

由源程序到程序运行

贺利坚 主讲



汇编语言程序设计
Assembly Language

由写出源程序到执行可执行文件的过程

文本编辑



源程序文件 .asm

```
...  
mov ax, 0123H  
mov bx, 0456H  
add ax, bx  
...
```

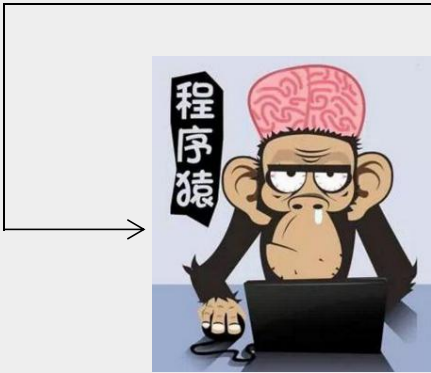


连接

可执行文件 .exe

相关的描述信息

...
B82301 BB5604
01DB
...



编译

目标文件 .obj

```
...  
B82301 BB5604  
01DB  
...
```



运行程序



计算机

编辑源程序

p4-1.asm - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
assume cs:codesg
codesg segment
start: mov ax,0123H
      mov bx,0456H
      add ax,bx
      add ax,ax
```

File Edit Search View Options Help

UNTITLED1

```
assume cs:codesg

codesg segment
    start:mov ax,0123h
           mov bx,0456h
           add ax,bx
           add ax,ax

           mov ax,4c00h
           int 21h
```

D:\masm\p4-1.asm * - EditPlus

文件(F) 编辑(E) 视图(V) 搜索(S) 文档(D) 管理工程 工具(T)

浏览器(B) Zen Coding(Z) 窗口(W) 帮助(H)

目录 素材

[D:] 新加卷

- D:\
- masm
- ex

p15-3.asm
P15-3.EXE
P15-3.OBJ
p4-1.asm

所有文件 (*.*)

p4-1.asm

```
1  assume cs:codesg
2  codesg segment
3      mov ax,0123H
4      mov bx,0456H
5      add ax,bx
6      add ax,ax
7
8      mov ax,4c00h
9      int 21h
10 codesg ends
11 end
```

需要帮助, 请按 F1 键 行 10 列 12 11 00 PC

test - Microsoft Visual C++ [break] - [test.asm]

File Edit View Insert Project Debug Tools Window Help

[Globals] [All global members] [No members - Create New Class...]

Workspace 'test': 1 prc

- test files
 - Source Files
 - test.asm
 - Header Files
 - Resource Files

