アルゴリズム B レポート課題 No. 2

2021 年 1 月 4 日配布

提出期限：2021 年 1 月 25 日 23:59

注意

- kibaco の「課題」機能を使い，**PDF ファイル**で提出すること．（PDF ファイル以外のファイル形式では提出しないこと．）
- レポートの最初に学修番号と名前を記入すること．
- 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. 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^{39} 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^{39} 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．
2. 以下の問いに答えよ．
   (a) 方程式 $45X + 73Y = 1$ の整数解 (X, Y) を 1 組求めよ．
   (b) 合同式 $45X \equiv 14 \pmod{73}$ を満たす整数 X で，$0 \leq X < 73$ を満たすものをすべて求めよ．
3. 次のオイラーの φ 関数の値を求めよ．

   (a) $\varphi(104)$　(b) $\varphi(546)$

4. 以下の問いに答えよ．
   (a) 31 を法として，2 の位数を求めよ．（すなわち，$(\mathbb{Z}/31\mathbb{Z})^\times$ における $2 + 31\mathbb{Z}$ の位数を求めよ．）
   (b) 31 を法とする原始根を 1 つ求めよ．（すなわち，$(\mathbb{Z}/31\mathbb{Z})^\times$ の生成元を 1 つ求めよ．）
5. ルジャンドル記号 $\left(\dfrac{349}{521}\right)$ の値を求めよ．
6. n を自然数とする．$(n-1)!$ を n で割った余りはビット演算量 $O(n \log^2 n)$ で計算できることを示せ．