

一. 第二章题目

1. 给定一个实数, 会因为该实数表示成单精度浮点数 (float) 而发生误差。不考虑NaN和Inf的情况, 该绝对误差的最大值为_____ **A** _____

A. 2^{103} B. 2^{104} C. 2^{230} D. 2^{231}

2. 运行下述代码, 结果为: $2^{24}+1$

```
for (int x = 0; ; ++x) {  
    float f = x;  
    if (x != (int)f) {  
        printf("%d", x);  
5         break;  
    }  
}
```

3. 运行下述代码, 结果为: **2, -1, 0, 1, -2, -1, 0, 1**

```
int x = 33554466; // 2^25+34  
int y = x + 8;  
for(; x < y; ++x) {  
    float f = x;  
5    printf("%d", x - (int)f);  
}
```

4. 在遵守 IEEE 754 标准的一台机器上声明如下三个变量double f, g, h, 判断:

若 $f > g$, 则 $f + 1 > g + 1$: **F**

若 $f > g \ \&\& \ g > 1$, 则 $f - 1 > g - 1$: **F**

二.【汇编大题】以下提供了一段代码的 C 语言、汇编语言以及运行到某一时刻栈的情况

I. 互相翻译 C 语言代码和汇编代码，补充缺失的空格（标号相同的为同一格）。

```

0000000000400596 <func>:
400596: sub $0x28,%rsp
40059a: mov (4)____,%rax
4005a3: mov %rax,0x18(%rsp)
5 4005a8: xor %eax,%eax
4005aa: mov (%rdi),%rax
4005ad: mov 0x8(%rdi),%rdx
4005b1: cmp %rdx,%rax
4005b4: jge (1)____
10 4005b6: mov %rdx,(%rdi)
4005b9: mov %rax,0x8(%rdi)
4005bd: mov 0x8(%rdi),%rax
4005c1: test %rax,%rax
4005c4: jne 4005cb <func+0x35>
15 4005c6: mov (%rdi),%rax
4005c9: jmp (2)____
4005cb: mov (%rdi),%rdx
4005ce: sub %rax,%rdx
4005d1: mov %rdx,(%rsp)
20 4005d5: mov %rax,0x8(%rsp)
4005da: mov (3)____,%rdi
4005dd: callq 400596 <func>
4005e2: mov 0x18(%rsp),%rcx
4005e7: xor %fs:0x28,%rcx
25 4005f0: (5)____ 4005f7 <func+0x61>
4005f2: callq 400460 <__stack_chk_fail@plt>
4005f7: add (6)____,%rsp
4005fb: retq

30 00000000004005fc <main>:
4005fc: sub $0x28,%rsp
400600: mov %fs:0x28,%rax
400609: mov %rax,0x18(%rsp)
40060e: xor %eax,%eax
35 400610: movq 0x69,(%rsp)
400618: movq 0xfc,0x8(%rsp)

```

```

400621: mov %rsp,%rdi
400624: callq 400596 <func>
400629: mov %rax,%rsi
40 40062c: mov $0x4006e4,%edi
400631: mov $0x0,%eax
400636: callq 400470 <printf@plt>
40063b: mov 0x18(%rsp),%rdx
400640: xor (4)____,%rdx
45 400649: (5)____ 400650 <main+0x54>
40064b: callq 400460 <__stack_chk_fail@plt>
400650: mov $0x0,%eax
400655: add (6)____,%rsp
400659: retq

```

```

typedef struct{ long a; long b; } pair_type;
long func(pair_type *p) {
    if (p->a < p->b) {
        long temp = p->a;
5      p->a = p->b;
        p->b = temp;
    }
    if ((7)____ ) return p->a;
    pair_type np;
10    np.a = (8)____;
    np.b = (9)____;
    return func(&np);
}
int main(int argc, char* argv[]) {
15    pair_type np;
    np.a = (10)____;
    np.b = (11)____ ;
    printf("%ld", func(&np));
    return 0;
20 }

```

(1) _____

(2) _____

(3) _____

(4) _____

(5) _____

(6) _____

(7) _____

(8) _____

(9) _____

(10) _____

(11) _____

附: 一些可能用到的字符的 ASCII 码表

\n	space	"	%	()	,	0	A	a
0x0a	0x20	0x22	0x25	0x28	0x29	0x2c	0x30	0x41	0x61

II. 补充栈的内容。使用 16 进制，可以不写前导多余的 0；对于给定已知条件后仍无法确定的值，填写“不确定”；已知程序运行过程中寄存器%fs 的值没有改变

	0x0000000000000000
	0xc76d5add7bbeaa00
	0x00007fffffffdf60
5	(a) _____
	(b) _____
	0x0000000000400629
	(c) _____
	(d) _____
10	0x0000000000000001
	0x0000000000000069
	0x0000000000000093
	(e) _____
	0x00000000ff000000
15	(f) _____
	0x0000000000000000
	(g) _____
	(h) _____
	(i) _____
20	0x0000000000000000
	(j) _____
	(k) _____
	0x000000000000002a
	0x000000000000003f
25	0x00000000004005e2
	// stack top (low address)

III. 程序运行结果为_____.

答:

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

25

```
0x0000000000000002a
0x0000000000000003f
0x00000000004005e2
// stack top (low address)
```

III. 21