M_032

ミラー・レービン素数判定アルゴリズムの高速化

Testing Primality Loosely: Make Miller-Rabin Test Faster

武田 雄人† 清水 將吾†† 大場 充‡
Yuto Takeda Shougo Shimizu Mitsuru Ohba

1. 序論

インターネットに代表される開放的なコンピュータネットワーク上の通信では,情報の盗聴や改ざんのリスクがある. それらのリスクを回避する技術の1つが,情報の暗号化である. 現在広く利用されている暗号として*RSA*暗号がある. *RSA*暗号では大きな2つの素数を用いて鍵を生成するため,与えられた整数が素数であるかの判定を高速に行えることが望ましい. しかし,素数であるかを確定的に判定するには$O(n^{1/2})$時間程度かかる[1]ため,大きな数に対しては多大な時間がかかるという問題がある. これに対し,確率的な素数判定として,ミラー・レービン素数判定法[2]や,フェルマーテストを改良した方法[3]が用いられている. フェルマーテストでは合成数であると判定できないカーマイケル数と呼ばれる数が存在するため,ミラー・レービン素数判定法が現在の主流となっている. このミラー・レービン素数判定法は$O((\log n)^3)$時間で素数判定を行える.

しかし,近年の計算機速度の向上により,鍵の解読に要する時間が短くなったため,暗号に用いる鍵のビット長が長くなり,それだけ素数判定に要する時間も長くなっている. このため,計算時間に関する応用上の改善がなければ,素数判定に依然多大な時間が必要となり,暗号鍵の生成に時間がかかる.

本稿では,この問題を解決するために,ユークリッドの互除法とミラー・レービン素数判定法を組み合わせた方法[4]にフェルマーテストを組み合わせた素数判定法を提案する. 更に,ミラー・レービン素数判定法と提案手法の素数判定時間を比較し,評価した結果について報告する.

2. 素数判定法

2.1 フェルマーテスト

フェルマーテストの基本となっているフェルマーの小定理とは,P を素数とし,a を P と互いに素な整数としたとき,素数の必要条件に関する次式,

$$a^{P-1} \equiv 1 \ (mod\ P) \qquad (1)$$

が成立するという定理である.

フェルマーテストでは式(1)が成立するとき,P は素数であると判定し,成立しない場合,P は合成数であると判定する. しかし,フェルマーの小定理を成立させる合成数も存在する. このような合成数を擬素数という. 擬素数の中で特に,全ての a に対してフェルマーの小定理を成立させる擬素数をカーマイケル数[5]といい,素数であるかどうかを正しく判定できないためフェルマーテストの欠点となっている.

本稿ではフェルマーの小定理から以下の式(2)を導出し,これをフェルマーテストと呼ぶ.

$$a^{(P-1)/2} \equiv \pm 1 \ (mod\ P) \qquad (2)$$

式(2)の場合,式(1)による素数判定よりも,計算量が少ないと言う利点がある.

† 広島市立大学大学院 情報科学研究科博士前期課程
†† 広島市立大学 情報科学部
‡ 広島市立大学大学院 情報科学研究科

2.2 ミラー・レービン素数判定法

ミラー・レービン素数判定法は,nを素数判定したい奇数とし,$n-1=2^k q$ と表せるように奇数qを取り,$gcd(n,a)=1$ を満たすaを $1< a < n$の範囲で任意に取るとき,式(3)(4)が満足されるならばnは合成数であると判定する方法である. この式(3)(4)における¬は否定を表す.

$$a^q \neg\equiv 1 \ (mod\ n) \qquad (3)$$

$$a^{2^i q} \neg\equiv 1 \ (mod\ n) \quad (i = 0,1, \ldots, k-1) \qquad (4)$$

このミラー・レービン素数判定法は,フェルマーテストの欠点であるカーマイケル数も正しく判定できるという長所がある. しかし,選択した整数 a の値によっては素数を合成数であると判定してしまう. この誤判定をする整数の割合は,a が取りうる整数全体の 1/4 以下であることが証明されている[2]. このため,ミラー・レービン素数判定法は,複数の底で判定を行うことが必要になるが,前段階として確定的な合成数判定を効果的に行うことができれば,より効率的に素数判定を行えると考えられる.

