question 1

1. `xor %eax, %eax` 可将 `%eax` 置零

```
int foo(int op, int a, int b) {
    int result = 0;
    switch(op) {
        case 0:
            result = a;
            result &= b;
            break;
        case 1:
            result = a;
            result |= b;
            break;
        case 2:
            result = a;
            result ^= b;
            break;
        case 3:
            result = ~a;
            break;
        case 4:
            result = a + b;
            break;
    }
    return result;
}
```

question 2

```
typedef enum {MODE_A, MODE_B, MODE_C, MODE_D, MODE_E} mode_t;
int switch3(int *p1, int *p2, mode_t action) {
    int result = 0;
    switch(action) {
        case MODE_A:
            result = *p1;
            *p1 = *p2;
            break;
        case MODE_B:
            result = *p2 + *p1;
            *p2 = result;
            break;
        case MODE_C:
            *p2 = 59;
            result = *p1;
            break;
        case MODE_D:
            *p2 = *p1;
            result = 27;
            break;
```

```
        case MODE_E:
            result = 27;
            break;
        default:
            result = -1;
    }
    return result;
}
```

question 3

1. `%eax = 0x8048395`
2. `%eip = 0x804839b`

question 4

```
int lolwut(char *s) {
    int i, n;
    n = 0;
    for (i = 0; s[i] != 0; i++) {
        if (s[i] - '0' > 9) {
            return -1;
        }
        n = n*10 + s[i] - '0';
    }
    return n;
}
```

```
subl $4, %esp
movl %ebx, (%esp)
```

```
0xffff000c
```

question 5

1.

address	
0xffffd830	4
0xffffd82c	0x080483e6
0xffffd828	0xffffd848
0xffffd824	%ebx
0xffffd820	3
0xffffd81c	0x080483be
0xffffd818	0xffffd828
0xffffd814	4
0xffffd810	2

2. `0xffffd818`
3. `0xffffd810`

question 6

1. `%ebp = 0x80003c`
2. `%esp = 0x7ffffc`
3.

```
&x = 0x800038
&y = 0x800034
```

4.

address	
0x800040	return address
0x80003c	0x800060
0x800038	0x53
0x800034	0x46
...	not used
0x800004	0x800038
0x800000	0x800034
0x7ffffc	0x300070

5. `0x800008 ~ 0x800030` are not used by `proc`

question 7

part 1

1. 查看 `0000:00 ~ 0000:1f` 的内存

```
-d 0000:00 1f
0000:0000  60 10 00 F0 08 00 70 00-08 00 70 00 08 00 70 00   `.....p...p...p.
0000:0010  08 00 70 00 60 10 00 F0-60 10 00 F0 60 10 00 F0   ..p.`...`...`...
```

2.

```
C:\>debug
-r cs
CS 073F
:1000
-r ip
IP 0100
:0
```

然后将那些命令都输进去。。。

```
-a 1000:0
1000:0000 mov ax,1
1000:0003 mov ds,ax
1000:0005 mov ax,[0000]
1000:0008 mov bx,[0001]
1000:000C mov ax,bx
1000:000E mov ax,[0000]
1000:0011 mov bx,[0002]
1000:0015 mov ax,bx
1000:0017
-a 1000:15
1000:0015 add ax,bx
1000:0017 add ax,[0004]
1000:001B mov ax,0
1000:001E mov al,[0002]
1000:0021 mov bx,0
1000:0024 mov bl,[000c]
1000:0028 add al,b1
1000:002A
-
```

