**电 子 科 技 大 学**

**实 验 报 告**

**学生姓名： 学号： 指导教师：蒲晓蓉**

**实验地点：主楼A2-413 实验时间： 2024年11月24日**

1. **实验室名称：计算机实验室**
2. **实验项目名称：虚拟内存综合实验**
3. **实验学时：4**
4. **实验原理：**

4.1内存地址映射原理

在操作系统中，存在逻辑地址、线性地址和物理地址之间的映射关系。逻辑地址是程序中使用的地址，通过段表映射到线性地址，线性地址再通过页表映射到物理地址。

4.2 Bochs 模拟器原理

Bochs 是一个完全靠软件模拟 Intel x86 的模拟器，能够模拟从启动到重启的整个 PC 环境，包括外设等。它自带调试器 bochsdbg，可以从 PC 机刚启动时开始模拟，这为调试操作系统提供了便利。

1. **实验目的：**

通过实验，掌握段页式内存管理机制，理解地址转换的过程。

1. **实验内容：**

使用软件bochs配置Linux 0.11的虚拟运行环境，在Linux中运行一段无限循环的代码，通过bochs的调试工具找到变量j的地址并验证其正确性。

1. **实验器材（设备、元器件）：**

计算机

1. **实验步骤：**

8.1 下载并安装bochs2.5.1

根据实验指导书内容下载并安装bochs2.5.1，安装完成后配置bochs与Linux0.11实验环境，完成后如图1所示。

