Good proofs are:

1. correct
2. complete
3. clear
4. brief
5. "elegant"
6. well-organized
7. in order

Fermat's Last Thm:

$$\forall n > 2, \neg\exists x, y, z \in \mathbb{N}^+$$
$$x^n + y^n = z^n$$

Problem:

Find a sequence of moves to go from

A	B	C
D	E	F
H	G	

to

A	B	C
D	E	F
G	H	

Legal Move: Slide a letter into a adjacent blank square.

Thm: There is no sequence of legal moves to invert G&H and return all other letters to their original position.

Natural Order

1	2	3
4	5	6
7	8	9

Row moves

Ex:

A	B	C
D	G	
E	F	H

$\Longrightarrow$

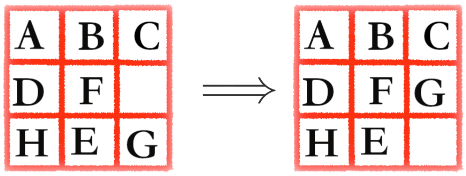
A	B	C
D		G
E	F	H

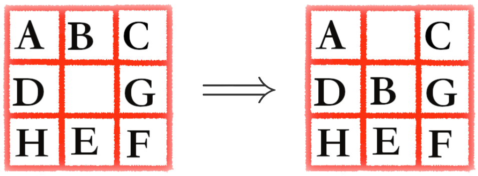
Lemma 1:

A row move does not change the order of the items.

Proof: ~~Obvious~~. In a row move, we move an item from cell i into an adjacent cell i-1 or i+1. Nothing else moves. Hence the order of items is preserved.□

Column moves

Ex: 

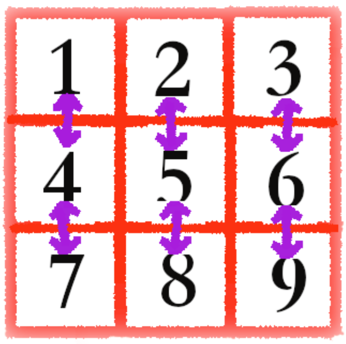
Ex: 

Lemma2:

A column move changes the relative order of precisely 2 paris of items.

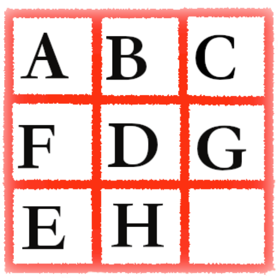
Proof: In a column move, we move an item in cell i to a blank spot in cell i-3 or i+3 . When an item moves 3 positions, it changes order with 2 items(i-1,i-2 or i+1,i+2).☐

Order Changes in Column moves:



Def:

A pair of letter L1&L2 form an **inversion**, also known as an inverted pair, if L1 precedes L2 in alphabet, but L1 appears after L2 in the puzzle.



(D,F),(E,F),(E,G) ——3 inverions in the left puzzle.

Lemma 3:

During a move, the number of inversions can only increases by 2, decrease by 2 or stay same.

Pf: Row move :No changes (by Lemma 1)

Column move: 2 pairs change order (by Lemma 2)——Note: In a column move, two pairs reverse their order. If they were in order, they become inverted. If they were inverted, they become in order.

A: both pairs were in order originally before the column move. $\Longrightarrow$ number of inversions ↑ 2

B: both pairs were inverted originally before the column move. $\implies$ number of inversions $\downarrow$ 2

C: one of the pairs inverted while one of the pairs which is not inverted $\implies$ stays the same. $\square$

Corollary 1: During a move, the parity (evenness/oddness) of the number of inversions does not change.

Pf: Adding or subtracting 2 does not change the parity. $\square$

Lemma 4:

In every state reachable from $\begin{array}{|c|c|c|}\hline A & B & C \\ \hline D & E & F \\ \hline H & G & \\ \hline\end{array}$,the parity of the number of inversions is odd.

Pf: by induction.(Note: Invariant proofs are always by induction.)

Inductive hypothesis: P(n): After any sequence of n moves from $\begin{array}{|c|c|c|}\hline A & B & C \\ \hline D & E & F \\ \hline H & G & \\ \hline\end{array}$,the parity of the number of inversions is odd.

Base Case: n=0, the number of inversions in the start state is 1. $\implies$ parity is odd. And the hypothesis is satisfied.

Inductive Step: For $n \geq 0$, show $P(n) \implies P(n+1)$

Consider any sequence of n+1 moves,m_1,...,m_{n+1}

By **I.H.**(P(n)) we know that parity after m_1,...m_n is odd.

By **Corollary** 1, we know parity of the number of inversions does not change during m_{n+1}. $\implies$ the parity after m_1,m_2,...,m_n,m_{n+1} is odd. $\implies$ P(n+1). $\square$

Pf of Thm: The parity of the number of inversions in desired state is even(0). By Lemma 4, the desired state cannot be reached from $\begin{array}{|c|c|c|}\hline A & B & C \\ \hline D & E & F \\ \hline H & G & \\ \hline\end{array}$ $\square$

Strong Induction Axiom

Let P(n) be any predicate. If P(0) is true & $\forall n, (P(0) \land P(1) \land P(2) ... \land P(n)) \implies P(n+1)$ is true, then $\forall n$, P(n) is true.

Unstacking Game

Thm: All strategies for the n-block game produce the same score $S(n) = \frac{n(n-1)}{2}$.

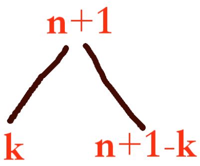
Ex: S(8) = 28

Pf: By strong indcution.

I.H. P(n)

BaseCase: n = 1, S(1) = 0;

Inductive Step: Assume P(1), P(2), ... ,P(n) to prove P(n+1).

Look at n+1 blocks 

,$1 \leq k \leq n$.

$$
\begin{aligned}
S(n+1) &= k(n+1-k) + P(k) + P(n+1-k) \\
&= k(n+1-k) + \frac{k(k-1)}{2} + \frac{(n+1-k)(n+1-k-1)}{2} \\
&= \frac{2k(n+1-k) + k(k-1) + (n+1-k)(n-k)}{2} \\
&= \frac{(n+1-k)(n+k) + k^2 - k}{2} \\
&= \frac{n^2 + nk + n + k - nk - k^2 + k^2 - k}{2} \\
&= \frac{n^2 + n}{2} \\
&= \frac{(n+1)(n+1-1)}{2} \square
\end{aligned}
$$