

HW#2 Key

1. Ex. 4.2

	opcode	(including prefix) object code (bytes)	actually try on computer
(#1) (b) Sub WOp, ax	66 29	7 bytes	66 29 05 00 00 00 00 Mode R/M 32 addr. of WOp
	prefix for 16-bit operation.		
(c) Sub eax, 10	83	3	83 E8 0A 10 (1 byte)
(d) add DOp, 10	83	7	83 05 00 00 00 02 0A addr. of DOp
(e) add eax, [ebx]	03	2	03 03
(f) sub [ebx], eax	29	2	29 03
(i) inc ebx	43	1	43
(j) dec AL	FE	2	FE C8
(m) neg eax	F7	2	F7 D8
(n) neg bh	F6	2	F6 DF
(p) neg DWORD PTR [ebx]	F7	2	F7 1B
	bw size mem		

(#3) (b)	before EBX: FFFFFFF5 ECX: 000001A2	instr. sub ebx, ecx	after EBX: FFFFFFF3 ECX: 000001A2 SF, ZF, CF, OF (1) (0) (0) (0)	(-) - (+) ⇒ (-) + (-)
→ (c)	BX: FF75 CX: 01A2	sub cx, bx	BX: FF75 CX: 022D	(+) - (-) ⇒ (+) + (+) SF(0), ZF(0), CF(1), OF(0)
(d)	DX: 014B	add dx, 40H	DX: 018B	SF(0), ZF(0), CF(0), OF(0)
(f)	AX: 0A20 WOp: FF20	add ax, WOp	WOp: FF20 AX: 0940	SF(0), ZF(0), CF(1), OF(0)
→ (g)	AX: 0A20 WOp: FF20	sub WOp, ax	WOp: F500 ax: 0A20	(-) - (+) ⇒ (-) + (-) SF(1), ZF(0), CF(0), OF(0)
(l)	EBX: FFFFFFFF	neg ebx	EBX: 00000001	SF(0), ZF(0)
(m)	CL: 5F	neg CL	CL: A1	SF(1), ZF(0)
(n)	WOp: FB3C	neg WOp	WOp: 04C4	SF(0), ZF(0)

2. Ex. 4.3.

(#1) (a) $\begin{pmatrix} \text{EAX}: \text{FFFFFFE4} \\ \text{EBX}: 00000002 \end{pmatrix} \xrightarrow{\text{mul ebx}} \begin{pmatrix} \text{EAX}: \text{FFFFFFC8} \\ \text{EDX}: 00000001 \end{pmatrix} \begin{matrix} \text{CF}=1 \\ \text{OF}=1 \end{matrix}$

$\text{eax} * \text{ebx} \Rightarrow \text{edx: eax}$

$\rightarrow (c) \text{AX}: \text{FFFF} \xrightarrow{\text{mul AX}} \begin{pmatrix} \text{AX}: 0001 \\ \text{DX}: \text{FFFE} \end{pmatrix} \begin{matrix} \text{CF}(1) \\ \text{OF}(1) \end{matrix}$

$\text{ax} * \text{ax} \Rightarrow \text{dx: ax}$

(d) $\begin{pmatrix} \text{AL}: 0F \\ \text{BH}: 4C \end{pmatrix} \xrightarrow{\text{mul BH}} \text{AX}: 0474, \text{CF}(1), \text{OF}(1)$

$\text{AL} * \text{BH} \Rightarrow \text{AX}$

(g) $\begin{pmatrix} \text{EAX}: \text{FFFFFFE4} \\ \text{EBX}: 000004C2 \end{pmatrix} \xrightarrow{\text{imul ebx}} \begin{pmatrix} \text{EAX}: \text{FFFF7AC8} \\ \text{EDX}: \text{FFFFFFFF} \end{pmatrix}, \text{CF}(0), \text{OF}(0)$

$\text{eax} * \text{ebx} \Rightarrow \text{edx: eax}$

(h) $\begin{pmatrix} \text{EAX}: \text{FFFFFFE4} \\ \text{DWop}: \text{FFFFFFFF3A} \end{pmatrix} \xrightarrow{\text{imul dwop}} \begin{pmatrix} \text{EAX}: 000015A8 \\ \text{EDX}: 00000000 \end{pmatrix}, \text{CF}(0), \text{OF}(0)$

$\text{eax} * \text{dwop} \Rightarrow \text{edx: eax}$

$\rightarrow (k) \begin{pmatrix} \text{AL}: F0 \\ \text{BH}: 4C \end{pmatrix} \xrightarrow{\text{imul bh}} \text{AX}: 03C0, \text{CF}(1), \text{OF}(1).$

$\text{AL} * \text{BH} \Rightarrow \text{AX}$

(#3) (b) $\begin{pmatrix} \text{EAX}: \text{FFFFFFE4} \\ \text{EBX}: 000004C2 \end{pmatrix} \xrightarrow{\text{imul eax, ebx}} \text{EAX}: \text{FFFF7AC8}, \text{CF}(0), \text{OF}(0)$

