课程编号:COM07023　　北京理工大学 2017 - 2018 学年第一学期

2015 级汇编语言程序设计期末试题 B 卷

班级_____ 学号_____ 姓名_____ 成绩_____

说明：① 闭卷考试。
② 考试时间两小时。
③答案直接写在题后，考试完毕后，试卷一律交回。

一、单项选择题（每道题 1 分，共 10 分）。

1. 汇编语言源程序中，每个语句由四项组成，如语句要完成一定功能，那么该语句中不可省略的项是（　　）。
A. 名字项　　B. 操作码项　　C. 操作数项　　D. 注释项

2. 32 位指令指针寄存器是（　　）。
A. EIP　　B. SP　　C. EBP　　D. EBX

3. 在汇编语言中，（　　）是十六进制数的正确表示形式。
A. 0XB012　　B. B012H　　C. 0B012H　　D. 0B012

4. 在 MASM 中，把 BL 的最低 4 位置 1 的语句是（　　）。
A. OR BL, 0FH　　B. OR BL, 0F0H
C. AND BL, 0F0H　　D. NOT BL

5. 16 位实模式下，当 CX 初始化为 0 时，LOOP 循环的执行次数为（　　）。
A. 0　　B. 1　　C. 65535　　D. 65536

6. 下列指令执行后可能会使 EBX 改变的指令是（　　）。
A. TEST EBX, 1　　B. CMP EBX, 1
C. OR EBX, 0　　D. XOR EBX, 1

7. 比较两个带符号的数 A、B，当 A=B 时程序转移，测试的条件为（　　）。
A. ZF=1　　B. ZF=0　　C. SF=1　　D. SF=0

8. 定义子程序的伪指令是（　　）。
A. PROC/ENDP　　B. MACRO/ENDM
C. SEGMENT/ENDS　　D. REPT/ ENDM

9. 判断两个带符号数的大小关系，若要实现 EAX≥EBX 时执行分支 LOP1，那么在“CMP EAX, EBX”指令后应跟的分支指令是（　　）。
A. JNC LOP1　　B. JAE LOP1　　C. JC LOP1　　D. JGE LOP1

10. 为使 ECX=-1 时，转至标号 L1 位置处继续执行而编制了一段指令序列，其中错误的指令序列是（　　）。
A. ADD ECX, 1　　JZ L1
B. SUB ECX, 0FFFFFFFFH　　JZ L1

C. AND ECX, 0FFFFFFFFH JZ L1
D. XOR ECX, 0FFFFFFFFH JZ L1

二、填空题（每空 1 分，共 30 分）。

1. 32 位寄存器中用作累加器的寄存器是_____。
2. 32 位环境下，LOOP 指令的循环次数放在_____寄存器。
3. ECX 的值为 0B0EC600H。CX 寄存器值为_____H，CL 寄存器值为_____H。
4. 实模式下，给定段基址 0001H，则 CPU 可能的寻址范围的物理地址是从_____H 到_____H。
5. 某 CPU 地址总线 16 位，数据总线 16 位，则 CPU 的寻址能力为_____Byte，CPU 的内存间同时传输的数据大小为_____Byte。
6. 如果一个系统由 A 和 B 两个模块组成，在 A 模块中要调用 B 模块中的 B_SUB 子程序（类型为 FAR），则在 A 模块的开始应该用_____语句对 B_SUB 子程序予以说明。在 B 模块中应该用_____语句对 B_SUB 子程序予以说明。
7. 下列指令中的操作码助记符是_____，标号是_____，操作数是_____。

```
LOP1:   DEC     AL
```

8. 语句 BUF WORD 10H DUP(3 DUP(2，10H)，3，5) 汇编后，为变量 BUF 分配的存储单元字节数是_____。（结果 10 进制表示）
9. 执行下面指令后，写出各标志位的值(EAX 初始值 0060H)。

```
SUB EAX,EAX
```