之后不断按 `-t`

1~4

```
-t

AX=0001  BX=0000  CX=0000  DX=0000  SP=00FD  BP=0000  SI=0000  DI=0000
DS=073F  ES=073F  SS=073F  CS=1000  IP=0003   NV UP EI PL NZ NA PO NC
1000:0003 8ED8          MOV     DS,AX
-t

AX=0001  BX=0000  CX=0000  DX=0000  SP=00FD  BP=0000  SI=0000  DI=0000
DS=0001  ES=073F  SS=073F  CS=1000  IP=0005   NV UP EI PL NZ NA PO NC
1000:0005 A10000        MOV     AX,[0000]                       DS:0000=0008
-t

AX=0008  BX=0000  CX=0000  DX=0000  SP=00FD  BP=0000  SI=0000  DI=0000
DS=0001  ES=073F  SS=073F  CS=1000  IP=0008   NV UP EI PL NZ NA PO NC
1000:0008 8B1E0100      MOV     BX,[0001]                       DS:0001=7000
-t

AX=0008  BX=7000  CX=0000  DX=0000  SP=00FD  BP=0000  SI=0000  DI=0000
DS=0001  ES=073F  SS=073F  CS=1000  IP=000C   NV UP EI PL NZ NA PO NC
1000:000C 89D8          MOV     AX,BX
-_
```

5~8

```
-t

AX=7000  BX=7000  CX=0000  DX=0000  SP=00FD  BP=0000  SI=0000  DI=0000
DS=0001  ES=073F  SS=073F  CS=1000  IP=000E   NV UP EI PL NZ NA PO NC
1000:000E A10000        MOV     AX,[0000]                       DS:0000=0008
-t

AX=0008  BX=7000  CX=0000  DX=0000  SP=00FD  BP=0000  SI=0000  DI=0000
DS=0001  ES=073F  SS=073F  CS=1000  IP=0011   NV UP EI PL NZ NA PO NC
1000:0011 8B1E0200      MOV     BX,[0002]                       DS:0002=0070
-t

AX=0008  BX=0070  CX=0000  DX=0000  SP=00FD  BP=0000  SI=0000  DI=0000
DS=0001  ES=073F  SS=073F  CS=1000  IP=0015   NV UP EI PL NZ NA PO NC
1000:0015 01D8          ADD     AX,BX
-t

AX=0078  BX=0070  CX=0000  DX=0000  SP=00FD  BP=0000  SI=0000  DI=0000
DS=0001  ES=073F  SS=073F  CS=1000  IP=0017   NV UP EI PL NZ NA PE NC
1000:0017 03060400      ADD     AX,[0004]                       DS:0004=1060
-
```

9~12

```
-t

AX=10D8  BX=0070  CX=0000  DX=0000  SP=00FD  BP=0000  SI=0000  DI=0000
DS=0001  ES=073F  SS=073F  CS=1000  IP=001B   NV UP EI PL NZ NA PE NC
1000:001B B80000        MOV     AX,0000
-t

AX=0000  BX=0070  CX=0000  DX=0000  SP=00FD  BP=0000  SI=0000  DI=0000
DS=0001  ES=073F  SS=073F  CS=1000  IP=001E   NV UP EI PL NZ NA PE NC
1000:001E A00200        MOV     AL,[0002]                       DS:0002=70
-t

AX=0070  BX=0070  CX=0000  DX=0000  SP=00FD  BP=0000  SI=0000  DI=0000
DS=0001  ES=073F  SS=073F  CS=1000  IP=0021   NV UP EI PL NZ NA PE NC
1000:0021 BB0000        MOV     BX,0000
-t

AX=0070  BX=0000  CX=0000  DX=0000  SP=00FD  BP=0000  SI=0000  DI=0000
DS=0001  ES=073F  SS=073F  CS=1000  IP=0024   NV UP EI PL NZ NA PE NC
1000:0024 8A1E0C00      MOV     BL,[000C]                       DS:000C=60
-
```

13

```
-t

AX=0070  BX=0060  CX=0000  DX=0000  SP=00FD  BP=0000  SI=0000  DI=0000
DS=0001  ES=073F  SS=073F  CS=1000  IP=0028   NV UP EI PL NZ NA PE NC
1000:0028 04B1          ADD     AL,B1
-
```

3.