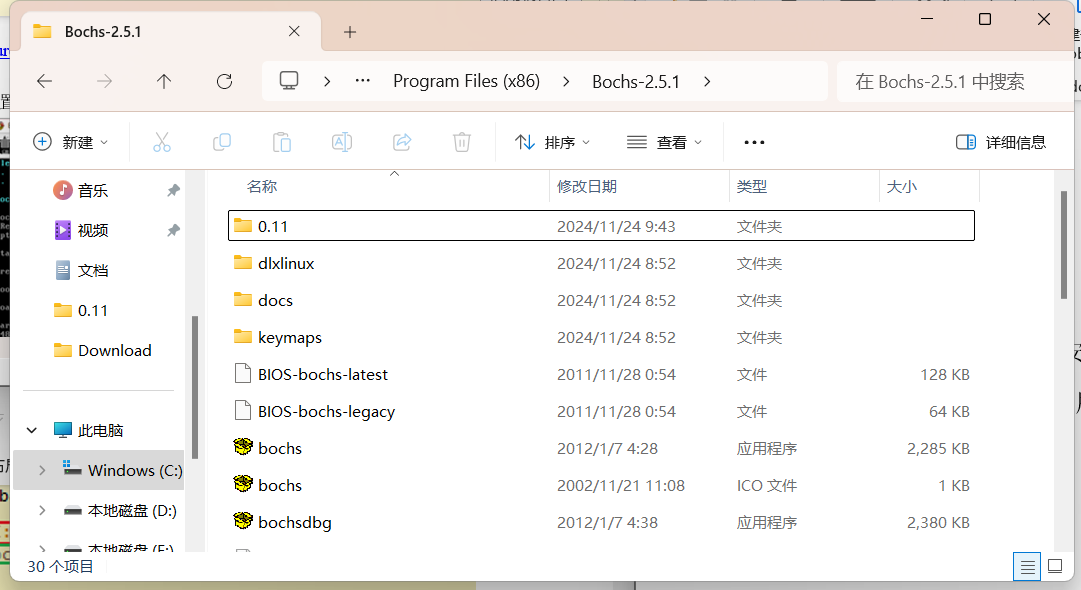


图1 完成bochs2.5.1与Linux0.11配置

8.2 准备测试文件

运行bochs，在打开的命令行中输入c，执行continue指令，启动Linux0.11，得到图2。

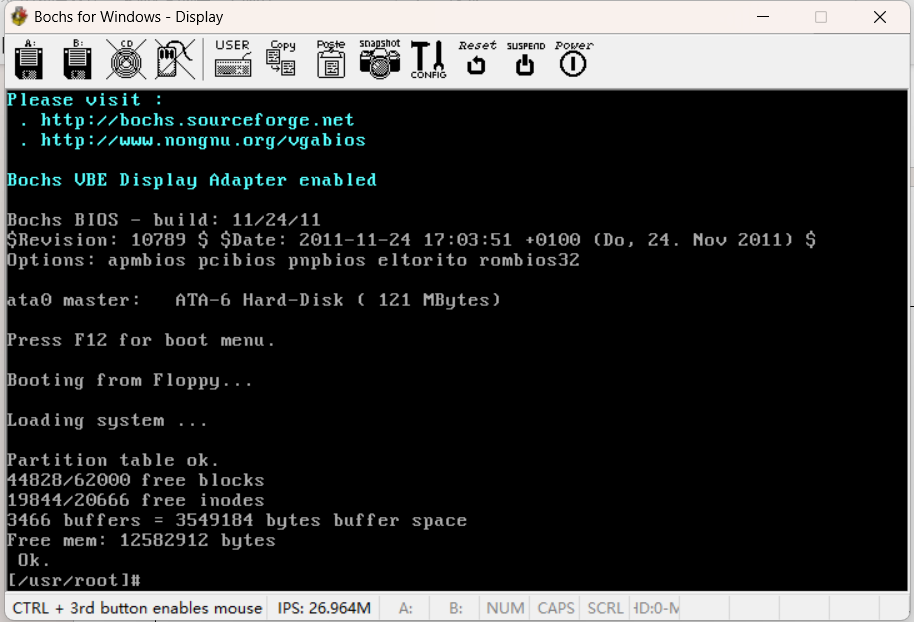


图2 启动Linux0.11

如图3，在bochs中先输入“cd /mnt/”指令进入mnt文件夹，在mnt文件夹下使用“vi test.c”指令进入vi编辑器对test.c文件进行编辑。

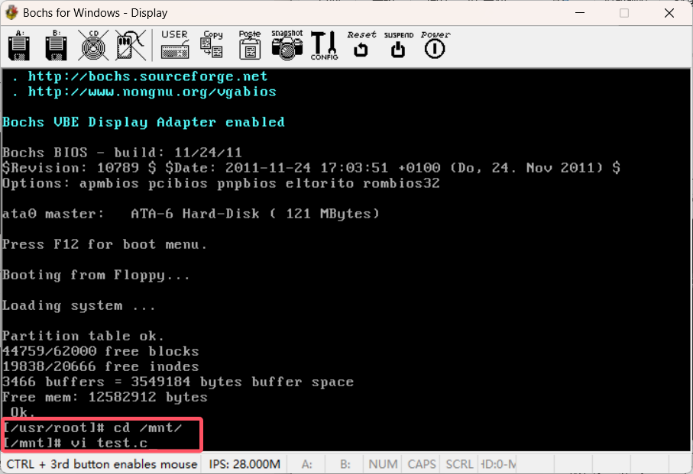


图3 进入mnt文件夹并进入vi编辑器

在vi编辑器中先按下“i”键进入输入模式，输入图4所示测试代码。输入完成后按esc键退出输入模式，输入“:wq”保存文件并退出vi编辑器。

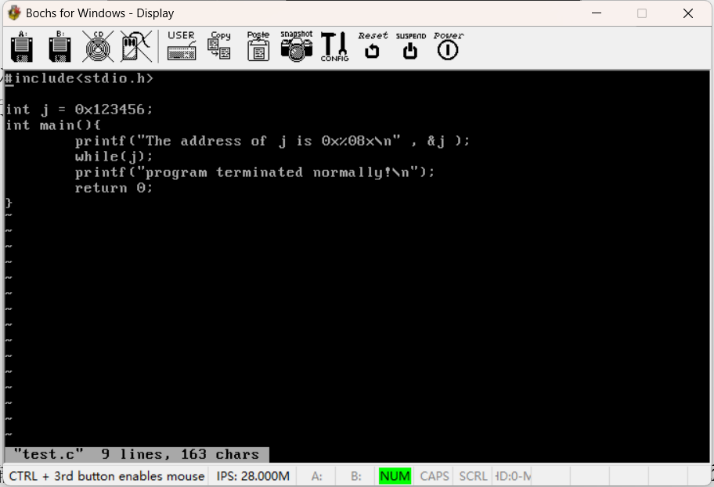


图4 test.c文件内容

退出vi编辑器后，在bochs中输入“gcc -o test test.c”指令将test.c文件编译为可执行文件test，编译完成后使用“ls”指令列出mnt文件夹下的所有文件，如图5所示，test已被正确编译。hello.c与hello文件为本人测试vi编辑器所用，与本实验无关。

