实验三 栈及内存访问

一、Debug 功能新增知识

1. Debug 的以下功能都支持以段寄存器（CS，DS，SS，ES）内容作为段地址。

- 用 Debug 的 D 命令查看内存中的内容；
- 用 Debug 的 E 命令改写内存中的内容；
- 用 Debug 的 U 命令将内存中的机器指令翻译成汇编指令（反汇编）；
- 用 Debug 的 A 命令以汇编语言的格式在内存中写入一条机器指令。

例如：-d ds:0 为用 d 命令查看从 ds:0 开始的内存单元中的内容

2. Debug 的 T 命令在设置 SS 的指令处不发生单步执行。具体而言，如果 T 命令执行时 IP 所指向的指令为设置 SS 的的指令，那么 CPU 会在执行完该设置 SS 的的指令后再执行多一条指令【其具体原因会在本课程之后的内容中介绍】。

二、实验任务

1.使用 Debug 将下面的程序段写入内存，用 T 命令逐条执行，根据指令执行后的实际运行结果填空【注：debug 默认采用 16 进制，因此不需要输入 16 进制数的后缀 h；分号后面的内容为注释，不需要输入 debug 中】。

```
mov ax,ffffh
mov ds,ax          ds=ffffh
mov ax,2200h
mov ss,ax       ss=2200h
mov sp,0100h
mov ax,[0]              ;ax = c0ea
add ax,[2]              ;ax = c0ea+0012=c0fc
mov bx,[4]              ;bx = 30f0
mov bx,[6]              ;bx = 2f31
push ax                 ;sp = fe ;修改的内存单元的地址是2200:fe,内容为c0fc
push bx                 ;sp = fc ;修改的内存单元的地址是2200:fc,内容为2f31
pop ax                  ;sp = fe ;ax= 2f31
pop bx                  ;sp = 100 ;bx= c0fc
push [4]                ;sp = fe ;修改的内存单元的地址是2200:fe,内容为30f0
push [6]                ;sp = fc ;修改的内存单元的地址是2200:fc,内容为2f31
```

```
-a 2003:00
mov  ax,073f
 mov ss,ax
mov sp,0120

mov cx,0010
mov dx,00bc

  push cx
  push dx
   pop cx
   pop dx

mov ax,2001
 mov ds,ax
 mov [0],cx
 mov [2],dx

    -r cs
    2003
    -r ip
    0
```

2.编写汇编语言程序，实现以下功能：将 073F:0100~073F:011f 这段空间当作栈，初始状态栈为空，设置 CX=10H，DX=BCH,利用栈交换 CX 和 DX 中的数据，完成交换后将 CX、DX 中的内容依次写入内存单元 20010H~20013H 中。

四、实验报告提交要求

需提交实验任务 2 的实验报告（注：可用 d 命令查看内存单元存放的值）