2.3 ハイブリッド方式

本稿で提案するミラー・レービン素数判定法とフェルマーテストのハイブリッド方式による素数判定のフローチャートを図1に示す. ここで n は素数判定したい奇数である.

本稿では,n を判定したい奇数としたとき,最初にユークリッドの互除法を用いて n が 3 か 5 を因数として持つかどうかの判定を行う. ここで 3 と 5 を選んだ根拠は,奇数全体で 3 または 5 を素因数に持つ数は全体の 7/15 であり,約半分の奇数をこの段階で判定することが可能だからである. 次に,3 と 5 を因数を持たないときに $a = 2$ のフェルマーテストを実行し,擬素数かどうかの判定を行う. このフェルマーテストにより合成数だと判定された数は必ず合成数であるのでそこで判定を終えることが出来る. 次に素数と判定された擬素数に対してのみミラー・レービン素数判定法を行い,最終的な判定を行う.

ハイブリッド方式はユークリッドの互除法またはフェルマーテストが合成数と判定すればその数は必ず合成数であるという性質を用いて,これらの判定を最初に行うことで判定したい奇数を短い時間で確定的な合成数判定を行うことが出来る. これにより,多くの奇数に対して計算コストのかかるミラー・レービン素数判定法を行わなくて済むため計算時間と判定精度を高めることが出来る.

3. 素数判定実験

3.1 実験方法

実験はハイブリッド方式と,ミラー・レービン素数判定法の判定時間と誤判定回数を比較して行う.

実験手順は以下の通りである.

(1) 判定する奇数を乱数を用いて 500000 個発生させる. この時,値の重複はあってもよい.
(2) 発生させた全ての奇数が,合成数か素数かを予め判定しておく.

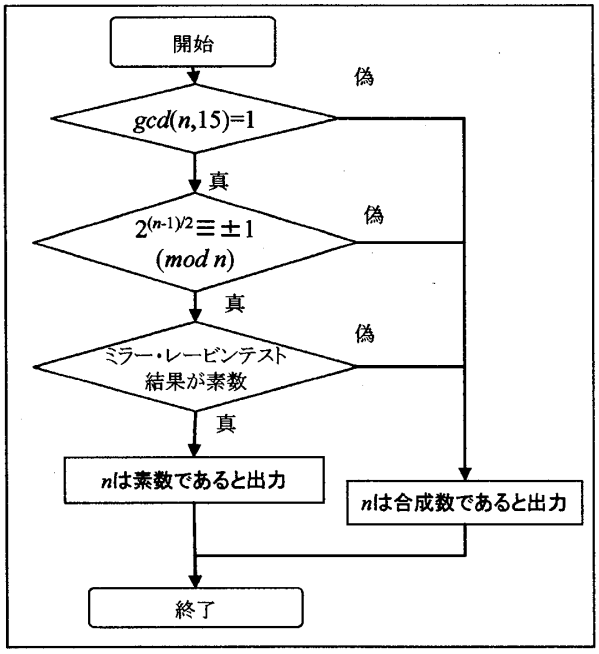

図 1. ハイブリッド方式のフローチャート

(3) 奇数が 3 か 5 の素因数を持つか調べるため 15 を用いてユークリッドの互除法を使う
(4) ハイブリッド方式による素数判定法を行い,その時間を測定し判定結果を求める.
(5) ミラー・レービン素数判定法を底の値を変えて複数回行い,その時間を測定し,判定結果を求める. この時の底は乱数で発生させる.
(6) 2 方式の素数判定結果と,(5)で求めておいた判定結果との相違を確認することで,2 方式の素数判定の判定精度を確認する.

素数判定は 24,26,28,30,32 ビットごとに 5 回ずつ行い,各ビットごとに素数判定にかかる時間の平均を求める.

