素数判定テストとカーマイケル数

中学 2 年 3 組 24 番　田代新之助

2018 年 5 月 2,3 日　第 72 回灘校文化祭

1　はじめに

本日は第 72 回灘校文化祭にお越し頂きありがとうございます。本稿では、大きな数が素数であるとき, どうすればそれを知ることができるかということについて考えていきたいと思います。

2　準備

定理 1(フェルマーの小定理)

p が素数、a が任意の自然数のとき

$$a^p \equiv a \pmod{p}$$

特に、a と p が互いに素な自然数のとき

$$a^{p-1} \equiv 1 \pmod{p}$$

定理 2(中国の剰余定理)

与えられた k 個の整数 $m_1, m_2, \cdots, m_k$ がどの二つも互いに素ならば、任意の整数 $a_1, a_2, \cdots, a_k$ に対し

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}, \\ x &\equiv a_2 \pmod{m_2}, \\ &\cdots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

を満たす整数 x が $m_1 m_2 \cdots m_k$ を法として一意的に存在する。

定義 3(位数)

互いに素な正の整数 m と整数 a に対して $a^d \equiv 1 \pmod{m}$ が成り立つような最小の正の整数 d を法 p における a の位数という。mod p における a の位数を n とすると,
$a^m \equiv 1 \pmod{p}$ を満たすとき m は n の倍数である。

3　素数判定法

例 1, 8629,8633,8641 について、素数であるかどうか調べよ。

このような小さな数 n については、$\sqrt{n}$ までの約数の可能性のすべての数で単純にチェックでき、約数を見つけられるか、そうでなければ n が素数であることがわかる。ですから 8629 と 8641 は素数であり、8633 は $89 \cdot 97$ と分解できて素数であることがわかる。

例 2,$m = 1137369476253104052311779730283443758629640 01$ について、素数であるかどうか調べよ。

このような大きな数だと、たとえコンピュータを使ったとしても、各平方根までの可能な約数を試すことはほとんど無理である。しかし、（コンピュータ上では）たいへん大きな数を法としてたいへん高いべき乗を計算することはそんなに難しくない。例えば、ここにあげた数 m について、コンピュータ上わずかな時間で

$$\begin{aligned} 2^m &\equiv 2^{1137369476253104052311779730283443758629640 01} \\ &\equiv 392419708153934990601200436926306159617900 20 \pmod{m} \end{aligned}$$

が計算できる。

フェルマーテスト

フェルマーの小定理の対偶をとると、これは次のように、自然数 n が合成数であるための十分条件を与える。

対偶

n と互いに素な整数 a が

$$a^{n-1} \not\equiv 1 \pmod{n}$$

を満たせば、n は合成数である。

この十分条件を用いて、次のように自然数 n の素数判定を行います。

1, パラメータとして、2 以上 n 未満の自然数 a を 1 つ定める。

2,a と n が互いに素でなければ「n は合成数」と出力して終了。

3,$a^{n-1} \not\equiv 1 \pmod{n}$ ならば「n は合成数」と出力して終了する。そうでないとき「n は確率的素数」と出力して終了する。

フェルマーテストが「合成数」と出力したとき、上のフェルマーの小定理の対偶によって n は実際に合成数である。しかし、上の対偶は十分条件を与えるのみで必要条件を与えるものではないので、「確率的素数」と出力された場合でも n は実際に素数であるとは限らない。素数でないにもかかわらず「確率的素数」と判定されてしまう合成数は擬素数と呼ばれる。

疑わしければ、「確率的素数」と出力された場合にはまた異なる a を用いて再びテストを行う。十分な回数だけ a を取り替えて繰り返せば、フェルマーテストが「確率的素数」と判定した数は実際に素数である可能性が高い。

しかし、カーマイケル数または絶対擬素数と呼ばれる ”反例” もある。カーマイケル数は合成数であるにもかかわらず、ほとんどいかなる a を用いても「確率的素数」と判定されてしまう。例えば、$n = 561$ は $3 \cdot 11 \cdot 17$ と分解できて合成数であるが $a^{561} \equiv a \pmod{561}$ である。

$a^{561} \equiv a \pmod{561}$ の証明

$a^{561} \equiv a \pmod 3$,$a^{561} \equiv a \pmod{11}$,$a^{561} \equiv a \pmod{17}$ を証明できれば十分である。なぜなら 3,11,17 でそれぞれ割れる数はそれらの積 $3 \cdot 11 \cdot 17$ で割りきれるから。第一の合同式について 3 が a を割り切るとき、両辺は 3 を法として 0。3 が a を割り切らないとき、フェルマーの小定理を使って $a^2 \equiv 1 \pmod 3$ なので、

