3

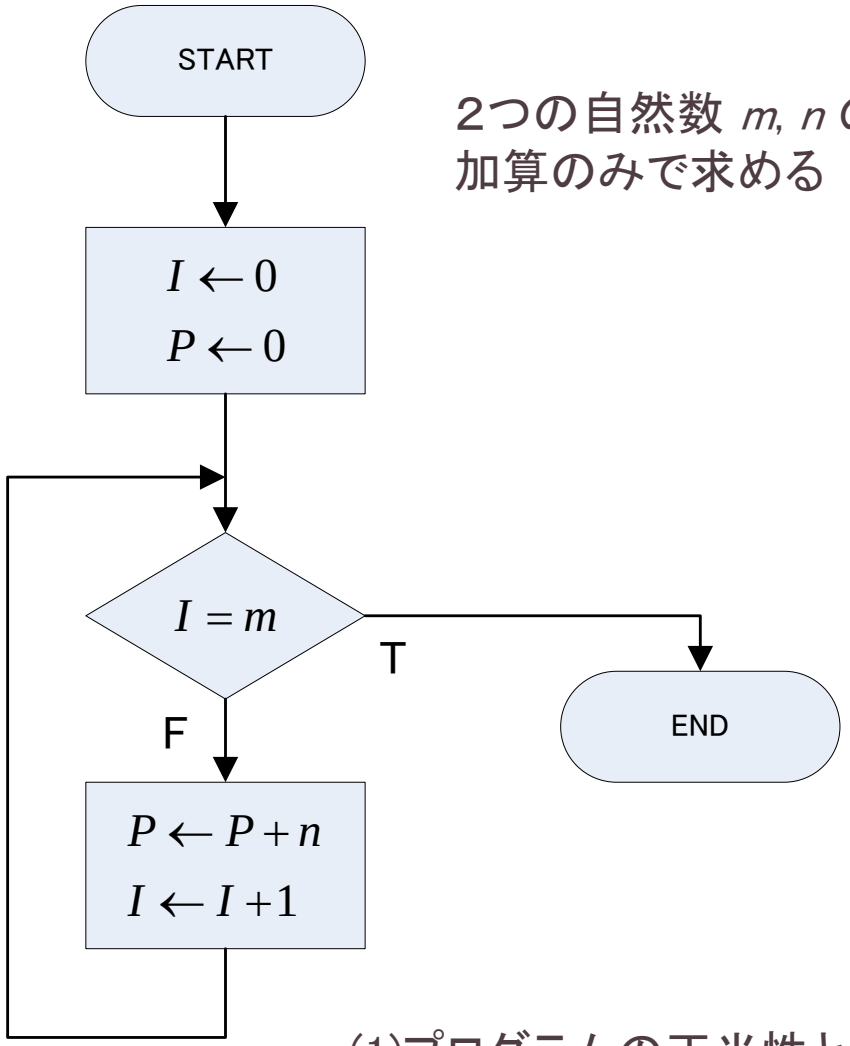
ソフトウェア工学

Software Engineering

プログラムの正当性

CORRECTNESS OF PROGRAMS

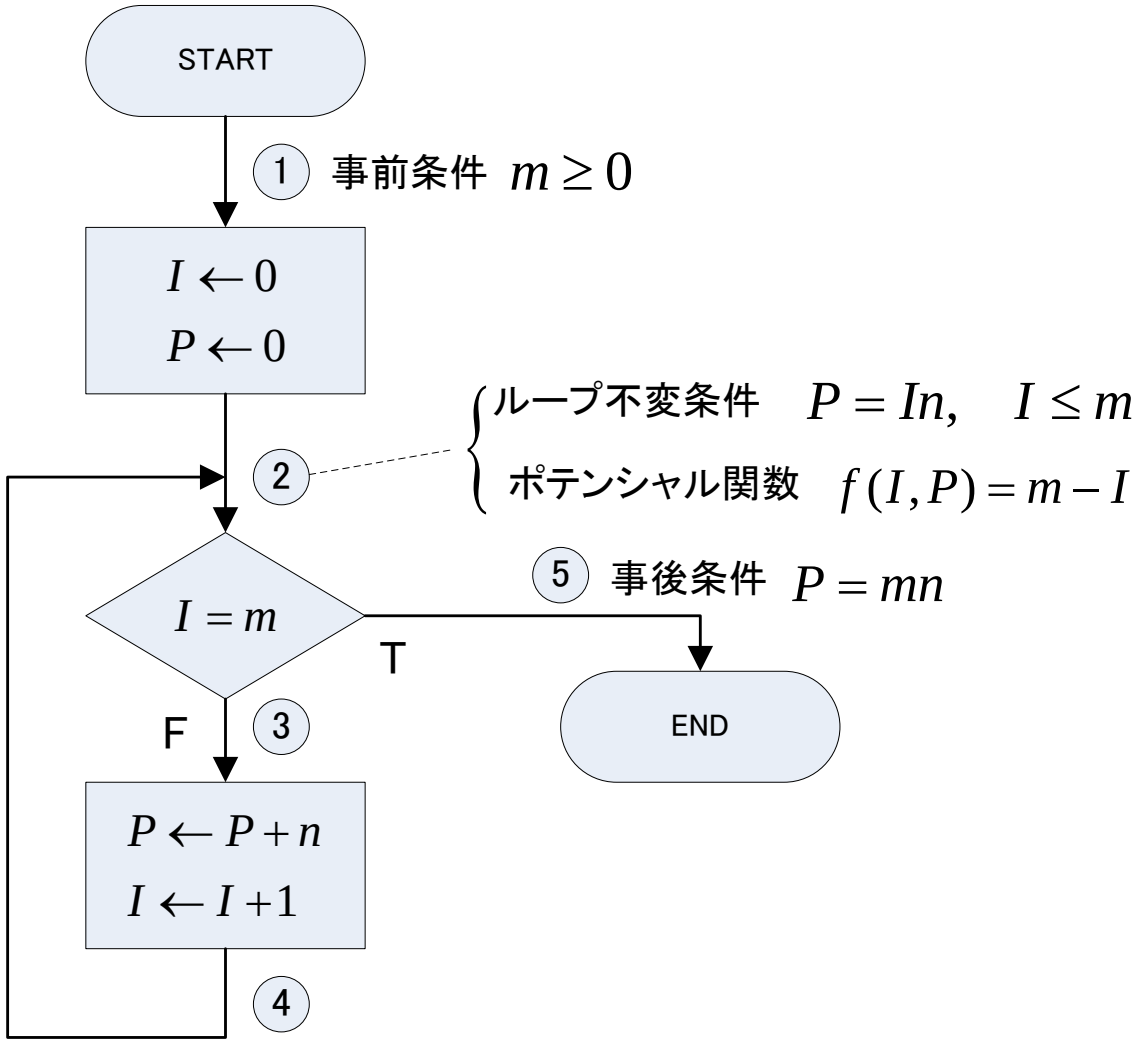
例題：つぎのプログラムの正当性を証明しなさい



2つの自然数 *m*, *n* の積を
加算のみで求める

(1)プログラムの正当性とは何か
(2)正当性をどのように証明するのか

アサーションとポテンシャル関数を付ける



mとnの積P

アサーション（assertion: 表明，断言）

アサーション---プログラム変数の値の間に成り立つ関係を表す命題

- 特定の位置（流れ図の辺）において定義される
- 制御がその位置に達したときは，その命題は常に真

- おもにつぎの3つの種類がある.

(1) **事前条件**(precondition)

プログラムの入口で定義

受け入れ可能な入力についての記述

```
m,n >= 0
```

(2) **事後条件**(postcondition)

プログラムの出口で定義

正しい出力が満たすべき条件の記述

```
p == m*n
```

(3) **ループ不変条件**(loop invariant)

ループの出入口で常に成り立つ関係式

```
P == I*n
 I <= n
```

ポテンシャル関数 (potential function)

ポテンシャル関数---プログラム変数の値を用い，整数値を返す関数.