```
.386
.model flat, stdcall
option casemap:none
; 说明程序中用到的库、函数原型和常量
includelib msvcrt.lib
printf      PROTO C :ptr sbyte, :vararg
; 数据区
.data
szMsg      byte "Hello World!", 0ah, 0
; 代码区
.code
start:
    mov     eax, OFFSET szMsg
    invoke  printf, eax
    ret
end
```

Address:	0x00404000
00404000	48 65 6C 6C 6F 20 57 6F Hello Wo
00404008	72 6C 64 21 00 00 00 00 rld!...
00404010	00 00 00 00 00 00 00 00
00404018	00 00 00 00 00 00 00 00
00404020	00 00 00 00 00 00 00 00
00404028	00 00 00 00 00 00 00 00
00404030	00 00 00 00 00 00 00 00
00404038	00 00 00 00 00 00 00 00
00404040	00 00 00 00 00 00 00 00
00404048	00 00 00 00 00 00 00 00
00404050	00 00 00 00 00 00 00 00
00404058	00 00 00 00 00 00 00 00
00404060	00 00 00 00 00 00 00 00
00404068	00 00 00 00 00 00 00 00

Name	Value
szMsg	0x48 'H'
EAX	0x00404000

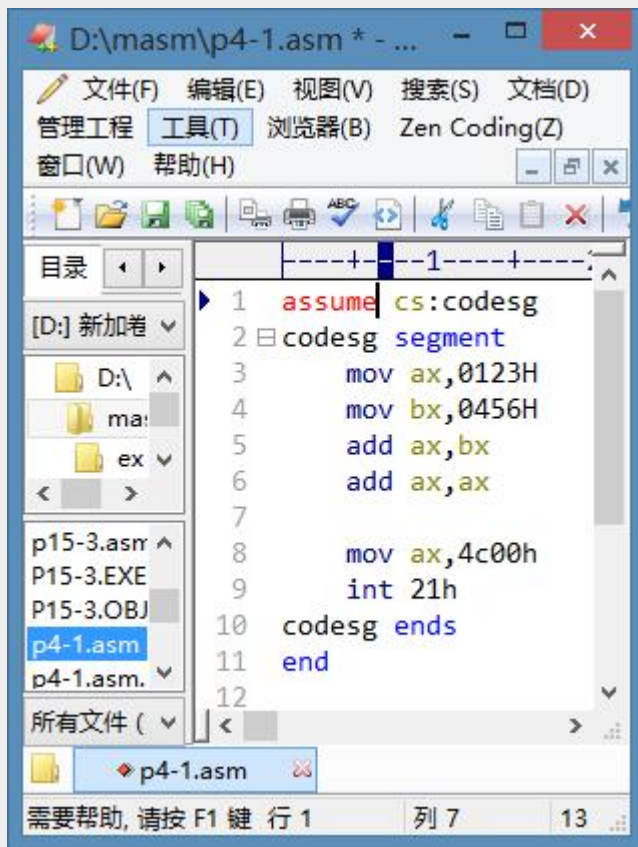
EAX = 00404000
EBX = 7FFDF000
ECX = 00000101
EDX = FFFFFFFF
ESI = 00000000
EDI = 00000000
EIP = 00401015
ESP = 0012FFC4
EBP = 0012FFF0
EFL = 00000246 CS = 001B
DS = 0023 ES = 0023
SS = 0023 FS = 0038
GS = 0000 OU=0 UP=0 EI=1
PL=0 ZR=1 AC=0 PE=1 CY=0

Loaded 'D:\WINNT\system32\msvcrt.dll', no matching symbolic information found.
Loaded 'D:\WINNT\system32\KERNEL32.DLL', no matching symbolic information found.

Build Debug Find in Files 1 Find in Files 2 Rg

Break at location breakpoint Ln 14, Col 1 REC COL OVR READ

编译



```
C:\>masm p4-1.asm
Microsoft (R) Macro Assembler Version 5.00
Copyright (C) Microsoft Corp 1981-1985, 1987. All rights reserved.
```

```
Object filename [p4-1.OBJ]:
Source listing [NUL.LST]:
Cross-reference [NUL.CRF]:

51798 + 464746 Bytes symbol space free
```

```
0 Warning Errors
0 Severe Errors
```

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

```
Source filename [ASM]: p4-1.asm
Object filename [p4-1.OBJ]:
Source listing [NUL.LST]:
Cross-reference [NUL.CRF]:

51798 + 464746 Bytes symbol space free
```

```
0 Warning Errors
0 Severe Errors
```

p4-1.asm	2017-2-5 22:20	ASM 文件	1 KB
P4-1.OBJ	2017-2-5 22:20	OBJ 文件	1 KB

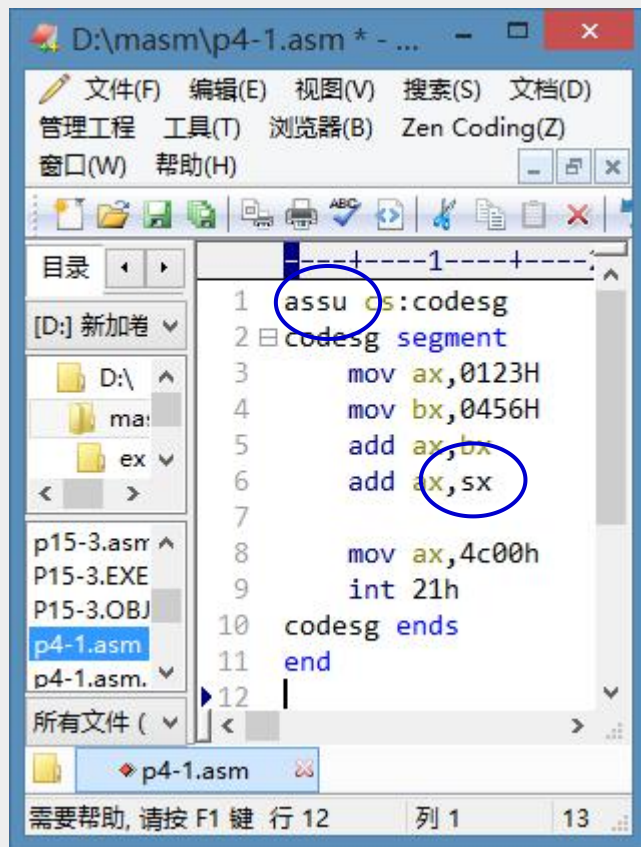
目标文件 (*.OBJ) 是我们对一个源程序进行编译要得到的最终结果。

列表文件 (*.LST) 是编译器将源程序编译为目标文件的过程中产生的中间结果。

交叉引用文件 (*.CRF) 同列表文件一样，是编译器将源程序编译为目标文件过程中产生的中间结果。

对源程序的编译结束，编译器输出的最后两行告诉我们这个源程序没有警告错误和必须要改正的错误。

提示语法错误



