一. 选择题

1. A
2. B(A 符号扩展,C 是 cltq,D 缺少 $ 符)
3. C(A`%rsp` 是例外,B 可用于判断是否为零的是`test`,D 移位操作设置进位条件码, 但把溢出条件码设置为零)
4. C 解析：`'0'` 的 ASCII 码为 48，`'1''2''7'` 在跳转表中未出现
5. B 解析：A.`leal` 指令做普通算术运算；C.caller saved 寄存器才需要；D. 还需要 `OF`
6. C
7. D 解析：A. 条件传送不支持单字节传送；B. 如果`?:` 涉及到的两个表达式中有一个出错或者有副作用，用条件传送会导致非法行为；C. 如果被旁路的分支的计算量很大，计算就白做了；D. 从目标寄存器的名字可以推断出条件传送指令的操作数长度
8. A 本题考察 x86-64 中的一些基本指令，答案为 A。a 项错误，原因是 `idivq` 将余数存在`%rdx` 中，将商存在`%rax` 里。b 项错误，间接跳转的正确书写格式应为 `jmp *%rax`。c 项错误，算术右移指令应为 `sar`。
9. A。解析：本题考察 x86-64 条件码，答案为 A。`cmpq a,b` 相当于通过`b-a` 的值来设置条件码。`SF ^ OF` 为 1 表示 `b < a`（减法结果要么负溢出要么为负数），于是`~(SF ^ OF)` 表示 `b >= a`，再与上 `b != a` 的条件`~ZF`，就可以得到最终结果`b > a`。

二. 填空题

```
long func(long a, long b) {
    long ans = 1;
    while (b > 0) {
        if (b & 1)
        ans = ans * a;
        b = b >> 1;
        a = a * a;
    }
    return ans;
}
```

三. 大题

I.

```
(1) 4005bd <func+0x27>
(2) 4005e2 <func+0x4c>
(3) %rsp
(4) %fs:0x28
```

```
(5) je
(6) $0x28
(7) p->b == 0
(8) p->a - p->b
(9) p->b
(10) 105
(11) 252
```

II.

```
......
    0x0000000000000000(u)
    0xc76d5add7bbeaa00
    0x00007fffffffdf60(u?)
(a) 0x0000000000000069
(b) 0x00000000000000fc
    0x0000000000400629
(c) // unknown
(d) 0xc76d5add7bbeaa00
    0x0000000000000001(u)
    0x0000000000000069
    0x0000000000000093
(e) 0x00000000004005e2
    0x00000000ff000000(u)
(f) 0xc76d5add7bbeaa00
    0x0000000000000000(u)
(g) 0x000000000000002a
(h) 0x0000000000000069
(i) 0x00000000004005e2
    0x0000000000000000(u)
(j) 0xc76d5add7bbeaa00
(k) // unknown
    0x000000000000002a
    0x000000000000003f
    0x00000000004005e2
// stack top (low address)
```

III. 21