

《汇编语言程序设计实验》注意事项

请大家在本校汇编教学网站上下载 2017 版的实验报告样例和评分原则（即：“2017 实验报告样例”和“2017 实验报告评分原则”），**上机前做好准备，需要完成实验报告中除“实验记录与分析”和“总结与体会”以外的全部内容（实验报告电子版提交时间是当次实验课的课时结束后的次日，推迟提交将影响成绩）**。上机时主要是验证所做结果是否正确，记录实验中看到的现象（如果截图，必须对截图中反映的信息给出文字说明），分析讨论各种现象的内在原理，找出错误的原因，以促进对课本知识的理解。

到机房上机要**签到、以班级为单位安排座位、检查实验报告预习情况等**；提前完成的需经过老师检查后方可离开机房。

请大家参考配套的《80X86 汇编语言程序设计上机指南》（华中科技大学出版社 2007 年）相关内容。

上机使用的**相关软件**（例如：虚拟机 DOSBOX，汇编程序 MASM60，调试工具 TD；混合编程时采用 BC31；WIN32 编程采用 MASM32）请从汇编教学网站上下载（比如 MASM60TD 的压缩包等）。在自备 U 盘里拷贝相关软件和电子版实验报告（预习报告），实验报告文件名格式：

CS1601_U201612345 张三丰_1. DOC

实验课程成绩=实验报告（70%）+现场实验操作表现（20%）+现场问答讨论（10%）

注意：考勤将影响上述现场部分的评分，无故缺勤 1/3 以上上机实验学时者，实验课程成绩为不及格。

全部实验（8 次上机完成 5 个实验）完成之后要提交实验报告的合订本纸质版，即 5 个实验报告的整合，作为终结成绩（每次实验后只需要提交电子版的实验报告，**注意**，为避免没有收到邮件，学生必须收到回复邮件后才算确认提交成功。5 个实验完毕后，提交纸质报告，是 5 个报告的合订本，外加一个统一的封面）。提交纸质版实验报告的同时，还需要将每次实验的实验报告电子版、所有源程序、执行程序一起打包提交。实验报告评分中包括实验完成质量与撰写质量。

另外请注意，从实验报告评分原则可以看出，汇编语言程序设计实验更强调实验的过程与思考，而不是把某个功能的程序调通了就完事。一个如实记录了实验过程及分析思考的实验报告的成绩，就算程序没有调通，都可能比一个程序没有问题但没有什么过程记录与思考的实验报告成绩高很多。

《汇编语言程序设计实验》

实验一任务

实验名称：实验一 编程基础

本实验课内学时 4+4，即占用两周课内实验课时，实验报告在第二次课内学时完成后的次日提交。

一. 实验目的和要求

- (1) 掌握汇编源程序编辑工具、汇编程序、连接程序、调试工具 TD 的使用；
- (2) 理解数、符号、寻址方式等在计算机内的表现形式；
- (3) 理解指令执行与标志位改变之间的关系；
- (4) 熟悉常用的 DOS 功能调用；
- (5) 熟悉分支、循环程序的结构及控制方法，掌握分支、循环程序的调试方法；
- (6) 加深对转移指令及一些常用的汇编指令的理解。

二. 实验内容

(上机实验环境说明：在机房计算机上建议大家使用 VMWare Workstation 的虚拟机环境，或者 DOSBox 虚拟机；在自己的计算机上可以使用 DOSBox 虚拟机。源程序编辑工具可以使用记事本、EDIT、或 C 语言的编辑器；汇编程序使用 MASM 6.0;连接程序使用 LINK；调试工具使用 TD；具体介绍可参见教材第 7 章及《80X86 汇编语言程序设计上机指南》，相关软件可以到教学网站上下载)

