アルゴリズム B 演習 No. 11 2013 年 1 月 4 日配布

11. 素数判定法

2 以上の自然数 n が与えられたとき，n が素数であるか判定する問題を考える．n が偶数であるかどうかは容易に判定できることに注意する．

- **試し割算** (trial division) による方法は次の通りである．n を 3 以上の奇数とする．n を 3 以上 $\lfloor\sqrt{n}\rfloor$ 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．この方法では，n が合成数のとき，同時に n の約数も求められる．
- 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** (Fermat's little theorem) という．この定理は問題 9-11 から直ちに従う．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．
- n を奇数の合成数として，$n-1 = 2^s t$（t は奇数）と表す．b を n と互いに素な整数とする．n と b が次の条件を満たすとき，n を b を底とする**強擬素数** (strong pseudoprime) という．

  $b^t \equiv 1 \pmod{n}$ または

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

  n を奇数の合成数とすると，$0 < b < n$ 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 $1/4$ であることが知られている．
- **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．

1. 整数 b を $0 < b < n$ の範囲でランダムに選び，$\gcd(n, b)$ を計算する．
2. $\gcd(n, b) > 1$ ならば，n は合成数である．
3. $\gcd(n, b) = 1$ のとき，条件 (1) が成り立つかどうか判定する．
4. 条件 (1) が成り立たなければ，n は合成数である．

上の手続きを k 回繰り返して，合成数と判定されることがなければ，n は $1-(1/4)^k$ 以上の確率で素数である．

- ヤコビ記号を用いて同様の判定を行う**ソロヴェイ・シュトラッセンの素数判定法** (Solovay-Strassen primality test) がある．この判定法では，条件 (1) の代わりに

$$b^{(n-1)/2} \equiv \left(\frac{b}{n}\right) \pmod{n}$$

を用いる．判定を k 回繰り返して合成数と判定されなければ，素数である確率は $1-(1/2)^k$ 以上となる．

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．四則演算のビット演算量として，No. 7 で与えたものを使うものとする．

11-1. 上述した試し割算による方法で一度も割り切れなかったとき，確かに n が素数であることを示せ．

11-2. 試し割算による素数判定のビット演算量は，最悪の場合 $O\bigl(n^{1/2}(\log n)^2\bigr)$ であることを示せ．

11-3. フェルマーの小定理を問題 9-11 を用いずに示せ．

11-4. $2^{118} \bmod 119$ を計算することで，119 が合成数であることを示せ．

11-5. $561 = 3 \cdot 11 \cdot 17$ がカーマイケル数であることを示せ．

11-6. 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，条件 (1) が成り立つことを示せ．

11-7. ミラー・ラビンの素数判定法において，n が素数である確率を 99% 以上にするためには，繰り返し回数 k をいくつ以上にすればよいか求めよ．

11-8. $n = 561$ に対して，n と互いに素な整数 b で，条件 (1) が成り立たないものを一つ求めよ．

11-9. ミラー・ラビンの素数判定法のビット演算量は $O\bigl(k(\log n)^3\bigr)$ であることを示せ．（問題 9-7 の結果を用いてよい．）