# LAB03-B 17376283 李智健

## **Question 1**

### 1. 写入代码

```
-a 1000:0000
1000:0000 mov ax,ffff
1000:0003 mov ds,ax
1000:0005 mo∨ ax,2200
1000:0008 mov ss,ax
1000:000A mov sp,0100
1000:000D mov ax,[0]
1000:0010 add ax.[2]
1000:0014 mov bx,[4]
1000:0018 add bx,[6]
1000:001C push ax
1000:001D push bx
1000:001E pop ax
1000:001F pop bx
1000:0020 push [4]
1000:0024 push [6]
1000:0028
```

### 逐条执行

```
AX-0000 BX-0000 CX-0000 DX-0000 SP-00FD BP-0000 SI-0000 DI-0000
DS=073F ES=073F SS=073F CS=1000 IP=0000 NV UP EI PL NZ NA PO NC
                             MOV
                                        AX, FFFF
1000:0000 B8FFFF
AX=FFFF BX=0000 CX=0000 DX=0000 SP=00FD BP=0000 SI=0000 DI=0000
DS=073F ES=073F SS=073F CS=1000 IP=0003 NV UP EI PL NZ NA PO NC
1000:0003 SEDS
                              MOU
                                        DS,AX
 -t
AX=FFFF BX=0000 CX=0000 DX=0000 SP=00FD BP=0000 SI=0000 DI=0000
DS=FFFF ES=073F SS=073F CS=1000 IP=0005 NV UP EI PL NZ NA PO NC
1000:0005 B80022 MOV AX,2200
AX=2200 BX=0000 CX=0000 DX=0000 SP=00FD BP=0000 SI=0000 DI=0000
DS=FFFF ES=073F SS=073F CS=1000 IP=0008 NV UP EI PL NZ NA PO NC
1000:0008 SED0
                              MOV
                                        SS,AX
AX=2200 BX=0000 CX=0000 DX=0000 SP=0100 BP=0000 SI=0000 DI=0000
DS=FFFF ES=073F SS=2200 CS=1000 IP=000D NV UP EI PL NZ NA PO NC
                             MOV
1000:000D A10000
                                      AX,[0000]
                                                                                     DS:0000=C0EA
```

```
AX=COEA BX=0000 CX=0000 DX=0000 SP=0100 BP=0000 SI=0000 DI=0000
DS=FFFF ES=073F SS=2200 CS=1000 IP=0010 NV UP EI PL NZ NA PO NC
1000:0010 03060200
                       ADD
                                   AX,[0002]
                                                                         DS:0002=0012
AX=COFC BX=0000 CX=0000 DX=0000 SP=0100 BP=0000 SI=0000 DI=0000
DS=FFFF ES=073F SS=2200 CS=1000 IP=0014 NU UP EI NG NZ NA PE NC
1000:0014 8B1E0400
                         MOU
                                  BX,[0004]
                                                                         DS:0004=30F0
AX=COFC BX=30F0 CX=0000 DX=0000 SP=0100 BP=0000 SI=0000 DI=0000
DS=FFFF ES=073F SS=2200 CS=1000 IP=0018 NV UP EI NG NZ NA PE NC
1000:0018 031E0600
                        ADD
                                   BX,[0006]
                                                                         DS:0006=2F31
AX=COFC BX=6021 CX=0000 DX=0000 SP=0100 BP=0000 SI=0000 DI=0000
DS=FFFF ES=073F SS=2200 CS=1000 IP=001C NV UP EI PL NZ NA PE NC
                          PUSH
1000:001C 50
                                  ĤΧ
AX=COFC BX=6021 CX=0000 DX=0000 SP=00FE BP=0000 SI=0000 DI=0000
DS=FFFF ES=073F SS=2200 CS=1000 IP=001D
                                                NU UP EI PL NZ NA PE NC
1000:001D 53
                         PUSH
                                  BX
AX=COFC BX=6021 CX=0000 DX=0000 SP=00FC BP=0000 SI=0000 DI=0000
DS=FFFF ES=073F SS=2200 CS=1000 IP=001E
                                                 NU UP EI PL NZ NA PE NC
                         POP
1000:001E 58
-t
AX=6021 BX=6021 CX=0000 DX=0000 SP=00FE BP=0000 SI=0000 DI=0000
DS=FFFF ES=073F SS=2200 CS=1000 IP=001F NU UP EI PL NZ NA PE NC
                          POP
1000:001F 5B
                                  RX
-t.
AX=6021 BX=C0FC CX=0000 DX=0000 SP=0100 BP=0000 SI=0000 DI=0000
DS=FFFF ES=073F SS=2200 CS=1000 IP=0020 NV UP EI PL NZ NA PE NC
1000:0020 FF360400
                        PUSH
                                                                         DS:0004=30F0
-t
AX=6021 BX=C0FC CX=0000 DX=0000 SP=00FE BP=0000 SI=0000 DI=0000
DS=FFFF ES=073F SS=2200 CS=1000 IP=0024 NV UP EI PL NZ NA PE NC
1000:0024 FF360600
                        PUSH
                                  1000061
                                                                         DS:0006=2F31
-\mathbf{t}
AX=6021 BX=C0FC CX=0000 DX=0000 SP=00FC BP=0000 SI=0000 DI=0000
DS=FFFF ES=073F SS=2200 CS=1000 IP=0028
                                                NU UP EI PL NZ NA PE NC
1000:0028 0000
                         ADD
                                 [BX+SI],AL
                                                                         DS:COFC=00
```