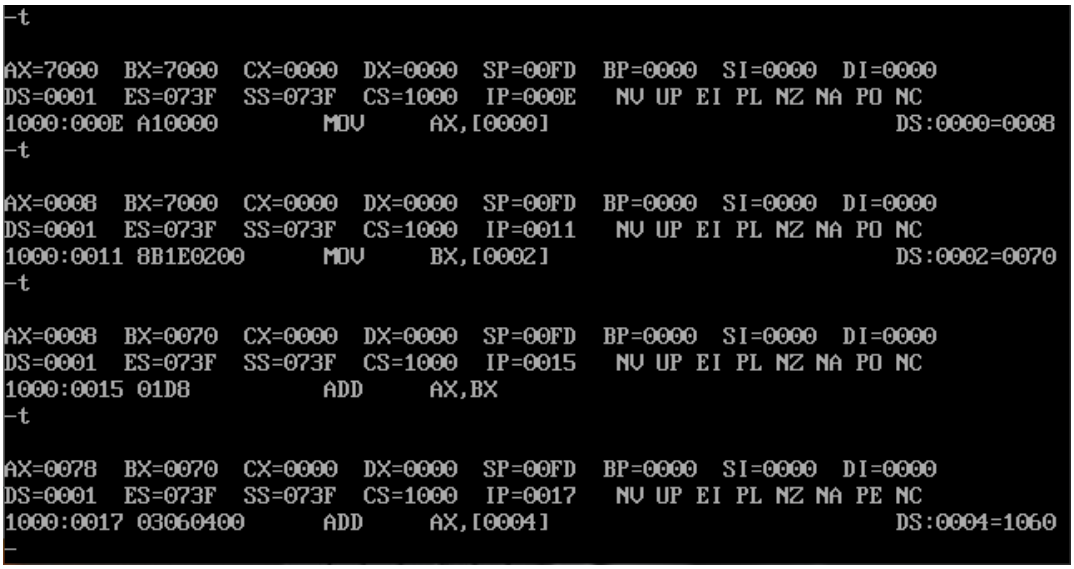
(1) AX=0008
(2) BX=7000
(3) AX=7000
(4) AX=0008
(5) BX=0070
(6) AX=0078
(7) AX=10D8
(8) AX=0000
(9) AX=0070
(10) BX=0000
(11) BX=0060
(12) AX=00D0

part 2

1. `00000~9ffff` 主存储器

   `a0000~bffff` 显存

   `c0000~fffff` 各种 ROM

2. 
```
-t

AX=7000  BX=7000  CX=0000  DX=0000  SP=00FD  BP=0000  SI=0000  DI=0000
DS=0001  ES=073F  SS=073F  CS=1000  IP=000E   NV UP EI PL NZ NA PO NC
1000:000E A10000        MOV     AX,[0000]                       DS:0000=0008
-t

AX=0008  BX=7000  CX=0000  DX=0000  SP=00FD  BP=0000  SI=0000  DI=0000
DS=0001  ES=073F  SS=073F  CS=1000  IP=0011   NV UP EI PL NZ NA PO NC
1000:0011 8B1E0200      MOV     BX,[0002]                       DS:0002=0070
-t

AX=0008  BX=0070  CX=0000  DX=0000  SP=00FD  BP=0000  SI=0000  DI=0000
DS=0001  ES=073F  SS=073F  CS=1000  IP=0015   NV UP EI PL NZ NA PO NC
1000:0015 01D8          ADD     AX,BX
-t

AX=0078  BX=0070  CX=0000  DX=0000  SP=00FD  BP=0000  SI=0000  DI=0000
DS=0001  ES=073F  SS=073F  CS=1000  IP=0017   NV UP EI PL NZ NA PE NC
1000:0017 03060400      ADD     AX,[0004]                       DS:0004=1060
-
```

3. 三个数字分别代表黑色、绿色、灰色