# Author: Keith Stellyes

## A few proofs regarding algorithms

## A proof on bubble sort

A sorted set is defined as follows (Where $S_0$ is the initial element):

$$S_k \leq S_{k+1} \vee$$
$$S_k = |S| - 1$$

```
procedure bubbleSort(S : Ordered set)
    swapped ← true
    while swapped
        swapped ← false
        for n → |S| - 2
            if S_n > S_{n+1}
                Swap(S_n, S_{n+1})
                swapped ← true
```

# A proof to solve a problem from Knuth regarding Euclidean Algorithm

2. [15] Prove that $m$ is always greater than $n$ at the beginning of step **E1**, after it has already occurred once. Where E1 is part of the algorithm, **E**:

**Algorithm E:**

**E1**: Divide $m$ by $n$ and let $r$ be the remainder.
**E2**: If $r = 0$: return n
**E3**: $m \leftarrow n, n \leftarrow r$ goto **E1**

Proof:

Prove that $m_k > n_k$ where $k > 0$

Let:

$m_k = n_{k-1}$
$n_k = m_{k-1} \bmod n_{k-1}$
$n_k \neq 0$
$k = 0$ at the first time at **E1**
$k > 0$

$m_k > n_k \rightarrow$
$n_{k-1} > m_{k-1} \bmod n_{k-1}$

**Case I** $m_{k-1} = n_{k-1}$:

Impossible:
$m_{k-1} = n_{k-1} \rightarrow m_{k-1} \bmod n_{k-1} = 0$
$n_k = m_{k-1} \bmod n_{k-1} = 0 \rightarrow$
$n_k = 0 \land n_k \neq 0$ Contradiction

**Case II** $m_{k-1} > n_{k-1}$:

1. $m_{k-1} > n_{k-1} \rightarrow$
2. $n_{k-1} > m_{k-1} \bmod n_{k-1}$
3. $m_k > n_k$

**Case III** $m_{k-1} < n_{k-1}$:

1. $m_{k-1} < n_{k-1} \rightarrow$
2. $m_{k-1} \bmod n_{k-1} = m_{k-1} \rightarrow$
3. $m_k = n_{k-1} > m_{k-1} \land$ Definition of case
4. $n_k = m_{k-1}$ 2
5. $m_k > n_k$