本稿では,ミラー・レービン素数判定法の判定回数は 10 から 19 回とし,この回数の間に合成数又は素数の判定が先に 10 回出た方の判定結果を最終的な判定結果とする. この判定結果の確率は誤判定をする確率を 1/4 とすることで式(5)のように求めることができる.

$$ {}_nC_9(3/4)^9(1/4)^{n-9}(3/4) \qquad (5) $$

式(5)は誤判定を下す確率で,この式から 0. 008702 の確率で誤判定を下すと計算することができる. 従って,この判定回数で十分な精度が得られると考えられる.

3.2 実験結果と考察

図 2 は 3. 1 節で述べた実験を行い,その判定時間をグラフにしたものである. 実験に使用した計算機の CPU は Xeon(TM) 2. 80GHz デュアル,メモリは 2. 00GB である. 実装は Java 言語により行い,Java 実行環境には Java2 Standard Edition Version 1. 4. 2 を用いた.

このグラフよりハイブリッド方式の方がミラー・レービンテストよりも 5〜7 倍程度高速に素数判定を行う事が出来ることがわかる.

表 1 は,今回の素数判定実験において,各ビット長の乱数の合計 2500000 個の数で,ハイブリッド方式とミラー・レービン素数判定法が誤判定を起こした確率である. 表 1 より, 判定精度はどちらも大きな差はないことがわかる.この実験

表 1. 誤判定の確率

ビット長	ハイブリッド方式	ミラー・レービン素数判定法
24	0	0
26	0	0
28	0	0
30	$4*10^{-7}$	$4*10^{-7}$
32	0	0

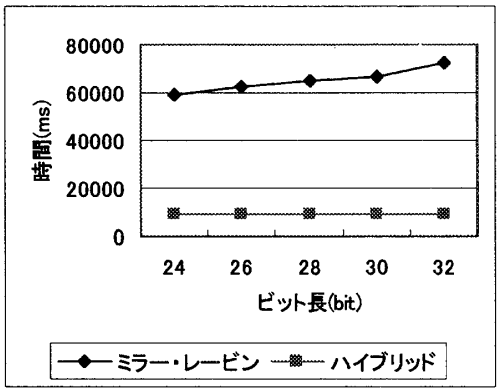

図 2. 素数判定に要した時間

結果からハイブリッド方式は素数判定時間を短くできることが言える.

4. まとめと今後の課題

本稿では,高速な素数判定法として,ユークリッドの互除法とフェルマーテストとミラー・レービン素数判定法を組み合わせたハイブリッド方式を提案した. 素数判定実験を通して,このハイブリッド方式はミラー・レービン素数判定法だけの素数判定よりも効率がよいことを確認した.

今後の課題として,図 2 から,ハイブリッド方式の方が高速に素数判定できると言う事を実用的な面で確認するため, 現在暗号で用いられている 512 ビット程度での素数判定実験を行い,ハイブリッド方式の素数判定時間,判定精度を確認することが挙げられる. また,ミラー・レービン素数判定法の改良や,APR テスト[6]などの 1980 年以降提案されている素数判定法との比較実験が挙げられる.

5. 参考文献

[1] *Thomas, I. , trans.* : *Greek Mathematical Works:Thales to Euclid. Loeb Classical Library 335. Harvard University Press, Cambridge ,Massachusetts,and London,England.*

[2] *Rabin, M. O.* : *Probabilistic algorithm for testingprimality. J. NumberTheory* 12, 128-138(1980).

[3] 武田雄人：広島市立大学 平成 17 年度卒業論文カーマイケル数表を用いた有限長自然数の素数判定法の評価(2006).

[4]岡本英司：暗号理論入門[第 2 版],pp17,共立出版株式会社(2002).

[5] *Carmichael,R. D.* : *On composite numbers P which satisfy the Fermat congruence* $a^{P-1} \equiv 1$ *(mod P). The Amer. Math. Monthly* 19, 22-27(1912).

[6] *L. M. Adleman, C. Pomerance, R. S. Rumely* : *On distinguishing prime numbers from composite numbers. Ann. Math*, 117:173-206(1983).