

## アルゴリズム B 演習 レポート課題 No. 2

2019 年 1 月 11 日配布

提出日：2019 年 1 月 25 日

### 注意

- 1 枚目に学修番号・氏名を書くこと。
- レポートが複数枚にわたるときは、左上をホッチキス等で綴じること。
- A4 レポート用紙を使用すること。

### 問題

1.  $b$  を 3 以上の整数とする. 正の整数  $n$  の  $b$  進表記  $n = (a_{m-1} \dots a_1 a_0)_b$  を求めるときのビット演算量は  $O((\log n)^2)$  であることを示せ. ただし,  $n$  は 2 進表記で与えられているものとして, 四則演算のビット演算量として演習問題 No. 8 で与えたものを使うものとする. また, ビット演算量の評価において,  $b$  は定数であると見なしてよい.
2. 以下の問いに答えよ.
  - (a) 方程式  $77X + 91Y + 143Z = 1$  の整数解  $(X, Y, Z)$  を 1 組求めよ.
  - (b) 合同式  $x \equiv 17 \pmod{23}$ ,  $x \equiv 69 \pmod{74}$  を満たす整数  $x$  で  $0 \leq x < 23 \cdot 74$  の範囲にあるものをすべて求めよ.
3. 以下の問いに答えよ.
  - (a) ルジャンドル記号  $\left(\frac{399}{743}\right)$  の値を求めよ.
  - (b) 合同式  $x^2 \equiv 2 \pmod{31}$  を満たす整数  $x$  で,  $0 \leq x < 31$  を満たすものをすべて求めよ.
4. 以下の問いに答えよ.
  - (a)  $2^{406} \pmod{407}$  を計算することで 407 が合成数であることを示せ.
  - (b) 301 は 6 を底とする擬素数であるが, 6 を底とする強擬素数ではないことを示せ.