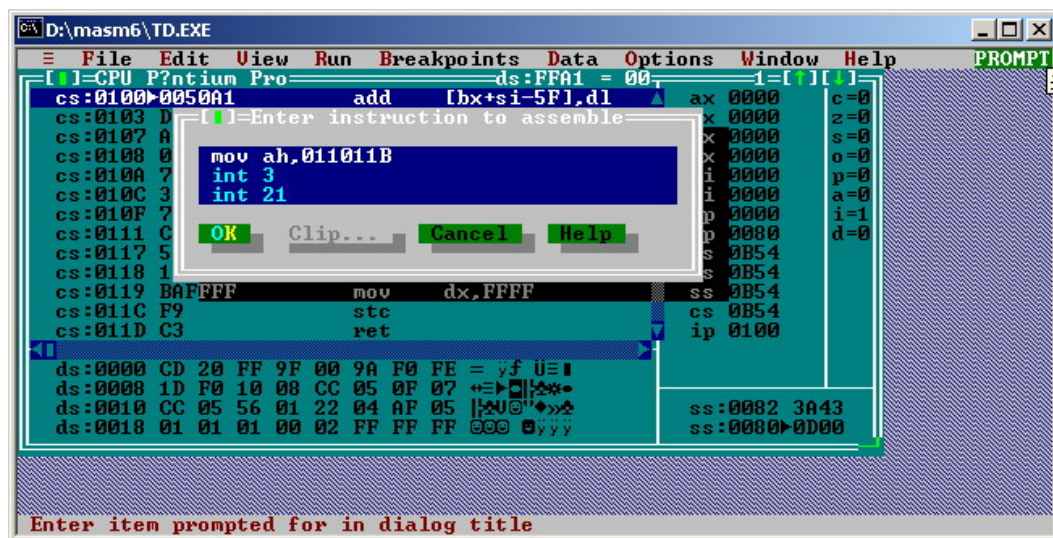
任务 1. 《80X86 汇编语言程序设计》教材中 P31 的 1.14 题。

要求：(1) 直接在 TD 中输入指令，完成两个数的求和、求差的功能。求和/差后的结果放在(AH)中。

(2) 请事先指出执行指令后(AH)、标志位 SF、OF、CF、ZF 的内容。

(3) 记录上机执行后的结果，与 (2) 中对应的内容比较。

在 TD 中输入指令语句的操作提示：将 TD 中的代码显示区置为当前区域，光标移到期望修改的行后，直接输入汇编指令；当输入了第一个字符时，TD 自动弹出如下图所示的指令编辑窗口。每输入完一条指令，按回车键，这时输入的指令即可出现在光标处，同时光标自动下移一行，以便输入下一条指令。



任务 2. 《80X86 汇编语言程序设计》教材中 P45 的 2.3 题。

要求：(1) 分别记录执行到“MOV CX, 10”和“INT 21H”之前的(BX),(BP),(SI),(DI)各是多少。

(2) 记录程序执行到退出之前数据段开始 40 个字节的內容，指出程序运行结果是否与设想的一致。

操作提示：使用 TD.EXE 调试程序时，应先单步执行各个语句，每执行一条语句，都应观察数据段中的內容以及相应寄存器的变化。首先注意观察对 DS 寄存器的赋值过程，并在 TD 的数据窗口定位待观察的数据区位置。其次，单步执行循环体两遍且正确理解了循环体语句的含义后，可在“MOV AH, 4CH”处设置断点，然后直接执行到断点处，回答(1)和(2)的问题。

任务 3. 《80X86 汇编语言程序设计》教材中 P45 的 2.4 题的改写。

要求：(1) 实现的功能不变，但对数据段中变量访问时所用到的变址寄存器采用 32 位寄存器。

(2) 记录程序执行到退出之前数据段开始 40 个字节的內容，检查程序运行结果是否与设想的一致。

(3)在 TD 代码窗口中观察并记录机器指令代码在内存中的存放形式，并与 TD 中提供的反汇编语句及自己编写的源程序语句进行对照,也与任务 2 做对比。

(相似语句记录一条即可，重点理解机器码与汇编语句的对应关系，尤其注意操作数寻址方式的编码形式，比如寄存器间接寻址、变址寻址、32 位寄存器与 16 位寄存器编码的不同、段前缀在代码里是如何表示的等)。

(4) 观察连续存放的二进制串在反汇编成汇编语言语句时，从不同字节位

置开始反汇编，结果怎样？理解 IP/EIP 指明指令起始位置的重要性。

操作提示：要让 TD 从任意指定地址开始反汇编，需要使用 TD 在代码显示区的 Goto 功能，即鼠标选中代码显示区，点击右键将显示带有 Goto 的菜单，选中 Goto 菜单项，输入 CS:XXXX 即可（XXXX 是你希望录入的偏移地址）。

任务 4. 设计实现一个网店商品信息管理的程序。

1、实验背景

有一个老板在网上开了 1 个网店 SHOP，网店里 n 种商品销售。每种商品的信息包括：商品名称（10 个字节，数据段中定义时，名称不足部分补 0），折扣（字节类型，取值 0~10；0 表示免费赠送，10 表示不打折，1~9 为折扣率；实际销售价格=销售价*折扣/10），进货价（字类型），销售价（字类型），进货总数（字类型），已售数量（字类型），推荐度【=（进货价/实际销售价格+已售数量/（2*进货数量））*128，字类型】。老板管理网店信息时需要输入自己的名字（10 个字节，数据段中定义时，不足部分补 0）和密码（6 个字节，数据段中定义时，不足部分补 0），登录后可查看商品的全部信息；顾客（无需登录）可以查看网店中每个商品除了进货价以外的信息。

