```
1           ;代码清单11-1
2           ;文件名：c11_mbr.asm
3           ;文件说明：硬盘主引导扇区代码
4           ;创建日期：2011-5-16 19:54
5
6           ;设置堆栈段和栈指针
7           mov ax,cs
8           mov ss,ax
9           mov sp,0x7c00
10
11          ;计算GDT所在的逻辑段地址
12          mov ax,[cs:gdt_base+0x7c00]         ;低16位
13          mov dx,[cs:gdt_base+0x7c00+0x02]    ;高16位
14          mov bx,16
15          div bx
16          mov ds,ax                           ;令DS指向该段以进行操作
17          mov bx,dx                           ;段内起始偏移地址
18
19          ;创建0#描述符，它是空描述符，这是处理器的要求
20          mov dword [bx+0x00],0x00
21          mov dword [bx+0x04],0x00
22
23          ;创建#1描述符，保护模式下的代码段描述符
24          mov dword [bx+0x08],0x7c0001ff
25          mov dword [bx+0x0c],0x00409800
26
27          ;创建#2描述符，保护模式下的数据段描述符（文本模式下的显示缓冲区）
28          mov dword [bx+0x10],0x8000ffff
29          mov dword [bx+0x14],0x0040920b
30
31          ;创建#3描述符，保护模式下的堆栈段描述符
32          mov dword [bx+0x18],0x00007a00
33          mov dword [bx+0x1c],0x00409600
34
35          ;初始化描述符表寄存器GDTR
36          mov word [cs: gdt_size+0x7c00],31   ;描述符表的界限（总字节数减一）
37
38          lgdt [cs: gdt_size+0x7c00]
39
40          in al,0x92                          ;南桥芯片内的端口
41          or al,0000_0010B
42          out 0x92,al                         ;打开A20
43
44          cli                                 ;保护模式下中断机制尚未建立，应
45                                              ;禁止中断
46          mov eax,cr0
47          or eax,1
48          mov cr0,eax                         ;设置PE位
49
50          ;以下进入保护模式... ...
51          jmp dword 0x0008:flush              ;16位的描述符选择子：32位偏移
52                                              ;清流水线并串行化处理器
53          [bits 32]
```

```
54
55     flush:
56           mov cx,00000000000_10_000B          ;加载数据段选择子(0x10)
57           mov ds,cx
58
59           ;以下在屏幕上显示"Protect mode OK."
60           mov byte [0x00],'P'
61           mov byte [0x02],'r'
62           mov byte [0x04],'o'
63           mov byte [0x06],'t'
64           mov byte [0x08],'e'
65           mov byte [0x0a],'c'
66           mov byte [0x0c],'t'
67           mov byte [0x0e],' '
68           mov byte [0x10],'m'
69           mov byte [0x12],'o'
70           mov byte [0x14],'d'
71           mov byte [0x16],'e'
72           mov byte [0x18],' '
73           mov byte [0x1a],'O'
74           mov byte [0x1c],'K'
75
76           ;以下用简单的示例来帮助阐述32位保护模式下的堆栈操作
77           mov cx,00000000000_11_000B          ;加载堆栈段选择子
78           mov ss,cx
79           mov esp,0x7c00
80
81           mov ebp,esp                         ;保存堆栈指针
82           push byte '.'                       ;压入立即数（字节）
83
84           sub ebp,4
85           cmp ebp,esp                         ;判断压入立即数时，ESP是否减4
86           jnz ghalt
87           pop eax
88           mov [0x1e],al                       ;显示句点
89
90    ghalt:
91           hlt                                 ;已经禁止中断，将不会被唤醒
92
93 ;-------------------------------------------------------------------------------
94
95           gdt_size         dw 0
96           gdt_base         dd 0x00007e00      ;GDT的物理地址
97
98           times 510-($-$$) db 0
99                            db 0x55,0xaa
```