アルゴリズム B 演習 レポート課題 No. 2

2017 年 1 月 20 日配布

提出締め切り：2017 年 2 月 8 日（水）

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 を自然数，a を N と互いに素な N より小さい自然数とする．環 $\mathbb{Z}/N\mathbb{Z}$ において $a \bmod N$ の逆元を計算するときのビット演算量は $O((\log N)^3)$ であることを示せ．ただし，以下のことを用いてもよい．
   - n ビット以下の 2 個の自然数の加算・減算のビット演算量は高々 n である．
   - n ビット以下の 2 個の自然数の乗算・除算のビット演算量は高々 n^2 である．
   - a, b は $a > b$ を満たす互いに素な自然数とする．拡張ユークリッドの互除法によって $aX + bY = 1$ を満たす整数 X, Y を求めるときに必要な除算回数は $O(\log b)$ である．
2. 以下の問いに答えよ．
   （a）合同式 $299x + 230 \equiv 274 \pmod{349}$ を満たす整数 x で $0 \leq x < 349$ の範囲にあるものをすべて求めよ．
   （b）合同式 $x \equiv 12 \pmod{67}$, $x \equiv 17 \pmod{73}$ を満たす整数 x で $0 \leq x < 67 \cdot 73$ の範囲にあるものを求めよ．
3. 以下の問いに答えよ．
   （a）ルジャンドル記号 $\left(\dfrac{737}{887}\right)$ の値を求めよ．
   （b）$x^2 \equiv 14 \pmod{31}$ を満たす整数 x で $0 \leq x < 31$ の範囲にあるものをすべて求めよ．
4. 以下の問いに答えよ．
   （a）$f(x) = x^2 + 1$, $x_1 = 3$ として，ρ 法を用いて 221 を素因数分解せよ．
   （b）フェルマー法を用いて 943 を素因数分解せよ．