实验报告二

一、实验目的：

了解什么是Debug，学习使用Debug的基本功能，熟练使用Debug调试汇编程序。

二、实验任务：

1．使用Debug，将下面的程序段写入内存，逐条执行，观察每条指令执行后CPU中相关寄存器的内容变化。

|  |  |
| --- | --- |
| 机器码 | 汇编指令 |
| b8 20 4e  05 16 14  Bb 00 20  01 d8  89 c3  01 d8  b8 1a 00  bb 26 00  00 d8  00 dc  00 c7  b4 00  00 d8  04 9c | mov ax, 4e20h ;(ax)=4e20h  add ax, 1416h ;(ax)=(ax)+1416h  mov bx, 2000h ;(bx)=2000h  add ax, bx ;(ax)=(ax)+(bx)  mov bx, ax ;(bx)=(ax)  add ax, bx ;(ax)=(ax)+(bx)  mov ax, 001ah ;(ax)=001ah  mov bx, 0026h ;(bx)=0026  add al, bl ;(al)=(al)+(bl)  add ah, bl ;(ah)=(ah)+(bl)  add bh, al ;(bh)=(bh)+(al)  mov ah, 0 ;(ah)=0  add al, bl ;(al)=(al)+(bl)  add al,9ch ;(al)=(al)+9ch |

