

HW#2 Key

1. ex. 4.2

	opcode	object code (bytes)	(including prefix) actually try on Computer
(#1) (b) Sub WDop, ax	66 29	7 bytes	66 29 05 00 00 00 00 in mode R/M #2 addr. of WDop
		pref for 16-bit operation.	
(c) Sub eax, 10	83 3	1 byte	83 E8 0A
(d) add DWop, 10	83 7	10 bytes	83 05 00 00 00 02 0A addr. of DWop
(e) add eax, [ebx]	03 2	2	03 03
(f) sub [ebx], eax	29 2	2	29 03
(g) inc ebx	43 1	1	43
(h) dec AL	FE 2	2	FE C8
(i) neg eax	F7 2	2	F7 D8
(j) neg bh	F6 2	2	F6 DF
(k) neg DWORD PTR ^{dw size mem} [ebx]	F7 2	2	F7 1B

	before	matrix	after
(#3) (b)	(EBX: FFFF FF 95 ECX: 00 00 01 A2)	sub ebx, ecx \Rightarrow	EBX: FFFF FD D3 ECX: 00 00 01 A2 (-) - (+) \Rightarrow (-) + (-)
\rightarrow (c)	(BX: FF 95 CX: 01 A2)	sub cx, bx \Rightarrow (BX: FF 75 CX: 02 2D)	(+) - (-) \Rightarrow (+) + (+) SF(0), ZF(0), CF(1), OF(0)
(d)	DX: 01 4B	add dx, 40H \Rightarrow DX: 01 8B	SF(0), ZF(0), CF(0), OF(0)
(f)	(AX: 0A20 WDop: FF 20)	add ax, wdop \Rightarrow (WDop: FF 20 AX: 09 40)	SF(0), ZF(0), CF(1), OF(0)
\rightarrow (g)	(AX: 0A20 WDop: FF 20)	sub wdop, ax \Rightarrow (WDop: F5 00 AX: 0A20)	(-) - (+) \Rightarrow (-) + (-) SF(1), ZF(0), CF(0), OF(0)
(l)	EBX: FFFF FFFF	$\underline{\text{neg ebx}}$ \Rightarrow EBX: 00 00 00 01	SF(0), ZF(0)
(m)	CL: 5F	$\underline{\text{neg cl}}$ \Rightarrow CL: A1	SF(1), ZF(0)
(n)	WDop: FB3C	$\underline{\text{neg wdop}}$ \Rightarrow WDop: 04 C4	SF(0), ZF(0)

2. Ex. 4.3.

(#1) (a) $\begin{cases} \text{EAX: FFFF FF E4} \\ \text{EBX: 00 00 00 02} \end{cases}$ $\underline{\text{mul ebx}} \Rightarrow \begin{cases} \text{EAX: FFFF FF C8} \\ \text{EDX: 00 00 00 01} \end{cases}$, $(CF = 1, OF = 1)$

\rightarrow (c) $AX: FFFF$ $\underline{\text{mul AX}}$ $\Rightarrow \begin{cases} AX: 0001 \\ DX: FFFE \end{cases}$, $(CF(1), OF(1))$

(d) $\begin{cases} AL: OF \\ BH: 4C \end{cases}$ $\underline{\text{mul BH}}$ $\Rightarrow \begin{cases} AX: 0474 \\ (AL \times BH \Rightarrow AX) \end{cases}, CF(1), OF(1)$

(g) $\begin{cases} \text{EAX: FFFF FF E4} \\ \text{EBX: 00 00 04 C2} \end{cases}$ $\underline{\text{imul ebx}}$ $\Rightarrow \begin{cases} \text{EAX: FFFF 7AC8} \\ \text{EDX: FFFF FFFF} \end{cases}$, $(CF(0), OF(0))$

(h) $\begin{cases} \text{EAX: FFFF FF E4} \\ \text{DWOP: FFFF FF 3A} \end{cases}$ $\underline{\text{imul dwop}}$ $\Rightarrow \begin{cases} \text{EAX: 00 00 15 A8} \\ \text{EDX: 00 00 00 00} \end{cases}$, $(CF(0), OF(0))$

\rightarrow (k) $\begin{cases} AL: F0 \\ BH: C4 \end{cases}$ $\underline{\text{imul bh}}$ $\Rightarrow \begin{cases} AX: 03C0 \\ (AL \times BH \Rightarrow AX) \end{cases}, CF(1), OF(1)$

(#3) (b) $\begin{cases} \text{EAX: FFFF FF E4} \\ \text{EBX: 00 00 04 C2} \end{cases}$ $\underline{\text{imul eax, ebx}}$ $\Rightarrow \begin{cases} \text{EAX: FFFF 7AC8} \\ (eax \times ebx \Rightarrow eax) \end{cases}$, $(CF(0), OF(0))$

(d) $\begin{cases} ECX: 00 00 7C E4 \\ DWOP: 00 00 65 ED \end{cases}$ $\underline{\text{imul ecx, dwop}}$ $\Rightarrow \begin{cases} ECX: 31B9 93 14 \\ (ecx \times dwop \Rightarrow ecx) \end{cases}$, $(CF(0), OF(0))$