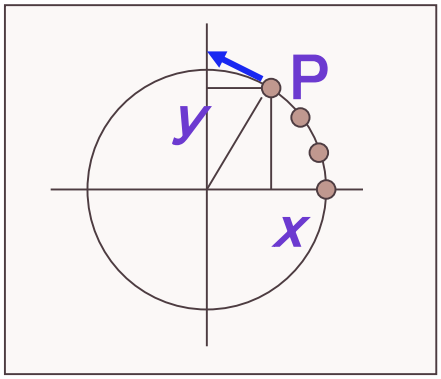
- 流れ図の特定の位置（辺）で定義される.
- その値（ポテンシャル）は常に非負.
- 制御がここを通過する毎にその値が必ず減少する.

```
f(I,P) = m-I
```

ループ不変条件の補足

円をプロットするプログラム？

```
for(k = 0; k<n; k++) {
      x = r * cos(k* θ );
      y = r * sin(k* θ );
      plot (x,y);
}
```



■いかに証明するか？

$$x^2 + y^2 = r^2 (\cos^2 k\theta + \sin^2 k\theta) = r^2 (=\text{constant})$$

ループ不変条件

時間とともに**変化する**様子を説明するには，
何が時間によって**変化しない**かを説明する．

（類似例）**エネルギー保存の法則**

$$mgh + mv^2/2 = \text{constant}$$

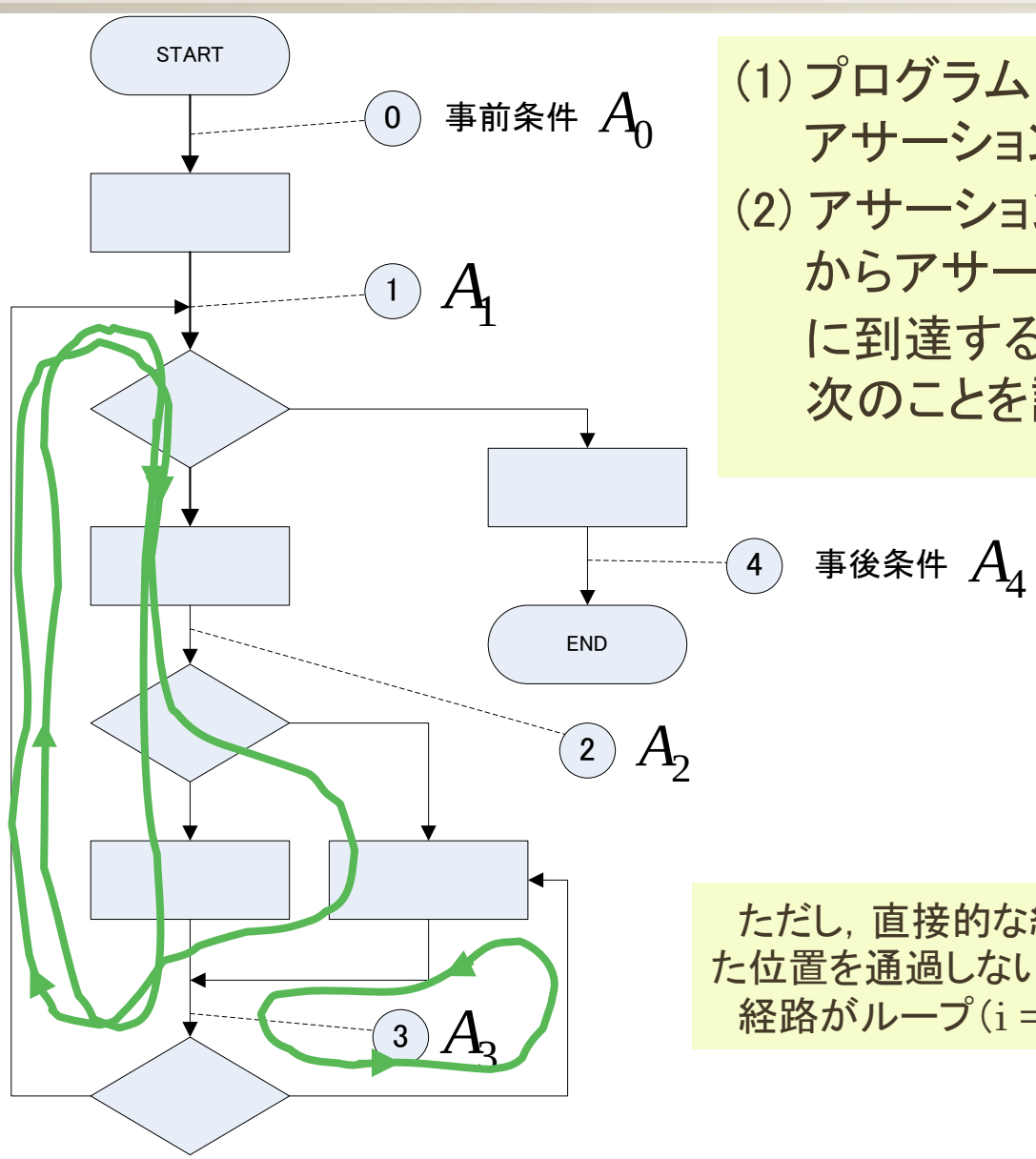
プログラムの正当性の定義

プログラムの正当性 (correctness)

