アルゴリズム B 演習 No. 12 2014 年 1 月 24 日配布

12. 素数判定・素因数分解

2 以上の自然数 n が素数かどうか判定する問題と，n が合成数のとき素因数分解する問題を考える．n が偶数かどうかは容易にわかる．また，素因数分解の際，n を 2 で割れるだけ割ることも容易である．そこで，以下では n を 3 以上の奇数とする．

まず素数判定のアルゴリズムについて述べる．

- **試し割算** (trial division) は次のような方法である．n を 3 以上 $\sqrt{n}$ 以下の奇数で順に割り，一度も割り切れなければ n は素数である．ビット演算量は最悪の場合 $O\big(n^{1/2}(\log n)^2\big)$ である．（四則演算のビット演算量には No. 8 のものを用いる．）
- p を素数，b を p と互いに素な整数とすると，$b^{p-1} \equiv 1 \pmod{p}$ が成り立つ．これを**フェルマーの小定理**という．この定理の対偶を考えると，n と互いに素な整数 b が存在して，$b^{n-1} \not\equiv 1 \pmod{n}$ ならば，n は合成数である．
- フェルマーの小定理の逆は一般には成り立たない．そこで，n を合成数，b を n と互いに素な整数として，$b^{n-1} \equiv 1 \pmod{n}$ が成り立つとき，n を b を底とする**擬素数** (pseudoprime) という．
- n を合成数とする．n と互いに素なすべての整数 b に対して n が b を底とする擬素数であるとき，n を**カーマイケル数** (Carmichael number) という．カーマイケル数は無限個存在することが知られている．
- n を奇数として，$n-1 = 2^s t$（t は奇数）と表す．n が素数ならば，n と互いに素なすべての整数 b に対して，次の条件が成り立つ．

$$b^t \equiv 1 \pmod{n} \quad \text{または}$$
$$b^{2^r t} \equiv -1 \pmod{n} \text{ を満たす } r\ (0 \le r \le s-1) \text{ が存在する．} \quad (1)$$

そこで，n を奇数の合成数として，n と互いに素な整数 b が条件 (1) を満たすとき，n を b を底とする**強擬素数** (strong pseudoprime) という．

- **ミラー・ラビンの素数判定法** (Miller-Rabin primality test) は次のようなアルゴリズムである．n を 3 以上の奇数として，n が素数かどうか判定したいとする．
  - 整数 b を $0 < b < n$ の範囲でランダムに選ぶ．$\gcd(b, n) > 1$ であるか，$\gcd(b, n) = 1$ であって条件 (1) が成り立たなければ，n は合成数である．

  n が合成数のとき上の手続きで合成数と判定されない確率は $1/4$ 以下であることが知られているので，この手続きを何回か繰り返して合成数と判定されなければ，n は高い確率で素数となる．手続き 1 回のビット演算量は $O\big((\log n)^3\big)$ である．

- ミラー・ラビンの素数判定法では素数であることを証明できない．素数であることを証明するためのアルゴリズムとして，ヤコビ和を用いる Adleman-Pomerance-Rumely 素数判定法，楕円曲線を用いる ECPP (elliptic curve primality proving) などがある．また，2002 年 Agrawal, Kayal, Saxena によって，素数判定の決定性多項式時間アルゴリズムである AKS アルゴリズムが発見された．

次に，合成数 n を素因数分解する問題を考える．

- **試し割算**は，同時に n の約数を見つけることができる．
- **ρ 法**は次のような方法である．写像 $f\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ を一つ固定する．例えば，$f(x) = x^2 + 1$ とする．$x_1 \in \mathbb{Z}/n\mathbb{Z}$ 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．このとき，$i = 1, 2, 3, \dots$ に対して，$\gcd(x_{2i} - x_i, n)$ を計算すると n の自明でない約数が得られることがある．ρ 法は，高い確率で，ビット演算量 $O\big(n^{1/4}(\log n)^3\big)$ 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．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. 2^{90} を 91 で割った剰余を求め，91 が合成数であることを示せ．

12-2. $561 = 3 \cdot 11 \cdot 17$ がカーマイケル数であることを示せ．

12-3. 561 は 2 を底とする擬素数であるが，2 を底とする強擬素数ではないことを示せ．

12-4. $f(x) = x^2 + 1$, $x_1 = 2$ として，ρ 法を用いて 161 を素因数分解せよ．

12-5. フェルマー法を用いて 2021 を素因数分解せよ．