call指令

当CPU执行 `call 标号` 时，相当于进行：

- push IP
- jmp near ptr 标号

当CPU执行 `call far ptr 标号` 时，相当于进行：

- push CS
- push IP
- jmp far ptr 标号

ret和retf指令

- ret：`pop IP`
- retf: `pop IP` `pop CS`

堆栈平衡

- EBP栈底指针
- ESP栈顶指针
- 进入call前与执行call后EBP和ESP的值不变
- push ebp：相当于 `sub,esp,4` 和 `mov [esp],ebp`
- pop ebp：相当于 `mov ebp,[esp]` 和 `add esp, 4`

补充指令

XCHG

- 交换指令只可以在寄存器之间、寄存器与存储器之间进行
- 两个操作数长度必须相等
- 例如：`XCHG AX,BX`

NOT

- 取反指令