素数とその探求
～素数の判定法を求めて～

2000MM025 伊藤　彰浩
指導教員　宮元　忠敏

1　はじめに

[1] に書いてあるように、整数論の基本定理は「1 より大きな任意の自然数は一意的に素数の積として表される」ことを主張しており、素数の役割は大変重要なものである。
ギリシアでは、Euclid が紀元前 300 年ごろに、「素数は無限に存在する」ことを証明している。さらに Eratosthenes は、独特な「Eratosthenes の篩」を用いて、素数を見つける方法を考え出した。
しかし、素数の実体というものは、なかなか容易にはつかめなかった。Euler、Fermat、Gauss、Legendre、Mersenne などの数学者達は、実体を求めようとして、努力し、「素数定理」を初めとして、いろいろな性質を発見した。
また、現代のコンピューター時代において、暗号体系で欠かすことのできない、重要なものが素数である。アメリカの RSA 体系が、その代表的な例である。そのようなことを [2] 等で知りそれを調べようと思った。そしてその素数の判定法を [5] や [6] を通して学んだ。また、素数の判定法によく用いられる Fermat の小定理や Euler 規準などに関して [7] を元にした。　本研究では、その素数について、まず素数の無限性について述べ、その次に大きな数に対して、できるだけわずかな操作で、より短い時間で、素数であるかどうか、判定する効率的なアルゴリズムを発見するための、いろいろな定理を示す。

2　合同式に基づく素数判定法

素数を特徴付ける Wilson の定理は有用に思われるが、階乗の計算に長時間必要とするため実際の判定法としては不向きである。Fermat の小定理は p が素数であり、a が $p \nmid a$ なる自然数ならば $a^{p-1} \equiv 1 \pmod{p}$ となることを主張している。しかし、この定理の逆はそのままの形では成り立たない。というのも $a^{N-1} \equiv \pmod{N}$ となる合成数 N と $a \geq 2$ が存在するからである。
(反例) $2^{340} \equiv 1 \pmod{341}$ である。それにも関わらず、Fermat の小定理の逆が成り立つ場合が発見された。

2.1　判定法 1

$N > 2$ とし、次を満たす整数 $a > 1$ が存在したとする：

1. $a^{N-1} \equiv 1 \pmod{N}$
2. $a^m \not\equiv 1 \pmod{N}$　　$(m = 1, 2, \cdots, N-2$ に対して)

このとき N は素数である。

この判定法の欠点：$N-2$ 回の掛け算と、法 N に関する剰余をみつけなければいけない。

2.2　判定法 2

$N > 1$ とし、次を満たす整数 $a > 1$ が存在したとする：

1. $a^{N-1} \equiv 1 \pmod{N}$
2. $a^m \not\equiv 1 \pmod{N}$　　$(m \mid N-1$ なるすべての $m < N$ に対して)

このとき N は素数である。
この判定法の欠点：$N-1$ のすべての約数を知らなければいけない。よって一般には多大の時間を要する。

2.3　判定法 3

$N > 1$ とし、$N-1$ のすべての素因数 q に対して次を満たす整数 a が存在したとする：

1. $a^{N-1} \equiv 1 \pmod{N}$
2. $a^{\frac{N-1}{q}} \not\equiv 1 \pmod{N}$

このとき N は素数である。

この判定法の欠点：$N-1$ の素因数を知る必要があるが判定法 2 よりは少ない数の合同式を調べればよい。

2.4　判定法 4

$N - 1 = F \cdot R, \gcd(F, R) = 1, F$ は完全に素因数分解された部分、R は分解しきれていない部分とし、つぎの a がみつかったとする：

1. $a^{RF} \equiv 1 \pmod{N}$
2. $\gcd(a^{\frac{RF}{q}} - 1, N) = 1$　$(\text{すべての } q \mid F)$

このとき N の各素因数は $mF + 1 (m \geq 1)$ の形をしている。
このことより次が導かれる。
上の $N-1$ の分解で $F > R$ であって条件を満たす a が存在すれば N は素数である。

3　Luca/Lehmer テスト

ここでは Mersenne 素数を調べる。
Mersennne 数 M_pは M_pが S_{p-2}を割るとき ($S_0 = 4, S_i = S_{i-1}^2 - 2, i \geq 1$) に限り素数である。$S_{p-2}$が M_pで割られたときの余りを p に対するLucaLehmer の剰余と

