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 mov 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

```
-r
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
1000:0000 B8FFFF        MOV     AX,FFFF
-t

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 8ED8          MOV     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
-t

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 8ED0          MOV     SS,AX
-t

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
1000:000D A10000        MOV     AX,[0000]                       DS:0000=C0EA
```

```
AX=C0EA  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
-t

AX=C0FC  BX=0000  CX=0000  DX=0000  SP=0100  BP=0000  SI=0000  DI=0000
DS=FFFF  ES=073F  SS=2200  CS=1000  IP=0014   NV UP EI NG NZ NA PE NC
1000:0014 8B1E0400      MOV     BX,[0004]                       DS:0004=30F0
-t

AX=C0FC  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
-t

AX=C0FC  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
1000:001C 50            PUSH    AX
-t

AX=C0FC  BX=6021  CX=0000  DX=0000  SP=00FE  BP=0000  SI=0000  DI=0000
DS=FFFF  ES=073F  SS=2200  CS=1000  IP=001D   NV UP EI PL NZ NA PE NC
1000:001D 53            PUSH    BX
```

```
AX=C0FC  BX=6021  CX=0000  DX=0000  SP=00FC  BP=0000  SI=0000  DI=0000
DS=FFFF  ES=073F  SS=2200  CS=1000  IP=001E   NV UP EI PL NZ NA PE NC
1000:001E 58            POP     AX
-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   NV UP EI PL NZ NA PE NC
1000:001F 5B            POP     BX
-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    [0004]                          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    [0006]                          DS:0006=2F31
-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   NV UP EI PL NZ NA PE NC
1000:0028 0000          ADD     [BX+SI],AL                      DS:C0FC=00
```

填空题答案

```
ax = C0EA
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?

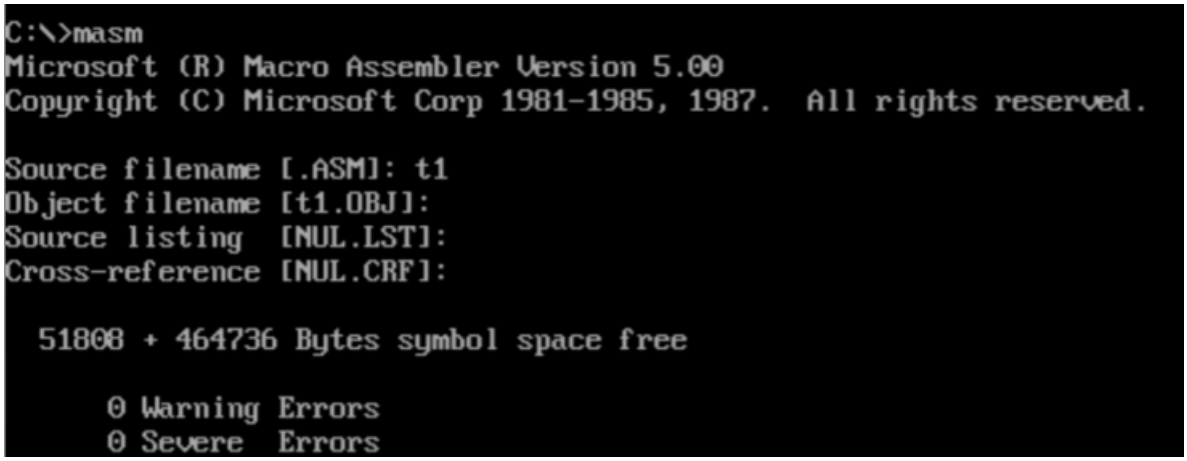
因为 `mov sp, 10` 改变了栈偏移量

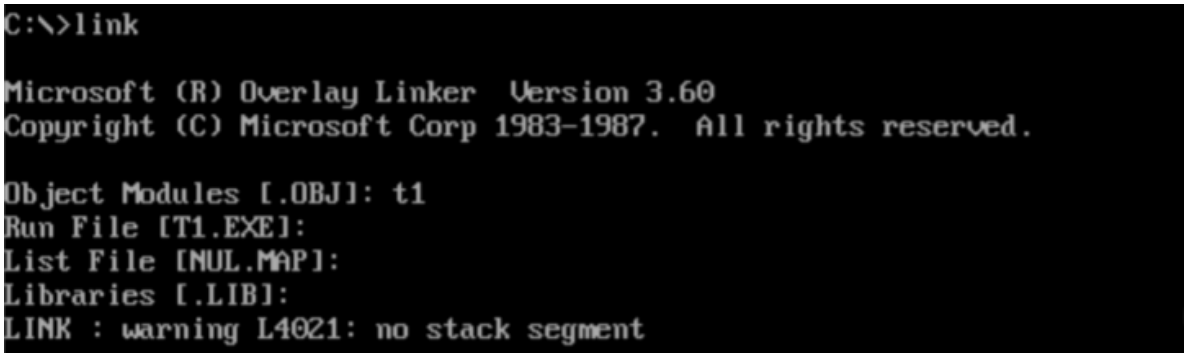
Question 2

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：





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
pop ax	076A	0000	2000	000C	06
pop bx	076A	7206	2000	000E	00

调试命令	ax	bx	ss	sp	栈顶
push ax	076A	7206	2000	000C	6A
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。