IA-32 寻址模式

立即寻址：指令直接给出操作数

寄存器寻址：寄存器R内容就是操作数

存储器寻址：（段寄存器）+ 偏移量 + 基址寄存器 + 变址寄存器 \* 比例系数(S)

通常，S= 1/2/4/8

相对寻址：PC + 偏移量(A)



|  |  |
| --- | --- |
| 指令 | 实现思路/细节 |
| Push |  |
| Pop | Mov from (R[sp]) |
| Mul | 1. 如果一个操作数，那么另一个操作数在AL/AX/EAX中，结果存放在AX/DX-AX/EDX-EAX中 2. 如果两个操作数DST , SRC 不说自明 3. 如果三个操作数，REG, SRC, IMM   把SRC与IMM相乘，存入REG |
| Div | 同上，低位结果为商，高位为余数 |
| Test | 与指令，不返回结果 |
| 控制转移 | 段间转移（也叫远转移far）  段内转移（分为近转移(near)、短转移(short)）  此外，两种转移都有直接转移、间接转移（取reg的值）之分  目的地址计算方式——相对转移（相对EIP）、绝对转移  IA-32系统中，段内直接转移都是相对转移、段内间接转移都是绝对转移 |
| （控制转移中）条件转移 | Ja jb 表示无符号整数A,B关系  Jg jl 表示有符号整数A,B关系 |