呼ばれる。すなわち、M_pが素数ならば、$LucaLehmer$ の剰余は 0 である。

4 Fermat 数

Fermat の小定理の逆を用いて Pepin が Fermat 数の素数性を調べる方法を示した。

4.1 判定法 5

$F_n = 2^{2^n} + 1 (n \geq 2)$ とし、$k \geq 2$ とする。このとき次の条件は同値である：

1. F_nは素数であり、かつ $(k/F_n) = -1$
2. $k^{(F_n-1)/2} \equiv -1 \pmod{F_n}$

(k/F_n) はLegendre 記号を示す。

5 擬素数

ここでは、因数の全数探索をせずに、数が合成数であることを示すために、Fermat の小定理をどのように使えるかを述べる。Fermat の小定理から、p が素数でかつ a が p で割り切れない整数なら、$a^{p-1} \equiv 1 \pmod{p}$ である。ここである正の奇数 n が素数であるかを問う。b で割り切れず $b^{n-1} \not\equiv 1 \pmod{n}$ であるような整数 b を見つけるとする。すると、Fermat の小定理から n は素数ではありえないことになる。数 b は n が合成数であるという事実の証拠と呼ばれる。こうしてこれが、数の素因数分解に頼らない合成数の判定法である。

5.1 合成数判定

$n > 0$ を奇数とする。つぎのような整数 b が存在すれば、n は合成数である。

1. $1 < b < n - 1$
2. $b^{n-1} \not\equiv 1 \pmod{n}$

興味は合成数であるかということより、素数であるかということにあるから、Fermat の小定理を数が素数であることの証明に使うことができるかどうかを問うのは理にかなっている。より正確にいえば、$n > 0$ はある整数 $1 < b < n - 1$ に対し、$b^{n-1} \equiv 1 \pmod{n}$ を満たす奇数であるとする。このとき n は必ず素数であるかということをライプニッツは肯定的であると思い、素数の判定法としてこれを用いた。その際には、計算を簡単にするために $b = 2$ を選んでいた。しかしこれは間違っていた。

しかし 341=11・31 は合成数である。この判定で ” 偽の肯定的 ” な結果を与える数は擬素数として知られる。言い換えれば、正の整数 n が奇数の合成数であって、ある整数 $1 < b < n - 1$ に対して $b^{n-1} \equiv 1 \pmod{n}$ を満たすとき底 b に関する擬素数と呼ばれる。100 パーセント正確ではないが有用である。

正の奇数 n が合成数で n と互いに素でない底 b が選ばれると n は底 b に関する擬素数にはならない。実用的には、計算を限界内に保つため単に小さい素数の中から底をいくつか選ぶ。n の最小の因数が非常に大きいとこれらの底はすべて n と互いに素になる。そこで、考えるべき問題は上で述べたものの改良版である。考える問題は正の奇数 n で n と互いに素な底 b に関して擬素数となるものがあるかどうかである。

言い換えると、合成数でなおかつすべての整数 b に関して $b^n \equiv b \pmod{n}$ を満たす正の奇数 n はあるか？これはCarmichael に考えられ Carmichale 数と呼ばれる。

奇数 $n > 0$ は合成数ですべての b に対して $b^n \equiv b \pmod{n}$ のとき Carmichael 数という。

5.2 Carmicahel 数

Carmichale 数の特徴はコーセルトによって与えられた。奇数の合成数 $n > 0$ がCarmichael 数であるのは、n の各素因数 p に対して、次の条件が成り立つときかつそのときに限る。

1. p^2は n を割り切らない。
2. $p - 1$ は $n - 1$ を割り切る。

6 Miller-Rabin の判定法

1.(入力) 素数判定をしたい奇数の合成数 n と $1 < b < n$ である整数 b を一つ与える。

2.$n - 1 = 2^s t$, ただし t は奇数、となる s と t を求める。(n を 2 で割れる限り繰り返す。)

3.判定条件「$b^t \equiv 1 \pmod{p}$ であるか、または、ある $0 \leq r < s$ について $b^{2^r t} \equiv -1 \pmod{n}$」をみたすかどうかを調べる。

4.(出力) 判定条件を満たしていれば「$Yes?$」を、そうでなければ「No」を返す。

ここから確率的素数判定法が得られる。

7 おわりに

判定法 1 ～ 4 まではある数が素数であることを確実に主張できる判定法である。しかしこれらの判定法は Miller-Rabin の判定法ほど効率的でも使いやすくも無い。現在の多くの計算機代数系は底の十分大きな集合に対して Miller-Rabin の判定法を利用している。

参考文献

[1] 好田　順治：素数の不思議, 現代数学社 (1999).

[2] Paulo Ribenboim 著：吾郷　孝視 訳：素数の世界 その探索と発見, 共立出版株式会社 (1995).

[3] Joseph H.Silverman 著：鈴木　治郎訳：はじめての数論, 株式会社ピアソン・エデュケーション (2001).

[4] 中島　匠一：代数と数論の基礎, 共立出版株式会社 (2000).

[5] 木田　祐司：初等整数論, 朝倉書店 (2001).

[6] S.C. コウチーニョ著：林　彬訳：暗号の数学的基礎, シュプリングラー・フェアラーク東京 (2001).

[7] 小林　昭七：なっとくするオイラーとフェルマー, 講談社 (2003).