アルゴリズム B 第 14 回

2021 年 1 月 25 日

14　素因数分解

合成数 n を素因数分解する問題を考える．合成数 n の自明でない約数を見つけるアルゴリズムがあれば，これを再帰的に繰り返せば素因数分解ができる．そこで，合成数 n の自明でない約数を見つける問題を考える．

n が偶数かどうかの判定は容易であり，合成数 n が偶数ならば 2 は n の自明でない約数である．以下では特に断らない限り n を奇数の合成数とする．また，乗除算を筆算と同様に行うものとして計算量を評価する．

試し割算

素数判定と同様に，**試し割算** (trial division) で n の約数を見つけることができる．n を 3 以上 $\sqrt{n}$ 以下の奇数で順に割る．もし一度も割り切れなければ n は素数だから，n が合成数ならそれまでに自明でない約数が見つかる．ビット演算量は最悪の場合 $O(n^{1/2}\log^2 n)$ である．

フェルマー法

n がほとんど同じ大きさを持つ 2 つの整数の積である場合に有効な，**フェルマー法** (Fermat method) と呼ばれる素因数分解法がある．

n を奇数の合成数とする．$n = ab$, $a \geq b \geq 3$ であるとき，$t = (a+b)/2$, $s = (a-b)/2$ とおく．このとき，$n = t^2 - s^2$ である．a と b がほとんど同じ大きさを持つとき，s は非常に小さくなる．そこで，t を $\lceil\sqrt{n}\rceil$ から順に大きくしていき，$t^2 - n$ が平方数となる t を探す．（0 も平方数と見なす．）$t^2 - n = s^2$ となれば，$a = t + s$, $b = t - s$ によって n の自明でない約数 a, b が求まる．

ρ 法

ρ 法 (ρ method) は 1975 年にポラードが提案した素因数分解アルゴリズムである．写像 $f\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ を 1 つ固定する．$x_1 \in \mathbb{Z}/n\mathbb{Z}$ を 1 つランダムに選び，$x_{i+1} = f(x_i)$ $(i = 1, 2, 3, \dots)$ によって $x_2, x_3, x_4, \dots$ を定める．ある i, j に対して，$x_i \not\equiv x_j \pmod{n}$ であるが，ある n の自明でない約数 d に対して $x_i \equiv x_j \pmod{d}$ となれば，n の自明でない約数を見つけることができる．実際，$\gcd(x_i - x_j, n)$ は d で割り切れるが n で割り切れないので，自明でない n の約数である．

写像 f としてはできるだけ「ランダムに」値を移すものを用いる．例えば，$f(x) = x^2 + 1$ が用いられる．

すべての $1 \leq i < j \leq k$ に対して $\gcd(x_i - x_j, n)$ を計算すると，最大公約数の計算が $k(k-1)/2$ 回必要である．さらに，$x_1, x_2, \dots, x_k$ を記憶するための領域が必要である．いくつかの改善方法が知られているが，ここでは**フロイドの周期発見法** (Floyd cycle-finding method) を紹介する．

フロイドの周期発見法

命題 14.1. S を集合，$f\colon S \to S$ を写像とする．$x_1 \in S$ として，$x_2, x_3, \dots \in S$ を $x_{i+1} = f(x_i)$ で定める．いま，自然数 $j < k$ に対して $x_j = x_k$ が成り立つとする．$l = k - j$, $m = l\lceil j/l \rceil$ とおく．このとき，$x_m = x_{2m}$ である．

命題 14.1 の仮定の下で，$y_i = x_{2i}$ と定義すると，$y_{i+1} = f(f(y_i))$ である．したがって，

$$y_1 = f(x_1), \quad x_{i+1} = f(x_i), \quad y_{i+1} = f(f(y_i))$$

によって x_i, y_i を計算し，x_i と y_i を比較することで，$x_t = x_{2t}$ となる自然数 t を発見できる．$t \leq m \leq k$ だから，f の計算回数と比較回数は $O(k)$ である．また，最新の x_i, y_i だけを記憶しておけばよい．

注意. ここで求めた t は，十分大きい i に対して $x_i = x_{i+t}$ を満たしているが，そのような性質を持つ最小の t とは限らない．

フロイドの周期発見法を用いると，ρ 法のアルゴリズムは次のように書ける．

```
1: RhoMethod(n, f)
2:     x ∈ ℤ/nℤ をランダムに選ぶ
3:     y = f(x)
4:     while true
5:         d = gcd(x − y, n)
6:         if 1 < d < n then
7:             return(d)
8:         x = f(x), y = f(f(y))
```

ここで，第 4 行の **while true** は無限ループを表している．入力 n, f やランダムに選んだ x によっては，このアルゴリズムは停止しないことがある．

ρ 法の計算量を評価するために次の命題を用いる．

命題 14.2. S を n 個の要素を持つ集合として，$0 < p < 1$ とする．$x_1, x_2, \ldots, x_k \in S$ を独立かつ一様ランダムに選ぶ．このとき，$k \geq 1 + \sqrt{2n \log(1/(1-p))}$ ならば，p 以上の確率で $x_i = x_j$ を満たす相異なる i, j が存在する．

例 (誕生日のパラドックス (birthday paradox)**).** 命題 14.2 で $n = 365$, $p = 1/2$ とすると，$k \geq 23.4\cdots$ となる．このことから，24 人いれば 1/2 以上の確率で同じ誕生日の人がいることがわかる．ただし，閏年を考えないものとし，誕生日は独立かつ一様に分布すると仮定している．なお，正確に計算すると 23 人で十分である．

命題 14.2 より，ρ 法によってある一定の確率で自明でない約数を見つけるために必要なビット演算量は，発見的 (heuristic) には，$O(n^{1/4} \log^3 n)$ である．

注意. このほかにも，$p-1$ 法，2 次篩(ふるい) 法，数体篩法，楕円曲線法など，さまざまな素因数分解法が知られている．しかし，これらのアルゴリズムはどれも指数時間または準指数時間のアルゴリズムである．