アルゴリズム B 演習 No. 12 2013 年 1 月 11 日配布

12. 素因数分解法

合成数 n が与えられたとき，n を素因数分解する問題を考える．そのためには，n の自明でない約数を見つける方法を考えれば十分である．n が偶数であるかどうかは容易に判定できるので，n が奇数の場合を考えればよい．

- 素数判定法として前回紹介した**試し割算**は，同時に n の約数を見つけることができる．しかし，ビット演算量は最悪の場合 $O\bigl(n^{1/2}(\log n)^2\bigr)$ であった（問題 11-2）．
- ***ρ* 法**は次のようにして n の約数を見つける方法である．写像 $f\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ を一つ固定する．$x_1 \in \mathbb{Z}/n\mathbb{Z}$ を一つ選び，$x_{i+1} = f(x_i)$ $(i = 1, 2, 3, \dots)$ 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 で割り切れるので，自明でない n の約数である．

  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．

  ρ 法は，高い確率で，ビット演算量 $O(n^{1/4}(\log n)^3)$ で n の自明でない約数を見つけることができる．（問題 12-5, 12-6 も参照せよ．）
- n がほとんど同じ大きさを持つ二つの整数の積である場合に有効な，**フェルマー法**と呼ばれる素因数分解法がある．

  n を奇数の合成数で，平方数ではないとする．$n = ab$, $a \geq b > 0$ 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．$t^2 - n = s^2$ 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．
- このほかにも，$p-1$ 法，$p+1$ 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．

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．

12-1. $f(x) = x^2 + 1$, $x_0 = 2$ として，ρ 法を用いて 119 を素因数分解せよ．

12-2. $f(x) = x^2 + 1$, $x_0 = 3$ として，ρ 法を用いて 253 を素因数分解せよ．

12-3. フェルマー法を用いて 1147 を素因数分解せよ．

12-4. フェルマー法を用いて 1763 を素因数分解せよ．

12-5. S を d 個の要素からなる有限集合とする．

(a) $x_1, x_2, \ldots, x_r \in S$ をランダムに選んだとき，どの二つも異なる確率を求めよ．

(b) λ を正の実数として，$r = 1 + \left\lceil \sqrt{2\lambda d} \right\rceil$ とする．$x_1, x_2, \ldots, x_r \in S$ をランダムに選んだとき，どの二つも異なる確率は $e^{-\lambda}$ 以下であることを示せ．必要ならば，実数 $0 < t < 1$ に対して $\log(1-t) < -t$ が成り立つことを用いてもよい．

（この現象は**誕生日のパラドックス**と呼ばれる．）

12-6. S を集合, $f\colon S \to S$ を写像とする．$x_1 \in S$ として, $x_2, x_3, \ldots \in S$ を $x_{i+1} = f(x_i)$ で定める．いま，自然数 $j < k$ に対して $x_j = x_k$ となっているとする．$l = k - j$, $m = l\lceil j/l \rceil$ とおくと，$x_m = x_{2m}$ となることを示せ．（このことから，$x_j = x_k$ となる自然数 $j < k$ を見つけるには，自然数 m を動かして $x_m = x_{2m}$ となるものを探せばよい．この方法は，j, k を動かして $x_j = x_k$ かどうか確かめるよりも，比較回数が少なく，記憶領域を大幅に節約することができる．この方法を**フロイドの周期発見法** (Floyd cycle-finding method) といい，ρ 法に応用することができる．）

12-7. n を奇数の合成数で，平方数ではないとする．$|d - \sqrt{n}| < \sqrt[4]{n}$ を満たす n の約数 d が存在するとき，フェルマー法の 1 回目の試行（$t = \left\lceil \sqrt{n} \right\rceil$ のとき）で n の約数 d が見つかることを示せ．