例如：

```
BNAME DB 'ZHANG SAN',0 ; 老板姓名（必须是自己名字的拼音）
BPASS DB 'test',0,0 ; 密码
N EQU 30
SNAME DB 'SHOP',0 ; 网店名称，用 0 结束
GA1 DB 'PEN',7 DUP(0),10 ; 商品名称及折扣
DW 35,56,70,25,? ; 推荐度还未计算
GA2 DB 'BOOK',6 DUP(0),9 ; 商品名称及折扣
DW 进货 12,销售 30,进货总数 25,已售数量 5,? ; 推荐度还未计
```

算

```
GAN DB N-2 DUP('Temp-Value',8,15,0,20,0,30,0,2,0,?,?) ;除了 2 个已经具体定义了的商品信息以外，其他商品信息暂时假定为一样的。
```

2、功能一：提示并输入登录用户的姓名与密码

（1）使用 9 号 DOS 系统功能调用，先后分别提示用户输入姓名和密码（第一行显示将要访问的网店名称）。

（2）使用 10 号 DOS 系统功能调用，分别输入姓名和密码。输入的姓名字符串放在以 in_name 为首址的存储区中，密码放在以 in_pwd 为首址的存储区中，进入功能二的处理。

（3）若输入姓名时只是输入了回车，则将 0 送到 AUTH 字节变量中，跳过功能二，进入功能三；若在输入姓名时仅仅输入字符 q，则程序退出。

3、功能二：登录信息认证

（1）使用循环程序结构，比较姓名是否正确。若不正确，则跳到（3）。

（2）若正确，再比较密码是否相同，若不同，跳到（3）。

（3）若名字或密码不对，则提示登录失败，并回到“功能一（1）”的位置，提示并重新输入姓名与密码。

（4）若名字和密码均正确，则将 1 送到 AUTH 变量中，进到功能三。

提示：字符串比较时，当采用输入串的长度作为循环次数时，若因循环次数减为 0 而终止循环，则还要去判断网店中定义的字符串的下一个字符是否是结束符 0，若是，才能确定找到了（这样做是为了避免输入的字符串仅仅是数据段中所定义字符串的子集的误判情况）。

4、功能三：计算指定商品的推荐度。

（1）提示用户输入要查询的商品名称。若未能找到该商品，重新提示输入商品名称。若只输入回车，则回到功能一（1）。

（2）判断登录状态，若是已经登录的状态，转到（3）。否则，转到（4）。

（3）在下一行显示该商品的名称，然后回到功能一（1）。

（4）计算该商品的推荐度，然后进入功能四。

要求尽量避免溢出。

提示：使用循环程序结构，注意寻址方式的灵活使用。结果只保留整数部分。

5、功能四：将功能三计算的推荐度进行等级判断，并显示判断结果。

（1）等级显示方式：若推荐度大于 100，显示“A”；大于 50，显示“B”；大于 10，显示“C”；其他，显示“F”。

提示：使用分支程序结构，采用 2 号 DOS 系统功能调用显示结果。

（2）使用转移指令回到“功能一（1）”处（提示并输入姓名和密码）。

—————**实验内容描述完毕。以下是相关说明，请认真阅读**—————

➤ **进度提示：**

第一次上机学时必须完成任务 1 至 3，可以考虑任务 4 的部分功能；第二次上机学时完成任务 4。

➤ **学生自主变更提示：**

学生可以自行调整实验内容，但自选的内容要能完成实验目的与要求，并经老师同意。任务 4 的内容不宜自行更改太多，因后续实验还会用到。

➤ **需要解决的问题提示：**

在完成上述任务过程中，需要大家按照下面的提示检查自己是否还存在未搞清楚的问题，鼓励大家自行设置新的问题并通过实验观察来解决。（这些问题可以合适的方式纳入到自己写的实验步骤、记录与分析以及总结中）