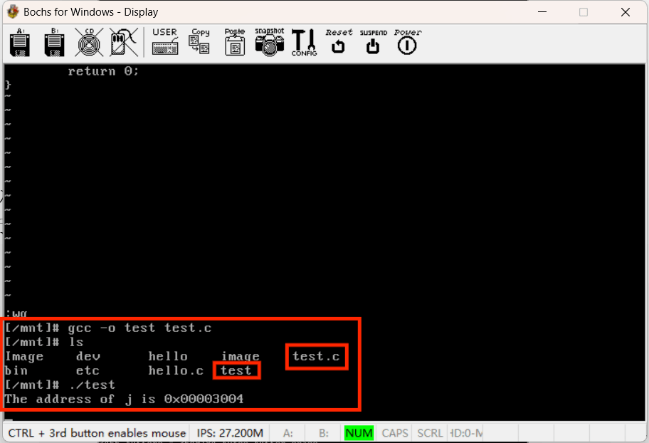


图5 编译test.c文件并运行test

输入“./test”指令执行test，输出结果如图5所示，得到j的地址为0x3004。

8.3 进入调试状态并寻找地址

在与bochs同时生成的命令行中按下“Ctrl键+c”，bochs暂停运行并进入调试状态，命令行中输出图6中所示信息。使用“c”或“n”命令使程序运行至cmp指令，然后使用“u/10”命令显示当前位置开始10条指令的反汇编代码，结果如图6所示。

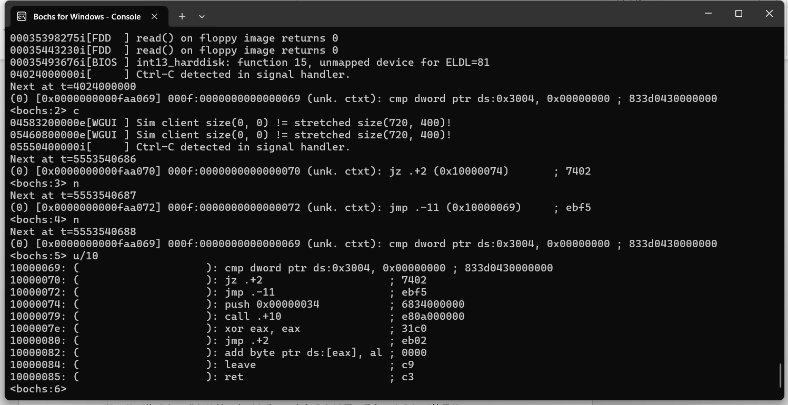


图6 中断运行后命令行输出信息

由图5与图6可知j保存在ds:0x3004该虚拟地址中，继续在命令行中输入“sreg”命令，输出结果如图7所示，得到ldtr的值为0x0068，转换为二进制为0000 0000 0110 1000，gdtr的地址为0x5cb8。