CF=_____，SF=_____，ZF=_____。

10. 将 AX 中高 8 位清 0 的指令是_____；将 AH 的低 4 位取反的指令是_____。
11. 请写出无条件转移指令中的段间间接转移的指令格式（32 位环境，转移地址保存在 EBX 所指向的内存单元）_____。
12. 数据段中有以下定义：

```
ARRAY1    EQU     16H
ARRAY2    DWORD   16H
```

指令 MOV EAX，ARRAY1 中源操作数的寻址方式为_____。
令 MOV EAX，ARRAY2 中源操作数的寻址方式为_____。
存 Addr 处开始的内存单元中存放着以下数据(十六进制形式)：

```
23 45 67 89 AB CD EF
```


14. 某
VA
VA
VAR
VAR5
设 VAR1 的
（1）VAR3
（2）VAR4
（3）VAR5 的
15. 在 16 位环境
(BP)=0080H，试计
（1）MOV [BP],
（2）MOV ES:6[
（3）MOV [0600H]

三、程序填空题（每空

1. 采用查询方式，实现
发送和接收出错的情况），
1 表示空闲）。补全下列空

```
SEND PROC
        PUSH EAX
        MOV DX，3FDH
ComBusy:
        IN AL，DX
        _____ AL，20H
        JZ ComBusy
        POP
```

寄存器。

H，CL 寄存器值为_____H。

储的寻址范围的物理地址是从_____H

CPU 的寻址能力为_____Byte。CPU 构

要调用 B 模块中的 B_SUB 子程序(类

_____语句对 B_SUB 子程序予以说明。

SUB 子程序予以说明。

号是_____，操作数是

，为变量 BUF 分配的存储单

。

AH 的低 4 位取反的指

境，转移地址保存在

_____。

。

试分别写出 Addr+3 处的字型数据，双字型数据的值。

字　型：_____。

双字型：_____。

14. 某程序数据段中定义了如下变量：

```
VAR1    DB      0, 1, 2, 3, 0DH, 0AH
VAR2    EQU     $-VAR1
VAR3    DW      VAR2 dup(8)
VAR4    DW      VAR3
VAR5    DD      5
```

设 VAR1 的偏移量为 0，则：

（1）VAR3 的偏移量为_____（结果用 10 进制表示）；

（2）VAR4 的偏移量为_____（结果用 10 进制表示）；

（3）VAR5 的偏移量为_____（结果用 10 进制表示）。

15. 在 16 位环境下，设(DS)=2000H，(ES)=3000H，(SS)=3200H，(BX)=0100H，(SI)=002

(BP)=0080H，试计算下列各指令的目标操作数的物理地址分别是：

（1）MOV [BP],AX　　物理地址为_____H；

（2）MOV ES:6[BX][SI],CX　　物理地址为_____H；

（3）MOV [0600H],AX　　物理地址为_____H。

三、程序填空题（每空 2 分，共 10 分）。

1. 采用查询方式，实现从 COM1 端口发送一个字符的子程序(字符在 AL 中，不考虑串

发送和接收出错的情况)，状态寄存器地址 3FDH，第 5 位为发送数据状态位(0 表示忙碌

1 表示空闲)。补全下列空格处的指令或语句。

```
SEND PROC
     PUSH EAX
     MOV DX, 3FDH
ComBusy:
     IN AL, DX
     _____ AL, 20H
     JZ ComBusy
     POP _____
     MOV DX, 3F8H
```

试分别写出 Addr+3 处的字型数据、双字型数据的值。

字　型：_____。

双字型：_____。

14. 某程序数据段中定义了如下变量：

```
VAR1    DB      0，1，2，3，0DH，0AH
VAR2    EQU     $-VAR1
VAR3    DW      VAR2 dup(8)
VAR4    DW      VAR3
VAR5    DD      5
```

