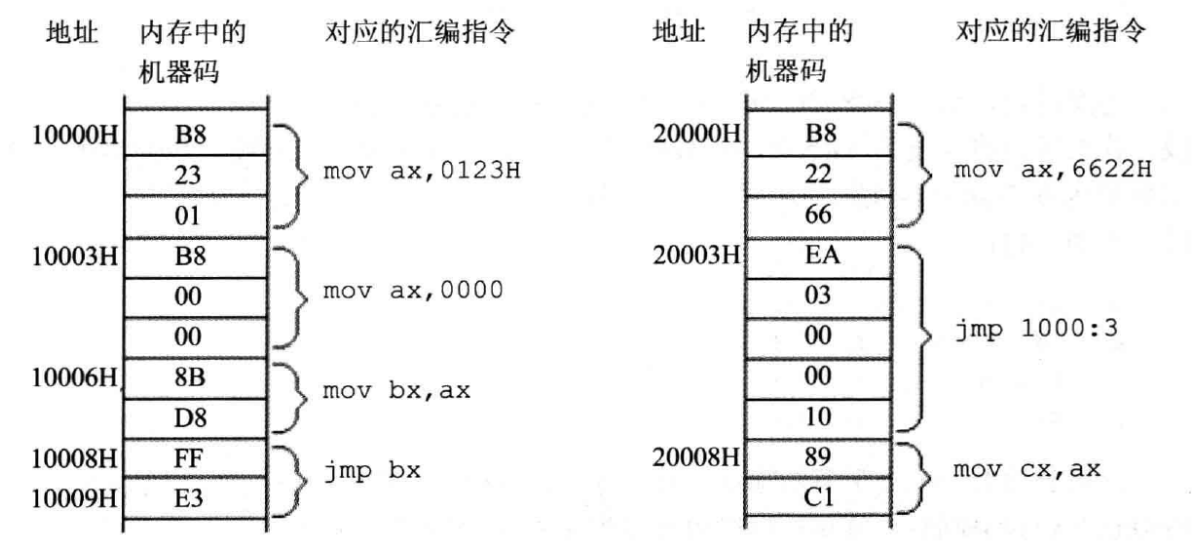


修改CS和IP

- 同时修改cs和ip: `jmp 段地址:偏移地址`
- 只修改ip: `jmp 寄存器`

如图所示：CPU初始状态CS=2000H，IP=0000H

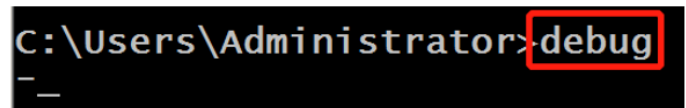
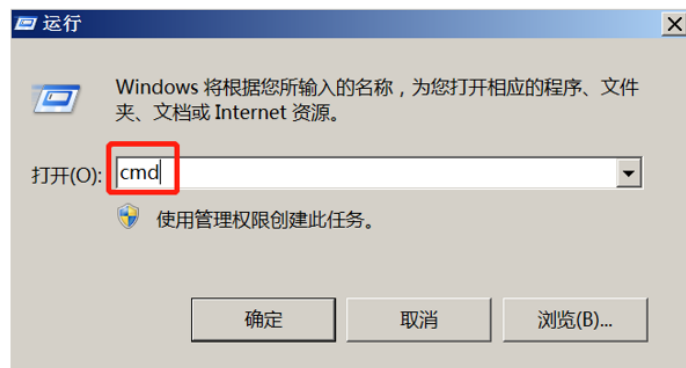


Debug调试

常用指令

- R命令查看、改变CPU寄存器的内容
- D命令查看内存中的内容
- E命令改写内存中的内容
- U命令将内存中的机器指令翻译成汇编指令
- T命令执行一条机器指令
- A命令以汇编指令格式在内存中写入一条机器指令

进入Debug



■ R命令查看寄存器内容

```
C:\Users\Administrator>debug
-r
AX=0000 BX=0000 CX=0000 DX=0000 SP=FFEE BP=0000 SI=0000 DI=0000
DS=0B09 ES=0B09 SS=0B09 CS=0B09 IP=0100 NV UP EI PL NZ NA PO NC
0B09:0100 F6C780 TEST BH,80
-r ax
AX 0000
:1111
-r
AX=1111 BX=0000 CX=0000 DX=0000 SP=FFEE BP=0000 SI=0000 DI=0000
DS=0B09 ES=0B09 SS=0B09 CS=0B09 IP=0100 NV UP EI PL NZ NA PO NC
0B09:0100 F6C780 TEST BH,80
```

