

注：所有汇编代码采用 AT&T 格式。

1. XXX 村的秘密武器——功能强大的 C 语言函数 `func` 的源代码因为粗心的小 z 打翻墨水而变得不可读；人们赶到现场时只看到了这段反汇编代码和小 z 回忆的代码大致形式，请你推测 `func` 的功能。

0000000000400497 <func>:

400497:	44 8d 46 ff	lea	-0x1(%rsi),%r8d
40049b:	45 85 c0	test	%r8d,%r8d
40049e:	7e 37	jle	4004d7 <func+0x40>
4004a0:	4c 8d 4f 04	lea	0x4(%rdi),%r9
4004a4:	eb 1f	jmp	4004c5 <func+0x2e>
4004a6:	48 83 c0 04	add	\$0x4,%rax
4004aa:	48 39 f0	cmp	%rsi,%rax
4004ad:	74 10	je	4004bf <func+0x28>
4004af:	8b 10	mov	(%rax),%edx
4004b1:	8b 48 04	mov	0x4(%rax),%ecx
4004b4:	39 ca	cmp	%ecx,%edx
4004b6:	7e ee	jle	4004a6 <func+0xf>
4004b8:	89 08	mov	%ecx,(%rax)
4004ba:	89 50 04	mov	%edx,0x4(%rax)
4004bd:	eb e7	jmp	4004a6 <func+0xf>
4004bf:	41 83 e8 01	sub	\$0x1,%r8d
4004c3:	74 12	je	4004d7 <func+0x40>
4004c5:	45 85 c0	test	%r8d,%r8d
4004c8:	7e f5	jle	4004bf <func+0x28>
4004ca:	48 89 f8	mov	%rdi,%rax
4004cd:	41 8d 50 ff	lea	-0x1(%r8),%edx
4004d1:	49 8d 34 91	lea	(%r9,%rdx,4),%rsi
4004d5:	eb d8	jmp	4004af <func+0x18>
4004d7:	f3 c3	repz retq	

```
void func(int arr[], int len) {
```

```
    ...
    for ()
        for () {
            if () {
            }
        }
}
```

2. 反汇编代码填空 (Linux x86-64 01 优化)

000000000400497 <fib>:

400497:	b8 01 00 00 00	mov	____, %eax
40049c:	83 ff 01	cmp	\$0x1, %edi
40049f:	77 ____	ja	4004a3 <fib+0xc>
4004a1:	f3 c3	repz	retq
4004a3:	55	push	%rbp
4004a4:	53	push	%rbx
4004a5:	48 83 ec 08	sub	\$0x8, %rsp
4004a9:	89 fb	mov	____, %ebx
4004ab:	8d 7f ff	____	-0x1(%rdi), %edi
4004ae:	e8 ____ ff ff ____	callq	400497 <fib>
4004b3:	89 c5	mov	____, %ebp
4004b5:	8d 7b fe	____	-0x2(%rbx), %edi
4004b8:	e8 ____ ff ff ____	callq	400497 <fib>
4004bd:	01 e8	add	____, %eax
4004bf:	48 83 c4 08	____	____, ____
4004c3:	5b	____	____
4004c4:	5d	____	____
4004c5:	c3	retq	

int fib(int n)

```
{
    if (n == 0 || n == 1)
        return 1;
    return fib(n - 1) + fib(n - 2);
}
```