#### 填空题答案

```
ax = C0FA

ax = C0FC

bx = 30F0

bx = 6021

sp = 00FE , 修改的内存单元的地址是 00FE, 内容为 C0FC

sp = 00FC , 修改的内存单元的地址是 00FC, 内容为 6021

sp = 00FE , ax=6021

sp = 0100 , bx=C0FC

sp = 00FE , 修改的内存单元的地址是 00FE, 内容为 30F0

sp = 00FC , 修改的内存单元的地址是 00FC, 内容为 2931
```

#### 2. 分析3.19中为什么2000:0~2000:f中的内容会发生改变?

因为 mov sp, 10 改变了栈偏移量

# **Question 2**

代码:

```
assume cs:codesg
codesg segment
 mov ax, 2000h
 mov ss, ax
 mov sp, 0
 add sp, 10
 pop ax
  pop bx
  push ax
  push bx
  pop ax
 pop bx
 mov ax, 4c00h
 int 21h
codesg ends
end
```

### 生成可执行文件的命令截图:

```
C:\>masm
Microsoft (R) Macro Assembler Version 5.00
Copyright (C) Microsoft Corp 1981-1985, 1987. All rights reserved.

Source filename [.ASM]: t1
Object filename [t1.OBJ]:
Source listing [NUL.LST]:
Cross-reference [NUL.CRF]:

51808 + 464736 Bytes symbol space free

O Warning Errors
O Severe Errors
```

```
C:\>link

Microsoft (R) Overlay Linker Version 3.60

Copyright (C) Microsoft Corp 1983-1987. All rights reserved.

Object Modules [.OBJ]: t1

Run File [T1.EXE]:

List File [NUL.MAP]:

Libraries [.LIB]:

LINK: warning L4021: no stack segment
```

调试命令	ax	bx	SS	sp	栈顶
mov ax,2000H	2000	0000	0769	0000	00
mov ss,ax	2000	0000	2000	0000	00
mov sp,0	2000	0000	2000	0000	00
add sp,10	2000	0000	2000	000A	6A
рор ах	076A	0000	2000	000C	06
pop bx	076A	7206	2000	000E	00

调试命令	0 <b>76</b> A	7 <b>80</b> 6	2990	0 <b>8</b> 8C	棧飯
push bx	076A	7206	2000	000A	06
pop ax	7206	7206	2000	000C	6A
pop bx	7206	076A	2000	000E	00
mov ax,4c00H	4C00	076A	2000	000E	00
int 21H	4C00	076A	2000	000E	00

# 3.提交查看过程的截图。

-d 075A:00	90 I	.00														
075A:0000	CD	20	$\mathbf{F}\mathbf{F}$	9F	$\Theta\Theta$	ΕA	$\mathbf{F}\mathbf{F}$	FF-AD	DE	4F	03	AЗ	01	8A	03	0
075A:0010	AЗ	01	17	03	AЗ	01	92	01-01	01	01	$\infty$	<b>0</b> 2	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	
075A:0020	$\mathbf{F}\mathbf{F}$	FF-FF	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	50	97	<b>4</b> C	01							
075A:0030	63	<b>96</b>	14	$\infty$	18	$\infty$	5A	07-FF	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	$\infty$	$\infty$	$\Theta\Theta$	$\infty$	cZ
075A:0040	05	00	$\infty$	$\infty$	$\infty$	$\infty$	$\infty$	00-00	$\infty$	$\infty$	$\infty$	$\infty$	$\infty$	$\infty$	$\infty$	
075A:0050	CD							00-00								. †
075A:0060	$\infty$							00-00								
075A:0070	00							00-00								
075A:0080								65-0D								t1.exe
075A:0090	<b>00</b>							00-00								
075A:00A0								00-00								
075A:00B0								00-00								
075A:00C0								00-00								
075A:00D0								00-00								
075A:00E0								00-00								
075A:00F0		00	<b>00</b>	00	<b>00</b>	<b>00</b>	00	00-00	<b>99</b>	<b>00</b>	<b>90</b>	<b>90</b>	$\Theta\Theta$	<b>00</b>	$\Theta\Theta$	
075A:0100	B8															