# QEMU

退出qemu

ctrl+a+x

利用qemu查看页表

先知行ctrl+a+c，再执行info mem

# GDB

## tui

启用图形：tui enable

将源码与汇编代码分割显示：layout split

展示源码：layout src

展示汇编：layout asm

展示寄存器：layout reg

聚焦于某个窗口：focus src/asm/reg

## 设置断点

在函数处设置断点：b 函数名

例：b kvminit

在源码某行设断点：b 文件地址/文件名:行号

例：b kernel/vm.c:128

在某地址处设断点：b \*地址值

例：b \*0x3ffffff10e

## 查看断点

info break

## 删除断点

删除指定断点：d 断点编号

例：d 2

删除指定编号范围的断点：d 起始断点编号-终止断点编号

例：d 2-8

## print

普通打印：print 变量名

打印数组：print \*argv@2

打印寄存器：p/x $pc

打印某地址处的指令：x/2i 地址或$pc

## next

next：单步执行下一行源码

nexti：单步执行下个汇编指令

## step

step：执行下一行代码（会进入函数）

stepi：执行下个汇编代码（会进入函数）

## frame

查看当前栈帧信息：info frame

查看参数信息：info args

获取所有栈帧：backtrace

切换到某个栈帧：frame 栈帧号