アルゴリズム B レポート課題 No. 2

2021 年 12 月 27 日配布

提出日：2022 年 1 月 17 日

注意

- レポートの最初に学修番号と名前を記入すること．
- 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．
- 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. 繰り返し 2 乗法で x^{148} を計算するのに必要な乗算回数を求めよ．
2. 以下の問いに答えよ．
   (a) 方程式 $52X + 89Y = 1$ の整数解 (X, Y) を 1 組求めよ．
   (b) 合同式 $52X \equiv 69 \pmod{89}$ を満たす整数 X で，$0 \leq X < 89$ を満たすものをすべて求めよ．
3. 連立合同式
$$\begin{cases} X \equiv 10 \pmod{17}, \\ X \equiv 9 \pmod{23}, \\ X \equiv 7 \pmod{29} \end{cases}$$
   を満たす整数 X で，$0 \leq X < 17 \cdot 23 \cdot 29$ を満たすものをすべて求めよ．
4. $\varphi(n)$ をオイラーの φ 関数とする．以下の問いに答えよ．
   (a) $\varphi(441)$ を求めよ．
   (b) $2^{510} \bmod 441$ を求めよ．
5. 以下の問いに答えよ．
   (a) ヤコビ記号 $\left(\dfrac{181}{391}\right)$ の値を求めよ．
   (b) $X^2 \equiv 181 \pmod{391}$ を満たす整数 X が存在するかどうか判定せよ．
6. m, n を自然数とする．以下の問いに答えよ．
   (a) 成分が整数である行列 $A = [a_{ij}]$ に対し，$A \bmod m = [a_{ij} \bmod m]$ と定義する．成分が整数である 2 次正方行列 $M = [a_{ij}]$ を考える．ただし，$0 \leq a_{ij} < m$ であるとする．このとき，$M^n \bmod m$ をビット演算量 $O((\log n)(\log^2 m))$ で計算できることを示せ[*1]．
   (b) 数列 $\{a_k\}$ を
$$a_1 = 3, \quad a_2 = 10, \quad a_{k+2} = 7a_{k+1} - 12a_k \quad (k \geq 1)$$
   で定義する．$a_n \bmod m$ をビット演算量 $O((\log n)(\log^2 m))$ で計算できることを示せ．

[*1] 本問において $f(m,n) = O(g(m,n))$ であるとは，ある実数 $c > 0$ と非負整数 n_0 が存在して，任意の非負整数 n に対し，
$$m \geq n_0 \text{ かつ } n \geq n_0 \implies 0 \leq f(m,n) \leq cg(m,n)$$
が成り立つことをいう．