知能ソフトウェア特論
Intelligent Software

プログラムの正当性（１）
正当性証明の基本原理
Correctness of Programs (1)
Basic Principle for Correctness Proof

1．アサーションとポテンシャル関数
(Assertions and Potential Functions)

プログラムの正当性を証明する理論的ツール

Theoretical tools for proving program correctness

- アサーション (assertion)
- ポテンシャル関数 (potential function)

Microsoftは，自社のプログラマに，プログラムに正当性アサーションを挿入させるようにしたところ，（正当性の証明までさせなくても）生産性が飛躍的に向上した.

Microsoft instructed every programmer to include assertions in every program code they wrote. Actually, Microsoft did not order the programmers to *prove* the assertions, but only made a rule that assertions should be included in the code and made it their standard procedure when writing programs. Consequently, that led to a dramatic improvement in the productivity of programmers.

アサーション (Assertion)

アサーションとは---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

(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

(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

An assertion is a logical statement that expresses a relationship among the values of program variables.

- It is defined on a particular position (a graphical edge of a flowchart) of the program.
- The statement should be true whenever the control reaches that particular position.
- Typically, three kinds of assertions are identified:

(1) A precondition is defined on the entrance to the program, expressing the conditions for acceptable input.

(2) A postcondition is defined on the exit of the program, expressing the conditions for correct output.

(3) A loop invariant is defined on the entrance and exit of a loop, expressing the conditions that should be true whenever the control reaches there.

ポテンシャル関数 (Potential Function)

ポテンシャル関数とは---プログラム変数を用いた関数.

- 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 1 以上減少する.

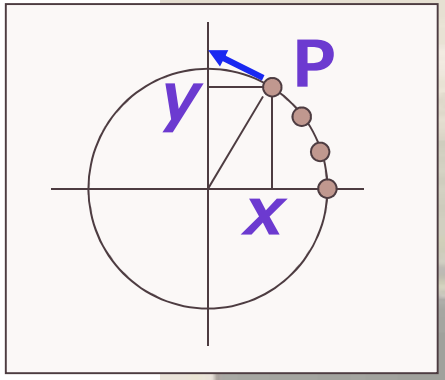
A potential function is a function using the values of program variables.

- It is defined on a particular position (a graphical edge of a flowchart) of the program.
- Its value (called the potential) should always be non-negative.
- The value should decrease by one or more, each time the control passes that position.

ループ不変条件の補足 (About Loop Invariants)

