GDB cheat sheet

call gdb
gdb prog, gdb --args prog [progargs]
r, run [args]   run the program
attach <pid>, detach   attach/detach gdb to/from process

navigating
c [ignore count]   continue
s, step [count]   continue until different src line
n, next [count]   like step, do not follow funciton calls
u, until [loc]   like next, but only src line below
fin, finish   continue until current function returns
advance <loc>   continue until location is reached
si, stepi, ni, nexti   like step and next for machine instr

breakpoints
break <loc>   set a breakpoint
break … if <cond>   set a conditional breakpoint
tbreak …   like break, but only for one shot
watch <expr>   stop when <expr> changes its value
clear <loc>   delete breakpoint at location
d, delete   delete all breakpoints, watchpoints, etc
handle <signal> [opt]   set how signals are handle. opt can be
                                [no]stop, [no]print, [no]pass
dis [N]   disable breakpoint N resp. all

examine data
frame <addr>, frame #   move to stack frame and print info
select-frame   like stack, but without printing info
bt, bt N, bt -N   print backtrace (call stack)
bt full   like bt, but with local variables
info f, info frame   print verbose info of the selected frame
info args, info locals   info on function args, local variables
info registers   print registers. Also: p/x $pc, x/i $pc
$pc, $fp, $sp   program cntr, frame pntr, stack pntr
info address <symb>   get address of symbol
info symbol <addr>   get the name of the symbol at addr
p, print <expr>   print value of given expr
p *array@len   print array of given length
x <addr>, x/N <addr>   print N bytes from memory
display <expr>   display expr whenever gdb stops
set pretty print on   print arrays nicer

show code
list <loc>   print source lines
list   list more source
disas [/m] start,+len   show disassembled source code

location <loc>
linenum   the line in the current source file
-offset, +offset $offset lines before/after current line
filename:linenum   given line in given source file
function   start of given function
*address   given address