$a^{561} = a^{2 \cdot 280+1} = (a^2)^{280} \cdot a \equiv 1 \cdot a \equiv a \pmod 3$

となります。第 2 の式と第 3 の式も同様にして証明できる。よって 11 が a を割り切るとき両辺は 11 を法として 0 であり、そうでなければ合同式 $a^{10} \equiv 1 \pmod{11}$ を使って

$a^{561} = a^{10 \cdot 56+1} = (a^{10})^{56} \cdot a \equiv 1 \cdot a \equiv a \pmod{11}$

が計算できる。最後に、17 が a を割り切るとき両辺とも 17 を法として 0 であり、そうでなければ $a^{16} \equiv 1 \pmod{17}$ を使って

$a^{561} = a^{16 \cdot 35+1} = (a^{16})^{35} \cdot a \equiv 1 \cdot a \cdot a \pmod{17}$

が計算できる。 □

このような例が R.D. カーマイケルによって 1910 年に指摘されたので、カーマイケル数と名付けられた。ちなみに先に述べた 561 は最小のカーマイケル数であり、10000 までのカーマイケル数は 561,1105,1729,2465,2821,6601,8911 の 7 つである。

これらを素因数分解すると

$$561 = 3 \cdot 11 \cdot 17 \qquad 1105 = 5 \cdot 13 \cdot 17 \qquad 1729 = 7 \cdot 13 \cdot 19$$
$$2465 = 5 \cdot 17 \cdot 29 \qquad 2821 = 7 \cdot 13 \cdot 31 \qquad 6601 = 7 \cdot 23 \cdot 41$$
$$8911 = 7 \cdot 19 \cdot 67$$

となり、これらはすべて 3 つの相異なる奇素数の積であることがわかる。よって、これだけを見るとカーマイケル数は 3 つの奇素数の積になっていると予想できるが、$62745 = 3 \cdot 5 \cdot 47 \cdot 89$ は 4 つの素数の積となっているカーマイケル数である。これより次のような予想ができる。

(A) すべてのカーマイケル数は奇数である。

(B) すべてのカーマイケル数は相異なる素数の積である。

(A) の証明

カーマイケル数の満たす合同式から

$a^n \equiv a \pmod n$

が $a = n - 1 \equiv -1 \pmod n$ に対して成り立つので

$(-1)^n \equiv -1 \pmod n$

を得る。このことは ($n = 2$ でなければ)n が奇数であることを意味している。 □

(B) の証明

n がカーマイケル数だと仮定する。p を n を割り切る整数とし、そして p^{e+1} が n を割り切る p の最大べきだとする。このとき、$e = 0$ を示せばよい。n がカーマイケル数より $a^n \equiv a \pmod{n}$ がすべての a について成り立つ。とくに、$a = p^e$ についても成り立つので、

$p^{en} \equiv p^e \pmod{n}$

が成り立つ。よって n は差 $p^{en} - p^e$ を割り切り、仮定より p^{n+1} は n を割り切るので、

p^{e+1} は $p^{en} - p^e$ を割り切る

ことが結論づけられる。したがって $\dfrac{p^{en} - p^e}{p^{e+1}} = \dfrac{p^{en-e} - 1}{p}$ は整数になる。このことが成り立つのは唯一 $e = 0$ しかない。 □

定理 4(カーマイケル数に対するコルセルトの判定法)

合成数 n がカーマイケル数である必要十分条件は、奇数かつ n を割り切る素数 p がすべて以下の 2 条件を満たすことである。

(1)p^2 は n を割り切れない。

(2)$p - 1$ は $n - 1$ を割り切る。

証明

最初に n は合成数とし、さらに n の素因数 p はすべて条件 (1) と (2) を満たすものとします。このとき n がカーマイケル数であることを証明する。

n を $n = p_1 p_2 p_3 \cdots p_r$ と素数の積に分解します。条件 (1) から、$p_1, p_2, \cdots p_r$ はすべて相異なります。条件 (2) から各 $p_i - 1$ は $n - 1$ を割り切り、よって各 i について,

