CS271 WK7 NOTES

RETURN Function
- Syntax:
  - → RET (Pop → EIP)
  - → Ret n pops return addr and n add. bytes.

Stack Frame
- AKA activation record
- Calling program pushes args onto stack
- Called PROC pushes old ebp, then sets ebp = esp, creating a stack frame.

New Addressing Modes
- immediate, Direct, Register all known
- now we use register indirect
  - ↳ access through an addr in a reg
- also Indexed addressing: using "distance" in a register.
- or Base-indexed: using start address in one register, offset in another and add to access memory.

Register Indirect Addressing
- [reg] = contents of memory at address reg
- Basically working with ptrs, as reg ≃ pointer to mem.
- can manipulate as in [reg + 12] where the address at reg would be reg + literal 12

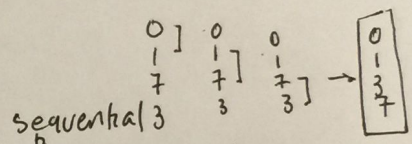
target > MP: first = MP + 1
target < MP: last = MP - 1

Arrays
- to access nth element, Add (n × data_size) to the offset of the first element.
- reading OOB results in jibberish
- Indexed Addressing can be used:

using list of DWORD

```
mov edi, 0
mov list[edi], eax // element 0
mov edi, 4
mov list[edi], eax // element 1!
```

Sort Types
- Bubble Sort
  - → $O(n^2)$ (inefficient)
  - → Compare values 2 by 2 ...



sequential

~~Binary~~ search
- Looking through an array to find a value.
- takes avg n/2 tries to find value in n-long list
- effective under 1000=n

Binary Search
- requires ARR is sorted
- Array (first, last) = range and target = target value.

1. range is (first, last). If first > last no match.
2. calculate Mid point of first, last
3. compare target to Mid part
   target = MP: found