アルゴリズム B 演習 No. 12　　2016 年 1 月 8 日配布

12. 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 n を 3 以上の奇数とする．

- **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．
- 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．この定理は問題 10-9 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．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（問題 12-5）．

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

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．$0 < b < n$ 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．
  - 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．

  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．

- 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．

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. $2^{246} \bmod 247$ を計算することで 247 が合成数であることを示せ．

12-2. 77 が b を底とする擬素数となるような整数 b で $0 < b < 77$ の範囲にあるものをすべて求めよ．

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

12-4. 奇数の合成数 n がカーマイケル数でないならば，$0 < b < n$ となる整数 b で，n が b を底とする擬素数となるものの個数は $\varphi(n)/2$ 以下であることを示せ．

12-5. n が奇数かつ素数ならば，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．

12-6. $n = 561$ に対して，n と互いに素な整数 b で，条件 (1) を満たさないものを一つ求めよ．

12-7. n を 3 以上の奇数とする．以下の問いに答えよ．

（a）n と互いに素な整数 b が

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

を満たさないとする．ただし右辺はヤコビ記号である．このとき n が合成数であることを示せ．

（b）$n = 561$ に対して，n と互いに素な整数 b で，条件 (2) を満たさないものを一つ求めよ．

（条件 (2) を用いた素数判定法はソロヴェイ・シュトラッセンの素数判定法 (Solovay-Strassen primality test) と呼ばれる．）

12-8. 整数 $n \geq 0$ に対して，$F_n = 2^{2^n} + 1$ とおく．$n > 1$ のとき，F_n が素数であるための必要十分条件は，$5^{(F_n-1)/2} \equiv -1 \pmod{F_n}$ であることを示せ．（この判定法はペパンの判定法 (Pépin's test) と呼ばれる．）