事前条件を満たす任意の入力に対して，つぎの2つの性質を満たすこと．

部分正当性 partial correctness	もし実行が停止すれば，その時点で事後条件が成り立つ （計算結果がもし得られれば，それは正しい）
停止性 termination	必ず実行が停止する （必ず計算結果が得られる）

部分正当性の証明方法(フロイドの方法)



(1) プログラムの各ループの少なくとも1カ所にアサーションを書く.

(2) アサーション A_i を書いた位置 i からアサーション A_j を書いた位置 j に到達するすべての経路ごとに次のことを証明する.

■位置 i で A_i が真のとき, その経路に沿ってプログラムを実行して位置 j に到達した時点で A_j は真である

ただし, 直接的な経路(途中で他のアサーションが書かれた位置を通過しない経路)についてのみでよい.
経路がループ(i = j) の場合も含めて証明する.

例題：①→② の証明

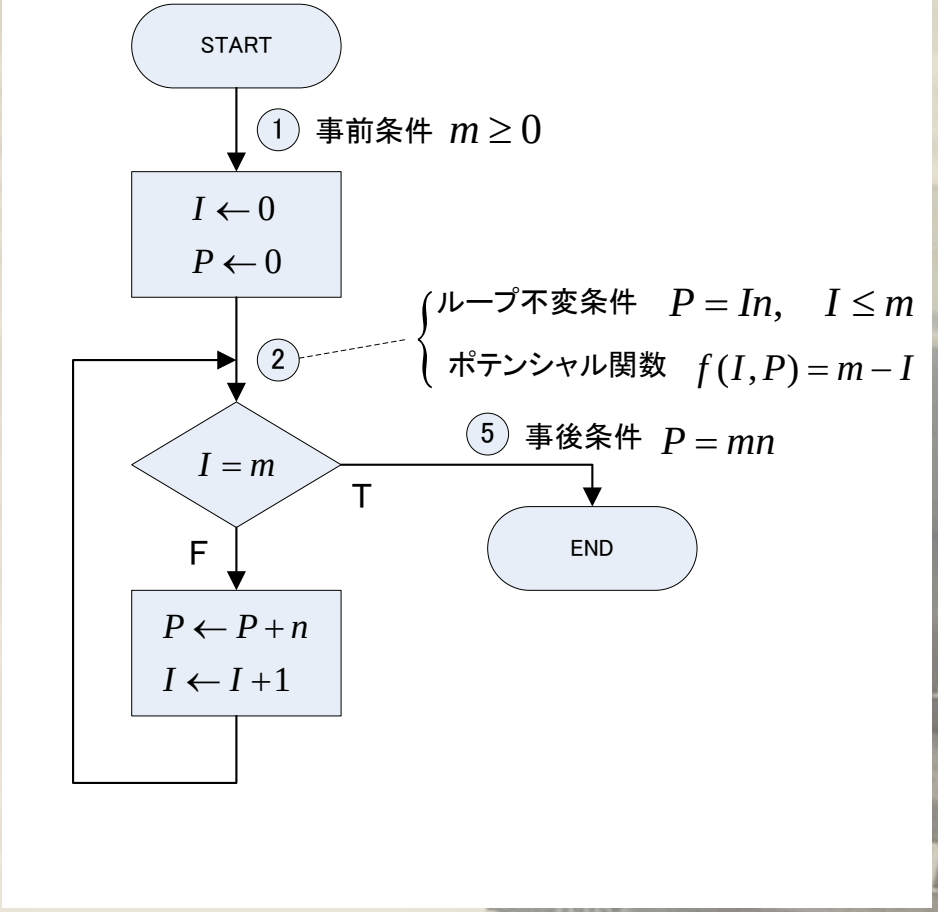
$m \geqq 0$, $I = 0$, $P = 0$ より

■ $P = In$ の証明