$\text{eax} * \text{ebx} \Rightarrow \text{eax}$

(d) $\begin{pmatrix} \text{ECX}: 00007CE4 \\ \text{DWop}: 000065ED \end{pmatrix} \xrightarrow{\text{imul ecx, DWop}} \text{ECX}: 31B99314, \text{CF}(0), \text{OF}(0)$

$\text{ecx} * \text{DWop} \Rightarrow \text{ecx}$

(g) $\text{EBX}: 000004C2 \xrightarrow{\text{imul ebx, -10}} \text{EBX}: \text{FFFFD06C}, \text{CF}(0), \text{OF}(0)$

$\text{ebx} * (-10) \Rightarrow \text{ebx}$

(i) $\text{EDX}: 00000064 \xrightarrow{\text{imul eax, edx, 10}} \text{EAX}: 000003E8, \text{CF}(0), \text{OF}(0)$

$\text{edx} * 10 \Rightarrow \text{eax}$

HW#2

Some selected problems - more details

EX 4.2 - Sub and OF flag

(#3)-(c)

(BX: FF75
CX: 01A2)

Sub CX, BX

⇒ (BX: FF75
CX: 022D)

borrow
01A2
- FF75
022D

$$\begin{array}{r} \oplus \\ - \ominus \\ \oplus \end{array} \equiv \begin{array}{r} \oplus \\ + \oplus \\ \oplus \end{array}$$

OF = 0

SF, ZF, CF, OF
(0) (0) (1) (0)

(#3)-(g)

(AX: 0A20
WDOP: FF20)

Sub WDOP, AX

⇒ (AX: 0A20
WDOP: F500)

FF20
- 0A20
F500

$$\begin{array}{r} \ominus \\ - \oplus \\ \ominus \end{array} \equiv \begin{array}{r} \ominus \\ + \ominus \\ \ominus \end{array}$$

OF = 0

SF, ZF, CF, OF
(1) (0) (0) (0)

EX 4.3 - Unsigned mul and CF/OF

(#1)-(a)

(EAX: FFFFFFFE4
EBX: 00000002)

mul ebx; $\text{eax} \times \text{ebx} \Rightarrow \boxed{\text{edx} = \text{eax}}$

⇒ (EAX: FFFFFFFC8
EDX: 00000001)

$$\begin{array}{r} \begin{array}{cccccccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \text{FF} & \text{FF} & \text{FF} & \text{FF} & \text{E} & 4 \\ \times & 0 & 0 & 0 & 0 & 0 & 0 & 2 \\ \hline \text{FF} & \text{FF} & \text{FF} & \text{F} & \text{C} & 8 \end{array} \end{array}$$

high half ≠ 0
⇒ CF/OF = 1

(#1)-(c)

AX: FFFF

mul AX; $\text{ax} \times \text{ax} \Rightarrow \boxed{\text{dx} = \text{ax}}$

⇒ (AX: 0001
DX: FFFE)

$$\begin{array}{r} \text{FFFF} \\ \times \text{FFFF} \\ \hline \text{E1} \\ \text{E1} \\ \text{E1} \\ \text{E1} \\ \text{E1} \\ \text{E1} \\ \text{E1} \\ \text{E1} \\ \text{E1} \\ \text{E1} \\ \hline \text{FFFFE001} \\ \text{DX} \quad \text{AX} \end{array}$$

high half ≠ 0
⇒ CF/OF = 1

Ex. 4.3.

(#1) - (K) — Signed # imul and CF/OF

(AL: F0
BH: C4

imul BH; — $AL * BH \Rightarrow AX$

$\Rightarrow AX: \boxed{03C0}$

$$\begin{array}{r} 100 \\ - \text{F0} \\ \hline 10 \end{array} \Rightarrow (-10)_H$$

$$\begin{array}{r} 100 \\ - \text{C4} \\ \hline 3C \end{array} \Rightarrow (-3C)_H$$

imul source
 if any bit in high half
 \neq sign ext. from
 lower half
 $\Rightarrow \text{CF/OF} = 1$

$$\begin{array}{r} -10 \\ * -3C \\ \hline \text{C0} \\ 30 \\ \hline \oplus 3C0 \end{array} \text{ Hex}$$

So, CF/OF = 1

EX 4.3

(#3) (b)

(EAX: FFFFFFFE4
EBX: 00004C2

imul eax, ebx; $eax * ebx \Rightarrow eax$

$\Rightarrow EAX: \underline{\text{FFFFFF7AC8}}$

imul dest, source
 if product fits in the dest-reg,
 CF/OF = 0
 else 1.

So, CF/OF = 0

interpreted as:

$$\begin{array}{r} 100000000 \\ - \text{FFFFFFFE4} \\ \hline -0000001C \end{array}$$

$$\begin{array}{r} -0000001C \\ * 00004C2 \\ \hline 38 \\ 150 \\ 70 \\ \hline \ominus 8538 \end{array} \text{ Hex}$$

represent in 2's

$$\begin{array}{r} 100000000 \\ - 00008538 \\ \hline \text{FFFFFF7AC8} \\ \Downarrow \\ \text{EAX} \end{array}$$