本次实验中需要学生尝试体会与解决的操作及问题可分为三类：

1. TD 的操作（直接在 TD 内输入指令，设置断点、单步执行程序、运行到断点、运行到指定的指令、查看寄存器的内容、查看标志寄存器的某个标志位的值、查看指定的存储单元的值、查看整个程序在内存中的存放方式）；

2. 将一个汇编源程序生成一个可执行文件的步骤，包括如何读懂汇编源程序在汇编过程中产生的错误信息；编辑工具的使用（使用 Edit， notepad 等需要

注意的问题)；

3. 操作数寻址方式的改变，对目标码产生的影响； DOS 系统功能调用中应注意的问题。

各实验任务中的具体提示如下表：

任 务 编 号	序 号	学生尝试的操作
任 务 1	1	打开 TD 之后，如何在代码区输入一条指令，并且执行这条指令？
	2	如何在代码区输入若干条指令后，再从输入的第一条指令开始执行？
	3	在输入一条指令中的数据时，若以 16 进制输入，需要注意什么问题？
	4	输入指令 MOV AH, -128 并执行 查看 AH 寄存器的内容
	5	执行一条指令后，如何查看寄存器的值（含 32 位寄存器）？如何修改寄存器的值？
	6	执行一条指令后，如何查看标志寄存器的值？
	7	将 A、B 视为有符号数，运算后得到的结果、所有标志位信息，与将 A、B 视为无符号数，再次做同样运算后得到的结果、所有标志位信息进行比较，有何不同？
	8	总结加减法对标志寄存器的影响？
任 务 2 和 任 务 3	1	如何将一可执行程序调入 TD，并查看代码区？理解机器码与汇编指令之间的对应关系？
	2	如何设置断点并运行到断点？
	3	如何使程序运行到光标的当前点？（假设活动光标在代码区，指向某一条指令）
	4	如何单步执行一条指令？（多种方法）
	5	在数据区找到数据段的方法？思考：是否可以用这一方法查看代码段甚至整个程序？（至少有三种方法：(1)goto, DS: 偏移地址, (2)goto, 直接输入：段寄存器的值：偏移地址；(3)直接在数据区用光标移动查找）
	6	修改某个指定的存储单元的值，如任务 2 中的 BUF2
	7	如何查看堆栈？
	8	如何汇编一个汇编源程序并链接产生可执行代码？

	9	如何读懂源程序在汇编过程中产生的错误?
	10	使用 DOS 系统功能调用前应注意保存 AX 寄存器的值
	11	查看 BUF2 等变量在 TD 中的表示形式并总结
	12	查看寄存器间接寻址、变址寻址的汇编源程序经汇编、链接后在 TD 中的表示形式? 总结源程序的指令和 TD 中的指令差异。
	13	单步执行循环体 2 遍, 查看数据段的变化

任务 4 中, 需要解决的问题提示:

功能编号	序号	学生尝试的操作
功 能 一、二	1	如何让 9 号功能调用显示的信息放在自己希望的位置?
	2	如果在 9 号功能调用时, 带显示字符串的结尾没有 “\$” 结束符会怎样?
	3	如果在 9 号功能调用前, 未对 DS 赋值, 或者未对 DX 给予正确的值, 结果会如何?
	4	10 号功能调用时, 输入的字符数超过定义的数量时, 它是如何处理的?
	5	匹配姓名时, 如何提高匹配速度?
	6	循环或转移时, 是否有多种指令的组合方式实现?
	7	注意观察转移指令机器码的编码方法, 观察对应标号的偏移地址与该编码之间的关系。
	8	检查循环程序, 是否可能出现死循环的情况。
功 能 三、四	1	是否可以简化一下计算公式。
	2	单步观察计算过程, 结果是否正确?
	3	用 TD 直接修改数据区的数值, 使得程序对应的每个分支都能得到验证。
	4	选取特殊的值, 观察计算结果溢出的情况。

➤ 实验报告撰写的提示:

实验一的实验报告形成过程提示:

(1) 第一个 4 学时上机前, 实验报告应完成任务 3 的源程序清单 (初稿, 允许有错误)。进入实验后, 完成实验操作并记录相关结果 (可以截图), 对结果进行分析说明 (每个任务中至少要对一个你觉得比较有价值的结果进行分析说明)。

写出对任务 1 至 3 的总体结论与体会。

(2) 第二个 4 学时上机前, 实验报告应完成任务 4 的步骤描述, 程序设计思想、流程图、源程序初稿等。进入实验后, 按照步骤完成程序调试、实验操作并记录相关结果 (可以截图), 对结果进行分析说明。在任务 1 至 3 的总结基础上, 写出对任务 4 的总体结论与体会。

(3) 最后提交的实验报告应包含对实验目的和要求以及实验内容的描述, 请复制上述页面中的相关内容, 但需要把所有提示都删除。

由于本次实验中的任务 1 至 3 主要完成验证性的操作与学习, 实验报告中可以简化对这部分的描述, 所以, 下面给出最后提交的实验一的实验报告必须要写的内容的提示 (格式要求见 “2017 实验报告样例”):

1 实验目的与要求

(照搬前面相关内容)

2 实验内容

(照搬前面相关内容)

3 实验过程

3.1 任务 1~3

3.1.1 任务 3 源程序

3.1.2 关键的实验记录与分析

(每个任务至少描述一个场景, 下面给出一个示例)

(1) 有符号数与无符号数运行结果的比较分析

给出你的观察记录与分析总结

(2) 单步执行一条指令的多种方法

给出你的观察记录与分析总结

(3) 32 位寄存器变址寻址方式的编码特点

给出你的观察记录与分析总结

3.2 任务 4

(参照 “2017 实验报告样例”)

3.2.1 设计思想及存储单元分配

3.2.2 流程图

3.2.3 源程序

3.2.4 实验步骤

3.2.5 实验记录与分析

4 总结与体会

(任务 1~3 的相关总结与体会)

(任务 4 的相关总结与体会)

参考文献

(要具体化实际的参考文献信息)