■ CS:IP所指向的内存单元处存放着机器码F6C780

■ 对应汇编指令 TEST BH,80

■ D命令查看内存中内容

```
C:\Users\Administrator>debug
-d
0B09:0100 F6 C7 80 74 05 C6 06 7D-97 01 E9 2D 01 3A C3 75 ...t...}...-...:u
0B09:0110 05 80 CF 80 EB D4 3C 0D-75 03 E9 18 34 00 F8 0A .....<.u...4...
0B09:0120 96 75 03 E9 17 01 B2 3A-38 14 75 1D 80 3E 0C 98 .u...:8.u...>..
0B09:0130 01 75 03 E8 23 E1 E8 5C-01 AC E8 58 01 89 3E 4E .u..#...\...X...>N
0B09:0140 99 C6 06 50 99 00 E9 B3-00 89 3E 4E 99 C6 06 50 ...P.....>N...P
0B09:0150 99 00 80 3E 0C 98 01 75-1D E8 8F E3 75 18 50 A0 ...>...u...u.P.
0B09:0160 2E 96 04 41 E8 2E 01 B0-3A E8 29 01 58 89 3E 4E ...A.....).X.>N
0B09:0170 99 C6 06 50 99 00 E8 B6-E0 74 06 E8 17 01 AC EB ...P.....t.....
-d 1000:0
1000:0000 20 20 20 20 20 20 20 20-20 20 00 00 00 00 00 00 .....
1000:0010 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
1000:0020 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
1000:0030 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
1000:0040 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
1000:0050 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
1000:0060 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
1000:0070 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
-e 1000:0 1 2 3 4 5 6 7 8 9 A B C
-d 1000:0 f
1000:0000 01 02 03 04 05 06 07 08-09 0A 0B 0C 00 00 00 00 .....
```

■ E命令将机器码写入内存

```
-e 1000:0 b8 01 00 b9 02 00 01 c8
-d 1000:0 2f
1000:0000 B8 01 00 B9 02 00 01 C8-09 0A 0B 0C 00 00 00 00
1000:0010 01 61 6D 2B 6E 63 2B 2B-00 00 00 00 00 00 00 00
1000:0020 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
-u 1000:0
1000:0000 B80100      MOV     AX,0001
1000:0003 B90200      MOV     CX,0002
1000:0006 01C8        ADD     AX,CX
1000:0008 090A        OR      [BP+SI],CX
1000:000A 0B0C        OR      CX,[SI]
1000:000C 0000        ADD     [BX+SI],AL
1000:000E 0000        ADD     [BX+SI],AL
1000:0010 01616D      ADD     [BX+DI+6D],SP
1000:0013 2B6E63      SUB     BP,[BP+63]
1000:0016 2B2B        SUB     BP,[BP+DI]
1000:0018 0000        ADD     [BX+SI],AL
1000:001A 0000        ADD     [BX+SI],AL
1000:001C 0000        ADD     [BX+SI],AL
1000:001E 0000        ADD     [BX+SI],AL
```

机器码	对应的汇编指令
b80100	mov ax, 0001
b90200	mov cx, 0002
01c8	add ax, cx

实验任务1

- 将下面三条命令写入从2000:0开始的内存单元中，利用这三条指令计算2的8次方

■ mov ax, 1 ■ add ax, ax ■ jmp 2000:0003

```
-a 2000:0
2000:0000 mov ax, 1
2000:0003 add ax, ax
2000:0005 jmp 2000:0003
2000:0007
-r cs
CS 0B09
:2000
-r ip
IP 0100
:0
-t

AX=0001 BX=0000 CX=0000 DX=0000 SP=FFEE BP=0000 SI=0000 DI=0000
DS=0B09 ES=0B09 SS=0B09 CS=2000 IP=0003 NV UP EI PL NZ NA PO NC
2000:0003 01C0      ADD     AX,AX
```

