アルゴリズム B レポート課題 No. 2

2023 年 1 月 16 日配布

提出日：2023 年 1 月 30 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^{182} 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 $46X + 67Y = 1$ の整数解 (X, Y) を 1 組求めよ．
   (b) 合同式 $46X \equiv 31 \pmod{67}$ 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．
   (c) 連立合同式
   $$\begin{cases} X \equiv 29 \pmod{46}, \\ X \equiv 14 \pmod{67} \end{cases}$$
   を満たす整数 X で，$0 \leq X < 46 \cdot 67$ を満たすものをすべて求めよ．
3. $\varphi(n)$ をオイラーの φ 関数とする．以下の問いに答えよ．
   (a) $\varphi(275)$ を求めよ．
   (b) 任意の自然数 n に対して，
   $$\sum_{d \mid n} \varphi(d) = n$$
   が成り立つことを示せ．ただし，左辺の和は n のすべての正の約数 d をわたる．
4. 29 を法とする原始根を 1 つ求めよ．（すなわち，$(\mathbb{Z}/29\mathbb{Z})^\times$ の生成元を 1 つ求めよ．）
5. 以下の問いに答えよ．
   (a) ルジャンドル記号 $\left(\dfrac{97}{211}\right)$ の値を求めよ．
   (b) ヤコビ記号 $\left(\dfrac{71}{689}\right)$ の値を求めよ．
6. n を自然数とする．$\displaystyle\prod_{k=1}^{n}(2k-1)$ をビット演算量 $O(n^2 \log^2 n)$ で計算できることを示せ．