アルゴリズム B レポート課題 No. 2

2020 年 1 月 6 日配布

提出日：2020 年 1 月 27 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. n を自然数とする．n の階乗 $n!$ を計算するときのビット演算量は $O(n^2 \log^2 n)$ であることを示せ．ただし，k ビットの自然数と l ビットの自然数の乗算のビット演算量は高々 kl であるとする．
2. x の冪乗の計算について，以下の問いに答えよ．
   (a) 繰り返し 2 乗法で x^{23} を計算するのに必要な乗算回数を求めよ．
   (b) 繰り返し 2 乗法より少ない乗算回数で x^{23} を計算する方法を示し，そのときの乗算回数を求めよ．ただし，乗算以外の演算は行わないものとする．
3. 以下の問いに答えよ．
   (a) 方程式 $58X + 67Y = 1$ の整数解 (X, Y) を 1 組求めよ．
   (b) 合同式 $58X \equiv 21 \pmod{67}$ を満たす整数 X で，$0 \leq X < 67$ を満たすものをすべて求めよ．
4. 連立合同式
$$\begin{cases} X \equiv 12 \pmod{28}, \\ X \equiv 13 \pmod{55}, \\ X \equiv 90 \pmod{93} \end{cases}$$
   を満たす整数 X で，$0 \leq X < 28 \cdot 55 \cdot 93$ を満たすものをすべて求めよ．
5. ルジャンドル記号 $\left(\dfrac{383}{653}\right)$ の値を求めよ．
6. p を奇素数とする．1 以上 p 未満の自然数の中に，p を法とする平方剰余と平方非剰余が同じ数だけ存在することを示せ．