实验任务2

- 在PC机主板的ROM中写有一个生产日期，在内存FFF00H~FFFFFH的某几个单元中，请找到这个生产日期并试图改变它。

```
-d fff0:0 ff
FFF0:0000 EF 00 F5 65 F0 4D F8 41-F8 59 EC 39 E7 59 F8 2E ...e.M.A.Y.9.Y..
FFF0:0010 E8 D2 EF 59 FF F2 E6 6E-FE 53 FF 53 FF A4 F0 C7 ...Y...n.S.S...
FFF0:0020 EF 00 00 32 F2 E2 F5 66-0D 66 0D 66 0D 73 84 66 ...2...f.f.f.s.f
FFF0:0030 0D 09 F5 E9 DC F5 E8 F0-EE CB 50 B0 00 E6 43 90 .....P...C.
FFF0:0040 90 E4 40 90 90 8A E0 E4-40 86 C4 8B F8 58 C3 00 ..@.....@...X..
FFF0:0050 00 00 00 CF E9 AD ED FF-E7 E9 71 9E E9 69 9E 50 .....q..i.P
FFF0:0060 56 2E 03 36 A8 FE 2E 8B-34 2E 03 36 A8 FE B4 0E V..6...4..6....
FFF0:0070 2E AC 0A C0 74 04 CD 10-EB F6 5E 58 C3 FA B4 0B ....t.....^X...
FFF0:0080 E8 96 45 24 57 E8 A8 45-CB 00 00 00 00 00 00 00 ...E$W..E.....
FFF0:0090 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
FFF0:00A0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
FFF0:00B0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
FFF0:00C0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
FFF0:00D0 00 00 00 00 00 00 00 00-00 00 00 00 00 E8 93 FE .....
FFF0:00E0 CB 00 00 00 E9 09 8C 00-00 00 00 00 00 00 00 .....
FFF0:00F0 EA 5B E0 00 F0 30 34 2F-31 33 2F 31 38 00 FC 57 .[...04/13/18..W
-e ffff:5
FFFF:0005 30.31
-e ffff:6
FFFF:0006 34.25
-d ffff:0 f
FFFF:0000 EA 5B E0 00 F0 31 25 2F-31 33 2F 31 38 00 FC 57 .[...1%/13/18..W
```

实验任务3

■ 向内存从B8100H开始的单元中填写数据，如：

-e B810:0000 01 01 02 02 03 03 04 04

```
Administrator: C:\Windows\system32\cmd.exe - debug
-d fff0:0 ff
FFF0:0000 EF 00 F5 65 F0 4D F8 41-F8 59 EC 39 E8 A4 F8 2E ...e.M.A.Y.9.Y..
FFF0:0010 E8 D2 EF 59 FF F2 E6 6E-FE 53 FF 53 FF A4 F0 C7 ...Y...n.S.S...
FFF0:0020 EF 00 00 32 F2 E2 F5 66-0D 66 0D 66 0D 73 84 66 ...2...f.f.f.s.f
FFF0:0030 0D 09 F5 E9 DC F5 E8 F0-EE CB 50 B0 00 E6 43 90 .....P...C.
FFF0:0040 90 E4 40 90 90 8A E0 E4-40 86 C4 8B F8 58 C3 00 ..@.....@....X..
FFF0:0050 00 00 00 CF E9 AD ED FF-E7 E9 71 9E E9 69 9E 50 .....q..i.P
FFF0:0060 56 2E 03 36 A8 FE 2E 8B-34 2E 03 36 A8 FE B4 0E V..6....4..6....
FFF0:0070 2E AC 0A C0 74 04 CD 10-EB F6 5E 58 C3 FA B4 0B ....t.....^X....
FFF0:0080 E8 96 45 24 57 E8 A8 45-CB 00 00 00 00 00 00 00 ..E$w..E.....
FFF0:0090 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
FFF0:00A0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
FFF0:00B0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
FFF0:00C0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
FFF0:00D0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
FFF0:00E0 CB 00 00 00 E9 09 8C 00-00 00 00 00 00 00 00 .....
FFF0:00F0 EA 5B E0 00 F0 30 34 2F-31 33 2F 31 38 00 FC 57 .[...04/13/18..w
-e ffff:5
FFFF:0005 30.31
-e ffff:6
FFFF:0006 34.25
-d ffff:0 f
FFFF:0000 EA 5B E0 00 F0 31 25 2F-31 33 2F 31 38 00 FC 57 .[...1%/13/18..w
-
-e B810:0000 01 01 02 02 03 03 04 04
-e B810:0000 05 15 25 35 45 55 65 75
```