擬素数を用いた素数判定法について

松村　歩紀　　指導教員：田坂　浩二

1　序文

RSA 公開鍵暗号系や有限体上の離散対数問題に基づいた様々な暗号系では，ランダムな大きい素数を見つける必要がある．そこで用いられるのが，ある数が素数かどうかを確率的に判定する，確率的素数判定法である．

擬素数とは，確率的素数判定法に合格してしまう合成数のことである．素数判定法には確率的素数判定法と決定的素数判定法があり，確率的素数判定法では，素数である可能性が高いか，素数ではないかを判定する．つまり，確率的素数判定法において，擬素数の数を限りなく減らすことが精度の向上につながる．

本研究では，William-Shanks の Perrin 数列の性質を用いた Strong Primality Tests および，古典的な整数の合同についての定理 (オイラーの定理) に基づく擬素数を用いた確率的素数判定法の精度を検証する．

2　素数判定法

2.1　Strong Primality Tests

Perrin 数列を初期値 $A(1) = 0, A(2) = 2, A(3) = 3, n > 0$ に対し，

$$A(n+3) = A(n) + A(n+1) \tag{1}$$

と定める．また $n \leq 0$ に対し，

$$A(n) = A(n+3) - A(n+1) \tag{2}$$

と定義する．Perrin 数列は，素数 p に対して，

$$A(p) \equiv 0 \pmod{p} \tag{3}$$

$$A(-p) \equiv -1 \pmod{n} \tag{4}$$

を満たす．

n が奇合成数で，(3) を満たすとき，n を Perrin 擬素数という．Perrin 擬素数は無限個あり (J.Grantham,2010)，最初の Perrin 擬素数は $271441 = 521^2$，次の Perrin 擬素数は 904631 である．しかしこれらの数は，(4) を満たさない．そして (3)，(4) を同時に満たす合成数では稀であるといえる．その合成数を強 Perrin 擬素数とする．そこで，

$$A(-n-1), A(-n), A(-n+1), A(n-1), A(n), A(n+1) \tag{5}$$

の 6 つの値を求め，Adams-Shanks[1] は，強 Perrin 擬素数を用いた素数判定法を考察した．それによれば，素数は (5) の値によって，S タイプ，I タイプ，Q タイプに分けられることがわかっている．

素数全体の $\frac{5}{6}$ が I タイプ，Q タイプに属し，10^{14} 以下には I タイプも Q タイプも擬素数がない (アルノー,1991)．また Kurtz-Shanks-Williams$50 * 10^9$ 以下の 55 個のタイプ S 擬素数の Table を作成した．

2.2　種々の擬素数

$(\frac{b}{n})$ をヤコビ記号としたとき，n が奇素数ならば，n では割り切れない任意の整数 b に対して，

$$b^{(n-1)/2} \equiv (\frac{b}{n}) \bmod n \tag{6}$$

が成立する．n が奇合成数で，b が $gcd(n, b) = 1$ かつ，(6) を満足するとき，n を整数 b を底とするオイラー擬素数という．

オイラー擬素数の他に強擬素数，フェルマー擬素数などの擬素数が存在する．そして強擬素数ならばオイラー擬素数であり，オイラー擬素数ならばフェルマー擬素数である [2].

3　主結果 (観察)

Kurtz-Shanks-Williams の Table にある強 Perrin 擬素数のリストが強擬素数であるかを確かめた．10^9 以下の結果は以下である．

表 1　10^9 以下の強 Perrin 擬素数と強擬素数との関係

素数判定法	強擬素数
27664033	×
46672291	×
102690901	×
130944133	×
517697641	×
545670533	×
801123451	×
855073301	×
970355431	×

ここから，Strong Primality Tests+ 強擬素数は，よりよい素数判定法であることが観察できる．

4　今後の課題

Strong Primality Tests と強擬素数を組み合わせることで，どの程度良くなるのかを検証していきたい．

参考文献

[1] William Adams and Daniel Shanks,Strong Primality Tests That Are Not Sufficient,MATHEMATICS OF COMPUTATION,39(1982),255-300

[2] 櫻井幸一 数論アルゴリズムと楕円暗号理論入門 丸善出版株式会社，2012

[3] Richard Guy 未解決問題集 朝倉書店，2010