- In last week's lectures we considered logically what happens when loops are executed.

- We identified the invariants for some loops

- We applied the while rule to show that loops are correct.

- The while rule involved showing that if the invariant and the loop condition held before execution of the loop then the invariant should also hold after execution of the body of the loop if the loop is correct.

- There is another slightly different way of reasoning about loops.

- A loop could be executed $0, 1, 2, \ldots$ times i.e. the number of times executed is a natural number.

- Proving that a loop is correct can be seen a proof over some subset of the natural numbers

- Lets look at some properties of the natural numbers

- The Peano Axioms give a recursive definition of the Natural Numbers (These are the principles describing the set of Natural Numbers)

  1. $0 \in Nat$

  2. If $x \in Nat$, then $Sx \in Nat$. Sx is the notation used to represent $x + 1$.

  3. If $x \in Nat$, then $0 \neq Sx$ for any x. i.e. 0 is not the successor of any number.

  4. If $x, y \in Nat$ and $Sx = Sy$ then $x = y$. If the successor of x and y is the same number, then x and y are the same number.

  5. If $A \subseteq Nat$ and if $0 \in A$ and if whenever $x \in A$, $Sx \in A$ then $A = Nat$. Using the successor function is the only way to generate natural numbers.

- Even though the Natural Numbers form an infinite set, properties of this set can be proved..How?...mathematical induction

- To prove that a property is true for all the natural numbers

  1. Show the property is true for 0

  2. Show that whenever the property is true for x then it is also true for the successor of x.

- Consider some proofs by induction...

- Functions can be defined over the Natural Numbers (an infinite set) How?

- The following definitions are recursive(inductive) definitions

- $Add(x, 0) = x$
  $Add(x, Sy) = S(Add(x, y))$

- Addition can also be defined in terms of the binary infix operator $+$
  $x + 0 = x$
  $x + Sy = S(x + y)$

- $x + 1 = x + (S0) = S(x + 0) = S(x) = Sx$

- Multiplication as repeated addition

- $x * 0 = 0$
  $x * (y + 1) = x * y + x$

- Factorial: $fac(n) = 1*2*...*(n-1)*n$
  $fac(0) = 1$
  $fac(n + 1) = (n + 1) * fac(n)$

- Exponentation: raising a number to a power.

- $3^2 = 3 * 3 = 9$ $2^3 = 2 * 2 * 2 = 8$

- $a^0 = 1$
  $a^{n+1} = a^n * a$

- All these functions are defined inductively

- Prove the Law of exponents by induction i.e.$a^{m+n} = a^m * a^n$

- Prove $(a^m)^n = a^{m*n}$