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. $\boxed{i^p \equiv i \pmod{p}}$*, 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 $i^m \not\equiv i \pmod{m}$.