$$n - 1 = (p_i - 1)k_i \qquad k_i \text{ は整数}$$

と表せます。任意の整数 a をとる。p_i を法とした a^n の値を以下のように計算します。まず p_i が a を割り切るときは明らかに

$$a^n \equiv 0 \equiv a \pmod{p_i}$$

です。p_i は a を割り切らないとき、フェルマーの小定理を使って

$$\begin{aligned} a^n &= a^{(p_i-1)k_i} && n - 1 = (p_i - 1)k_i \text{ より} \\ &= (a^{p_i-1})^{k_i} \cdot a \\ &\equiv 1^{k_i} \cdot a \pmod{p_i} && \text{フェルマーの小定理より } a^{p_i-1} \equiv 1 \pmod{p_i} \\ &\equiv a \pmod{p_i} \end{aligned}$$

よって、$a^n - a$ は各素数 $p_1, p_2, \cdots, p_r$ で割り切れるので、それらの積 $n = p_1 p_2 \cdots p_r$ でも割り切れる (素数 $p_1, p_2, \cdots, p_r$ はすべて異なることに注意)。したがって $a^n \equiv a \pmod{n}$ であり、これはすべての n について成り立つことを示す。これで n がカーマイケル数であることが示された。

次に、すべてのカーマイケル数が条件 (1) と (2) を満たすことを証明する。

n をカーマイケル数とする。カーマイケル数の性質 (A) と (B) より、n は奇数で相異なる奇素数 $p_1, p_2, \cdots, p_r$ の積

$n = p_1 p_2 \cdots p_r$ に分解できる。よって、条件 (1) は明らか。中国剰余定理より、$1 \leq k \leq r$ を満たす k に対して

$$a \equiv a_k \pmod{p_k}$$

を満たす整数 a が存在する。この a について、$a^{n-1} \equiv 1 \pmod{n}$ より、

$$a^{n-1} \equiv 1 \pmod{p_k}$$

が成り立つので、

$${a_k}^{n-1} \equiv 1 \pmod{p_k}$$

が成り立つ。これと a_k の位数が $p_k - 1$ であることから、$p_k - 1$ は $n - 1$ を割り切る。 □

定理 5(素数の性質)

p を奇素数とし、$p - 1 = 2^k q$,q は奇数と表す。a を p で割り切れない任意の整数とする。このとき以下の 2 つの性質が成り立つ。

(i)a^q は p を法として 1 に合同である。

(ii)$a^q, a^{2q}, a^{4q}, \cdots, a^{2^{k-1}q}, a^{2^k q}$ の内一つは p を法として -1 に合同である。

証明

a と p は互いに素なので $a^{p-1} \equiv 1 \pmod{p}$(フェルマーの小定理). これより数のリスト

$a^q, a^{2q}, a^{4q}, \cdots, a^{2^{k-1}q}, a^{2^k q}$

を調べると、このリストの最後の数は p を法として 1 に合同であること ($2^k q$ は $p - 1$ に等しいので) がわかります。さらに、リストにある各数は直前の数の平方になっている。したがって、以下の 2 つの可能性だけが考えられる。

(i) リストの最初の数が p を法として 1. に合同である。

(ii) リストのある数が p を法として 1 に合同でなく、それを平方するとき、p を法として 1 に合同になる。この性質に該当する唯一の数は p を法として -1 に合同であり、この場合、リストは p を法として -1 に合同な数を含んでいる。 □

この性質を使って、合成数に対するラビン・ミラー判定法を得る。すなわち n が奇数であり、n が前述の素数の性質をもたないとすると、その数は合成数でなくてはなりません。さらに多くの a の値に対して n が素数の性質をもつとき、n は素数の可能性が高くなります。

定理 6(合成数に対するラビン・ミラー判定法)

n を奇数とし、奇数 q で $n - 1 = 2^k q$ と表す。以下の条件が両方とも成り立つとき、n は合成数である。

(a)$a \not\equiv 1 \pmod{n}$

(b)$i = 0, 1, \cdots, k - 1$ すべてに対して、$a^{2^i q} \not\equiv -1 \pmod{n}$

4　おわりに

最後までお読みいただきありがとうございます。はじめて部誌を書きました。TEX を使うのも初めてで大変でしたが、なんとか書き終えることができました。フェルマーの小定理が素数判定に応用できることを知って、このことを調べると他にも素数にいろいろな性質があり、素数の世界はとても奥深いものだと思いました。

参考文献

[1] はじめての数論 (Joseph H. Silverman)
[2] LATEX 2ε 美文書作成入門 (奥村晴彦・黒木裕介)