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);
} (This program plots a circle?)
```



■いかに証明するか？ (How to prove?)

$x^2 + y^2 = r^2 (\cos^2 k\theta + \sin^2 k\theta) = r^2$ (=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．

LOOP INVARIANTS

To explain how the system will vary with time,
explain what will not vary with time.

(類似例) エネルギー保存の法則　　$mgh + mv^2/2 = \text{constant}$

(Similar example) the energy conservation law

２．プログラムの正当性の定義
(Definition of correctness of program)

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.
A program is correct if, for all inputs satisfying the precondition, it has the following two properties.

(1) 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 If the execution has stopped, the postcondition is true at that moment. （計算結果がもし得られれば，それは正しい） The result of the computation, if we have obtained any, is correct.
(2) 停止性 termination	必ず実行が停止する The execution will eventually terminate. （必ず計算結果が得られる） We can always obtain the result of the computation.

3．部分正当性の証明方法 (How to prove partial correctness)

■ ループ不変条件がその位置で常に真であることを数学的帰納法で証明する.

- 基礎ケース: はじめてその位置に実行が到達したときに真であること.
- 帰納ステップ: いまその位置で真で，かつループの継続条件が真であるならば，再度その位置に実行が到達したときにも真であること.

■ ループ不変条件が真，かつ
ループの終了条件が真
ならば，事後条件が成り立つこと.

■ Prove that the loop invariant (*inv*) is true whenever the control reaches the specified position. This is proved by mathematical induction, i.e., by verifying the following two cases.
- Base case: The *inv* is true when the control reaches at the specified position for the first time.
- Induction step: If *inv* and the iteration condition of the loop are true at the specified position now, then *inv* will be also true when the control reaches there next time.

