

## 注意

- 第 1 問から第 4 問は答えのみ解答すればよい。
- 第 5 問から第 8 問は、答えだけでなく、どのような計算・議論をしたか分かるように詳しく書くこと。

## 問題

1. 次の関数の漸近評価を求め、 $O(\cdot)$  によって表せ。

(a)  $f_1(n) = 5n^9 + 8n^8 + 9n^5 + 1$ .

(b)  $f_2(n) = \sqrt{n \log n} + (\log n)^2 + \sqrt[3]{n^2}$ .

2. 空のスタックに対し、次の操作を行ったときの過程を図示せよ。ただし、 $\text{PUSH}(x)$  は  $x$  をスタックに挿入する操作を、 $\text{POP}$  はスタックから値を取り出す操作をそれぞれ表す。

$$\text{PUSH}(8) \rightarrow \text{PUSH}(6) \rightarrow \text{PUSH}(5) \rightarrow \text{PUSH}(3) \rightarrow \text{PUSH}(4) \rightarrow \text{POP} \rightarrow \text{POP} \rightarrow \text{PUSH}(1) \rightarrow \text{POP}$$

3. 空の 2 分探索木に対して次の順で要素を挿入したとき、最終的に得られる 2 分探索木を図示せよ。

$$28, 59, 36, 3, 19, 92, 49$$

4. 次の整数列 (\*) を考える。

$$80, 78, 97, 65, 27, 59, 44, 91 \quad (*)$$

(a) 整数列 (\*) を選択ソートによって昇順に整列し、その経過を図示せよ。

(b) 整数列 (\*) をクイックソートによって昇順に整列し、その経過を図示せよ。ただし、ピボットとして左端の要素を選ぶものとする。

5. 以下の問いに答えよ。

(a) 方程式  $83X + 43Y = 1$  の整数解  $(X, Y)$  を 1 組求めよ。

(b) 連立合同式

$$\begin{cases} X \equiv 8 \pmod{43}, \\ X \equiv 3 \pmod{83} \end{cases}$$

を満たす整数  $X$  で、 $0 \leq X < 43 \cdot 83$  を満たすものをすべて求めよ。

6. ルジャンドル記号  $\left(\frac{481}{947}\right)$  の値を求めよ。

7. 45 は 8 を底とする擬素数であることを示せ。

8.  $p$  を素数として、 $p \equiv 2 \pmod{3}$  を満たすとする。  $a$  を 0 以上  $p$  未満の整数とする。 整数  $x$  を

$$x \equiv a^{(2p-1)/3} \pmod{p}, \quad 0 \leq x < p$$

で定める。このとき、以下の問いに答えよ。

(a)  $x^3 \equiv a \pmod{p}$  が成り立つことを示せ。

(b) 問題の条件を満たす  $p$  と  $a$  が与えられたとき、 $x$  をビット演算量  $O((\log p)^3)$  で計算できることを示せ。ただし、四則演算のビット演算量は以下の通りとする。

- $k$  ビット以下の 2 つの整数の加減算のビット演算量は高々  $k$  である。
- $k$  ビットの整数と  $l$  ビットの整数の乗算のビット演算量は高々  $kl$  である。
- $k$  ビットの整数を  $l$  ビットの整数で割り商と剰余を得る除算のビット演算量は高々  $kl$  である。