Instructions	Opcode	Instructions	Opcode

MOV reg, reg
MOV reg, mem
MOV mem, reg
	100010dw oorrrmmm disp	RCL reg, 1
		RCL mem,1
			1101000w oo010mmm disp

MOV reg, imm	1011wrrr data	RCR reg, 1 RCR mem,1	1101000w oo011mmm disp
MOV mem, imm	1100011w oo000mmm disp data	ROL reg, 1 ROL mem,1	1101000w oo000mmm disp
MOVSX reg, reg MOVSX reg, mem	00001111 1011111w oorrrmmm disp	ROR reg, 1 ROR mem,1	1101000w oo001mmm disp
MOVZX reg, reg MOVZX reg, mem	00001111 1011011w oorrrmmm disp	RCL reg, CL RCL mem, CL	1101001w oo010mmm disp
MUL reg MUL mem	1111011w oo100mmm disp	RCR reg, CL RCR mem, CL	1101001w oo011mmm disp
NEG reg NEG mem	1111011w oo011mmm disp	ROL reg, CL ROL mem, CL	1101001w oo000mmm disp
NOT reg NOT mem	1111011w oo010mmm disp	ROR reg, CL ROR mem, CL	1101001w oo001mmm disp
OR reg, reg OR reg, mem OR mem, reg	000010dw oorrrmmm disp	RCL reg, imm RCL mem, imm	1100000w oo010mmm disp data
OR reg, imm OR mem, imm	1000000w oo001mmm disp	RCR reg, imm RCR mem, imm	1100000w oo011mmm disp data
POP reg	01011rrr	ROL reg, imm ROL mem, imm	1100000w oo000mmm disp data
POP mem	10001111 oo000mmm disp	ROR reg, imm ROR mem, imm	1100000w oo001mmm disp data

PUSH reg	01010rrr	ADD reg, reg
		ADD reg, mem
		ADD mem, reg
			000000dw oorrrmmm disp

PUSH mem	11111111 oo110mmm disp	SUB reg, reg
		SUB reg, mem
		SUB mem, reg
			001010dw oorrrmmm disp

PUSH imm	01101000 data		
INC reg INC mem	1111111w oo000mmm disp	DEC reg DEC mem	1111111w oo001mmm disp

MOD=11			Direct Effective Address			
R/M	W=0	W=1	R/M	MOD = 00	MOD = 01	MOD = 10
000	AL	AX	000	[BX]+[SI]	[BX]+[SI]+D_8	[BX]+[SI]+D_{16}
001	CL	CX	001	[BX]+[DI]	[BX]+[DI] +D_8	[BX]+[DI] +D_{16}
010	DL	DX	010	[BP]+[SI]	[BP]+[SI] +D_8	[BP]+[SI] +D_{16}
011	BL	BX	011	[BP]+[DI]	[BP]+[DI] +D_8	[BP]+[DI] +D_{16}
100	AH	SP	100	[SI]	[SI] +D_8	[SI] +D_{16}
101	CH	BP	101	[DI]	[DI] +D_8	[DI] +D_{16}
110	DH	SI	110	Direct Address	[BP] +D_8	[BP] +D_{16}
111	BH	DI	111	[BX]	[BX] +D_8	[BX] +D_{16}

Examples

[D → tells Data register say aa raha hai, ya memory say. Source is reference.]

[W → 0 8-bit operation; 1 16-bit operation]

1) MOV BL, AL

Opcode = 100010

D = 0

W = 0

MOD = 11 (Register to Register)

REG ⇒ Source Register = 000

R/M ⇒ 011

$$\underbrace{1000}_{8}\overbrace{1000}^{8} \qquad \underbrace{1100}_{C}\overbrace{0011}^{3} \Rightarrow 88C3h$$

Ans.

2) MOV CH, BL

opcode = 100010

D = 0 source is register.

W = 0 8 bit data.

MOD = 11 (Register to Register)

Reg = 011

R/M = 101

$$\underbrace{1000}_{8}\overbrace{1000}^{8} \qquad \underbrace{1101}_{D}\overbrace{1101}^{D} \Rightarrow 88DDh$$

Ans.

3- MOV AX, CX

Opcode = 100010
D = 0 CX is register
W = 1 16 bit

MOD = 11 (R-R)
Reg = 001
R/M = 000

$\overbrace{1000}^{8}\overbrace{1001}^{9}$ $\overbrace{1100}^{C}\overbrace{1000}^{8}$ => 89C8h Ans.

4- MOV CX, 0ABEh

OPcode = 1011
W = 1
Reg = 001

$\overbrace{1011}^{B}\overbrace{1001}^{9}$ BE 0A => B9 BE 0A h Ans.

5- MOV VAR1, DX. Var1 = 1BDh. +124

Opcode = 100010
d = 0
W = 1

MOD = 00 Without Displacement
Reg = 010
R/M = 110 → Direct Address.

$\overbrace{1000}^{8}\overbrace{1001}^{9}$ $\overbrace{0001}^{1}\overbrace{0110}^{6}$ => 8916 h Ans.