■ Prove that if *inv* is true and the termination condition of the loop is true, then the post condition of the loop is true.

例題

４．停止性の証明方法 (How to prove termination)

ポテンシャル関数について

つぎの事項を証明する.

■ 関数値（ポテンシャル）が常に非負であること（ループ不変条件）

■ その位置に実行が到達するたびに関数値（ポテンシャル）が１以上減少していること.

Prove the following properties of the potential function.

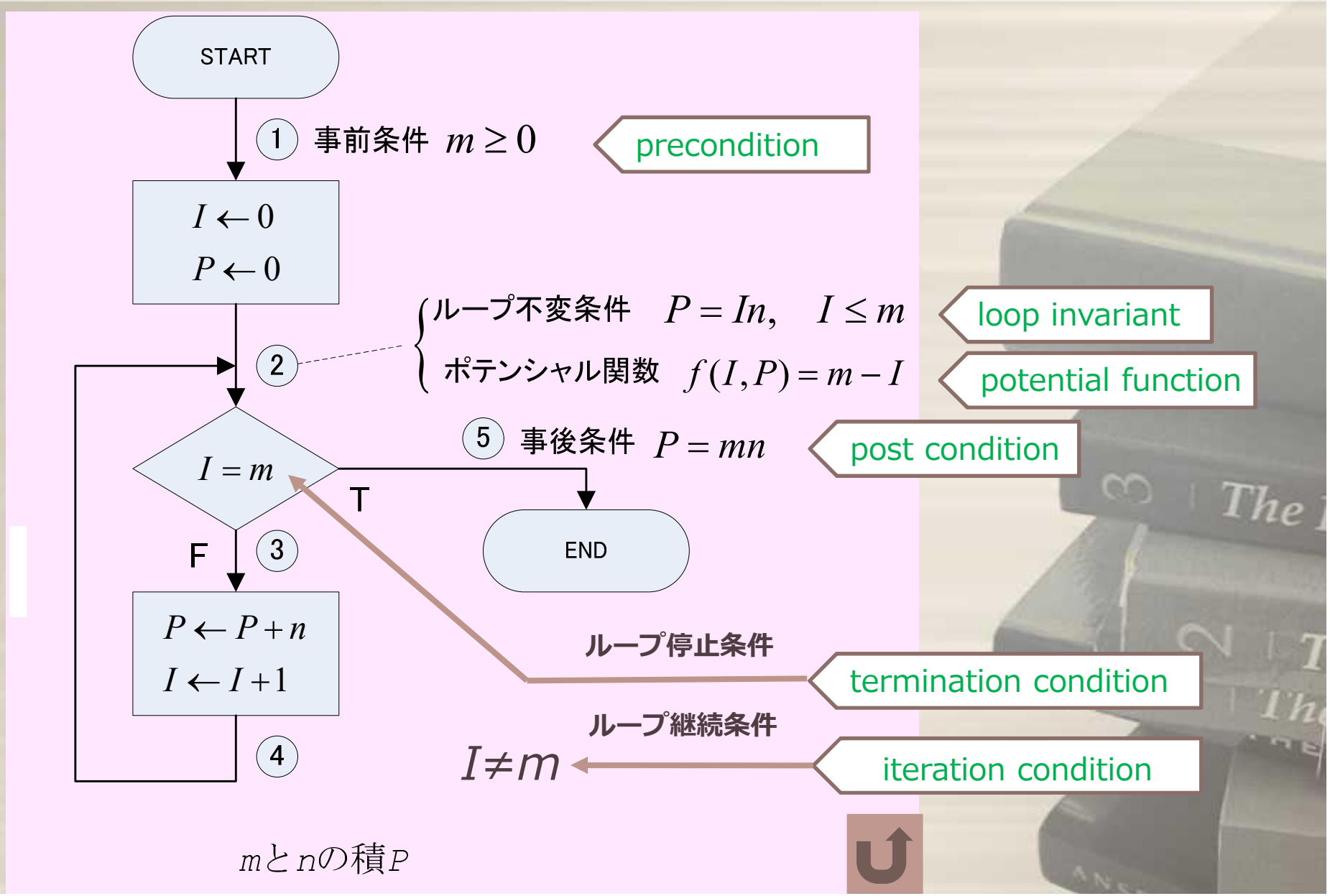
■The value of the function (called potential) is always non-negative. (loop invariant)

■The potential decreases by one or more, each time the control reaches the specified position.

例題

例題：２つの自然数 m, n の積を加算のみで求める

Example: Compute the product of two natural numbers m and n by using only addition



◆ループ不変条件　P = In の証明
(Proof of loop invariant P = In)

部分正当性の証明手順

Prove $P_k = I_k n$ (for all k=1,2,…) by induction.

(P_k と I_k は，②をk回目に通過したときの P と I の値)