$P - In = 0 - 0n = 0$

■ $I \leqq m$ の証明

$I - m = 0 - m = -m \leqq 0$



例題：②→② の証明

ループを1周した後の変数の値にダッシュ(’)を付けて表す。

■ P’ ＝ I’n の証明

P=In, P’=P+n, I’=I+1 より

P’ – I’n

= (P+n) – (I+1)n

= P– In = 0

■ I’ ≦ m の証明

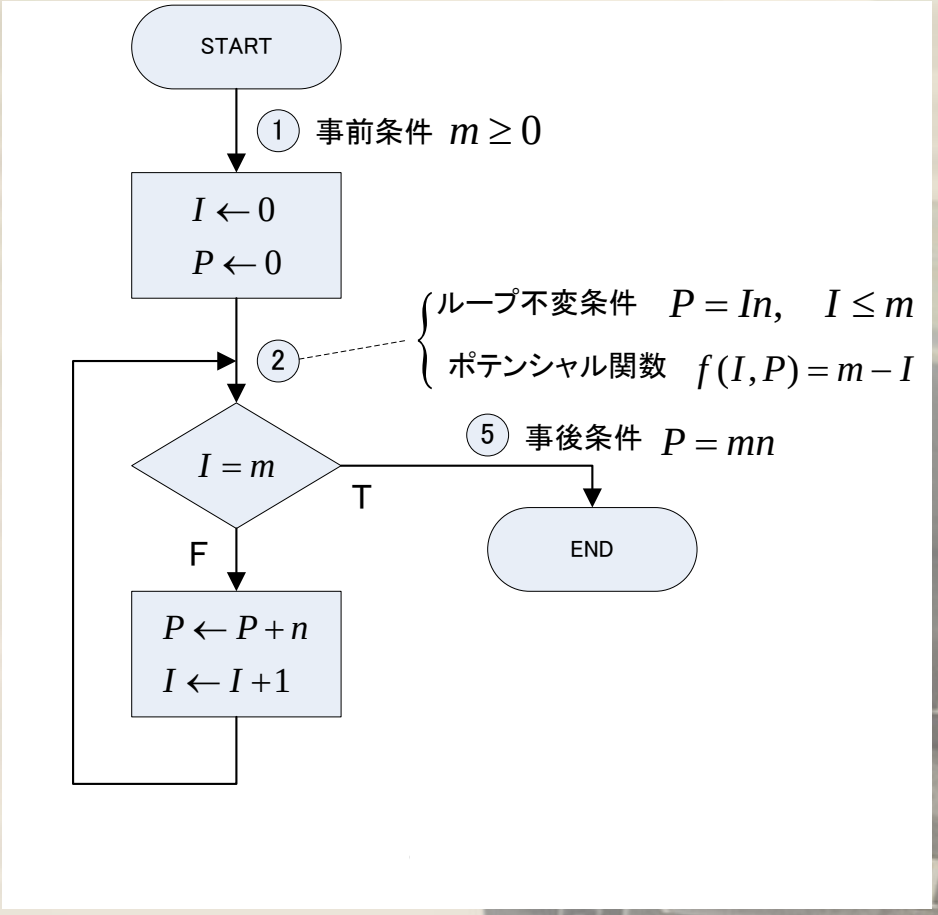
I ≦ m,

I≠m（whileループの継続条件）より

I ≦ m–1 であるから

I’ – m = (I+1) – m

= I – (m–1) ≦ 0



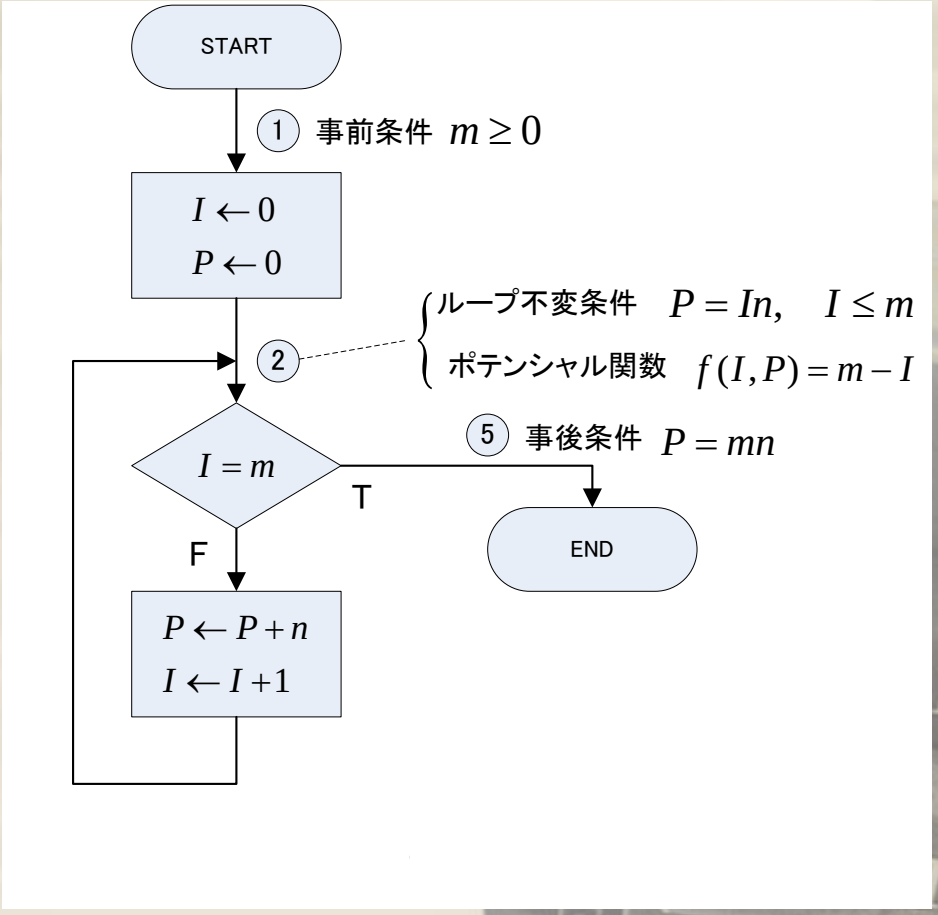
例題：②→⑤ の証明

■ P = mn の証明

P = In,

I = m（whileループの終了条件）より

P = mn



以上の3枚のスライドより，部分正当性が証明された。

停止性の証明方法

ポテンシャル関数について

つぎの事項を証明する.

