Name: _____

Directions: Work only on this sheet (on both sides, if needed); do not turn in any supplementary sheets of paper. There is actually plenty of room for your answers, as long as you organize yourself BEFORE starting writing. In order to get full credit, SHOW YOUR WORK.

1. (10) Consider what happens when the instruction **popl %edx** is executed. Circle all that are true:

(i) EDX changes.

(ii) ESP changes.

(iii) A word in memory changes.

2. Look at the second GDB session printout covered by May in the discussion section. (It consists of an assembly language program adapted from the example in Sec. 7 of our PLN unit on subroutines; output from **as -a**; and a GDB session.)

(a) (10) Look at the lines

```
(gdb) p/x $esp
$4 = 0xbfffcec4
```

Suppose this subroutine had had three arguments instead of two.[1] What value would have been printed out for ESP?

(b) (10) Suppose we were to push **$x+16** instead of **$x+4** on line 22.[2] Choose one:

(i) The assembler would announce an error.

(ii) The linker would announce an error.

(iii) GDB would announce an error.

(iv) A seg fault would occur.

(v) The program would run, and the final value in **sum** would be _____.

(c) (10) At what address does the **.text** segment begin?

3. (10) In the "**u/v/w** story" in Sec. 4.2 of our PLN unit on OS, suppose that in the absence of timesharing, the programs **u**, **v** and **w** would need 2 minutes, 5 hours and 4 hours to run, respectively. Then with timesharing, the total time by which **v** and **w** would delay the completion of **u** would be _____.

4. (30) The assembly language subroutine **preabx**, callable from any assembly language code, will print out the value in EAX at the time of the call. The code is in the file **preabx.s** (shown below), which consists of a total of 9 lines. Fill in the blanks:

[1]This condition applies only to this part, not the other parts in this problem.

[2]This condition applies only to this part, not the other parts in this problem.

```
.text
--------
preabx:
      --------
      --------
      call printf
      addl _________, %esp
      ret
z:    --------
```

5. (10) Fill in the blanks with numbers, possibly including 0: When an interrupt occurs, the CPU's interrupt-response circuitry will read _____ words from memory and write _____ words to memory. (Do not include the fetch of the first instruction of the ISR.)

6. (10) Based on our class materials, deduce the machine language instruction format of the CALL instruction we've been using. Your answer must consist only of 1s, 0s, IMMs, DDDs and SSSs and must fully state the roles of the fields, similar to the statement in our PLN unit on machine language: "[The] format for immediate-to-register move [is] 10111DDDIMM4, where 10111 is the op code, DDD denotes the destination register and IMM4 denotes a 4-byte immediate constant." It is required that you supply a full explanation of how you got your answer.

Solutions:

1. (i) and (ii)

2.a 0xbfffcec0

2.b (v), 9059

2.c 0x8048074

3. 4 minutes

4.

```
.globl preax
push %eax
$8
.string "%x"
```

5. 2, 3

6. 11101000IMM4, where IMM4 is the distance to the subroutine from the instruction following the call