(3)

6- MOV AX, [BX]

opcode = 100010

D= 1

W= 1

MOD= 00

REG= 000

R/M= 111

$$\underbrace{1000}_{8}\overbrace{1011}^{B}\quad \underbrace{00}\,\underbrace{000}_{0}\overbrace{111}^{7} \Rightarrow 8B07h$$

7- JL L1 IP= 2080h L1= 18Eh

Disp= 220Eh [IP+L1]

$$\underbrace{0000\,1111}_{\text{Opcode}}\quad 1000\overbrace{1100}^{cccc}\quad 0E\ 22$$

→

→

SUB BX, [DI]

opcode = 001010

D = 1

W = 1

MOD = 00

Reg = 011

R/M = 101

0010 1011 → 2B

0001 1101 → 1D

2B1D h

SUB [DI], BL

001010

D = 0

W = 0

00101000 → 28

2

ADD [BX][DI] + 1234h, AX

opcode = 000000

D = 0

W = 1

MOD = 10

Reg = 000

R/M = 001

0000 0001 → 01

1000 0001 → 81

34 12 h

displacement

ADD OFABE [BX][DI] , DX

opcode = 000000

D = 0

W = 1

MOD = 10

Reg = 010

R/M = 001

0000	0001	1001	0001
0	1	9	1

0191 BEFAh

ADD AX, [SI]

opcode = 000000

D = 1

W = 1

MOD = 00

REG = 000

R/M = 100

0	3	0	4
0000	0011	0000	0100

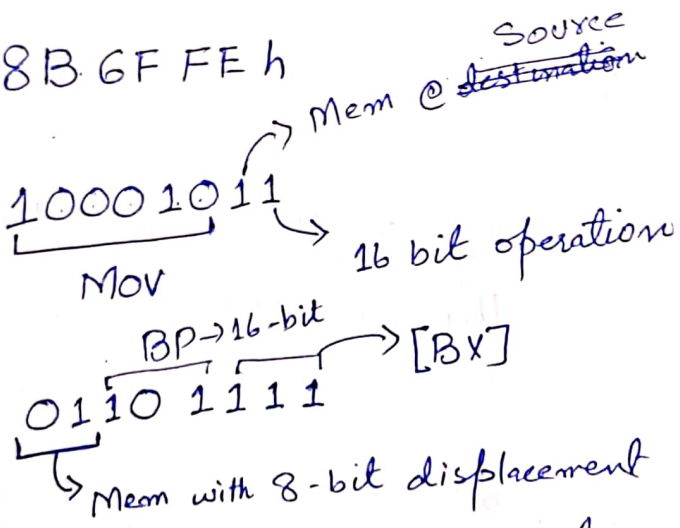
0304 h.

CHAPTER NO: 10

1) 8B 6F FEh
2) 89 A4 EA 01 h
3) F6 D8 h
4) 56 h
5) 33 41 CA h.

Sol

1) 8B 6F FE h

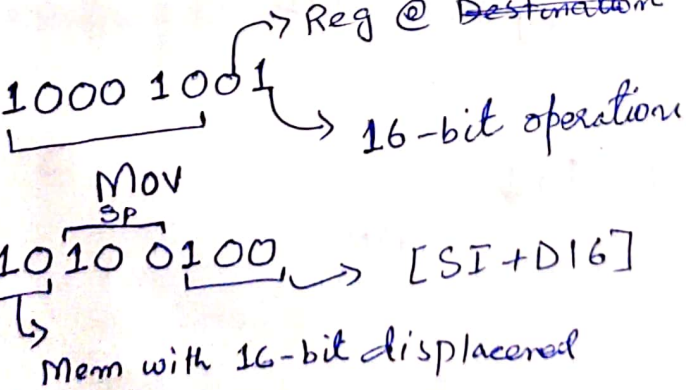


FE → 8 bit displacement

MOV BP, [BX+FEh]

ANS.

2) 89 → 1000 10 01



MOV [SI+01EA], SP

Ans.

3) F6 DB

F6 → 1111 0110 → 8 bit operation

NEG

DB → 11 011 011

Register operation

BL → 8 bit Register under Mod 11.

NEG BL ANS.

4) 56h

0101 0110 → SI

PUSH SI

Why SI?? → valid 16-bit

Why not DH?? → Invalid 8-bit

5) F7 E7

F7 → 1111 0111 → 16 bit

MUL

E7 → 11 100 111

Register DI

MUL DI

ANS.

6) D0 C0 h

D0 → 1101 0000 → 8 bit operation

Rotate → many possibilities.

C0 → 1 1000 0000 (ROL)

1 → register operand rotate.

AL → due to 8-bit operation

ROL AL, 1

ANS

7) 01 56 F7 h

01 → 0000 0001 → 16-bit operation

Register @ Source

ADD

56 → 0101 0110 → BP+D8

DX

0101 → Mem with D8

~~MOV~~ ADD [BP+F7], DX

ANS.

Conditional JUMP example.

JL L1 ; IP = 2080h ; and L1 = 8Eh

16-bit displacement

0111 cccc disp → 0111 1100 8E ⇒ 7C8E

(7 = 0111, C = 1100)

Label − IP = Disp

+ve forward JMP

−ve backward JMP