P_k and I_k are the values of P and I, respectively, when the control passes the position ② for just k-th time

- Base case (k=1)

  $P_1 - I_1 n = 0 - 0n = 0$

- Induction step

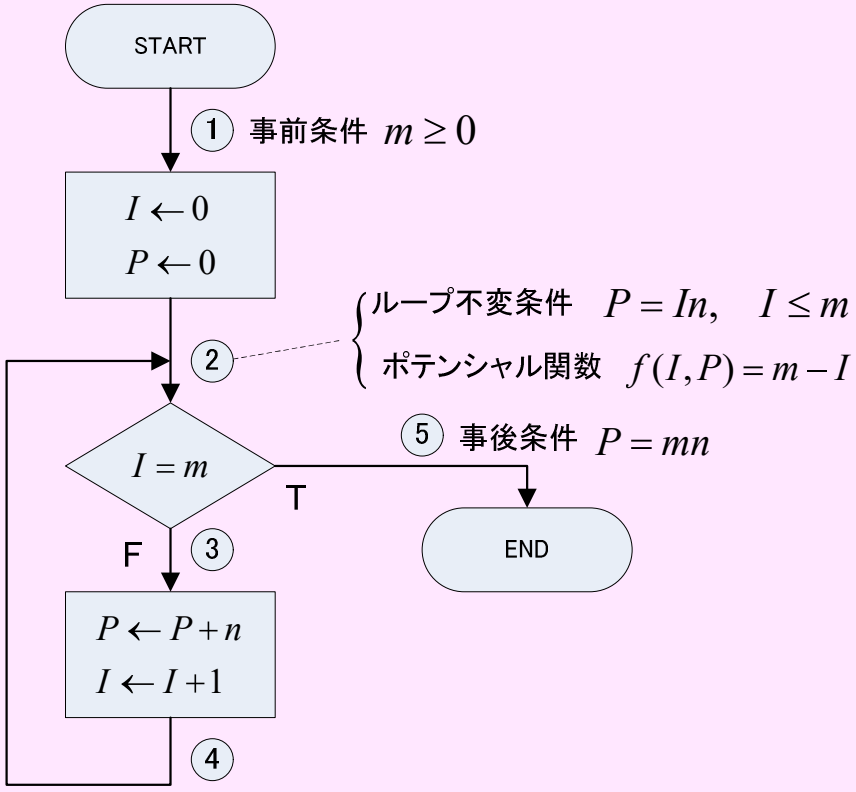
  Induction hypothesis : $P_k = I_k n$

  Iteration condition : $I_k \neq m$

  $P_{k+1} - I_{k+1} n$

  $= (P_k + n) - (I_k + 1)n$

  $= P_k - I_k n = 0$



mとnの積P

◆ループ不変条件　＆　終了条件 ⇒　事後条件　　の証明
Proof of “loop invariant & termination condition implies postcondition”

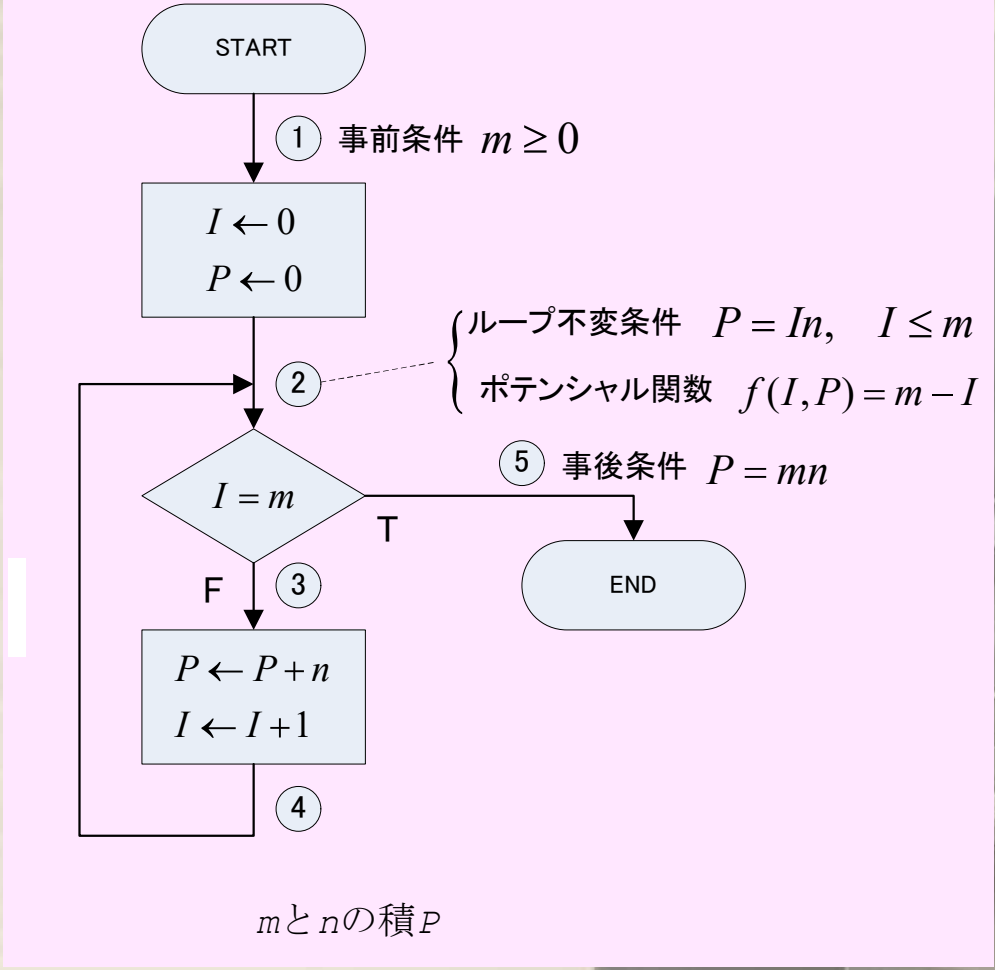
部分正当性の証明手順

■ ループ不変条件　　P = In
(loop invariant)

■ 終了条件　　I = m
(termination condition)

ゆえに：　(Therefore:)

■ 事後条件　P=mn
(postcondition)



mとnの積P

部分正当性　ＯＫ
(Partial correctness: Proved)

◆ポテンシャルの非負性　m - I ≧ 0　の証明
Proof of non-negative potential

停止性の証明手順

Prove $\mathbf{m - I_k \geqq 0}$ (for all k=1,2,…) by induction

- Base case (k=1)

  $\mathbf{m - I_1} = m - 0 = m \geqq 0$

- Induction step