```
C:\>masm p4-1.asm
Microsoft (R) Macro Assembler Version 5.00
Copyright (C) Microsoft Corp 1981-1985, 1987. All rights reserved.

Object filename [p4-1.OBJ]:
Source listing [NUL.LST]:
Cross-reference [NUL.CRF]:
p4-1.asm(1): error A2105: Expected: instruction or directive
p4-1.asm(3): error A2062: Missing or unreachable CS
p4-1.asm(6): error A2009: Symbol not defined: SX

51798 + 464746 Bytes symbol space free

0 Warning Errors
3 Severe Errors
```

两类错误

- ✗ Severe Errors
- ✗ 找不到所给出的源程序文件。

```
C:\>masm p4-1.asm;
Microsoft (R) Macro Assembler Version 5.00
Copyright (C) Microsoft Corp 1981-1985, 1987. All rights reserved.

51798 + 464746 Bytes symbol space free

0 Warning Errors
0 Severe Errors

C:\>
```

命令后加 ; 以简化过程

连接

```
C:\>link p4-1




Microsoft (R) Overlay Linker  Version 3.60
Copyright (C) Microsoft Corp 1983-1987.  All rights reserved.

Run File [P4-1.EXE]:
List File [NUL.MAP]:
Libraries [.LIB]:
LINK : warning L4021: no stack segment
```

```
C:\>link

Microsoft (R) Overlay Linker  Version 3.60
Copyright (C) Microsoft Corp 1983-1987.  All rights reserved.

Object Modules [.OBJ]: p4-1
Run File [P4-1.EXE]:
List File [NUL.MAP]:
Libraries [.LIB]:
LINK : warning L4021: no stack segment
```

 p4-1.asm	2017-2-5 22:20	ASM 文件	1 KB
 P4-1.EXE	2017-2-6 15:54	应用程序	1 KB
 P4-1.OBJ	2017-2-5 22:20	OBJ 文件	1 KB


```
C:\>link p4-11

Microsoft (R) Overlay Linker  Version 3.60
Copyright (C) Microsoft Corp 1983-1987.  All rights reserved.

Run File [P4-11.EXE]:
List File [NUL.MAP]:
Libraries [.LIB]:
LINK : fatal error L1093: P4-11.OBJ : object not found
```

 可执行文件(.EXE)是我们对一个程序进行连接要得到的最终结果。

 映像文件(.MAP)是连接程序将目标文件连接为可执行文件过程中产生的中间结果。

 库文件(.LIB)里包含了一些可以调用的子程序，如果我们的程序中调用了某一个库文件中的子程序，就需要在连接的时候，将这个库文件和我们的目标文件连接到一起，生成可执行文件。

 no stack segment，一个“没有栈段”的警告错误，可以不理睬这个错误。

 连接中可能会遭遇错误

 例：object nor found —— 找不到对象

```
C:\>link p4-1;

Microsoft (R) Overlay Linker  Version 3.60
Copyright (C) Microsoft Corp 1983-1987.  All rights reserved.

LINK : warning L4021: no stack segment
```

命令后加；
以简化过程

执行可执行程序

```
C:\>dir
Directory of C:\.
.           <DIR>           06-02-2017  15:54
..          <DIR>           01-01-1980   0:00
EX          <DIR>           03-02-2017   8:32
4-1        ASM             193 05-02-2017  19:25
4-1        EXE             527 05-02-2017  19:26
4-1        OBJ              68 05-02-2017  19:25
DEBUG      EXE            20,634 10-01-2000  20:00
DESKTOP    INI              317 19-10-2008  14:34
EDIT       COM             69,886 10-01-2000  20:00
EDIT       EXE             30,776 04-04-1996  13:30
EDLIN      COM              4,608 08-03-1983  12:00
LINK       EXE             64,992 21-05-1992  10:22
MASM       EXE            103,184 21-05-1992  10:21
P4-1       ASM              178 05-02-2017  22:20
P4-1       EXE             527 06-02-2017  16:06
P4-1       OBJ              69 05-02-2017  22:20
    13 File(s)            295,959 Bytes.
     3 Dir(s)            262,111,744 Bytes free.