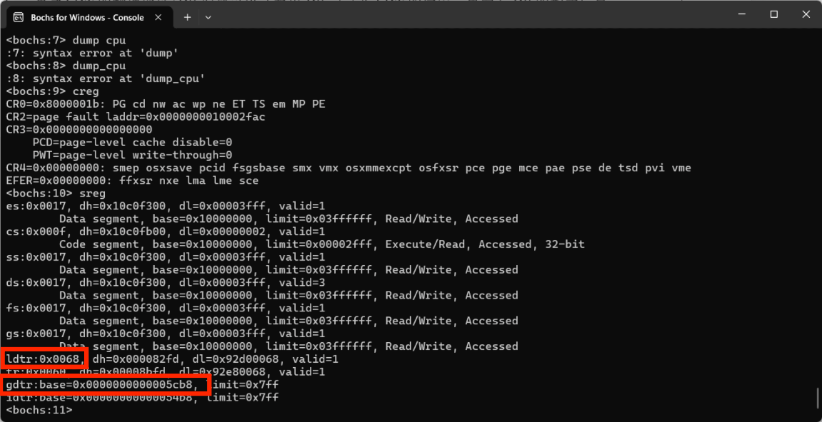


图7 使用sreg命令得到ldtr与gdtr的值

在命令行中输入“xp /32w x00005cb8”命令查找GDT表的前16项，得到结果如图8所示。因为LDTR是一个16位的局部描述符寄存器，其指向GDT中LDT描述符的选择符，选择符前13位是一个索引号，索引号指向段描述符，由于T1=0，所以高13位存放LDT在GDT中的索引值，即13，表示LDT放在GDT第14项，所以我们要查找的项的地址是“0x00005cb8 + 13\*8”。在命令行中继续输入“xp /2w 0x00005cb8+13\*8”命令查询GDT表的第14项，结果如图8所示，得到“0x0000000000005d20 <bogus+ 0>: 0x92d00068 0x000082fd”，后两个数值与图7中ldtr所在行的dl与dh一致，得到的结果准确。

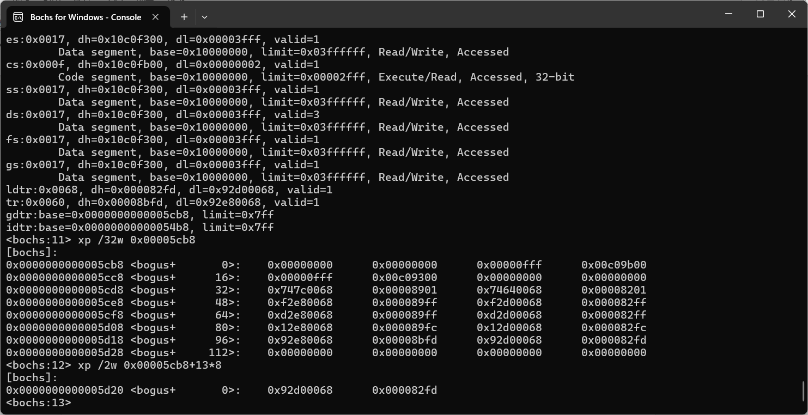


图8 查询GDT表中第14项

将0x92d00068与0x000082fd转换为二进制得到：

1001 0010 1101 0000 0000 0000 0110 1000与

0000 0000 0000 0000 1000 0010 1111 1101。将其与图9中段描述符中所存储的信息对照组合可得到LDT的物理地址为0x00fd92d0。



图9 段描述符结构

使用“xp /8w 0x00fd92d0”命令查找LDT表中的前4项，得到图10中所示结果。其中LDT表的第三项为0x00003fff与0x10c0f300，与图7中ds所在行的dl与dh一致，故得到的描述符正确。

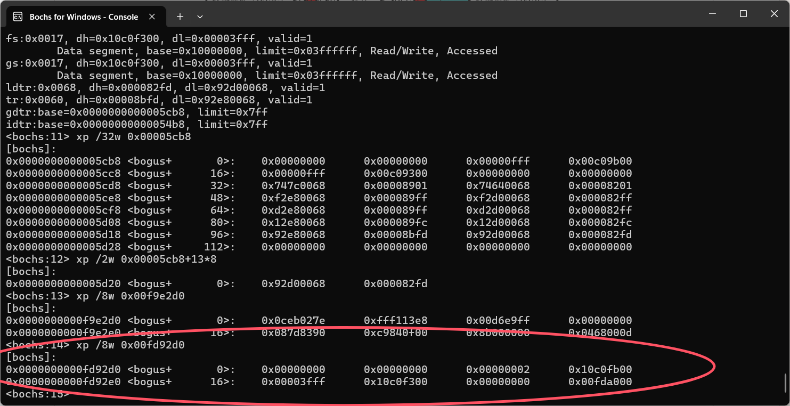


图10 LDT表的前4项

将0x00003fff与0x10c0f300转换为二进制得到：

0000 0000 0000 0000 0011 1111 1111 1111与

0001 0000 1100 0000 1111 0011 0000 0000。合成得到的地址为0x10000000，即为ds段在线性地址空间中的起始地址。段基址+段内偏移得到线性地址为0x10000000 + 0x3004 = **0x10003004**。使用“calc ds:0x3004”命令验证所得线性地址是否正确，得到图11所示结果，可见计算得到的线性地址结果正确。

