1. 为什么在装载时要把内存中剩余的p\_memsz - p\_filesz字节的内容清零？

否则若上一次装载时若旧的p\_filesz大于新的p\_filesz，位于它们之间的数据没有被覆盖而仍然存在，执行程序时，eip指针可能会访问到新的p\_filesz后面的内容，出现难以预料的效果。清零可以保证p\_filesz与p\_memsz之间均为安全值0，防止这种情况发生。