More proofs :

Ex: Let a, b, c be integers. If $a|b$ & $b|c$ then $a|c$.

Pf: If $a|b$ then $b = p \cdot a$ If $b|c$ then $c = q \cdot b$

thus $c = q \cdot b = q \cdot p \cdot a = m \cdot a$ integers p, q, m.

Thus $a|c$.

Ex: prove if $m+n$ & $n+p$ are even integers where m, n, p are integers then $m+p$ is even.

pf: $m+n = 2k$ some k, $n+p = 2l$ some integer l.

$m = 2k - n$ $\qquad$ $p = 2l - n$

$m+p = 2k - n + 2l - n = 2k + 2l - 2n$

$= 2(k + l - n)$

$\square$

Ex: prove that if n is a perfect square then $n+2$ is not a perfect square.

pf: n a perfect square $\Rightarrow$ $n = k^2$ $\quad$ $n+2 = k^2 + 2$

well we might know that no perfect squares are 2 apart.

but this isn't a rigorous proof. Ideas ?

lets try contradiction:

Suppose n & $n+2$ are both perfect squares.

Then $n = k^2$ & $n+2 = p^2 \Rightarrow 2 = (n+2) - n = p^2 - k^2$

$= (p-k)(p+k) \Rightarrow$ either $p-k = 1, 2$ or $p+k = 1, 2$

AWLOG $p, k \geq 0$ So $p - k = 1$ & $p+k = 2$

$p = 1+k$

$1 + k + k = 2 \Rightarrow k = \frac{1}{2} \Rightarrow n = \frac{1}{4}$ $\rightarrow\leftarrow$ n an integer.

$\square$

Ex: prove that if n is a positive integer n is odd iff $5n+6$ is odd.

pf ($\Rightarrow$) If n is odd then $n = 2k+1$ for some integer k

So $5n+6 = 5(2k+1) + 6 = 10k + 11 = 2(5k+5) + 1$

So $5n+6$ is odd.

($\Leftarrow$) $5n+6$ is odd $\Rightarrow 5n+6 = 2k+1$ Some integer k.

$5n + 5 = 2k$ need to get $n = 2\sim +1$

lets try contrapositive! If n is even then $5n+6$ is even.

n even $\Rightarrow n = 2k$ some k. then $5n+6 = 10k+6$

$= 2(5n+3)$ so $5n+6$ is even.

$\square$

Proofs of equivalence : The last example is a proof of equivalence, It demonstrates the two statements are logically equivalent, To prove these we must show they imply each other. Sometimes there are multiple claims. Then we only need a sequence . i.e. If we have claims a, b, c.

and we show $a \Rightarrow b \Rightarrow c \Rightarrow a$ then we have $a \to b$ & $b \to a$ (via $b \to c \to a$) similarly for the rest.

$\boxed{\text{Examples on this at end of this lecture}}$

Existential proofs : Some propositions are of the form $\exists x\, P(x)$.

To show they hold we must exhibit such an x.

Ex : Let a, b be real numbers with $a < b$. prove there exists a real number x with $a < x < b$.

Does this seem true? why? $a = 0$, $b = 2$,

$a = 0.1$, $b = 0.11$ etc.

pf: chose $x = \frac{a+b}{2}$ this is the halfway point between a & b.

$\frac{a+b}{2} < b$ since $a < b \Rightarrow a+b < 2b \Rightarrow \frac{a+b}{2} < b$

Similarly $a < b \Rightarrow 2a < a+b \Rightarrow a < \frac{a+b}{2}$

So $a < \frac{a+b}{2} < b$

$\square$

Ex: Prove there exists a prime p such that $2^p - 1$ is composite

Pf: $p = 11$ $\quad 2^{11} - 1 = 2048 - 1 = 2047 = 23 \cdot 89$.

However sometimes existential proof are weird — non-constructive.

Ex: Let $A = \dfrac{s_1 + s_2 + \cdots + s_n}{n}$ be the arithmetic mean of the real numbers $s_1, s_2, \ldots, s_n$. Prove there is some i s.t. $s_i \geq A$.

Pf: How can we do this with no knowledge of s_i, A? Sounds like contradiction time! Our conclusion is $\exists i \, (s_i \geq A)$

So $\neg \exists i \, (s_i \geq A) \equiv \forall i \, (s_i < A)$ $\quad$ So Assume $A = \dfrac{s_1 + \cdots + s_n}{n}$

but all $s_i < A$ then $s_1 + s_2 + \cdots + s_n < A + A + \cdots + A$

$= nA \Rightarrow \dfrac{s_1 + \cdots + s_n}{n} < A$ $\quad \rightarrow\leftarrow$ to definition of A.

Thus there must be some i s.t. $s_i \geq A$. $\square$

digression on ZKP?.

This prove indirectly something must exist, but does not tell us what it is.

Counter examples: Some claims are just not true. Those are dealt with by counter examples.

Ex: For all positive integers n, $2^n + 1$ is prime

pf This is false $n = 3$ gives $2^3 + 1 = 9$

$\square$

Ex: Prove or disprove: The product of 2 irrational numbers is irrational.

Thoughts from class?

Pf: Not true: $\pi \cdot \frac{1}{\pi} = 1$.

Ex: Find a counterexample to the statement: Every positive integer can be written as the sum of squares of 3 integers.

Pf: 7 can't. Only squares below 7 are 1, 4. But $7 = 4+1+1+1$ need 4 squares.

$\square$.

Equiv examples!

Ex: Show the following are equivalent: (i) a is less than b

(ii) the average of a & b is greater than a

(iii) " " " " " is less than b.

Pf (i) $\Rightarrow$ (ii) $a<b \Rightarrow 2a < a+b \Rightarrow a < \frac{a+b}{2}$

(ii) $\Rightarrow$ (iii) $a < \frac{a+b}{2} \Rightarrow 2a < a+b$ how to get $\frac{a+b}{2} < b$?

X

(ii) $\Rightarrow$ (i) $a < \frac{a+b}{2} \Rightarrow 2a < a+b \Rightarrow a < b$

(i) $\Rightarrow$ (iii) $a<b \Rightarrow a+b < 2b \Rightarrow \frac{a+b}{2} < b$

(iii) $\Rightarrow$ (i) $\frac{a+b}{2} < b \Rightarrow a+b < 2b \Rightarrow a < b$

Thus (i) $\Leftrightarrow$ (ii) & (i) $\Leftrightarrow$ (iii) $\square$.