

Questions in Quiz 2 are on the following assembly code. Comments are provided in the code below. No further hints will be provided.

Table 1

RIP (Hexadecimal)	Instruction	Comments
401293	<b>mov rdi, 4</b>	
401298	<b>call factorial</b>	; Returns 4! through rax
40129D	<b>mov rdi, rax</b>	
4012A0	<b>call print_number</b>	; Prints output of 24
4012A5	<b>jmp end_program</b>	
	<b>factorial:</b>	; Function receives 4 as input
4012A7	<b>cmp qword rdi, 1</b>	
4012AB	<b>jne continue_recursion</b>	; jump if comparison is not equal
4012AD	<b>mov rax, 1</b>	
4012B2	<b>ret</b>	; Return to instruction after call command
	<b>continue_recursion:</b>	
4012B3	<b>push rdi</b>	; Push value into stack
4012B4	<b>sub rdi, 1</b>	; Perform rdi-1 and store in rdi
4012B8	<b>call factorial</b>	
4012BD	<b>pop rdi</b>	; Pop value out of stack
4012BE	<b>mul rdi</b>	; Perform rax * rdi and store result in rax
4012C1	<b>ret</b>	

## CMSC313 Quiz 2

Student Name:

The table below is the content of stack when entering the factorial function. `rsp` pointer is at `0xFFB0` and it contains the value of `0x40129D` (the return address of the function call). Execute instructions until `RIP` reaches `0x4012AD` ('`mov rax, 1`' instruction). Fill in the stack content below and in the Pointer column, update the `rsp` pointer.

Stack Physical Addr	Stack Content	Pointer
FFE0		
FFD8		
FFD0		
FFC8		
FFC0		
FFB8		
FFB0	40129D	rsp (start)
FFA8		
FFA0		
FF98		
FF90		
FF88		
FF80		

What are the outputs of `rdi` and `rax` at specified times in `gdb` below:

```
b factorial
b *0x4012bd (pop rdi)
r
c
print $rdi          -> _____
c
c
c
c
print $rax          -> _____
```