アルゴリズム B 演習 レポート課題 No. 2

2013 年 1 月 11 日配布

提出日：2013 年 1 月 25 日

注意

- 1 月 25 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

以下の 6 問のうち，**4 問**に解答せよ.

1. 自然数 n に対し，$(n-1)!$ を n で割った剰余が $O(n(\log n)^2)$ のビット演算量で計算できることを示せ．ただし，乗算と除算のビット演算量は演習問題 No. 7 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．また，k ビットの自然数を l ビットの自然数で割って商と剰余を求める計算は高々 kl のビット演算量で行うことができる.
2. 拡張ユークリッドの互除法を用いて，$48X + 33Y = 57$ を満たす整数 X, Y を一組求めよ.
3. 合同式 $x \equiv 2 \pmod 5$, $x \equiv 3 \pmod 7$, $x \equiv 4 \pmod{11}$ を満たす整数 x で $0 \leq x < 5 \cdot 7 \cdot 11$ の範囲にあるものを求めよ.
4. 次の問いに答えよ.
   (a) ヤコビ記号 $\left(\dfrac{17}{253}\right)$ の値を求めよ.
   (b) 合同式 $x^2 \equiv 17 \pmod{253}$ の解の個数を求めよ．(253 は合成数であることに注意せよ.)
5. $1105 = 5 \cdot 13 \cdot 17$ がカーマイケル数であることを示せ.
6. ρ 法またはフェルマー法を用いて 3127 を素因数分解せよ．(ρ 法を用いる際は，写像 $f(x) = x^2 + 1$, 初期値 $x_1 = 14$ を用いること.)