アルゴリズム B 演習 No. 7 2012 年 11 月 30 日配布

7. 四則演算と冪乗

- 2 進法で表された二つの自然数の加算を考える．k ビット（2 進法で k 桁）の自然数の加算は，次の操作を k 回繰り返すことで行われる．
  - 足されるビット x，足すビット y，下の桁からの繰上ビット z に対して，

    $$x + y + z = 2c + r$$

    によって，足した結果ビット r，上の桁への繰上ビット c を定める．ここで，$x, y, z, r, c \in \{0, 1\}$ である．

  このビット演算を単位に求めた計算量を**ビット演算量** (bit complexity) という．したがって，高々 k ビットの二つの自然数の加算のビット演算量は高々 k である．
- 高々 k ビットの二つの自然数の減算は，高々 k のビット演算量でできる（ただし，ビット演算を適切に拡張するものとする）．
- k ビットの自然数と l ビットの自然数の乗算は，筆算と同様に行うと，高々 kl のビット演算量でできる．実際には，より高速なアルゴリズムが知られている．
- 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 のビット演算量でできる．
- x を乗法の定義された代数系（正確には半群）の要素，n を自然数として，x^n の計算を考える．素朴な方法は，順に $x^2, x^3, \ldots, x^n$ と，x による乗算を $n-1$ 回繰り返す方法である．乗算回数がより少ない方法を以下で述べる．n の 2 進展開を $n = (n_k \ldots n_1 n_0)_2$ とする．ただし，$n_k = 1$ とする．

  $$x_0 = x, \quad x_i = {x_{i-1}}^2 = x^{2^i} \quad (i = 1, 2, \ldots, k)$$

  と定める．この計算は k 回の乗算でできる．このとき，

  $$x^n = \prod_{\substack{n_i = 1 \\ 0 \le i \le k}} x_i$$

  によって x^n が計算できる．

  $$\nu(n) = \#\{i \mid n_i = 1, 0 \le i \le k\}$$

  とおくと，x^n の計算に必要な乗算の回数は，$k + \nu(n) - 1$ 回である．この方法を**繰り返し二乗法**という．（繰り返し二乗法には，乗算の順序がこれと異なるものもあるので注意せよ．）

問題

解答に際して，その問題より前にある問題の結果を用いてもよい．

四則演算のビット演算量として，前ページで述べたものを使うものとする．

7-1, 7-2 は，2 進法のまま計算すること．

7-1. 2 進法で表された二つの整数 1011 と 11001 の積を筆算で求めよ．

7-2. 2 進法で表された整数 11001000 を 1011 で割った商と剰余を筆算で求めよ．

7-3. 自然数 a を 2 進法で表すと，$\lfloor \log_2 a \rfloor + 1$ 桁であることを示せ．

7-4. $n!$ を 2 進法で表したときの桁数は $O(n \log n)$ であることを示せ．

7-5. $n!$ を定義通りに計算する，すなわち，$1! = 1$, $k! = (k-1)! \cdot k$ $(k \geq 2)$ によって計算するとき，ビット演算量は $O\big(n^2 (\log n)^2\big)$ であることを示せ．

7-6. 自然数 n に対して，次の公式が成り立つ．

$$\sum_{k=1}^{n} k^3 = \frac{1}{4}\big(n(n+1)\big)^2.$$

（a）左辺を計算するときのビット演算量は $O\big(n(\log n)^2\big)$ であることを示せ．

（b）右辺を計算するときのビット演算量は $O\big((\log n)^2\big)$ であることを示せ．

7-7. 素朴な方法で 3^n を計算したときのビット演算量は $O(n^2)$ であることを示せ．

7-8. 繰り返し二乗法で x^{12} を計算したときの乗算の回数を求めよ．

7-9. x^{15} の計算を考える．

（a）繰り返し二乗法で x^{15} を計算したときの乗算の回数を求めよ．

（b）繰り返し二乗法よりも少ない乗算回数で x^{15} を計算する方法を一つ与えよ．

7-10. 繰り返し二乗法で x^n を計算したときの乗算の回数は $2\lfloor \log_2 n \rfloor$ 以下であることを示せ．

参考書

数論アルゴリズムに関する参考書として以下を挙げる．

[1] N. コブリッツ著，櫻井幸一訳『数論アルゴリズムと楕円暗号理論入門』（シュプリンガー・フェアラーク東京，1997；丸善出版，2012）．

[2] 中村憲『数論アルゴリズム』（朝倉書店，2009）．