

3 次の文章を読み、下の問に答えよ。(100点)

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

有名な公開鍵暗号である RSA 暗号はフェルマーの小定理を利用して設計されている。17 世紀の数学者フェルマーは完全数の研究の中からフェルマーの小定理を発見した。自然数 n は、その全ての正の約数の和が $2n$ に等しいとき、完全数と呼ばれる。6 や 28 は完全数の例である。

$$1 + 2 + 3 + 6 = 2 \times 6$$

$$1 + 2 + 4 + 7 + 14 + 28 = 2 \times 28$$

そこで、自然数 n の全ての正の約数の和 $f(n)$ を求めるアルゴリズムについて考えてみよう。簡単なアルゴリズムとしては次のような方法がある。

アルゴリズム A

入力：自然数 n

出力： n の正の約数の和 $f(n)$

- ① $s \leftarrow 0, d \leftarrow 1$
- ② n を d で割った余りが 0 ならば $s \leftarrow s + d$
- ③ $d = n$ ならば s を出力し終了。
- ④ $d \leftarrow d + 1$ 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 アルゴリズム A の入力が終了するまでに何回の除算が必要であるか答えよ。

問 2 d が n の約数であれば $\frac{n}{d}$ も n の約数であることを利用して、アルゴリズム A を改良するアイデアを述べよ。ただし、平方根を計算する関数 $\text{sqrt}()$ は使ってよいものとする。

問 3 n を 2 で割れるだけ割って $n = 2^k \times m$ (m は奇数, $k \geq 0$) と表したとき、

$$f(n) = (2^{k+1} - 1) \times f(m)$$

が成り立つことを説明せよ。

問 4 計算機上では 2 で割る除算は 2 進数のシフト演算で行われるので、その実行時間はほとんど無視してよい。問 2 と問 3 の工夫をアルゴリズム A に加えたとき、必要な除算 (2 で割る除算を除く) の回数はおおよそ何回になるか、 k, n を用いた式で答えよ。