Miller-Rabin 強擬素数の約数計算について

宮本泉*
IZUMI MIYAMOTO

1 はじめに

Miller-Rabin 法は、ランダムに選んだ base の自然数をもとにして、与えられた自然数が素数であるかどうかを判定する方法です。この判定法は、確率的判定法のひとつで、素数ではない、もしくは、素数かもしれないのいずれかを判定します。自然数が素数でないと、この方法は、適当な base をとれば素数ではないと判定します。そこで、与えられた自然数に対して、どれくらい小さい数が適当な base となるかが調べられています。本報告は、その様な実験結果の一つです。

2 素数判定

自然数に関する素数問題として、次のことがらがある。

- 自然数が素数であるかどうか判定する。
- 自然数を素因数分解する。

本報告は素数判定に関してであり、その判定法は 2 種類ある。

- 確定的素数判定法
- 確率的素数判定法

素数が高い確率で求める。求めた数が素数でないと擬似素数という。

上にあげたことからの実行に要する計算時間は、おおむね次の通りです。

- 確定的素数判定法→長時間かかる。
- 確率的素数判定法→短時間できる。
- 素因数分解→困難。RSA暗号に利用されている。

参考に、確定的素数判定法を以下に簡単に紹介する。n 素数かどうかを判定する奇数の自然数とする。

*miyamoto1@gmail.com
3 確率的数判定法

Z : 整数環, Z/nZ : 整数を n で整除した余りの数 (mod n の数) の作る環とする。

n が奇素数で、a が n - 1 以下の自然数のとき、下のことがらが成立する。したがって、特に、成立しないときは素数ではないと判定できる。

- Fermat 法
  
a^{n-1} = 1 \text{mod } n (Fermat の小定理)  
  \rightarrow (\mathbb{Z}/n\mathbb{Z}\backslash\{0\}) \text{が乘法に関して群であることを利用。}

- Solovay-Strassen 法
  
a^{(n-1)/2} = (a/n) \text{mod } n (Euler 基準, Euler テスト)
  ここでは、(a/n) は Jacobi 記号,
  1 : 平方剩余, -1 : 非平方剩余, 0 : その他。

- Miller-Rabin 法
  次節で。\rightarrow (\mathbb{Z}/n\mathbb{Z}\backslash\{0\}) \text{が乘法に関して巡回群であることを利用。}

- Lucas テスト
  説明略。Miller-Rabin 法と組合わせると効果的。

4 Miller-Rabin 法

n が奇素数で、a が n - 1 以下の自然数のとき次の成立する。

n - 1 = 2^t \times t, t は奇数とすると,

\[ a^t = 1 \text{mod } n \]

または、これが成立しないときは、\[ b^a \] から始めて,

\[ b \rightarrow b^2 \text{をある } k(1 \leq k \leq s - 1) \text{回繰返して、} b^2 = -1 \text{が成立。} \]
この方法の起源は、M. Artjuhov(1966), Certain criteria for the primality of numbers connected with the little Fermat theorem, Acta Arith. 12 (1966/67), 355-364, (in Russian) らしい。

70年代中に、J.L.Selfridge がこの方法を使っている。
Miller-Rabin 法による質数を、(a を base とする) 強質数 (J.L.Selfridge?) という。

$n$ が合成数で、上が成立する確率は 1/4 以下 (Monier 1980, Rabin 1980) が知られている。
ランダムに $a$ を選んでテストを繰返せば、高い確率で素数判定が可能となる。

強質数かつ Lucas テストによる質数は見つかってないらしい。
→BPSW 法。（現在通常使用されていると思われる確率的素数判定法。）
BPSW 法 — 反例は見つかっていないと書いてある。（T. R. Nicely の Web ページ 2012.）

Miller-Rabin 法 (続き)

一般リーマン予想 (GRH)/拡張リーマン予想 (ERH)
これを仮定すると、$a \leq 2(\log n)^2$ のすべての $a$ を base として判定すれば、確定的判定になる。（E. Bach (1990). G. Miller (1976) では、$a \leq O(\log n)^2$）
（これを実行するより AKS 確定的判定法の方が理論的に速いらしい。）
（実験的には、$a \leq \log n$ で十分そうですという話もあるようです。）

2-強質数、2,3-強質数、2,3,5-強質数、・・・
と、小さい素数たちを base としたときに、最小の質数数は何になるかを考える。このようにして求めた最小の質数数より小さい数は、Miller-Rabin 法で素数であると判定できる。

5 小さい素数を base とする強質素数

$\psi_k$ を the smallest strong pseudoprime to all of the first $k$ primes とする。Jaeschke (1993) computed $\psi_k$ from $k = 5$ to 8 and gave upper bounds for $k = 9$ to 11.（確認?: Jiang and Deng 2012, 105 時間 by
\( \psi_9, \psi_{10}, \psi_{11} \leq 3825123056546413051 \) \((p \leq 31)\)

\( \psi_9, \psi_{10}, \psi_{11} \) as above

\( \psi_{12} = 318665857834031151167461 \) \((p \leq 37)\)
\( \psi_{13} = 3317044064679887385961981 \) \((p \leq 41)\)
\( \psi_{14} = 6003094289670105800312596501 \) \((p \leq 43)\)
\( \psi_{15} = 59276361075595573263446330101 \) \((p \leq 47)\)
\( \psi_{16}, \psi_{17} = 564132928021909221014087501701 \) \((p \leq 59)\)
\( \psi_{18}, \psi_{19} = 154326786444342061687767640751301 \) \((34 \text{桁}, p \leq 67)\)
\( \psi_{20} > 10^{36} \) \((p \leq 71)\)

(http://mathworld.wolfram.com/StrongPseudoprime.html などより。)

### 6 強擬素数の性質

On the difficulty of finding reliable witnesses (W. R. Alford, A. Granville, C. Pomerance(1994)) より。

- 合成数 \( n \) で、それ判定できる base が \( (\log n)^{1/(3 \log \log \log n)} \) 以上となるものが無限個存在する。

(上記の計算は、どこまで行ってもきりがない。それが分かっていても ...) 

- \( n \) は base とする強擬素数 \( \rightarrow \)

すべての \( n \) の素因数 \( p \) に対して、\( a \) の \( \mathbb{Z}/p\mathbb{Z} \) の乘法群における order の 2-part は同じ (Prop.1.1)。

本研究の目的

小さな素数を base として、擬素数の性質を利用してその約数を求める。

擬素数となって素数判定できない数の判定ができるようになる。

### 7 (小さな素数を使った) 強擬素数の約数計算

7.1 Fermat 擬素数で強擬素数ではないとき

Miller-Rabin 法の計算手順において、
\[ \exists b \text{ such that } b \neq -1, b^2 \equiv 1 \pmod{n}, (Z/nZ \text{ は体ではない}), \text{ Gcd}(b \pm 1, n) > 1. \]

Fermat 擬素数で強擬素数ではない例：Miller-Rabin 法により、
\[ n = 561, a = 2, n - 1 = 560 = 2^4 \cdot 35 \]
\[ b = ((2^{35})^2) = 2^{4 \cdot 35} = 2^{8 \cdot 35} = 1 \pmod{571} \]
\[ \Rightarrow 571 \]
\[ b = 2, b^2 = 2^2 = 1 \pmod{571} \]
\[ (b - 1) \text{ 或 } (b + 1) = 0 \pmod{571} \]
\[ \text{Gcd}(b \pm 1, n) = 17, \text{Gcd}(67 - 1, 561) = 33, (17 \times 33 = 561) \text{ と, } n \text{ の約数が得られる。} \]

7.2 強擬素数の約数の計算方法

base a として、小さい素数（通常は a = 2, 3, 5, 7）を利用することを考える。
とりあげず、n - 1 を割る素数の中で、3, 5, 7 を利用することにする。

強擬素数の約数計算の例 1:
\[ n = 4681, a = 2; n - 1 = 2^3 \cdot t \text{ で } a^t = 1 \pmod{n}, 3 \text{ は } (n - 1) \text{ を利用する。} \]
\[ n - 1 = 4680 = 2^3 \cdot 585 = (2^3 \cdot 9 \cdot 65), a^t = 2^{585} = 1 \pmod{4681} \]
実は、
\[ b = 2^{585/9} = 2^{(n - 1)/(9 \cdot 8)} = 32 \mod{4681} b^3 = 2^{585/3} = 1 \pmod{4681} \]
\[ (b - 1)(b^2 + b + 1) = 0 \pmod{4681} \]
そこで、Gcd(b - 1, n) = Gcd(32 - 1, 4681) = 31 (4681 = 31 \times 151)

強擬素数の約数計算の例 2:
\[ n = 29341, a = 2; n - 1 = 2^2 \cdot t \text{ で } a^t = 2 \pmod{n}, 3 \text{ は } (n - 1) \text{ を利用する。} \]
\[ 29340 = 2^2 \cdot 7335 = (2^2 \cdot 3^2 \cdot 5 \cdot 163), 2^8 = 1 \pmod{29341} \]
\[ b = 2^8 = 1 \pmod{29341} \]
\[ (b - 1)(b^2 + b + 1) = 0 \pmod{n} \]
\[ \text{Gcd}(b + 1, n) = \text{Gcd}(7929 + 1, 29341) = 793 = 13 \cdot 61 \]
\[ \text{Gcd}(c + 1, n) = \text{Gcd}(7929 + 1, 29341) = 793 = 13 \cdot 61 \]
\[ n = 13 \times 37 \times 61 \]

7.3 the smallest strong pseudoprime などの数 \( \psi_i \) の約数計算

\[ n = \psi_1 \text{ として、} b = a^{(n - 1)/m} \pmod{n} \text{ なる } a^{(n - 1)/m} \text{ を以下に示す。} \]
\[ \psi_1 = 2047 \text{ 失敗。後ほど。。} \]
\[ \psi_2 = 2^{(n - 1)/(9 \cdot 2)} \quad \text{(p \leq 3)} \]
\[ \psi_3 = 2^{(n - 1)/(9 \cdot 16)} \quad \text{(p \leq 5)} \]
\[ \psi_4 = 2^{(n - 1)/(3 \cdot 2)}, 2^{(n - 1)/(5 \cdot 2)} \quad \text{(p \leq 7)} \]
\[ \psi_5 = 2^{(n - 1)/(7 \cdot 2)} \quad \text{(p \leq 11)} \]
\[ \psi_6 = 2^{(n - 1)/(27 \cdot 2)}, 2^{(n - 1)/(27 \cdot 2)}, 2^{(n - 1)/(27 \cdot 2)}, 2^{(n - 1)/(27 \cdot 2)}, 7 \ldots \quad \text{(p \leq 13)} \]
\[ \psi_7 = \psi_8 \quad 5^{(n - 1)/(3 \cdot 32)} \quad \text{(p \leq 19)} \]
\[ \psi_9 = \psi_{10} = \psi_{11} = 2^{(n-1)/(3\cdot 2)}, 5^{(n-1)/(3\cdot 2)}, 7^{(n-1)/(3\cdot 2)}, \ldots \quad (p \leq 31) \]
\[ \psi_{12} = 5^{(n-1)/(27\cdot 4)} \quad (p \leq 37) \]
\[ \psi_{13} = 5^{(n-1)/(9\cdot 4)} \quad (p \leq 41) \]
\[ \psi_{14} = 3^{(n-1)/(27\cdot 4)} \quad (p \leq 43) \]
\[ \psi_{15} = 2^{(n-1)/(27\cdot 2)}, 2^{(n-1)/(5\cdot 2)} \quad (p \leq 47) \]
\[ \psi_{16} = \psi_{17} = 5^{(n-1)/(9\cdot 4)}, 7^{(n-1)/(9\cdot 2)} \quad (p \leq 59) \]
\[ \psi_{18} = \psi_{19} = 2^{(n-1)/(7\cdot 2)}, 7^{(n-1)/(9\cdot 4)} \quad (p \leq 67) \]

7.4 強擬素数の約数計算の例

強擬素数の例1：1000以下の168個のすべての素数をbaseとする強擬素数

強擬素数の例2：541までの100個のすべての素数をbaseとする強擬素数
【定義】Carmichael 数 \( \iff \) すべての \( \gcd(a, n) = 1 \) となる数 \( a \) に対して、\( n \) は \( a \)-Fermat 素数となる。

前述の 2 つの例は Carmichael 数なので、\( a \)-強擬素数とはならない \( a \) を選んでも約数計算は可能であるが、

618 枚の例 \( b = 2^{(n-1)/(2 \cdot 3)}, 3^{(n-1)/(2 \cdot 3)}, 5^{(n-1)/(2 \cdot 3)}, \ldots \mod n \)
\[ \rightarrow \gcd(b + 1, n) > 1 \]
1189 枚の例 \( b = 2^{(n-1)/(2 \cdot 3)}, 2^{(n-1)/(2 \cdot 7)}, 7^{(n-1)/(2 \cdot 3)} \mod n \)
\[ \rightarrow \gcd(b + 1, n) > 1 \]

