Homework7

姓名 学号

Q1

一个C函数fun具有如下代码体：(参数从右向左入栈)

```
*p = d;
return x-c;
```

执行这个函数体的IA32代码如下：

```
Movsbl  12(%ebp), %edx // 较小的byte->dword, s表示符号填充，z表示0填充
Movl    16(%ebp), %eax
Movl    %edx, (%eax)
Movswl  8(%ebp), %eax
Movl    20(%ebp), %edx
Subl    %eax, %edx
Movl    %edx, %eax
```

写出函数fun的原型，给出参数p, d, x, c的类型和顺序。写出求解过程。

Answer1

Q2

- Suppose the initial value of %esp is 0x7FFFFFC4, initial value of %ebp is 0x7FFFFFF4.
- The value stored in address 0x7FFFFFC0 is 0x120, value stored in address 0x7FFFFFC4 is 0x200, the value stored in address 0x7FFFFFF4 is 0x2710.
- We have following x86 assembly code executed sequentially:

```
pushl %ebp (instruction 1)
movl %esp,%ebp (instruction 2)
popl %ebp (instruction 3)
```

Question: After each instruction executed, what is the value of %esp and %ebp

Answer2

(1) Instruction 1:

(2) Instruction 2:

(3) Instruction 3:

Q3(1)

右边是C语言源代码文件func.c对应的汇编代码，请写出对应的C语言代码；

- 画出Line 24执行前栈的状态，以及此时寄存器%edi, %esi, %edx, %ecx, %rsp的值；

```
.LC0:
    .string "%d %d"
.LC1:
    .string "%d %d %d\n"

main:
    subq    $24, %rsp
    leaq    8(%rsp), %rdx
    leaq    12(%rsp), %rsi
    movl    $.LC0, %edi
    movl    $0, %eax
    call    __isoc99_scanf
    movl    12(%rsp), %ecx
    movl    8(%rsp), %edx
    movl    %edx, %esi
    xorl    %ecx, %esi
    movl    $.LC1, %edi
    movl    $0, %eax
    call    printf
    movl    $0, %eax
    addq    $24, %rsp
    ret
```

Answer3(1)

- 假设进入main函数前%rsp的值为0x8000420（代码中出现的局部变量，要标记在栈图中；图中标记内存地址）

Answer3(2)