IA-32 App Binary Interface (ABI)

calling sequence: call x-bar(a, 1, b) from foo

bar calls baz(a, gore(b, a+b))

push caller-save registers
arguments pushed in reverse order
use call inst.

push old frame ptr
move stack ptr down (create space for locals)
push callee-save registers

do work in subroutine

caller-saved

EAX, ECX, EDX

callee-saved

EBX, EDI, ESP

pop callee-save regs

ret addr

old EBP

locals

callee-save

ret addr

old EBP

locals

callee-save
if (cond) 
  evaluate condition
  conditional branch to else part
  // then part
  .then: do then part
  jump to rest
else 
  .else: do else part
  .rest: rest
  // else part
  }
}
// rest

while (cond) 
  jump test
  // body
  .body:
  code for loop body
  .test: evaluate cond
  conditional branch to start of body
  rest
  // rest