1.NEMU 在什么时候进入了保护模式？

nemu 在实模式下通过 lgdt 指令完成包括初始化段表（如 GDT）和描述符表寄存器（如 GDTR）等初始化操作后，系统通过将 CR0 寄存器中的 PE 位置为 1 进入保护模式. 在此之前 CR0 的 PE 位为 0.

kernel/start/start.S 文件中如下部分即是 nemu 进入保护模式的过程：

```
    lgdt    va_to_pa(gdtdesc) # See i386 manual for more information

# Complete transition to 32-bit protected mode by using long jmp
# to reload %CS and %EIP.  The segment descriptors are set up with no
# translation, so that the mapping is still the identity mapping.
    ljmp    $GDT_ENTRY(1), $va_to_pa(start_cond)

start_cond:
# Set up the protected-mode data segment registers
    movw    $GDT_ENTRY(2), %ax
    movw    %ax, %ds            # %DS = %AX
    movw    %ax, %es            # %ES = %AX
    movw    %ax, %ss            # %SS = %AX
# Enable protection
    movl    %cr0, %eax          # %CR0 |= PROTECT_ENABLE_BIT
    orl     $0x1, %eax
    movl    %eax, %cr0
```

2.在 GDTR 中保存的段表首地址是虚拟地址、线性地址、还是物理地址？为什么？

线性地址. 若 GDTR 中保存的是逻辑地址（虚拟地址），那么 GDTR 中的地址需要经过段处理器转换为线性地址，这一过程中也需要先知到段表首地址（GDTR）的线性地址，这就造成了死循环. 若 GDTR 中保存的地址是物理地址，由于段地址是线性的，两者无法放在一起处理. 故 GDTR 中保存的应该是线性地址.