设 VAR1 的偏移量为 0，则：

（1）VAR3 的偏移量为 6（结果用 10 进制表示）；

（2）VAR4 的偏移量为 18（结果用 10 进制表示）；

（3）VAR5 的偏移量为 26（结果用 10 进制表示）。

15. 在 16 位环境下，设(DS)=2000H，(ES)=3000H，(SS)=3200H，(BX)=0100H，(SI)=0020H，(BP)=0080H，试计算下列各指令的目标操作数的物理地址分别是：

（1）MOV [BP]，AX　　物理地址为 20080 H；

（2）MOV ES:6[BX][SI]，CX　　物理地址为 30126 H；

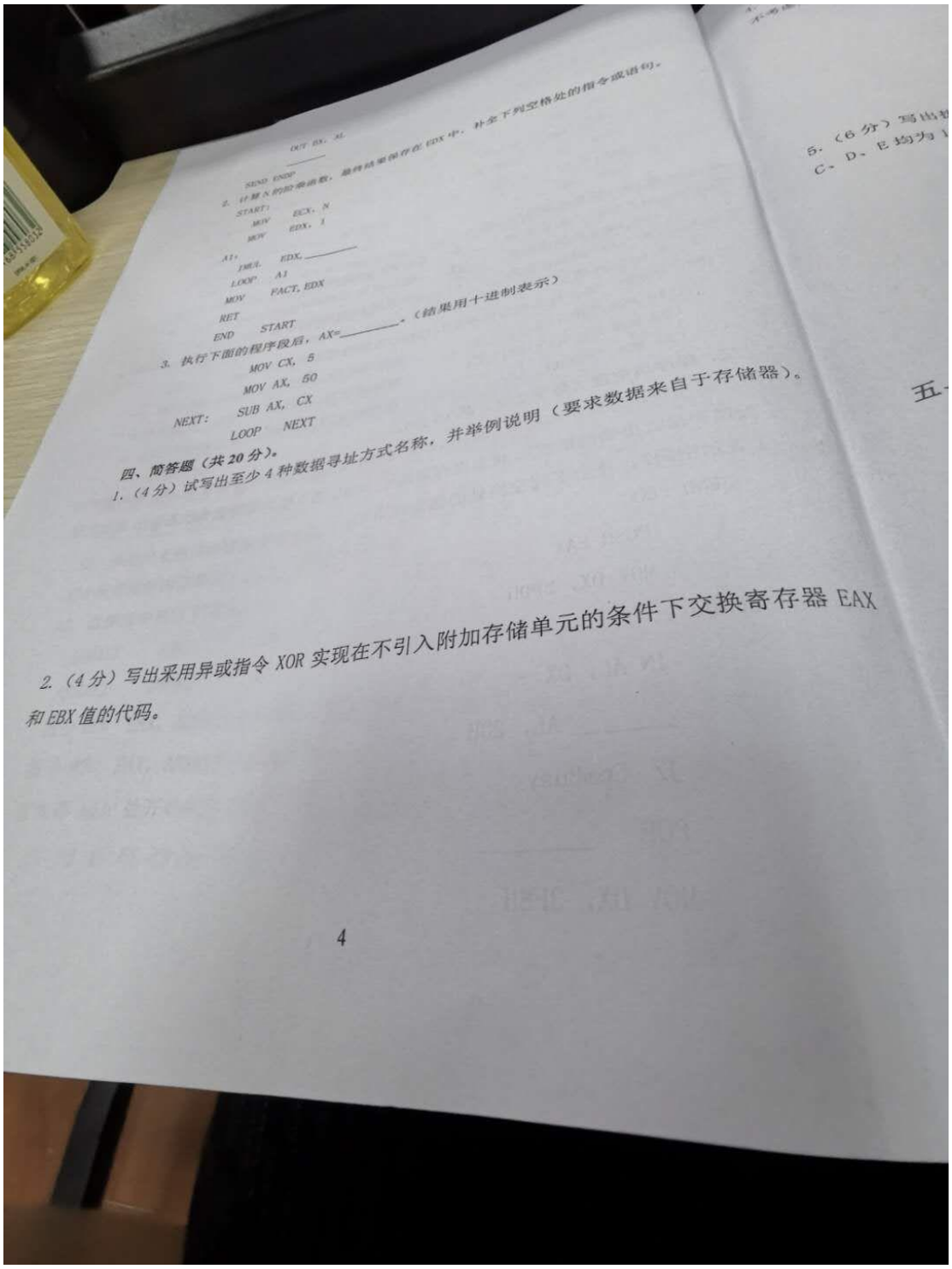
（3）MOV [0600H]，AX　　物理地址为 20600 H。

三、程序填空题（每空 2 分，共 10 分）。

1. 采用查询方式，实现从 COM1 端口发送一个字符的子程序(字符在 AL 中，不考虑串口发送和接收出错的情况)，状态寄存器地址 3FDH，第 5 位为发送数据状态位(0 表示忙，1 表示空闲)。补全下列空格处的指令或语句。

```
SEND PROC
        PUSH EAX
        MOV DX，3FDH

ComBusy:
        IN AL，DX
        _____ AL，20H
        JZ ComBusy
        _____
        _____
```



DOT ES:, AL
_____
SSUD ENDP

2. 计算 N 的阶乘函数，最终结果保存在 EDX 中，补全下列空格处的指令或语句。

```
START:  MOV     ECX, N
        MOV     EDX, 1
A1:     IMUL    EDX, _____
        LOOP    A1
        MOV     FACT, EDX
        RET
END     START
```

3. 执行下面的程序段后，AX=_____。（结果用十进制表示）

```
        MOV CX, 5
        MOV AX, 50
NEXT:   SUB AX, CX
