アルゴリズム B 演習 第 14 回

2024 年 1 月 22 日

14　素因数分解

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．

14-1. $f(x) = x^2 + 1$, $x_1 = 1$ として，ρ 法を用いて 259 を素因数分解せよ．

14-2. $f(x) = x^2 + 2$, $x_1 = 1$ として，ρ 法を用いて 391 を素因数分解せよ．

14-3. フェルマー法を用いて 4757 を素因数分解せよ．

14-4. フェルマー法を用いて 4897 を素因数分解せよ．

14-5. $n = 3683$ とする．t を $\lceil\sqrt{3n}\rceil$ から順に大きくしていき，$t^2 - 3n$ が平方数となる t を探すことで n を素因数分解せよ．（このように，小さな k について t を $\lceil\sqrt{kn}\rceil$ から順に大きくしていき，$t^2 - kn$ が平方数となる t を探す方法を一般化フェルマー法という．）

14-6. p, q を相異なる素数として，$n = pq$ とする．n と $\varphi(n)$ の値が与えられたとき，p と q をビット演算量 $O(\log^3 n)$ で計算できることを示せ．ただし，k ビットの自然数 m に対して，$\lfloor\sqrt{m}\rfloor$ をビット演算量 $O(\log^3 n)$ で計算できるとする[*1]．

14-7. p, q を相異なる素数として，$n = pq$ とする．$n = 3403$, $\varphi(n) = 3280$ であるとき，p と q を求めよ．

[*1] この計算量は例えば，数値計算の二分法で実現される．ニュートン法など，より高速なアルゴリズムも知られている．