<ch6. Double Fault Exception>.

Case: stack overflow (the guard page is hit).

a special mem page at the bottom of a stack.
? (to detect stack overflow)
accessing it will cause a Page fault.

① CPU looks up the page fault handler (in IDT)
tries to push the interrupt stack frame onto the stack.

② current rsp still points to gaurd page
⇒ a second page fault (double)

③ ... (recursively)

Sol: switching stacks (x86-64).
when an exception occurs, (hardware level)
switch to a predefined, known-good stack.

Interrupt Stack Table (IST): 7 pointers to
each exception handler
IDT entry → (each) 'stack pointer' field.

(让 double fault 对应 IST 中 #1. stack ptr.
在CPU异常时，自动切换为该栈.
该切换会在所有入栈操作之前进行 ⇒ 避免 triple fault).

Hardwares (for switching stacks).

used by CPU when privilege level changes.

① Task State Segment (TSS)
- Privilege stack table ([u64; 3])
- Interrupt stack table ([u64; 7]).
- I/O Map Base Address

② Global Descriptor Table (GDT)
- Switching between user & kernel
- Loading a TSS structure.

- contains the segments of the program. (before paging)

(Recall: "Three Easy Pieces")