(g) $EBX: 00 00 04 C2$ $\underline{\text{imul ebx, -10}}$ $\Rightarrow \begin{cases} EBX: FFFF D0 6C \\ (ebx \times -10 \Rightarrow ebx) \end{cases}$, $(CF(0), OF(0))$

(i) $EDX: 00 00 00 64$ $\underline{\text{imul eax, edx, 10}}$ $\Rightarrow \begin{cases} EAX: 0000 03 E8 \\ (edx \times 10 \Rightarrow eax) \end{cases}$, $(CF(0), OF(0))$

HW#2

Some selected problems - more details

EX 4.2 — Sub and OF flag

(#3)-(c)

$$(BX: FF75)$$

$$(CX: 01A2)$$

$$\underline{\text{Sub } CX, BX}$$

$$\begin{array}{r}
 \text{borrow} \\
 01A2 \\
 - FF75 \\
 \hline
 022D
 \end{array}$$

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

$OF = \phi$

$$\Rightarrow (BX: FF75)$$

$$(CX: 022D)$$

$$SF, ZF, CF, OF$$

$$(0) \quad (0) \quad (1) \quad (0)$$

(#3)-(g)

$$(AX: 0A20)$$

$$(WDop: FF20)$$

$$\underline{\text{Sub WDop, AX}}$$

$$\begin{array}{r}
 FF20 \\
 - 0A20 \\
 \hline
 F500
 \end{array}$$

$$SF, ZF, CF, OF$$

$$(1) \quad (0) \quad (0) \quad (0)$$

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

$OF = \phi$

$$\Rightarrow (AX: 0A20)$$

$$(WDop: F500)$$

EX 4.3 — Unsigned mul and CF/OF

(#1)-(a)

$$(EAX: FFFF FFE4)$$

$$(EBX: 00 00 00 02)$$

$$\underline{\text{mul ebx}}; \quad \underline{eax * ebx} \Rightarrow \boxed{edx = eax}$$

$$\begin{array}{r}
 \begin{array}{cccc}
 1 & 1 & 1 & 1 \\
 \hline
 FF & FF & FF & E4 \\
 \times 0 & 0 & 0 & 0 \\
 \hline
 1 & FF & FFFF & C8
 \end{array}
 \end{array}$$

$$\Rightarrow (EAX: FFFFFFC8) \quad \left(\begin{array}{l} \text{high half} \neq \phi \\ \Rightarrow CF/OF = 1 \end{array} \right)$$

(#1)-(c)

$$AX = FFFF$$

$$\underline{\text{mul AX}}; \quad \underline{ax * ax} \Rightarrow \boxed{DX = AX}$$

$$\Rightarrow (AX: 0001)$$

$$(DX: FFFE)$$

$$\begin{array}{r}
 \begin{array}{c}
 FFFF \\
 \times FFFF \\
 \hline
 E1
 \end{array}
 \end{array}$$

$$\begin{array}{r}
 \begin{array}{c}
 E1 \\
 E1 \\
 E1 \\
 \hline
 EFFF \\
 EFFF \\
 EFFF \\
 \hline
 \boxed{FFFE} \quad \boxed{0001} \\
 \hline
 DX \quad AX
 \end{array}
 \end{array}$$

$$\left\{
 \begin{array}{l}
 \text{high half} \neq \phi \\
 \Rightarrow CF/OF = 1
 \end{array}
 \right.$$

Ex. 4.13.

(#1) -(K) — Signed # imul and CF/OF

$$(AL : F\phi)$$

$$(BH : C4)$$

imul BH ; — $AL * BH \Rightarrow AX$

$$\Rightarrow AX : (\phi 3 | C\phi)$$

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

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

imul source

if any bit in high half
≠ sign ext. from
lower half
 $\Rightarrow OF/CF = 1$

$$\begin{array}{r} -10 \\ * -3C \\ \hline C0 \end{array}$$

$$\begin{array}{r} 30 \\ \hline + 3C0 \end{array}$$

So, $CF = 1$

Ex 4.3

(#3) (b)

$$EAX : FFFF7FE4$$

$$EBX : 000004C2$$

imul eax, ebx ; eax * ebx \Rightarrow eax

$$\Rightarrow EAX : FFFF7AC8$$

interpreted as:

$$\begin{array}{r} 100000000 \\ - FFFF7FE4 \\ \hline -00000001C \end{array}$$

imul dest, source

if product fits in the dest-reg,
 $CF/OF = \phi$
else,

So, $CF/OF = \phi$

$$\begin{array}{r} -00000001C \\ * 000004C2 \\ \hline 38 \\ 150 \\ 70 \\ \hline 8538 \end{array}$$

Hex

represent in 2's

$$\begin{array}{r} 100000000 \\ - 00008538 \\ \hline FFFF7AC8 \end{array}$$

EAX