  帰納法の仮定：　$m - I_k \geqq 0$
  (induction hypothesis)

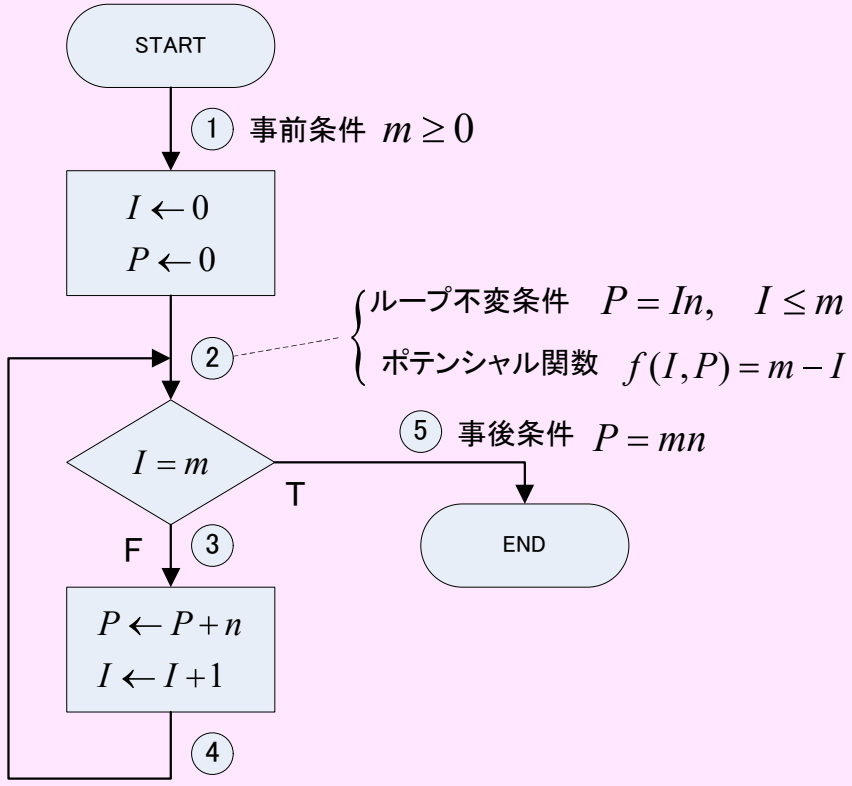
  ループの継続条件：　$I_k \neq m$
  (iteration condition of the loop)

  Therefore,　$m - I_k \geqq 1$

  $\mathbf{m - I_{k+1}}$

  $= m - (I_k + 1)$

  $= (m - I_k) - 1 \geqq 0$



mとnの積P

◆ポテンシャルが１以上減少することの証明
Proof of decrease of potential

停止性の証明手順

$f(I_k,P_k) - f(I_{k+1},P_{k+1})$

$= (m - I_k) - (m - I_{k+1})$

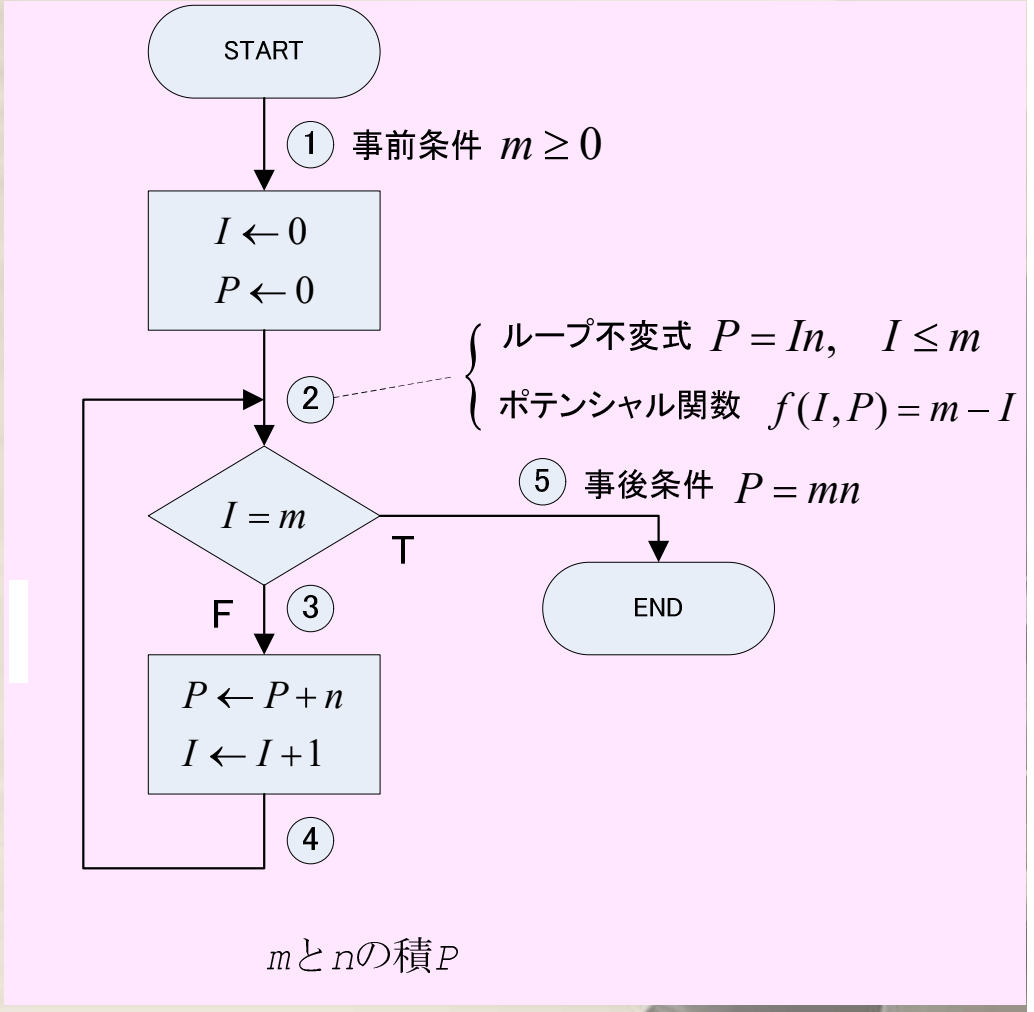
$= - I_k + I_{k+1}$

$= - I_k + (I_k + 1)$

$= 1 \geqq 1$

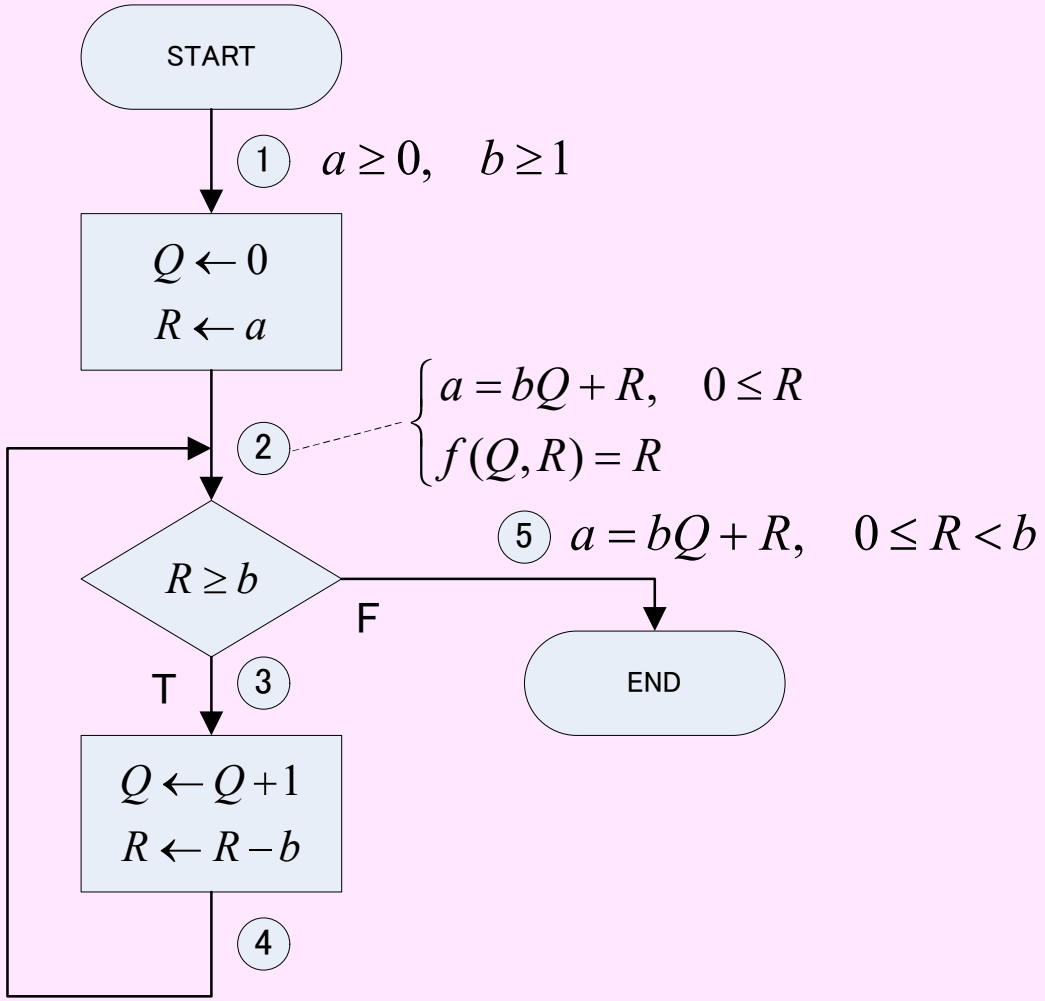
停止性　ＯＫ

(Termination: Proved)



mとnの積P

演習問題１　a÷bの商Qと余りR
EXERCISE 1　Quotient and remainder for a÷b



$a \div b$ の商 Q と余り R

Prove the correctness of the flowchart program given in the figure, which computes the quotient Q and the remainder R when a non-negative integer *a* and a positive integer *b* are given as input.