1 x86 processor operations and features

1.1 Modes of operation

- **Protected mode** → This is the native(*default*) processor state. The idea is that multiple processes can run but they are each given their own section of memory meaning that means that they can't interact with processes directly. This allows us to stop from illegal operations that could possibly cause a process to fail.
- **Real address mode** → The idea is that it allows us to directly access hardware components. It's useful if we are going to be working at a hardware level and interacting with hardware devices as it allows us to more easily access those devices.
- **System management mode** → Provides an operating system with mechanisms for power management and security. Main use of this mode is if we are designing a system very specific to a chip. It helps us to build something very specific to the processor.

2 Register fundamentals

- x86 is a 32-bit processor which means that each register is 32 bits in size.
- Example registers: EAX, EBX, ECX, EDX
  - You can access just 16 bits by dropping the E i.e by giving AX, BX, CX, DX.
  - You can access 8-bit high registers using: AH, BH, CH, DH.
  - You can access 8-bit low registers using: AL, BL, CL, DL.
- Here are some registers(note that these are just conventions associated with each registers, in general all these registers can be used):
  - eax → Extended accumulator, automatically used by multiplication and division instructions.
  - ebx → General purpose.
  - ecx → Used as loop counter by the CPU.
  - edx → General purpose.
  - esi → High speed memory transfer.
  - edi → High speed memory transfer.
  - ebp → Used to reference function parameters and local variables on the stack(very important).
  - esp → A pointer to the current stack address(very important).

3 Special purpose registers

- EIP → The instruction pointer. It points to the address of the next instruction.
- EFLAGS → Flags to denote the status of of an operation:
  - CF(carry flag) → Tells us if an operation had a carry.
  - OF(overflow flag) → Tells us if an operation had an overflow.
  - SF(sign flag) → Tells us if a result was negative or positive.
  - ZF(zero flag) → Tells us if the result is zero.
  - AC(auxiliary carry).
  - PF(parity flag).