助记符怎么写 两字节 四字节 六字节 八字节

串行通信的校验位如何识别

寻址方式

mov 操作数的限制

add sub 逻辑位运算 和mov限制相同

mul div 后面只能跟 寄存器或者存储单元

16位间接寻址只能用BX BP SI DI

[AX]是错的

中断

实模式和保护模式下的中断都有256种

push pop执行对于esp的变化情况

16进制数规范写法

第一位是字母，前面加0

cpu 地址总线 数据总线

数据总线：同时传输数据的并行能力

地址总线：寻址范围 2^n

总频 外频 倍频

总频=外频×倍频

不会影响CF标志位的指令

inc dec not 各种jmp

特权级

CPL：CS的最低两位，表示当前运行程序的特权级

RPL：段选择符的最低两位，表示请求访问特权级

DPL：在段描述中，表示允许访问该段的最低特权级

浮点运算

real8 real4代表什么

real8 双精度浮点数 64位

real4 单精度浮点数 32位

real8 3.2

qword 3. 浮点数3.0

qword 3 整数3

如何计算内存的带宽

带宽=位宽×总线频率/8 单位 MB/s

定时器 计数器

对某个频率的时钟信号进行计数

1MHz的信号 1ms计数一次 问计数值

1ms对应频率为1KHz

1M / 1K = 1K

逻辑左移

给一个寄存器，逻辑左移或者算术左移两三位，问结果

数据有关寻址方式和转移地址有关寻址结合

段内转移只改变IP或者EIP，不改变CS

段内间接转移：

Jump word ptr [bx] 从bx指向的内存单元取一个字（16位）赋给IP

Jump dword ptr [ebx] 从ebx指向的内存单元取两个字（32位）赋给EIP

段间转移的助记符超过后面的操作数长度，先改变IP/EIP，然后改变CS

段间间接转移

Jump dword ptr [bx] 从bx指向的内存单元取两个字，第一个字（16位）赋给IP，第二个字（16位）赋给CS

Jump fword ptr [ebx] 从ebx指向的内存单元取三个字，第一和第二个字（32位）赋给EIP，第三个字（16位）赋给CS

分段 分页

分页线性地址怎么转换为物理地址

10+10+12

页目录索引+页表索引+页面内偏移量

CR3寄存器给出页目录基址20位

页目录基址加上页目录索引×4得到页表描述符，高20位是页表基址

页表基址加上页表索引×4得到页描述符，高20位是页面基址

页面基址加上12位页内偏移量就是物理地址

给一个地址，从里面读出一个字或者双字的数据

小端法

100 Dup（?）定义100个

问定义了多少个字节

算术运算指令、逻辑运算指令、无符号和带符号的比较指令

判断下一个执行哪条指令

浮点运算指令

栈往下生长，地址往上增加

书上的例子

fld b 装载一个浮点数b到st（0）

fst c 把st（0）的浮点数保存到内存单元c

fmul st(0)，st（1）

fadd st（0），st（1）

单独一个fadd，st（0）和st（0）相加放到st（1），st（0）出栈

Add sub 看作无符号数和带符号数时怎样会溢出

分开判断

无符号数溢出：就看运算后最高位有没有进位或者借位，导致的CF=1，有就是溢出

带符号数溢出，就看正+正得不得负数，再看负+负得不得正数，正-负得不得负数，负-正得不得正数，得就是溢出，OF=1，如果只是正+负、正-正、负-负，就不会溢出

非flash存储介质

内存DRAM、磁盘

Flash介质

U盘、固态盘SSD

USB2.0和USB3.0的差异体现在哪里

3.0是全双工，2.0是半双工（主要）

2.0和3.0都采用了差分方式

3.0的数据驱动能力更强，数据传输速率高

RS-232C的电平标准

什么表示逻辑1：-5V到-15V

什么表示逻辑0：+5V~+15V

invoke是伪指令，需要展开成几条汇编指令

浮点运算

st（0）栈顶指针，st（i）的i是距离栈顶的长度

FPR0

浮点寄存器栈是一个循环栈，向下生长，最下面是FPR0

ST是软栈，是变化的

FPR是硬栈，是固定的，随着栈的变化，st（0）会指向不同的FPR

Loop循环次数

Cx=0时循环2^32次

指令的OR AND是在程序运行的时候执行

AND eax,ebx

指令中表达式的算术或者逻辑运算是在编译的时候完成

MOV eax, 1 AND 1

MOV eax, 4+5

Xor互换 eax和ebx

Xor eax,ebx

Xor ebx,eax

Xor eax,ebx

反汇编局部变量、全局变量、静态变量如何表示

局部变量：local temp1,temp2:dword

除法溢出：商超出寄存器表示范围，寄存器位数=除数的位数

EQU 和 =

都不占用内存

EQU只能定义一次

=可以定义多次，覆盖前面的

判断内外中断：中断是否在CPU外部

奇偶校验是RAM的，属于外部

简答题

反汇编码

对子程序的调用规则

cdecl、fastcall、stdcall

转换为对应的C语言

主程序是两次调用子程序，把调用写对，子程序写对

注意子程序的函数名前的\_\_stdcall和\_\_fastcall

主程序参数从右至左压入栈

子程序中，[EBP+8]是第一个参数[EBP+0CH]是第二个参数，+10H是第三个，四个字节一个int参数

子程序就是加减乘除

输出也要写对 打印一个什么东西