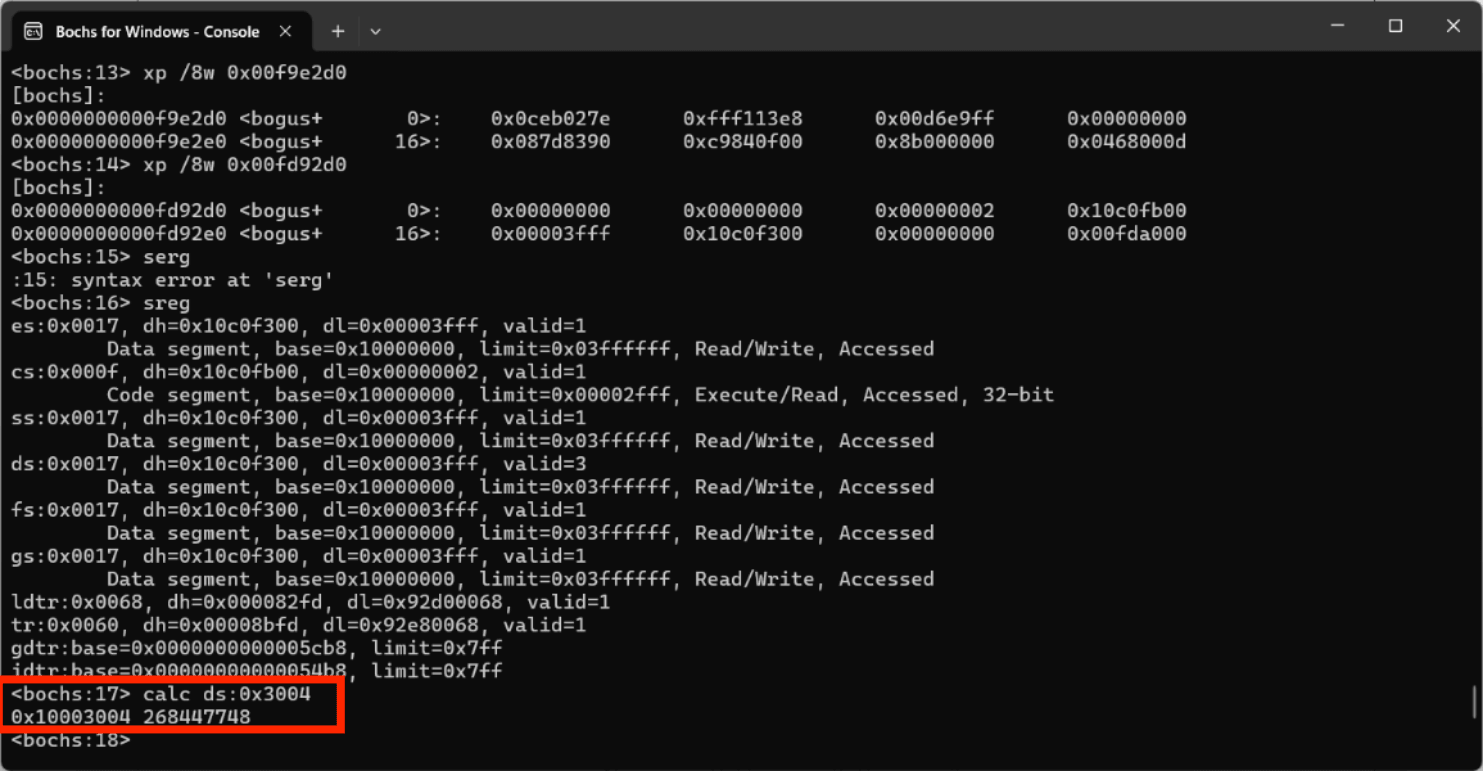


图11 验证线性地址正确性

图12展示了线性地址变成物理地址的过程，首先需要算出线性地址中的页目录号、页表号和页内偏移，它们分别对应了32位线性地址的10位+10位+12位，所以0x10003004的页目录号是64，页号3，页内偏移是4。IA-32下，页目录表的位置由CR3寄存器指引。图7中，使用“creg”指令得到“CR3=0x00000000”，即页目录的基地址为0。因此使用“xp /68w 0”命令查看页目录，得到图13。

