反汇编指令

入栈出栈指令

- `push` ： 入栈
- `pushad` ： 将eax、ecx、edx、ebx、esp、ebp、esi、edi 全部压入栈中
- `pop` ： 出栈
- `popad` ： 将eax、ecx、edx、ebx、esp、ebp、esi、edi 全部弹出

整数运算指令

- `add` ： 加
- `inc` ： 自增1，自身加1
- `dec` ： 自减1
- `sub` ： 减
- `mul` ： 无符号乘
- `imul` ： 有符号乘
- `div` ： 无符号除
- `idiv`： 有符号除
- `cmp` ： 整数比较，相当于sub，但是不保存相减后的结果，只改变标志位（AF、CF、DF、PF、SF、ZF）
- `test` ： 判断寄存器的值是否为0，如：`test eax,eax` 判断寄存器eax是否为0

条件跳转指令

无符号数条件转移指令

指令	关系	检测条件	功能描述
JE/JZ	==	ZF=1	Jump Equal or Jump Zero 等于转移
JNE/JNZ	!=	ZF=0	Jump Not Equal or Jump Not Zero 不等于时转移
JA/JNBE	>	CF=0 && ZF=0	Jump Above or Jump Not Below or Equal 高于时转移
JAE/JNB	>=	CF=0	Jump Above or Equal or Jump Not Below 高于或等于跳转
JB/JNAE	<	CF=1	Jump Below or Jump Jump Not Above or Equal 低于转移
JBE/JNA	<=	CF=1 || ZF=1	Jump Below or Equal or Jump Not Above 低于或等于转移

有符号条件转移指令

指令	关系	检测条件	功能描述
JE/JZ	==	ZF=1	Jump Equal or Jump Zero 等于转移
JNE/JNZ	!=	ZF=0	Jump Not Equal or Jump Not Zero 不等于时转移
JG/JNLE	>	SF=OF && ZF=0	Jump Greater or Jump Not Less or Equal 高于时转移
JGE/JNL	>=	SF=OF || ZF=1	Jump Greater or Equal or Jump Not Less 高于或等于跳转
JL/JNGE	<	SF!=OF && ZF=0	Jump Less or Jump Jump Not Greater or Equal 低于转移
JLE/JNG	<=	SF!=OF || ZF=1	Jump Less or Equal or Jump Not Greater 低于或等于转移

特殊算数标志位条件转移指令

指令	检测条件	功能描述
JC/JB/JNAE	CF=1	Jump Carry 有进（借）位时转移
JNC/JNB/JAE	CF=0	Jump Not Carry 无进（借）位时转移

常用浮点运算、浮点栈

- `fld`：将数据压入到浮点栈中，相当于整数的push操作
- `fstp`：浮点数出栈，相当于整数的pop操作
- `fadd`：加
- `fsub`：减
- `fmul`：无符号数乘
- `fimul`：有符号数乘

- `fdiv`：无符号数除
- `fidiv`：有符号数除

补充

- `mov`：移动、赋值
- `lea`：去掉地址的方括号，再赋值
- `rol`：左移
- `xor`：异或
- `and`：与
- `or`：或
- `not`：非

> ⚠️注意：带方括号的数才是地址值，不带方括号的就是普通的数值，即使它长得像一个地址值