

中国科学院大学

课程编号: B63002Y

课程名称: 汇编语言

注意事项:

1. 考试时间为 90 分钟, 考试方式 闭卷;
2. 全部答案写在答题纸上;
3. 考试结束后, 请将本试卷和答题纸、草稿纸一并交回。

一、填空 (25 分)

(1) 求下列有符号字节整数的补码 (用 16 进制数表示):

-128 = _____; 123 = _____;

(2) 已知 C 程序结构变量 s_var 定义如下:

```
struct S1 {  
    char c;  
  
    short s[2];  
  
    int i; } s_var;
```

求: 变量 s_var 占据的内存字节数 = _____;

s_var.i 相对 s_var 的 Offset = _____;

(3) 在 x86-Linux 平台上, 已知

```
union { unsigned short s[2]; unsigned int i; } u;
```

```
u.s[0] = 0x2356; u.s[1] = 0x80ab;
```

求: u.i = _____;

(4) 执行下述 x86 程序片断:

```
mov    $0x80, %al  
add    $0x88, %al
```

求 AL 寄存器的值: _____;

求标志位 CF=_____; OF=_____; SF=_____;

(5) 执行下述 x86 程序片断:

```
0x08048074:      call    1f  
0x08048079:  1: pop     %eax
```

求: %eax = _____;

二、改错题 (12 分)

读下面程序段，找出其中的错误，并在不改变程序原意的情况下给出正确的写法

(1) 原程序段

```
...
L1:
    mov     (%edx), %eax
    cmp     %eax, %ebx
    add     $4, %edx
    jne     L1
    ...
```

修改后的程序段:

(2) 原程序段

```
...
.type      func, @function
.globl     func
func:
    push    %ebp
    mov     %esp, %ebp
    mov     8(%ebp), %eax
    add     12(%ebp), %eax
    ret
```

修改后的程序段:

三、读程序(18 分)

读下列程序，给出程序的功能描述

(1)

```
.section .text
.type func1, @function
.globl func1
func1:
    mov     4(%esp), %eax
    test    %eax, %eax
    jns     L1
    neg     %eax
L1:
    ret
```

程序功能: _____

```
(2)
.section .text
.type func2, @function
.globl func2
func2:
    mov     4(%esp), %edx
    xor     %ecx, %ecx
L1:
    mov     (%edx), %al
    test    %al, %al
    jz      L2
    inc     %ecx
    inc     %edx
    jmp     L1
L2:
    mov     %ecx, %eax
    ret
```

程序功能: _____

```
(3)
.section .text
.type func3, @function
.globl func3
func3:
    movl    8(%esp), %edx
    movl    4(%esp), %eax
    fldz
    testl   %edx, %edx
    jle     L2
    leal    (%eax,%edx,8), %edx
L1:
    faddl   (%eax)
    addl    $8, %eax
    cmpl    %edx, %eax
    jne     L1
L2:
    ret
```

程序功能: _____

四、补充完整 (15 分)

(1) Hello.S 输出字符串 "Hello World\n"

```
.section _____
    output:    .ascii  "Hello World\n"
.section _____
_____
_start:
    movl    $4, %eax
    movl    $1, %ebx
    movl    $output, %ecx
    movl    $12, %edx
    int     $0x80
    movl    $1, %eax
    movl    $0, %ebx
    int     $0x80
```

(2) 比较两个有符号整数的参数值, 返回较大的值

```
.globl compare
.type  compare, @function
compare:
    movl    4(%esp), %edx
    movl    8(%esp), %eax
    _____
    _____
    _____
L1: ret
```

(3) 调用子程序 int strcmp(const char *s1, const char *s2)

```
.globl func
.type  func, @function
func:
    push    %ebp
    mov     %esp, %ebp
    sub     $16, %esp
    movl    8(%ebp), %edx        /* address of string s1 */
    movl    12(%ebp), %ecx       /* address of string s2 */
    _____
    _____
    call    strcmp
    ...
    ret
```

五、写程序（30 分）

用汇编语言完成下列子过程的编写，要求符合 X86-Linux-32 ABI 的调用约定

(1) 10 分

```
int var_ele(int n, int a[n][n], int i, int j) {  
    return a[i][j];  
}
```

程序:

(2) 10 分

```
char *delchar(char *str, char c)  
{  
    从字符串参数 str 中删除所有的字符参数 c，返回删除字符后的字符串地址。字符串均以  
    '\0' 字符结尾。  
}
```

程序:

(3) 10 分

```
int findmaxelement(int array[], int length)  
{  
    在长度为 length 的一维整数数组 array 中找出最大的元素，返回该元素的数组索引值；  
    若 length=0，返回-1。  
}
```

程序: