フェルマーテストとミラー・ラビン素数判定法

フェルマーテスト

フェルマーの小定理の対偶をとると，次のような，自然数 n が素数でないための十分条件が求まる。

命題　n と互いに素なある整数 a が　$a^{n-1} \not\equiv 1 \pmod{n}$　を満たすならば，n は素数でない。

この命題を用いて自然数 n の素数判定をするアルゴリズムを，フェルマーテストという。

n を 3 以上の奇数とし，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。

1　a と n が互いに素でなければ「素数でない」と出力して終了。

2 「$a^{n-1} \equiv 1 \pmod{n}$」のときは「素数でないと判定されなかった」として，3 に移る。
　そうでないときは「素数でない」と出力して終了する。

3　2 のテストを十分な回数行ったときは「素数の可能性が高い」と出力して終了し，まだ十分でないときは，異なる a を用いて 2 のテストを行う。

「素数でない」と出力された場合，n は必ず素数でない。しかし，「素数の可能性が高い」と出力された場合，n が実際に素数であるとは限らない。

さらに，n と互いに素な如何なる a を用いても「素数の可能性が高い」と判定されてしまう合成数 n が存在する。このような数を，カーマイケル数という。カーマイケル数は小さい方から

561，1105，1729，2465，2821，6601，8911，……

であり，無限に多く存在することが知られている。

したがって，フェルマーテストは完全な確率的素数判定法ではない。カーマイケル数でも「素数でない」と確率的に判定できる方法として，次のミラー・ラビン素数判定法がある。

ミラー・ラビン素数判定法

補題　p を素数とするとき，合同方程式　$x^2 \equiv 1 \pmod{p}$　の解は　$x \equiv \pm 1 \pmod{p}$

証明　　$x^2 \equiv 1 \pmod{p}$　より　$(x-1)(x+1) \equiv 0 \pmod{p}$

p は素数であるから，　$x-1, x+1$　の少なくとも一方は p の倍数である。

よって，　$x-1 \equiv 0$　または　$x+1 \equiv 0 \pmod{p}$

すなわち　$x \equiv 1$　または　$x \equiv -1 \pmod{p}$

逆も成り立つ。

□

この補題を用いて，次のようにフェルマーテストを精密化することを考える。

n は奇数であるから，　$\dfrac{n-1}{2}$　は整数である。よって，　$a^{n-1} \equiv 1 \pmod{n}$ が成り立ったとき，

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

nが素数であるとすると，補題により

$$a^{\frac{n-1}{2}} \equiv 1 \quad \text{または} \quad a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

対偶により，$a^{\frac{n-1}{2}} \not\equiv 1$ かつ $a^{\frac{n-1}{2}} \not\equiv -1 \pmod{n}$ のときnは素数でない。すなわち，フェルマーテストでは，nは「素数でないと判定されなかった」が，$a^{\frac{n-1}{2}}$ を計算することにより「素数でない」と判定される可能性がある。

さらに，$\dfrac{n-1}{2}$が偶数で，かつ $a^{\frac{n-1}{2}} \equiv 1$ のとき，nは「素数でないと判定されなかった」が，$a^{\frac{n-1}{4}}$ を計算することにより「素数でない」と判定される可能性がある。

このようにして，カーマイケル数であっても「素数でない」と確率的に判定する方法がミラー・ラビン素数判定法である。ただし，効率的に判定するために，次の命題を用いる。

命題　nは3以上の奇数とし，$n-1=2^s \cdot d$ と表す。ここで s は正の整数で，d は奇数である。

このとき，nの倍数でないある整数aについて

$$a^{2^{s-1}\cdot d} \not\equiv -1,\ a^{2^{s-2}\cdot d} \not\equiv -1, \cdots\cdots,\ a^{d} \not\equiv -1,\ a^{d} \not\equiv 1 \pmod{n}$$

のすべてが成り立つならば，nは素数でない。

証明　nは素数であると仮定する。

フェルマーの小定理により，$a^{n-1} \equiv 1 \pmod{n}$ が成り立つから

$$a^{2^s \cdot d} \equiv 1 \pmod{n}$$

よって　　$\left(a^{2^{s-1}\cdot d}\right)^2 \equiv 1 \pmod{n}$

補題により　　$a^{2^{s-1}\cdot d} \equiv 1$ または $a^{2^{s-1}\cdot d} \equiv -1 \pmod{n}$

仮定より，$a^{2^{s-1}\cdot d} \not\equiv -1 \pmod{n}$ であるから，$a^{2^{s-1}\cdot d} \equiv 1 \pmod{n}$

$s-1>0$ のとき，同様にして $a^{2^{s-2}\cdot d} \equiv 1$ または $a^{2^{s-2}\cdot d} \equiv -1 \pmod{n}$

仮定より，$a^{2^{s-2}\cdot d} \not\equiv -1 \pmod{n}$ であるから，$a^{2^{s-2}\cdot d} \equiv 1 \pmod{n}$

これを繰り返すと，$a^{d} \equiv 1 \pmod{n}$ となる。これは，$a^{d} \not\equiv 1 \pmod{n}$ と矛盾する。

ゆえに，nは素数でない。

□

フェルマーテストの2を次のように変えたものがミラー・ラビン素数判定法である。

$n-1=2^s \cdot d$　(sは正の整数で，dは奇数)と表す。このとき

$$a^{d} \equiv 1,\ a^{d} \equiv -1,\ a^{2d} \equiv -1,\ \cdots\cdots,\ a^{2^{s-1}\cdot d} \equiv -1 \pmod{n} \quad \cdots\cdots①$$

が成り立つかどうかを左から順に調べ，成り立つものが1つでもあったときは「素数でないと判定されなかった」として，3に移り，1つもなかったときは「素数でない」と出力して終了する。

計算法としては，まず，a^{d} をnで割った余りを求める。このとき

$\left(a^{d}\right)^{2}=a^{2d}$，$\left(a^{2d}\right)^{2}=a^{2^{2}\cdot d}$，……，$\left(a^{2^{s-2}\cdot d}\right)^{2}=a^{2^{s-1}\cdot d}$

が成り立つから，2 乗して n で割った余りを求めることを繰り返して，①が成り立つか調べればよい。

a を無作為に選んだとき，n が奇数の合成数であるにもかかわらず，「素数でないと判定されなかった」を返す確率は，$\frac{1}{4}$ 以下であることが知られている。

註　「素数でないと判定されなかった」とき，①の少なくとも 1 つが成り立つが，n が素数でなくても

$x\equiv 1$　または　$x\equiv -1$　$\Rightarrow$　$x^{2}\equiv 1 \pmod{n}$

は成り立つから，　$a^{n-1}\equiv 1 \pmod{n}$　が成り立つ。