C:\>p4-1

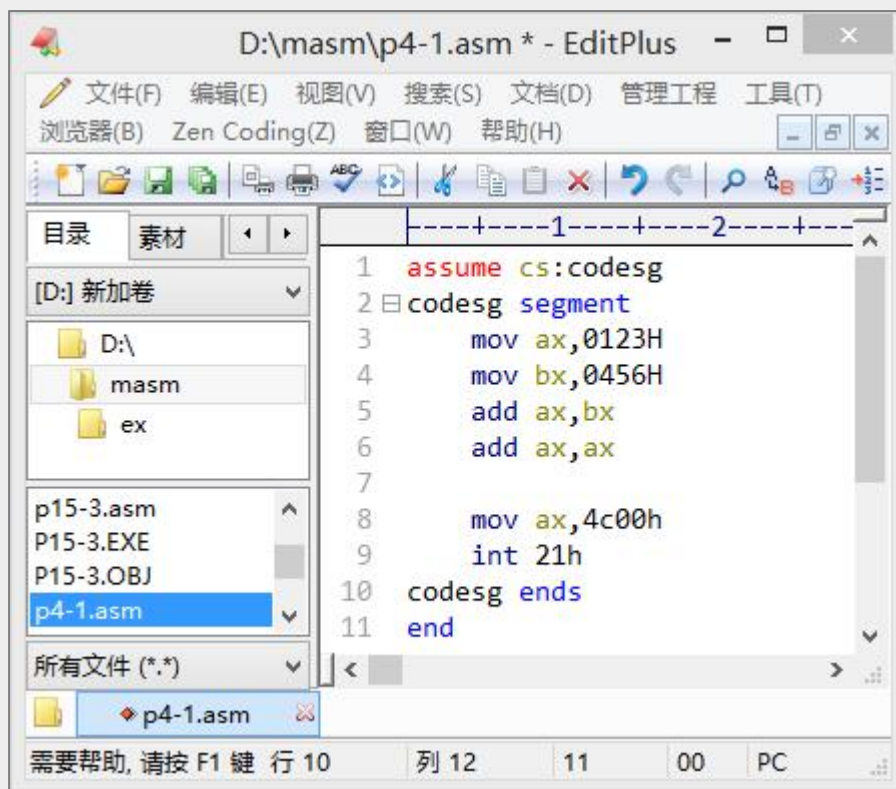
C:\>
```

🖥️ 我们的程序没有像显示器输出任何信息。

程序只是做了一些将数据送入寄存器和加法的操作，而这些事情，我们不可能从显示屏上看出来。

🖥️ 程序执行完成后，返回，屏幕上再次出现操作系统的提示符。

小结



```
C:\>masm p4-1.asm
Microsoft (R) Macro Assembler Version 5.00
Copyright (C) Microsoft Corp 1981-1985, 1987. All rights reserved.

Object filename [p4-1.OBJ]:
Source listing [NUL.LST]:
Cross-reference [NUL.CRF]:

51798 + 464746 Bytes symbol space free

0 Warning Errors
0 Severe Errors
```

```
C:\>link p4-1

Microsoft (R) Overlay Linker Version 3.60
Copyright (C) Microsoft Corp 1983-1987. All rights reserved.

Run File [P4-1.EXE]:
List File [NUL.MAP]:
Libraries [.LIB]:
LINK : warning L4021: no stack segment
```

```
C:\>p4-1
```

```
C:\>
```

源文件
.asm






目标文件
.obj

目标文件
.obj



可执行文件
.exe

 p4-1.asm	2017-2-5 22:20	ASM 文件	1 KB
 P4-1.EXE	2017-2-6 15:54	应用程序	1 KB
 P4-1.OBJ	2017-2-5 22:20	OBJ 文件	1 KB

... B82301 BB5604 01DB ...