        LOOP NEXT
```

四、简答题（共 20 分）。

1.（4 分）试写出至少 4 种数据寻址方式名称，并举例说明（要求数据来自于存储器）。

五

2.（4 分）写出采用异或指令 XOR 实现在不引入附加存储单元的条件下交换寄存器 EAX 和 EBX 值的代码。

OUT DX, AL

_____

SEND ENDP

2. 计算 N 的阶乘函数，最终结果保存在 EDX 中，补全下列空格处的指令或语句。

```
START:
    MOV     ECX, N
    MOV     EDX, 1
A1:
    IMUL    EDX, _____
    LOOP    A1
    MOV     FACT, EDX
    RET
END     START
```

3. 执行下面的程序段后，AX=_____。（结果用十进制表示）

```
        MOV CX, 5
        MOV AX, 50
NEXT:   SUB AX, CX
        LOOP NEXT
```

四、简答题（共 20 分）。

1.（4 分）试写出至少 4 种数据寻址方式名称，并举例说明（要求数据来自于存储

4.（6 分）编写用移
不考虑边界条件，

5.（6 分）写
C、D、E 均为

五、读

）写出采用异或指令 XOR 实现在不引入附加存储单元的条件下交换寄存
的代码。

```
        OUT DX, AL
        _____
SEND ENDP
```

2. 计算 N 的阶乘函数，最终结果保存在 EDX 中，补全下列空格处的指令或语句。

```
START:
    MOV     ECX, N
    MOV     EDX, 1
A1:
    IMUL    EDX, _____
    LOOP    A1
    MOV     FACT, EDX
    RET
END     START
```

3. 执行下面的程序段后，AX=_____。（结果用十进制表示）

```
        MOV CX, 5
        MOV AX, 50
NEXT:   SUB AX, CX
        LOOP    NEXT
```

