アルゴリズム B 演習 No. 12　　　　2017 年 1 月 20 日配布・2017 年 1 月 27 日修正

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 10-8 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 12-4）．

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

  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．また，四則演算のビット演算量として，No. 8 で与えたものを使うものとする．

12-1. 試し割算による素数判定のビット演算量は $O\big(\sqrt{n}(\log n)^2\big)$ であることを示せ．

12-2. $2^{220} \bmod 221$ を計算することで $\underline{221}$ が合成数であることを示せ[*1]．

12-3. $2465 = 5 \cdot 17 \cdot 29$ がカーマイケル数であることを示せ．

12-4. 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．

12-5. $n = 2465$ 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．

12-6. a を 2 以上の整数とする．p を $a^2 - 1$ を割り切らない奇素数として，

$$n = \frac{a^{2p} - 1}{a^2 - 1}$$

とおく．以下の問いに答えよ．

(a) n が合成数であることを示せ．

(b) $n - 1$ が $2p$ で割り切れることを示せ．

(c) n が a を底とする擬素数であることを示せ．

12-7. 整数 a と 2 以上の自然数 n が以下の条件を満たすとする．

- $a^{n-1} \equiv 1 \pmod{n}$.
- $n - 1$ のすべての素因数 q に対して，$a^{(n-1)/q} \not\equiv 1 \pmod{n}$.

このとき，n が素数であることを示せ．

12-8. 問題 12-7 を $a = 5$, $n = 73$ に適用して，73 が素数であることを示せ．

[*1] 下線部を修正しました．