アルゴリズム B 演習 レポート課題 No. 2

2014 年 1 月 10 日配布

提出日：2014 年 1 月 24 日

注意

- 1 月 24 日の授業までに提出すること．
- 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. (a) $\varphi(n)$ をオイラーの φ 関数とする．$\varphi(210)$ を求めよ．
   (b) 11^{100} を 210 で割った剰余を求めよ．
2. 合同式 $x \equiv 5 \pmod 7$, $x \equiv 4 \pmod 8$, $x \equiv 7 \pmod 9$ を満たす整数 x で $0 \leq x < 7 \cdot 8 \cdot 9$ の範囲にあるものを求めよ．
3. 次の問いに答えよ．
   (a) ルジャンドル記号 $\left(\dfrac{11}{43}\right)$ の値を求めよ．
   (b) 合同式 $x^2 \equiv 11 \pmod{43}$ の解をすべて求めよ．
4. 2 以上の自然数 $n_1, n_2, \ldots, n_r$ が与えられたとき，その積

   $$n = n_1 n_2 \cdots n_r$$

   は $O\big((\log n)^2\big)$ のビット演算量で計算できることを示せ．ただし，四則演算のビット演算量は演習問題 No. 8 で与えたものを用いるとする．すなわち，k ビットの自然数と l ビットの自然数の乗算は，高々 kl のビット演算量で行うことができるとする．