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.

1. (10) Fill in the blank: In addition to using a stack for subroutines, the Intel hardware also uses a stack for __________________________ arithmetic.

2. Look at the assembler output on p.113.

(a) (15) Suppose the instruction **jz done** will placed between lines 29 and 30. What would the 75F8 for **jnz top** change to?

(b) (15) Suppose after linking, it has been decided that the **.data** section will begin at 0x00052000. Then what will change, if anything, in lines 24-34, and what will be the new value there if there is a change?

3. (60) The following code goes through an array that is initially pointed to by EAX, and searches in the array for the value in EBX. The array is terminated by a 0. The result will be placed into EDX—either the index at which the value was found, or -1 if it was not found.

For example, if the array is (1,5,2,13,0) and the value to be searched for is 13, then 3 will be placed into EDX. A search for 5 will result in a 1 in EDX. If the value to be searched for is 88, then -1 will be placed into EDX. Fill in the blanks:

```
      movl %eax, %edi
top:  movl (%eax), %ecx
                                     # put 1 instruction here
      jz foundit
                                     # put 1 instruction here
      jz notthere
                                     # put 1 instruction here
      jmp top
notthere:
                                     # put 1 instruction here
      jmp done
foundit:
      subl %edi, %eax
                                     # put 1 instruction here
      movl %eax, %edx
done: addl $0, %esi  # dummy instruction
```

Solutions:

1. floating-point

2.a The inserted JZ has a 2-byte code like the others, so the JNZ will move 2 bytes further down. That will change its distance to **top** from -8 to -10, the latter being 0xf6. So, the new code for JNZ will be 75F6.

2.b The B900000000 will change to B900200500.

The 891D10000000 will also change. It is clear from inspection of lines 18 and 33 that register-to-memory MOV instructions have the format 891DIMM8, where IMM8 denotes an 8-byte constant. That constant, originally, 10000000, will change to 00200500 as above, so the new instruction will be 891D00200500.

3.

```
      movl %eax, %edi
top:  movl (%eax), %ecx
      cmpl %ecx, %ebx
      jz foundit
      cmpl $0, %ecx
      jz notthere
      addl $4, %eax
      jmp top
notthere:
      movl $-1, %edx
      jmp done
foundit:
      subl %edi, %eax
      shrl $2, %eax
      movl %eax, %edx
done: dec %esi
```