アルゴリズム B 演習 レポート課題 No. 2

2018 年 1 月 19 日配布

提出締め切り：2018 年 2 月 2 日（金）

注意

- 8 号館 6 階東側エレベーターホールのレポート入れに提出すること．
- 1 枚目に科目名・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 を正の奇数とする．n を 3 以上 $\sqrt{n}$ 以下の奇数で順に割ることで n が素数かどうか判定できる（試し割算）．この方法で素数判定を行うときのビット演算量は $O(\sqrt{n}(\log n)^2)$ であることを示せ．ただし，四則演算のビット演算量として演習問題 No. 8 で与えたものを使うものとする．
2. 以下の問いに答えよ．
   （a）合同式 $175x + 274 \equiv 194 \pmod{291}$ を満たす整数 x で $0 \leq x < 291$ の範囲にあるものをすべて求めよ．
   （b）合同式 $x \equiv 28 \pmod{57}$, $x \equiv 59 \pmod{89}$ を満たす整数 x で $0 \leq x < 57 \cdot 89$ の範囲にあるものをすべて求めよ．
3. 以下の問いに答えよ．
   （a）ルジャンドル記号 $\left(\dfrac{517}{967}\right)$ の値を求めよ．
   （b）p を 5 以上の素数とする．次の式が成り立つことを示せ．

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & (p \equiv 1, 11 \pmod{12} \text{ のとき}) \\ -1 & (p \equiv 5, 7 \pmod{12} \text{ のとき}) \end{cases}$$

4. 以下の問いに答えよ．
   （a）$2^{202} \bmod 203$ を計算することで 203 が合成数であることを示せ．
   （b）217 は 5 を底とする擬素数であるが，5 を底とする強擬素数ではないことを示せ．