四、简答题（共 20 分）。

1. （4 分）试写出至少 4 种数据寻址方式名称，并举例说明（要求数据来自于存储器）。

(1) MOV AX, [200H] 直接寻址

(2) MOV AX, [BX] 寄存器间接寻址

(3) MOV AX, [SI+100H] 寄存器相对寻址

(4) MOV AX, [BX+SI] 基址变址寻址

）写出采用异或指令 XOR 实现在不引入附加存储单元的条件下交换寄存器 B

的代码。

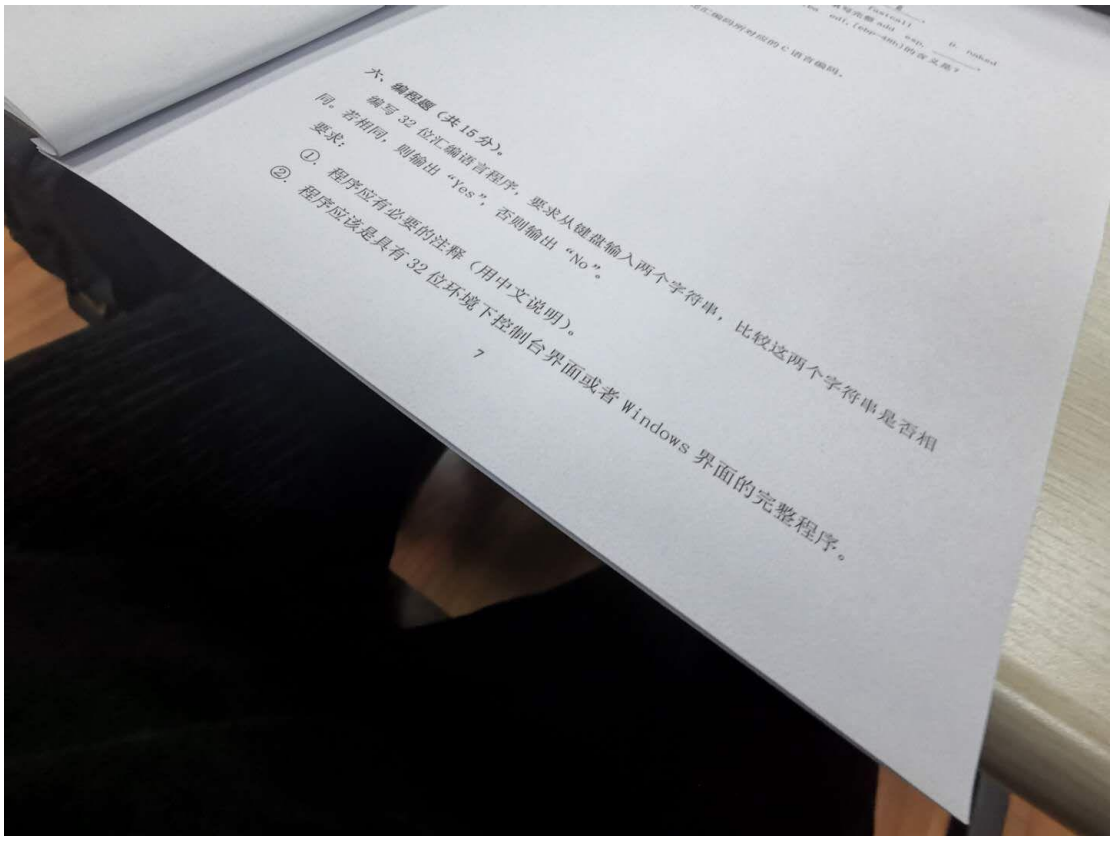
16 位或 32 位代码均可，代码中不能出现乘法指令）。

5.（6 分）写出执行 A=（B*C）/（D+4），余数送 E 的二进制运算的指令序列，其中 A、B、C、D、E 均为 16 位内存变量。

五、读反汇编码回答问题（共 15 分）。

有如下 32 位可执行文件的部分核心反汇编代码，阅读下列反汇编码后回答问题。

```
00401005   jmp      main (00401050)
0040100F   jmp      subproc (00401020)
.....
00401020   push     ebp
00401021   mov      ebp, esp
00401023   sub      esp, 48h
00401026   push     ebx
00401027   push     esi
00401028   push     edi
00401029   push     ecx
0040102A   lea      edi, [ebp-48h]
0040102D   mov      ecx, 12h
00401032   mov      eax, 0CCCCCCCCh
```