- 非負性：関数値が常に非負

  （ループ不変条件として証明）

- 減少性：その位置に実行が到達するたびに

  関数値が減少している

なぜこれで良いのか？
→もしプログラムが停止しなければ，上記の2つの条件は矛盾する。よって，プログラムは停止する。

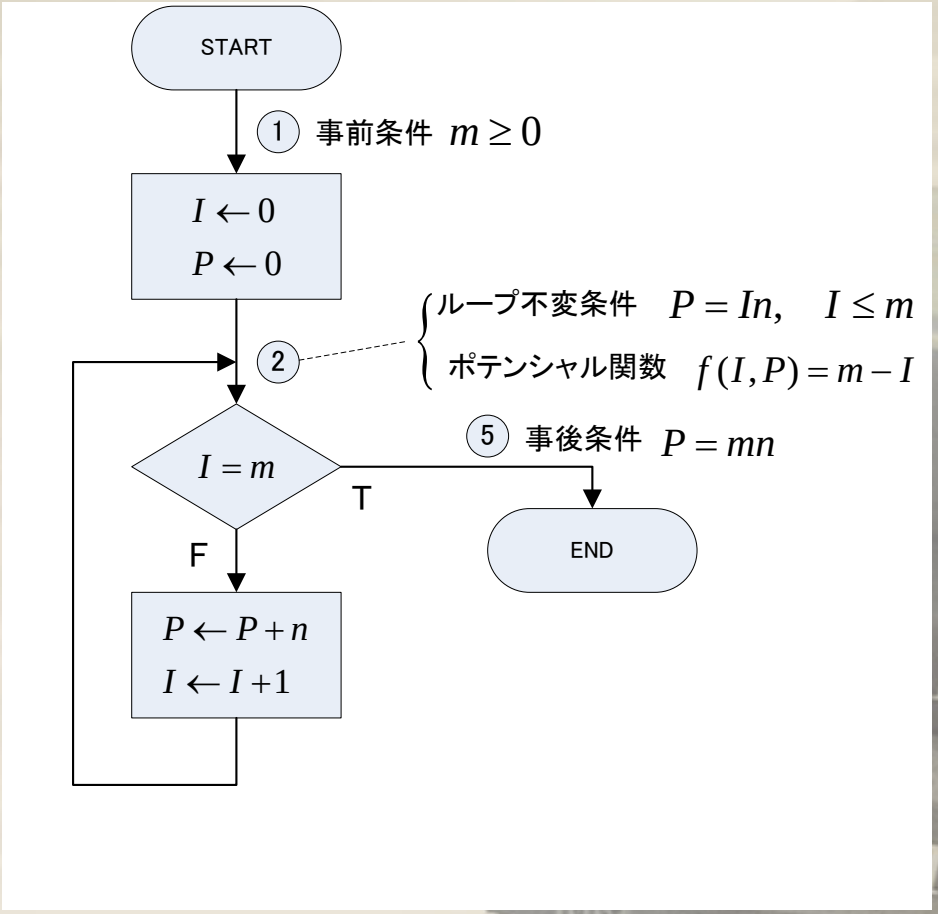
例題：非負性の証明

■ m – I ≧ 0 の証明