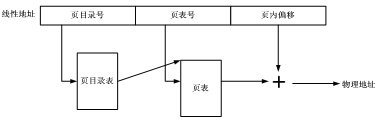


图12 线性地址变为物理地址过程

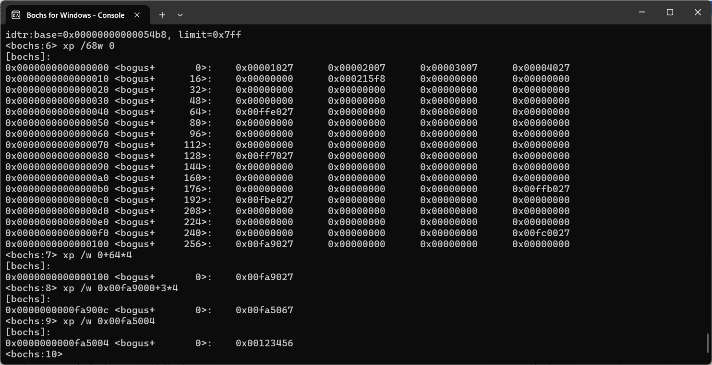


图13 页目录

页目录表和页表中的内容为1024个32位（大小4K）数。这32位中前20位为物理页框号，后面为一些属性信息（其中最重要的是最后一位P）。其中第65个页目录项即所找内容，使用“xp /w 0+64\*4”命令查看，得到结果如图14所示，故物理页框号为0x00fa9，页表位于物理内存中的0x00fa9000处。

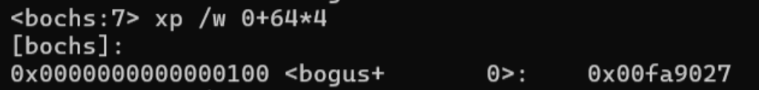


图14 物理页框号地址

由于线性地址0x10003004的页号为3，所以从该位置开始查找3号页表项的地址，使用“xp /w 0x00fa6000+3\*4”命令查看，得到图15结果。

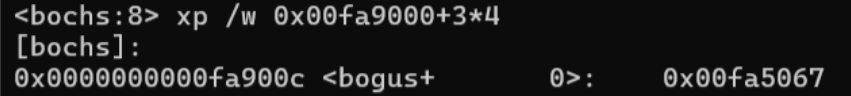


图15 物理页表项地址

因此线性地址0x10003004对应的物理页框号为0x00fa5，与页内偏移0x004相接后得到j的物理地址**0x00fa5004**。

1. **实验数据及结果分析：**

验证所得的物理地址是否正确，使用“xp /w 0x00fa5004”命令得到图16，可见变量j的值确实为最初test.c文件中所定义的值，所得数据正确。

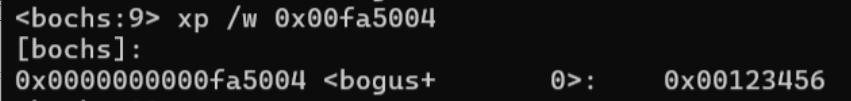


图16 验证数据准确性

虽然实验指导书中只需得到图16中的结果即可，但注意到test.c文件中的while循环退出后还有一段输出结果的代码，于是本人尝试修改变量j的值，使程序退出死循环，观察bochs中是否能够输出“program terminated normally!”。查阅资料得知，通过命令“setpmem 0x00fa5004 4 0”可将变量j的值修改为0x00000000，再使用“c”命令使bochs继续运行（图17），回到bochs窗口，在图18中可见输出了“program terminated normally!”，变量j的值被正确修改，test退出，实验完成。