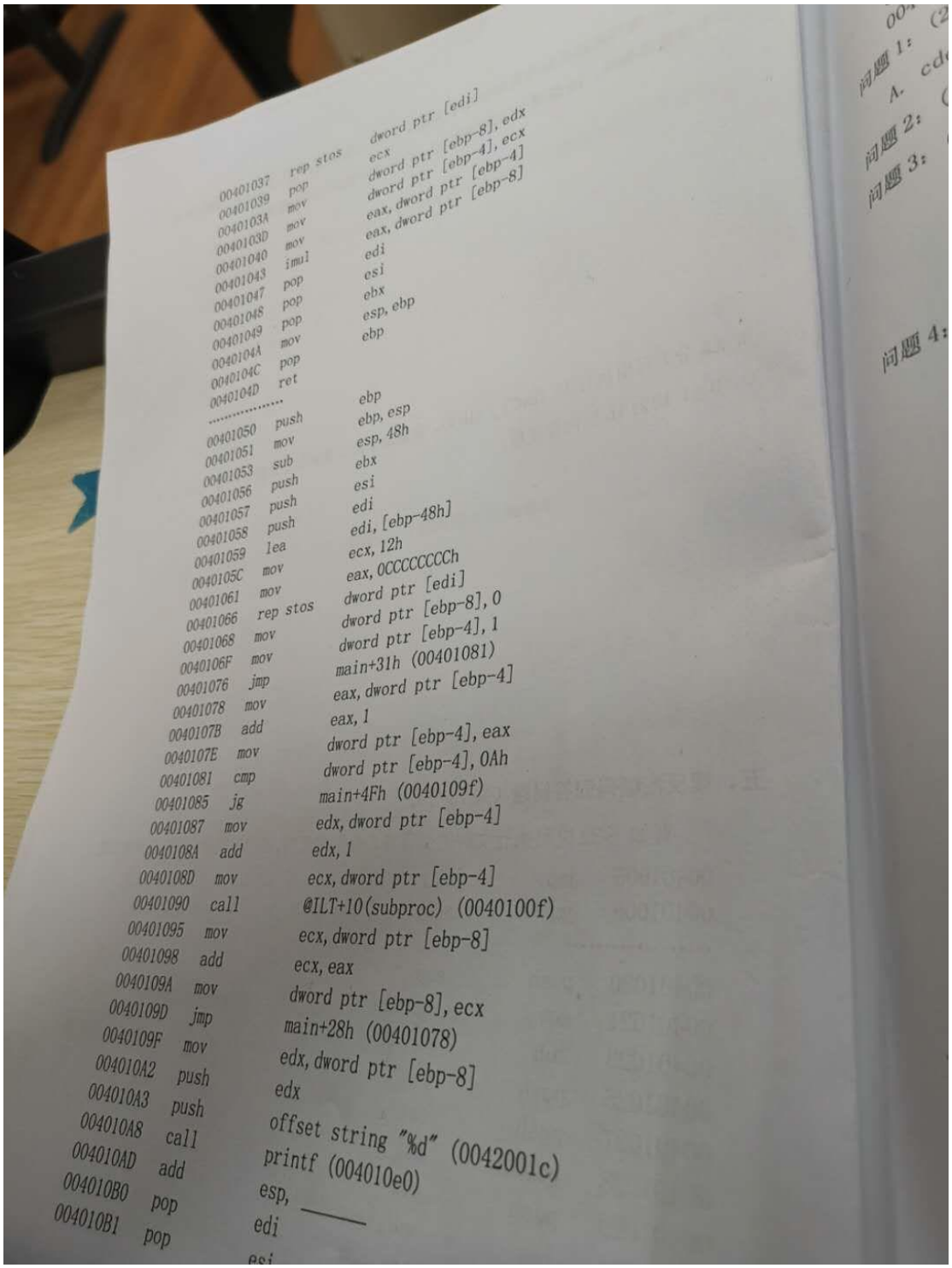
六、**编程题**（共15分）。

编写32位汇编语言程序，要求从键盘输入两个字符串，比较这两个字符串是否相同。若相同，则输出“yes”，否则输出“No”。

要求：

①. 程序应有必要的注释（用中文说明）。

②. 程序应该是具有32位环境下控制台界面或者Windows界面的完整程序。



```
00401037  rep stos    dword ptr [edi]
00401039  pop         ecx
0040103A  mov         dword ptr [ebp-8], edx
0040103D  mov         dword ptr [ebp-4], ecx
00401040  imul        eax, dword ptr [ebp-4]
00401043  pop         eax, dword ptr [ebp-8]
00401047  pop         edi
00401048  pop         esi
00401049  mov         ebx
0040104A  pop         esp, ebp
0040104C  ret         ebp
0040104D  .....
00401050  push        ebp
00401051  mov         ebp, esp
00401053  sub         esp, 48h
00401056  push        ebx
00401057  push        esi
00401058  push        edi
00401059  lea         edi, [ebp-48h]
0040105C  mov         ecx, 12h
00401061  mov         eax, 0CCCCCCCCh
00401066  rep stos    dword ptr [edi]
00401068  mov         dword ptr [ebp-8], 0
0040106F  mov         dword ptr [ebp-4], 1
00401076  jmp         main+31h (00401081)
00401078  mov         eax, dword ptr [ebp-4]
0040107B  add         eax, 1
0040107E  mov         dword ptr [ebp-4], eax
00401081  cmp         dword ptr [ebp-4], 0Ah
00401085  jg          main+4Fh (0040109f)
00401087  mov         edx, dword ptr [ebp-4]
0040108A  add         edx, 1
0040108D  mov         ecx, dword ptr [ebp-4]
00401090  call        @ILT+10(subproc) (0040100f)
00401095  mov         ecx, dword ptr [ebp-8]
00401098  add         ecx, eax
0040109A  mov         dword ptr [ebp-8], ecx
0040109D  jmp         main+28h (00401078)
0040109F  mov         edx, dword ptr [ebp-8]
004010A2  push        edx
004010A3  push        offset string "%d" (0042001c)
004010A8  call        printf (004010e0)
004010AD  add         esp, ____
004010B0  pop         edi
004010B1  pop         esi
```

```
004010B2    pop     ebx
004010B3    add     esp, 48h
004010B6    cmp     ebp, esp
004010B8    call    __chkesp (00401160)
004010BD    mov     esp, ebp
004010BF    pop     ebp
004010C0    ret
```