提示，可用E命令和A命令以两种方式将指令写入内存。注意用T命令执行时，CS:IP的指向。

2．将下面3条指令写入从2000:0开始的内存单元中，利用3条指令计算2的8次方。

mov ax, 1

add ax, ax

jmp 2000: 0003

3．查看内存中的内容：

PC机主板上的ROM中写有一个生产日期，在内存FFF00H~FFFFFH的某几个单元中，请找到这个生产日期并试图改变它。

提示，如果读者对实验的结果感到疑惑，请仔细阅读第1章中的1.15节。

4．向内存从B8100h开始的单元中填入数据，如：

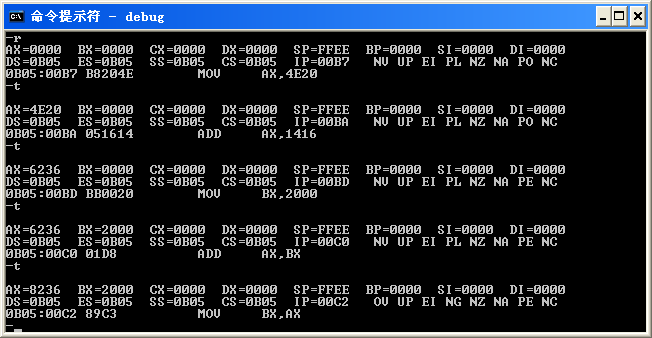
-e B810:0000 01 01 02 02 03 03 04 04

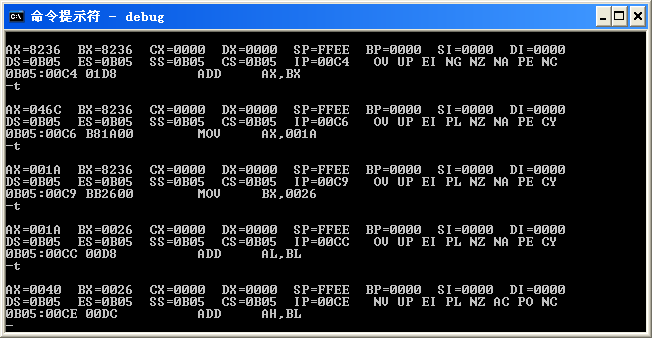
请读者先填写不同的数据，观察产生的现象；再改变填写的地址，观察产生的现象。

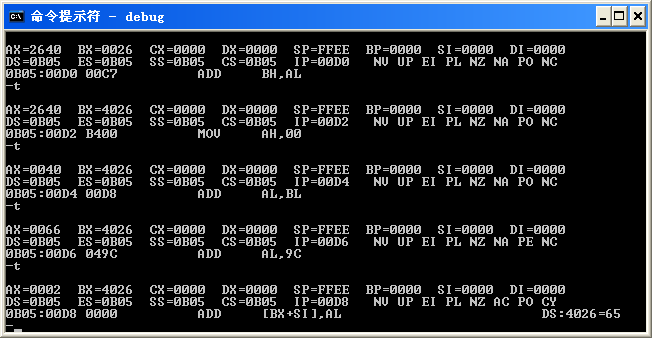
提示，如果读者对实验的结果感到疑惑，请仔细阅读第1章、中的1.15节。

三、实验过程：

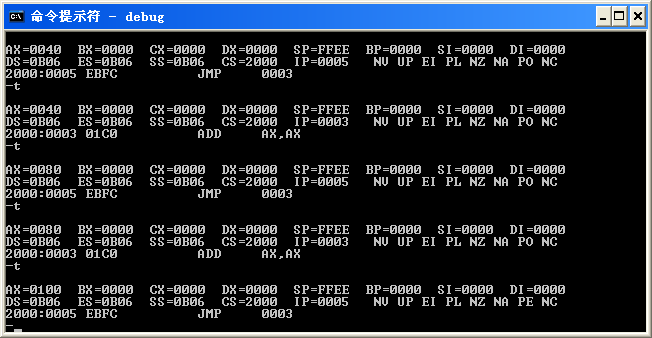
1．向内存中输入相应的指令，用t命令单步执行，记录每次CPU寄存器中的内容：



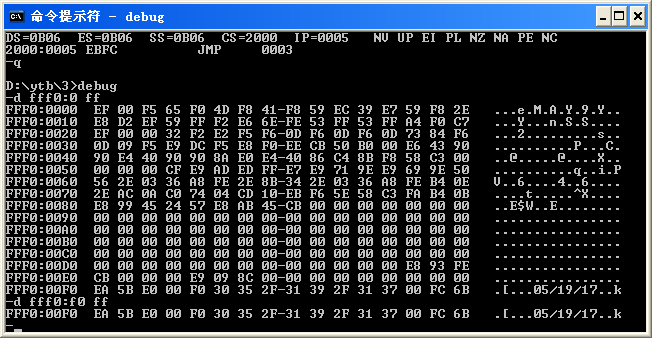




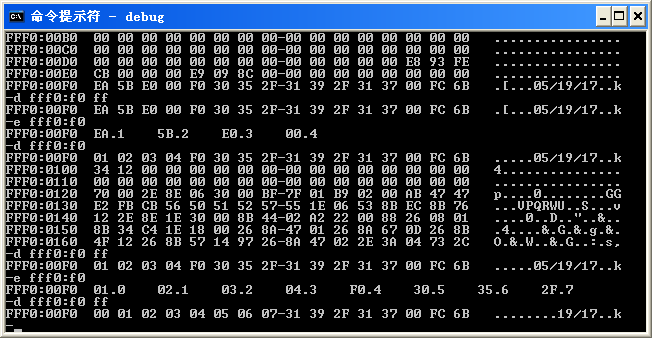
2．通过多次执行命令，每次寄存器ax的值翻倍，可以得到2的8次方为100h：



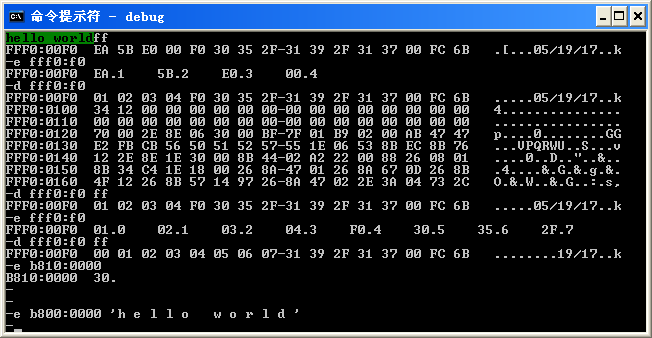
3．通过调用d命令可以看到生产日期为：2017年5月19日



通过e命令改变地址为FFF00~FFFFF的内容，d命令查看，正常情况其值不会被改变，但由于此次是在虚拟机中运行，其值有变化：



4．修改b800:0000处的内容，发现在控制台的左上角会发现彩色的字符：



四、实验总结：

在Debug中：

R命令：查看，修改CPU中寄存器的内容  
 D命令：查看内存中的内容  
 E命令：修改内存中的内容  
 U命令：将内存中的内容解释为机器指令和对应的汇编指令  
 T命令：执行CS:IP指向的内存单元处的命令  
 A命令：以汇编指令的形式向内存中写入指令

通过熟练掌握这些命令，为我们后续编程打下基础。