計算時間は、以上の例すべてで 1.5 秒程度。(GAP を使用)

強擬素数の例 3 (F. ARNAULT 1995): 337 枚（素因数 2 個、200 以下の 46 個の素数に対して強擬素数。)

\[ 803837457436941257079614341942108138837688287558145837488971522974273765336521865023361 \]
\[ 6396004545791504202360320976666966709872464965408232928738791850869166857328267761771029 \]
\[ 3896977394701670823042868710999743997654414484534115587245063409279022275296229414984230688 \]
\[ 16854043264575340183297861129896064845216191652872597534901 \]

\[ \bullet b = 2^{(n-1)/(2 \cdot 81)}, 2^{(n-1)/(2 \cdot 5)}, 5^{(n-1)/(4 \cdot 81)} \mod n \]
\[ \rightarrow \gcd(b + 1, n) > 1 \]

\[ \bullet b = 5^{(n-1)/(4 \cdot 81)} \mod n \]
\[ \rightarrow \gcd(b - 1, n) > 1 \]

これらの例を含め、ネットで見つけた強擬素数など約 100 個に対して約数計算を行って、これらについては、\( \psi_1 \) を除き成功している。

8 計算方法

計算方法: 素朴な Miller-Rabin 法。

GAP システムを使用: PowerMod(a, (n - 1)/m, n) : mod 計算の高速敵乗演算。

強擬素数の约数計算では、一つの base \( a \) に対して、\( n - 1 \) を割る 3 乗、5 乗、7 乗に対して \( a \) の \( (n - 1)/m \) の形の mod 計算の敵乗計算。

(337 枚の例: \( 2^{(n-1)/(2 \cdot 81)}, 2^{(n-1)/(2 \cdot 5)}, 5^{(n-1)/(4 \cdot 81)} \mod n, 他に、失敗している場合もあった。

\[ \rightarrow \text{結局、Miller-Rabin 法と同様の計算を複数回繰返していることになる。} \]

したがって、計算時間も同様になっているであろう。

それなら、base \( a \) を取りかえて、Miller-Rabin ともっと多くの回数繰返し行ってもよいではないか …。本報告では、base として小さい数を使うという考え方をしている。

【参考】GAP にある関連する関数

\[ \bullet \text{IsProbablyPrimeInt: BPSW 法を使った確率的素数判定。} \]

\[ \bullet \text{IsPrimeInt: 椎円曲線素数判定法を使用しているらしい。} \]

9 計算データ 2-SPRP-2-to-64

2^{64} までの 2-強擬素数のデータ 31894014 個,

\[ \psi_{11} < 2^{64} < \psi_{12} \]
9.1 計算データ 2-SPRP-2-to-64に関する実験

2,3,5,7-強擬素数：このデータ内で、2,3,5,7-強擬素数は、16826 個。
(Miller-Rabin 法のプログラムによる計算時間、1371 秒。)

その中で、本研究の方法で、n−1 の約数のうち 3, 5, 7 を使って、
約数を求めることができたもの 16207 個。
約数を求めることができなかったもの 619 個。この約数計算にかかった時間 4 秒。
(最初から約数計算までまとめたプログラムによる計算時間 1721 秒、
1371 + 4 << 1721 ?? 強擬素数 1 個の平均計算時間約 0.05ms なので、事前処理の時間？)
この 619 個 (最小 22749134240827 >> ψ4 = 3215031751) のなかで 2,3,5,7,11-強擬素数は、73 個。
その中で、同様にして約数を求めることができなかったもの 39 個。
この 39 個のうち、最後に残ったのは、2,3,5,7,11,13-強擬素数 5 個 (17-強擬素数にはならない)。
2,3,5,7,11,13-強擬素数で約数計算ができなかったものは 3 個で、次通り。
11718796901305940161, 15292237577737533661, 16697267137953148781.
計算データ 2-SPRP-2-to-64 の計算時間について、Miller-Rabin 法の計算は、1 個の数に対して、その数
が 1000 枠でも 1 秒とかからないので、計算速度は考慮しなかった。

