アルゴリズム B 演習 No. 12　　2015 年 1 月 23 日配布

12. 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 が偶数かどうかは容易に判定でき，n が偶数のとき 2 は n の自明でない約数である．よって，以下では n を 3 以上の奇数とする．

- 素数判定と同様に，**試し割算**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 $O\bigl(n^{1/2}(\log n)^2\bigr)$ である（問題 11-1）．
- **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 で割り切れるが n で割り切れないので，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，フロイドの周期発見法（問題 12-6）を合わせて用いることで，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．
- 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．
- 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．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．

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. $f(x) = x^2 + 1$, $x_1 = 2$ として，ρ 法を用いて 133 を素因数分解せよ．

12-2. $f(x) = x^2 + 1$, $x_1 = 3$ として，ρ 法を用いて 221 を素因数分解せよ．

12-3. フェルマー法を用いて 899 を素因数分解せよ．

12-4. フェルマー法を用いて 1517 を素因数分解せよ．

12-5. n を（合成数とは限らない）3 以上の奇数とする．$\lceil\sqrt{n}\rceil \le t \le (n+9)/6$ を満たすすべての整数 t に対して，$t^2 - n$ が平方数でないとする．このとき，n が素数であることを示せ．

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．）