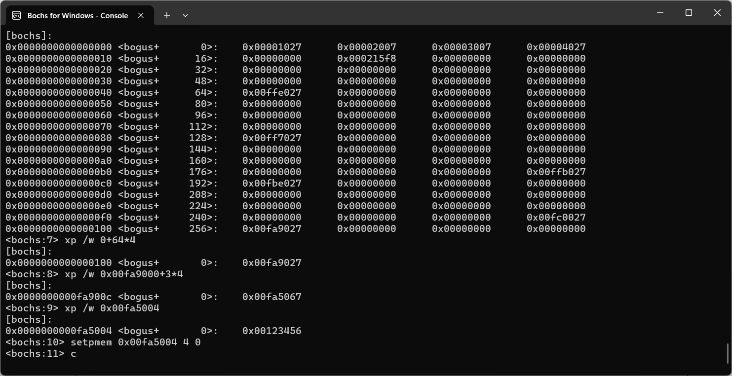


图17 修改j的值并使bochs继续运行

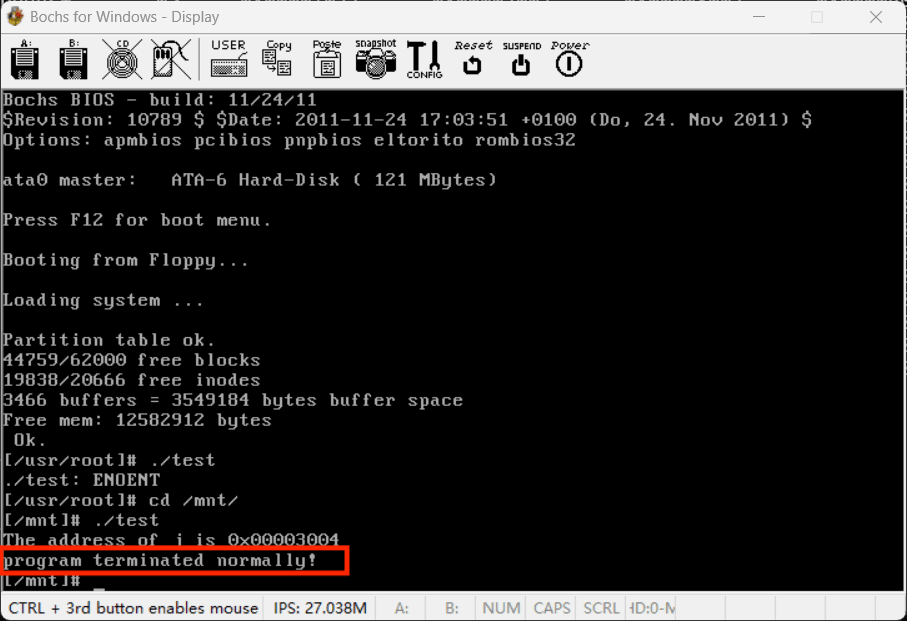


图18 恢复运行后bochs输出

1. **实验结论：**

通过本次实验，成功利用bochs搭建了 Linux 0.11 的虚拟运行环境，并深入理解了段页式内存管理机制以及地址转换的过程。在实验中，我准确地找到了变量在内存中的物理地址，并通过修改该地址的值，使程序退出了无限循环。

1. **总结及心得体会：**

在本次实验中，我对操作系统的内存管理机制有了更深入的理解。通过实际操作，亲身体验了从逻辑地址到物理地址的转换过程，感受到了操作系统底层的复杂性和精妙之处。

在实验过程中，我也遇到了一些困难和挑战。例如，对vi编辑器的使用不够熟练，需要花费一些时间去学习和掌握。此外，对于段表、页表等概念的理解也需要更加深入，才能更好地完成实验。

通过本次实验，我不仅提高了自己的实践能力和解决问题的能力，还培养了自己的耐心和细心。在今后的学习中，我将继续努力，深入学习操作系统的相关知识，为今后的研究和工作打下坚实的基础。

1. **对本实验过程及方法、手段的改进建议：**

在实验指导书中，可以增加更多关于vi编辑器的使用说明，帮助学生更好地掌握vi编辑器的使用方法，减少时间的浪费。指导书中的部分命令也已经过时，无法再使用，需要换为新的指令。除此之外，还可以提供更多的测试用例，让学生在不同的情况下进行实验，加深对内存地址映射原理的理解。

**报告评分：**

**指导教师签字：**