- 本研究プログラムによる総計算時間 1400~1800 秒程度。
- GAP の IsPrimeInt による計算時間 1788 秒。

【参考】Lucas テストの計算時間～Miller-Rabin 法 4, 5 回分程度らしい。
10 約数計算が失敗する強擬素数

計算データ 2-SPRP-2-to-64 に対して、最初、2,3,5,7 を base とする強擬素数を考えたが、base として、11,13、そして、17 も必要になった。

最後に残った、2,3,5,7,11,13-強擬素数 5 個 (17-強擬素数ではない)、そして、そのうちで約数計算ができなかったもの 3 個。

2,3,5,7,11,13-強擬素数 $n=16697267137953148781$ に対して、今まで、約数計算には $n-1$ の約数として 3,5,7 を考えていたが、13 も使ってみると、最初の 2 個の約数は得られなかった。

残った最後の 1 個は、

$$n = 16697267137953148781 = 1668195989 \times 10009175929$$
$$n - 1 = 16697267137953148781 - 1 = 2^2 \cdot 5 \cdot 11 \cdot 17 \cdot 53 \cdot 7868849 \cdot 10705001$$
$$1668195989 - 1 = 2^2 \cdot 53 \cdot 7868849$$
$$10009175929 - 1 = 2^3 \cdot 3 \cdot 7868849$$
$$\Rightarrow 2^{53} \cdot 7868849 = -1 \text{ mod } n, 3,7 \text{ も同様}, 5^{53} \cdot 7868849 = -1 \text{ mod } n.$$ (【参考】 $\psi_1 = 2047 = 23 \cdot 89, \psi_1 - 1 = 2 \cdot 3 \cdot 11 \cdot 31,$
$$23 - 1 = 2 \cdot 11, 89 - 1 = 2^2 \cdot 11 \Rightarrow 2^{11} = 2048 = 1 \text{ mod } \psi_1.)$$

本研究の方法で約数計算が失敗する強擬素数について、実験データとしては少ないが、多分、前に引申した強擬素数の性質と同様に、

- 合成数 $n$ が大になるにしたがって、それを判定できる base、および、使用する $n-1$ の約数、特に大になるような $n$ が存在するようだ。

- $n$ は $a$ を base とする強擬素数で、$r|(n-1)$ なる素数 $r$ をとると、

$\Rightarrow$ すべての $n$ の素因数 $p$ に対して、$r|(p-1)$ ならば、$a$ の $\mathbb{Z}/p\mathbb{Z}$ の乗法群における order の $r$-part は同じ？

などのことがらが考えられれたが、本報告直前に、次の実験結果が得られた。

11 合成数が base のとき

最後に残った、2,3,5,7,11,13-強擬素数 $n = 16697267137953148781$ のときは、6-強擬素数にはならない（素数判定としては、これで終了）。

$\Rightarrow$ $n$ のすべて素因数 $p$ に対して、2 と 3 は、$\mathbb{Z}/p\mathbb{Z}$ の乗法群における order の 2-part は同じであるが、6 はそうになっていない。

合成数が base のときの実験データ：$n = 16697267137953148781$

- PowerMod$(2, (n - 1)/2, n) = n - 1$
- PowerMod$(3, (n - 1)/2, n) = n - 1$
- PowerMod$(2, (n - 1)/4, n) = 4911275413865036381$
- PowerMod$(3, (n - 1)/4, n) = 6364565162097257266$
  $\neq n - 4911275413865036381$
- PowerMod$(6, (n - 1)/4, n) = 667890685918499885 \neq n - 1$
- PowerMod$(6, (n - 1)/2, n) = 1 \leftarrow \text{(Fermat 側素数)}$
他にも同様な例があるようで、実験続中です。

12 考察

実験ばかりしていて、考察として報告することはありませんが、終わりに、次の疑問点をあげます。

- $n - 1$ の約数の利用はいつできるのか。
  例えば、素数 $p, q | n$ で、$3 | (n - 1), 3 | (p - 1), 3 | (q - 1)$ のときはどうか？
  $n = 2p + 1, p$ は素数のかたちの強疑素数では、$n - 1$ の約数を考えるのは困難と思うが、このような例は見つからなかった。

- 合成数を base とするとき、つまり、$n$ は $a_1, a_2$-強疑素数であるが $a_1 \times a_2$-強疑素数ではないときに満たす条件は？

- $n - 1$ の約数を利用する方法と、Lucas テストやリーマン予想とは、何かの関連があるだろうか？