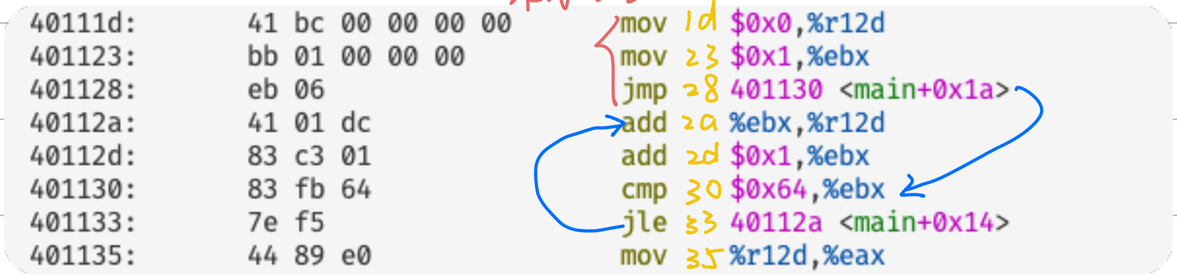
初始



```
40111d:    41 bc 00 00 00 00    mov 1d $0x0,%r12d
401123:    bb 01 00 00 00       mov 23 $0x1,%ebx
401128:    eb 06                jmp 28 401130 <main+0x1a>
40112a:    41 01 dc             add 2a %ebx,%r12d
40112d:    83 c3 01             add 2d $0x1,%ebx
401130:    83 fb 64             cmp 30 $0x64,%ebx
401133:    7e f5                jle 33 40112a <main+0x14>
401135:    44 89 e0             mov 35 %r12d,%eax
```

变的 reg：pc，%r12d，%ebx，flag

(1d, x, x, x)

↓

(23, 0, x, x)

↓

(28, 0, 1, x)

↓

(30, 0, 1, x)

↓

(33, 0, 1, 0)

↓ 开始第一个循环

(2a, 0, 1, 0)

↓

(2d, 1, 1, 0)

↓

(30, 1, 2, 0)

↓

(33, 1, 2, 0)

↓

第2次
↓

(2a, 1, 2, 0)

↓

(2d, 3, 2, 0)

↓

(30, 3, 3, 0)

↓

(33, 3, 3, 0)

↓

...... - -

↓

(2a, x, 99, 0)

4851

↓

(2d, x+99, 99, 0)

4950

↓

(30, x+99, 100, 0)

4950

↓

(33, x+99, 100, 0)

4950

↓

(2a, x+99, 100, 0)

4950

↓

(2d, x+99+100, 100, 0)

5050

$$\downarrow$$

$$(30,\ \underbrace{x+99+100}_{5050},\ 101,\ 0)$$

$$\downarrow$$

$$(33,\ \underbrace{x+99+100}_{5050},\ 101,\ 1)$$

$$\downarrow$$

$$(35,\ \underbrace{x+99+100}_{5050},\ 101,\ 1)$$

結束