証明済みのループ不変条件

I ≦ m

より明らか。



例題：減少性の証明

■ $m - I' < m - I$ の証明

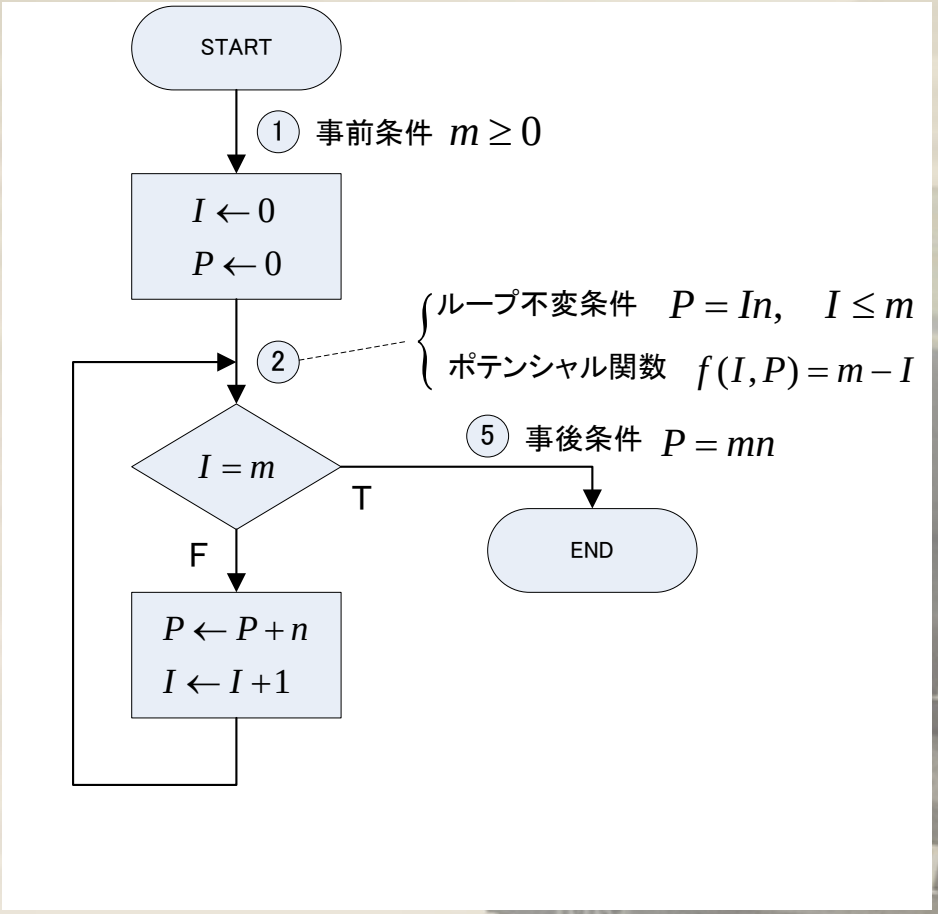
$I' = I + 1$ より

$(m - I') - (m - I)$

$= I - I'$

$= I - (I + 1)$

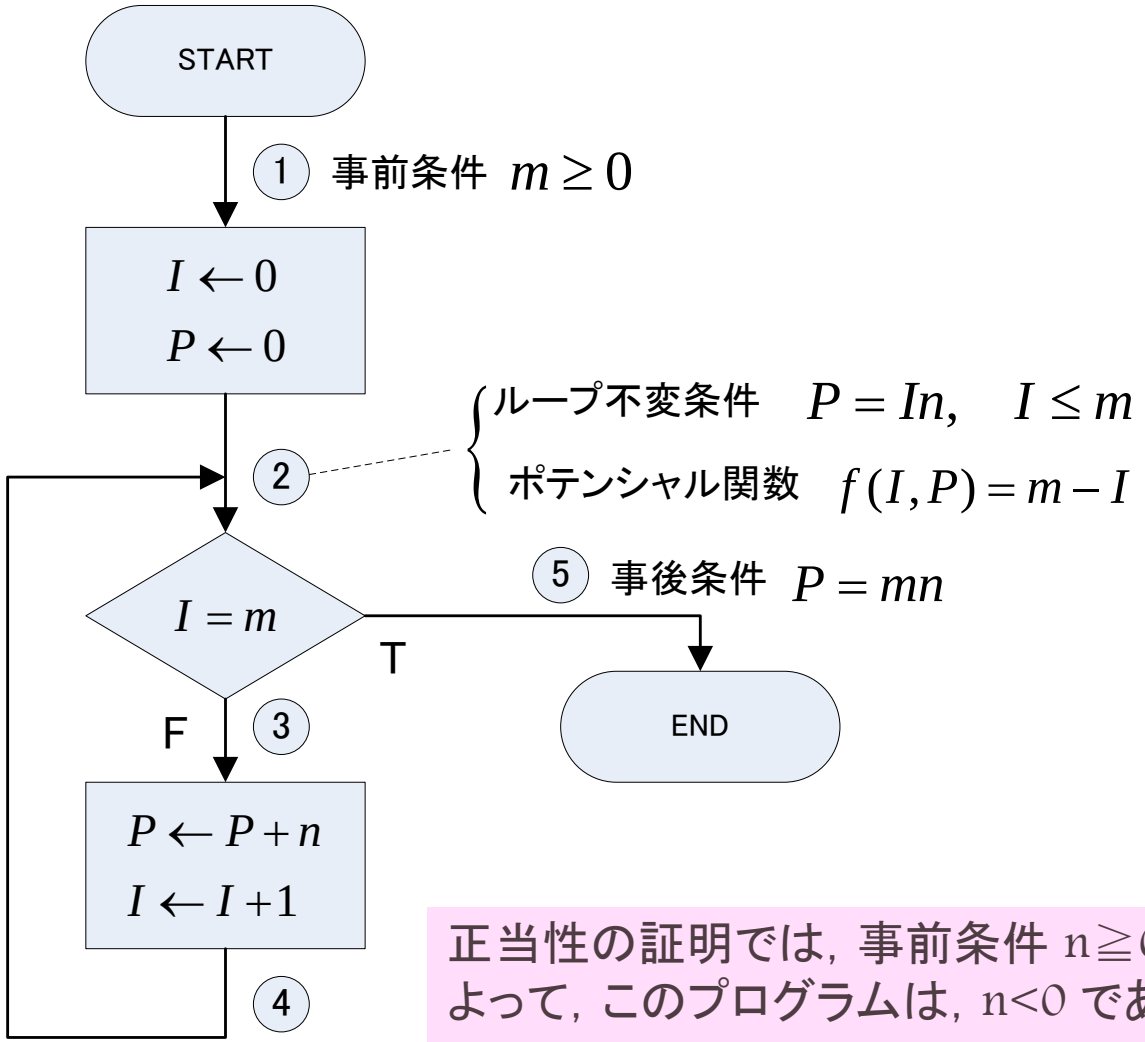
$= -1 < 0$



以上の2枚のスライドより，停止性が証明された。

部分正当性と停止性が証明されたので，正当性が証明された。

補足（自然数の加算）



正当性の証明では，事前条件 $n \geqq 0$ は必要なかった。
よって，このプログラムは，$n<0$ であっても正しく動く。

mとnの積P

演習問題 3

つぎのa÷bの商Qと余りRを求めるプログラムの正当性を証明しなさい