

13 素数判定

2 以上の自然数 n が素数かどうか判定する問題を考える. n が偶数かどうかは容易にわかる. そこで, 以下では特に断らない限り n を 3 以上の奇数とする. 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

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. この方法を試し割算 (trial division) という. ビット演算量は最悪の場合 $O(n^{1/2} \log^2 n)$ である. この方法では, n が合成数のとき, 同時に n の約数も求められる.

フェルマーテスト

フェルマーの小定理より, 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. 対偶を考えると, n を自然数として, 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. しかし, フェルマーの小定理の逆は一般には成り立たないので, $b^{n-1} \equiv 1 \pmod{n}$ が成り立っても n が素数とは限らない.

n を合成数とする. 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 (フェルマー) 擬素数 ((Fermat) pseudoprime) という. 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.

フェルマーの小定理を用いて素数判定を行うフェルマーテスト (Fermat test) のアルゴリズムは次のようになる. ただし, n は素数判定を行う 3 以上の奇数であり, k は反復回数である.

```

1: FERMATTEST( $n, k$ )
2:   for  $i = 1$  to  $k$ 
3:      $1 < b < n - 1$  を満たす整数  $b$  をランダムに選ぶ
4:     if  $\text{gcd}(b, n) > 1$  or  $b^{n-1} \not\equiv 1 \pmod{n}$  then
5:       return(「 $n$  は合成数である」)
6:   return(「 $n$  はカーマイケル数である, または, 高い確率で素数である」)

```

命題 13.1. n をカーマイケル数ではない奇数の合成数とする. $0 < b < n$ となる整数 b のうち, n が b を底とする擬素数となるのは全体の高々 $1/2$ である.

命題 13.1 より, n がカーマイケル数ではない奇数の合成数のとき, 誤って素数と判定する確率は 2^{-k} 以下である. 一方, カーマイケル数に対しては, フェルマーテストがうまく働かない. さらに, 次の定理が知られている.

定理 13.2 (Alford, Granville, Pomerance). カーマイケル数は無限個存在する.

ミラー・ラビンの素数判定法

命題 13.3. n を奇素数として, $n-1 = 2^s t$ (t は奇数) と表す. 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.

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

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.

命題 13.4. n を奇数の合成数, b を n と互いに素な整数とする. n が b を底とする強擬素数ならば, n は b を底とする擬素数である.

命題 13.5. n を奇数の合成数とする. $0 < b < n$ となる整数 b のうち, n が b を底とする強擬素数となるのは全体の高々 $1/4$ である.

命題 13.5 より, 強擬素数についてはカーマイケル数のような数は存在しない.

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. ただし, n は素数判定を行う 3 以上の奇数であり, k は反復回数である.

- 1: MILLER-RABIN(n, k)
- 2: **for** $i = 1$ **to** k
- 3: $1 < b < n-1$ を満たす整数 b をランダムに選ぶ
- 4: **if** $\text{gcd}(b, n) > 1$ or 条件 (1) が成り立たない **then**
- 5: **return**(「 n は合成数である」)
- 6: **return**(「 n は高い確率で素数である」)

命題 13.5 より, n が奇数の合成数のとき, 誤って素数と判定する確率は 4^{-k} 以下である. また, 第 4 行を 1 回実行したときのビット演算量は $O(\log^3 n)$ である. したがって, k を定数とすれば, ミラー・ラビンの素数判定法のビット演算量は $O(\log^3 n)$ である.

注意. 拡張リーマン予想 (extended Riemann hypothesis)^{*1} が成り立つことを仮定したとき, 条件 (1) を満たさない b が $b < 2 \log^2 n$ の範囲に存在することが知られている. したがって, 拡張リーマン予想が成り立てば, 素数判定の決定性多項式時間アルゴリズムが得られる.

注意. 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, 楕円曲線を用いる **ECPP** (elliptic curve primality proving) がよく用いられる. 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.

^{*1} ここでは, ディリクレの L 関数に対するリーマン予想の類似を指す. 一般リーマン予想 (generalized Riemann hypothesis) と呼ぶこともある.