第1章

1. Turbo Debug的例子
3. 三个段：DS, SS, CS
4. 四个X,两个I，两个P
5. EIP就是TD中的小箭头

第2章

码点、有符号数、无符号数

第3章

第3.1节

《计算机系统基础》，3.1.1，位移量

第3.2节

1. 内存是有编号的格子
2. 操作数分为三类：常数、寄存器、内存
3. 寻址方式由简单到复杂：
常数，寄存器
直接，间接，变址，基址加变址

4. ESP、EBP用在堆栈段中
5. 32位寄存器(EAX等)，无限制

6. 内存示意图：画格子，写编号，填内容，标变量。常量不要填
低位放低端，高位放高端
先定位，后取n个字节

第3.3节

普通指令

1. 指令分类：传送、运算、位操作、跳转
2. 两个操作数，不能同为内存
3. 两个操作数，类型要一致，或者一个类型明确

4. 字节 * 字节 -> 字 AL * OPS -> AX
 字 * 字 -> 双字 AX * OPS -> DX, AX
5. CMP减法
 TEST是与；不要结果，只影响标志位

6. 移位指令：
 S, H, A
 R, O, C

分支和循环

1. ZF, SF, OF, CF。
   OF，超有符号范围；CF，超无符号范围
2. G/L，大于/小于，有符号；A/B，高于/低于，无符号
3. LOOP

子程序调用

1. CALL：进栈，跳转；RET：出栈
2. PROC和ENDP
3. 堆栈法传参数
4. 保护现场和恢复现场
5. 堆栈内分配局部变量

第3.4节

程序优化方法，例如：
宽字节传送、计算
高效指令：移位代替乘除2
取消分支：用分支地址表
优化循环：用寄存器控制循环
第5、6章
使用串操作指令、SIMD指令

第3.5节

第3.6节

第4章

1. 外部符号，别人定义，本地用
 全局符号，本地定义，别人用
2. 局部变量和参数不是符号
3. .o文件中的节
4. 符号解析的含义
5. 重定位的含义

第5章

流水线及优化例程

第6章

高速缓存及优化例程

第7章

IN、OUT指令
IO方式

第8章

INT、IRET指令
实模式下，中断号 * 4，中断向量的物理地址