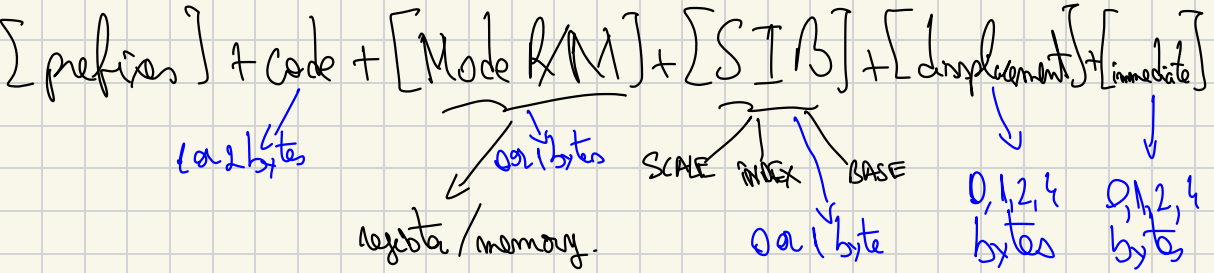
15.12.2023

Machine instruction representations

Internal format of an instruction



OBS: All are optional, but the "code" field.

Mode R/M

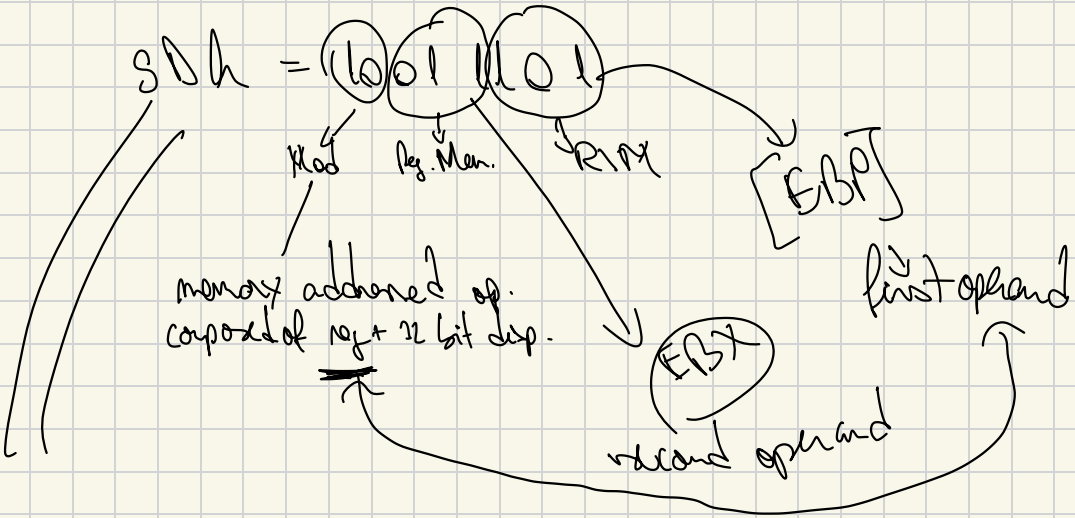
Mod	reg/opcode	R/M
7 6	5 4 3	2 1 0

SIB

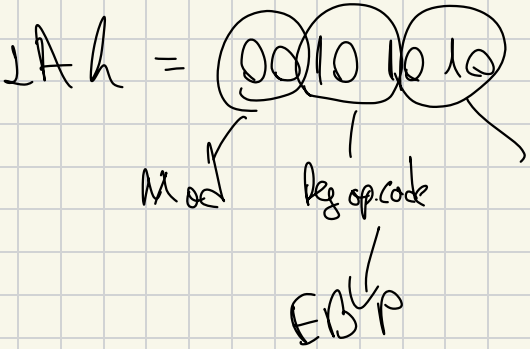
Scale	Index	Base
7 6	5 4 3	2 1 0

Table 2-2 Mode R/M

AMC			
	Eb	Gb	(10)
	Ev	Gv	(11)
	Gb	Eb	(12)
	Gv	Ev	(13)



⇒ instruction [EBP] + disp_of 32 bits, EBX



instr [EDX], EBP (or CH, CBP) memory register

F3h analyse at home

Table 2-3 for SIB byte

00 → scale 1
01 → scale 2
10 → scale 4
11 → scale 8

9Ch = 10 011 100

- Scale: 10 → Scale of 4
- Index: 011 → EBX*4
- Base: 100 → ESP

⇒ offset = [ESP + EBX*4]

SIB byte will generate the offset formula

Mod RM byte ne zice dacă avem registru sau var. din memorie

→ ne uităm la SIB byte

Jump instruction analysis.

Mecanism for jumps

You can perform a far jump only by using a pointer variable (on 6 bytes)

- 2 bytes segment
- 4 bytes offset.

CS: EIP currently execut instruction

you can only change the value of EIP by jmping

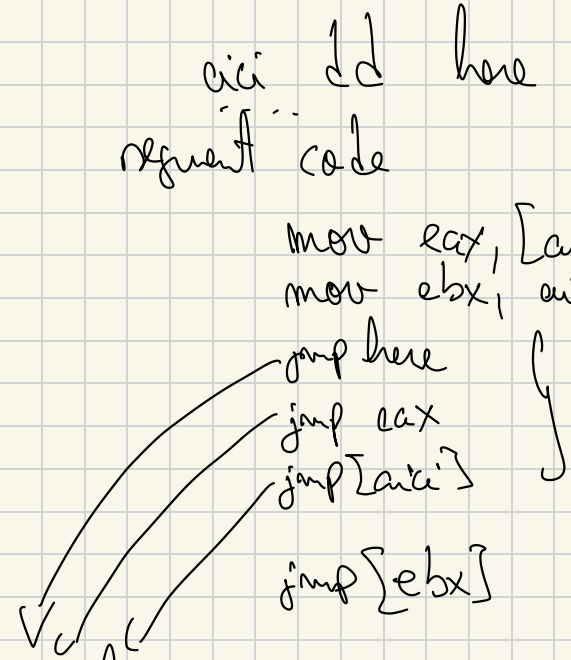
or CS:EIP by far jmping.

segment date

aici dd here

segment code

here: ....



offset(here)
aici

offset(aici)
EBX