A proof strategy

To prove

$$\forall x. \exists! y. P(x, y) \quad ,$$

for an arbitrary x construct the unique witness and name it, say as $f(x)$, showing that

$$P\big(x, f(x)\big)$$

and

$$\forall y. P(x, y) \implies y = f(x)$$

hold.

Disjunctions

- How to *prove* them as goals.
- How to *use* them as assumptions.

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: $\forall$ int n. $\left(n^2 \equiv 0 \pmod 4 \vee n^2 \equiv 1 \pmod 4\right)$

Let n be an integer.

RTP: ① $n^2 \equiv 0 \pmod 4$ $\vee$ ② $n^2 \equiv 1 \pmod 4$

Let's see if ① holds. ✗ ~ because $1 \not\equiv 0$

Let's see if ② holds. ✗

Case n is even; That is, $n = 2i$ for an int i.

Then $n^2 = (2i)^2 = 4(i^2)$ and so we have ①

Case n is odd; That is, $n = 2i+1$ for an int. i.

Then $n^2 = (2i+1)^2 = 4(i^2+i)+1$ so ② holds. $\boxtimes$

$a \equiv b \wedge b \equiv c \Rightarrow a \equiv c$

$a \equiv b \wedge p \equiv q \Rightarrow a+p \equiv b+q$

$a \equiv b \Rightarrow ac \equiv bc$

$4x \equiv 0 \pmod 4$

$4(i^2+i) \equiv 0 \pmod 4$

$4(i^2+i)+1 \equiv 0+1 = 1 \pmod 4$

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

$$P_1 \vee P_2$$

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.

A little arithmetic

Lemma 27 *For all positive integers* p *and natural numbers* m*, if* $\mathrm{m} = 0$ *or* $\mathrm{m} = \mathrm{p}$ *then* $\binom{\mathrm{p}}{\mathrm{m}} \equiv 1 \pmod{\mathrm{p}}$.

$$\binom{p}{m} = C^p_m = \frac{p!}{m!\,(p-m)!}$$

PROOF: Let p be a pos. int.
Let m be a nat. number.

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

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

Assume: $m=0$

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

and we are done.

Assume: $m=p$

$\binom{p}{m} = \binom{p}{p} = 1$ so we are done

$\boxtimes$

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: Let p be a prime.
Let m be an int. s.t. $0 < m < p$.

<u>RTP</u>: $\binom{p}{m} = \dfrac{p!}{m!\,(p-m)!}$ is a multiple of p.

$\binom{p}{m} = p \cdot \underbrace{\left[\dfrac{(p-1)!}{m!\,(p-m)!}\right]}$ and we wish to show that $\uparrow$ is an integer.

AMENDMENT

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

Know $m!\,(p-m)!$ divides $p \cdot (p-1)!$

Can it be that $m!\,(p-m)!$ divides p ?

Note that $m < p$, $m-1 < p$, ...

So every factor of $m!$ is below p.

Also $p-m < p$, $p-m-1 < p$, ...

So every factor of $(p-m)!$ is below p.

AMENDMENT

If $m!(p-m)! = 1$ Then $\dfrac{(p-1)!}{m!(p-m)!}$ is an integer.

Otherwise, p is not a prime factor of $m!(p-m)!$ and

Therefore, $m!(p-m)! \nmid p$ and so $m!(p-m)! \mid (p-1)!$ $\boxtimes$

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:

Consider cases:

- $m = 0$
- $m = p$
- $0 < m < p$

NB:

$$a \overbrace{\equiv}^{\text{predicate}} b \pmod{m} \rightsquigarrow \text{either true or false!}$$

$$\neq$$

$$(5 \underbrace{\bmod}_{\text{operation}} 2) = 1 \quad \times$$

$$(m+n)^p \overset{?}{\equiv} m^p + n^p \pmod{p}$$

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 and n be nat. numbers.
Let p be a prime.

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

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

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

$$\equiv \sum_{i=1}^{p-1} 0 \cdot m^i \cdot n^{p-i}$$, because $\binom{p}{i} \equiv 0 \pmod{p}$ for all $0 < i < p$

$$= 0$$

$\boxtimes$

AMENDMENT

p prime

work mod p

$$(m+n)^p \equiv m^p + n^p$$

$$(m+1)^p \equiv m^p + 1$$

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

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

$$\boxed{m^p \equiv m} \sim (\text{when } k = m)$$

mod p ~ prime

Fermat's Little Thm