アルゴリズム B 演習 No. 13　　2018 年 1 月 26 日配布

13. 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，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．
- **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．

13-1. $f(x) = x^2 + 1$, $x_1 = 1$ として，ρ 法を用いて 221 を素因数分解せよ．

13-2. $f(x) = x^2 + 2$, $x_1 = 1$ として，ρ 法を用いて 391 を素因数分解せよ．

13-3. フェルマー法を用いて 779 を素因数分解せよ．

13-4. フェルマー法を用いて 4087 を素因数分解せよ．

13-5. 非負整数 n に対して，$F_n = 2^{2^n} + 1$ とおく．（F_n を**フェルマー数**という．）以下の問いに答えよ．

（a）$n \geq 2$ ならば，F_n のすべての素因数 p は $p \equiv 1 \pmod{2^{n+2}}$ を満たすことを示せ．

（b）$F_5 = 2^{2^5} + 1 = 4294967297$ の自明でない約数を 1 つ求めよ．