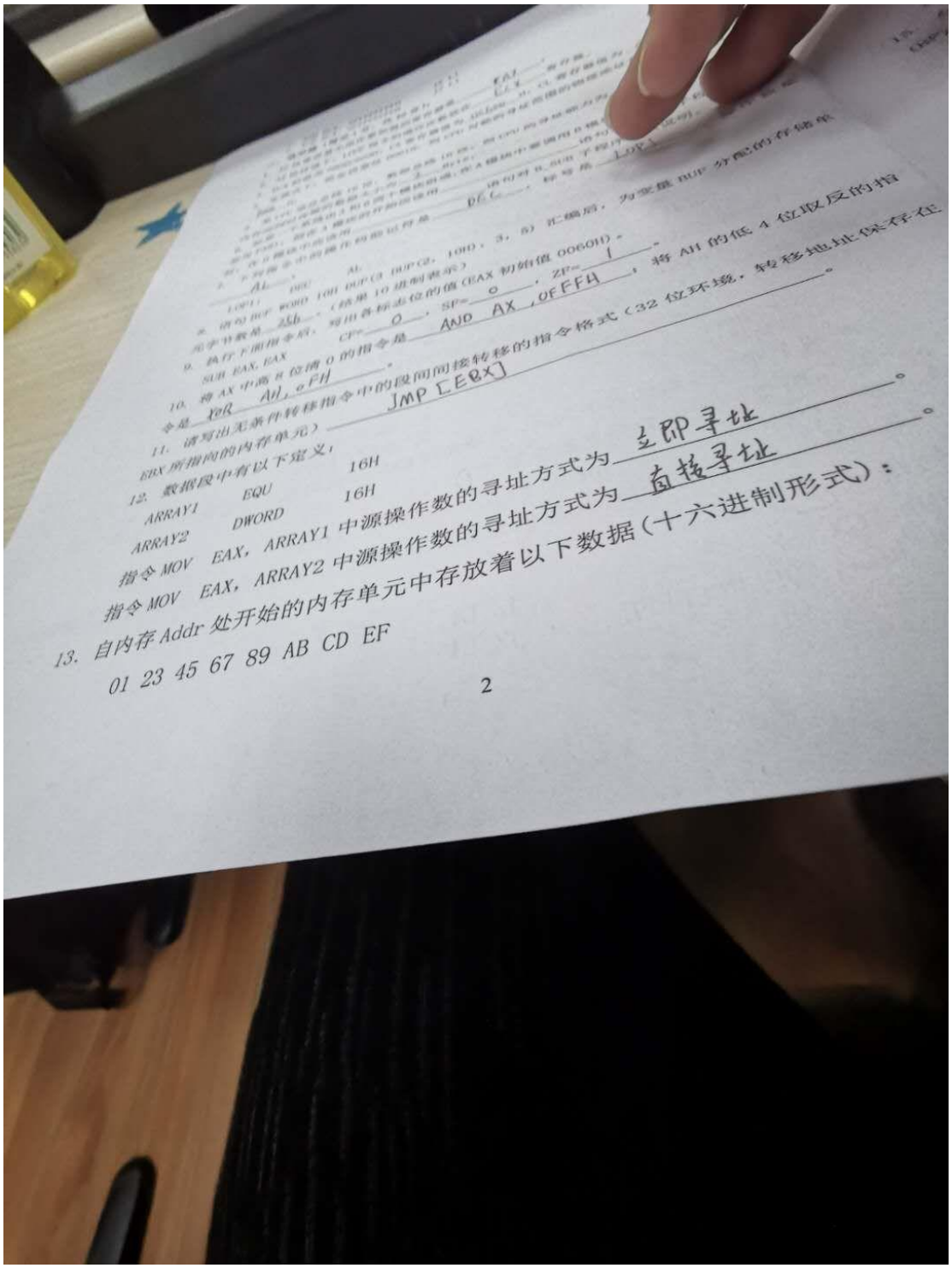
问题 1：(2 分)子程序 subproc 的参数调用规则为_____。

A. cdecl　　B. stdcall　　C. fastcall　　D. naked

问题 2：(2 分)将地址 004010AD 处的指令填写完整 add esp, _____。

问题 3：(3 分)地址 00401059 处指令 lea edi,[ebp-48h]的含义是?

问题 4：(8 分)写出上述汇编码所对应的 C 语言编码。



SUB EAX, EAX

10. 将 AX 中高 8 位清 0 的指令是 AND AX, 0FF4H ，将 AH 的低 4 位取反的指令是 XOR AH, 0FH 。

11. 请写出无条件转移指令中的段间间接转移的指令格式（32 位环境，转移地址保存在 EBX 所指向的内存单元） JMP FEBX 。

12. 数据段中有以下定义：

ARRAY1 EQU 16H

ARRAY2 DWORD 16H

指令 MOV EAX, ARRAY1 中源操作数的寻址方式为 立即寻址 。

指令 MOV EAX, ARRAY2 中源操作数的寻址方式为 直接寻址 。

13. 自内存 Addr 处开始的内存单元中存放着以下数据（十六进制形式）：

01 23 45 67 89 AB CD EF