

2

次の文章を読み、下の問に答えよ。(130点)

学習指導要領 (3) - 知・技 - イ

学習指導要領 (3) - 思・判・表 - イ

学習内容 (3) - イ アルゴリズムとプログラム

4で割って1余る素数は、必ず、2つの平方数の和となることが知られている。たとえば50以下では次のようになる。

$$5 = 1^2 + 2^2, \quad 13 = 2^2 + 3^2, \quad 17 = 1^2 + 4^2,$$

$$29 = 2^2 + 5^2, \quad 37 = 1^2 + 6^2, \quad 41 = 4^2 + 5^2$$

4で割って1余る素数 $p$ を入力したとき、 $p = a^2 + b^2$ を満たす自然数 $a, b$ をひと組出力するアルゴリズムとしては、次のようなものが考えられる。

アルゴリズム A

入力：4で割って1余る素数 $p$

出力： $p = a^2 + b^2$ を満たす自然数 $a, b$

- ①  $a \leftarrow 1$
- ②  $b \leftarrow a + 1$
- ③  $x \leftarrow a \times a + b \times b$
- ④  $x = p$ ならば $a, b$ を出力し終了。
- ⑤  $x < p$ ならば $b \leftarrow b + 1$ として③へ戻る。
- ⑥  $x > p$ ならば $a \leftarrow a + 1$ として②へ戻る。

ただし、 $\leftarrow$  は左辺の変数へ右辺の値を代入することを表すこととする。

問 1 素数 $p = 101$ に対し $p = a^2 + b^2$ を満たす自然数 $a, b$ をひと組求めよ。

問 2 素数 $p = 97$ に対し $p = a^2 + b^2$ を満たす自然数 $a, b$ をひと組求めよ。

問 3 アルゴリズム A に $p = 97$ を入力すると、終了するまでにステップ③は何回実行されるか説明せよ。

問 4 アルゴリズム A を実際にプログラミングすると、入力 $p$ の値によっては③において同じ数の2乗が何度も計算されてしまう。この点に関する効率化の方策をひとつ述べよ。