Baillie-PSW 素数判定法

Koki Hamada

2024 年 4 月 3 日

概要

このレポートは [2] の記述を基に Baillie-PSW 素数判定法について解説したものである．Baillie-PSW 素数判定法とは，底 2 のミラー・ラビン素数判定法とリュカの強素数判定法を組み合わせた手法である．このアルゴリズムは高速であり，擬素数の割合が相当少ないことが予想されている．そのため，最近のソフトウェアにおける素数判定法の実装でよく用いられている．

1 準備

1.1 記法

Definition 1.1. 整数 a, b の最大公約数を $\gcd(a, b)$ と書く．

1.2 平方剰余とルジャンドル記号，ヤコビ記号

Definition 1.2 (平方剰余)**.** n を正の整数[*1]とする．法 n の下で，正の整数 a が**平方剰余（quadratic residue）**であるとは，合同方程式 $x^2 \equiv a \pmod{n}$ の解が存在することである．存在しない場合，平方非剰余（quadratic nonresidue）であるという．

たとえば，法 5 の下では

$$1^2 \equiv 1, \quad 2^2 \equiv 4, \quad 3^2 \equiv 4, \quad 4^2 \equiv 1, \quad \pmod{5}$$

なので，1 と 4 は平方剰余，2 と 3 は平方非剰余である．

特に法が奇素数のとき，平方剰余は様々な性質を持つ．このことを表すために次の記法を導入する．

Definition 1.3 (ルジャンドル記号)**.** p を奇素数とする．正の整数 a について，

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } \gcd(a,p) \neq 1, \\ +1 & \text{if } a \text{ is a quadratic residue}, \\ -1 & \text{if } a \text{ is a quadratic nonresidue}, \end{cases} \tag{1}$$

と定義する．この (a/p) を**ルジャンドル記号（Legendre Symbol）**と呼ぶ．

たとえば，$p = 5$ のとき，

$$\left(\frac{1}{5}\right) = 1, \quad \left(\frac{2}{5}\right) = -1, \quad \left(\frac{3}{5}\right) = -1, \quad \left(\frac{4}{5}\right) = 1, \quad \left(\frac{5}{5}\right) = 0,$$

[*1] たとえば [7,8] では法 n を奇素数として平方剰余を定義しているが，平方剰余は法が素数である必要はない．しかし，ルジャンドル記号は素数である必要があるので，そういった利便性のために素数で定義されることがある．

となる．

ルジャンドル記号は法を奇素数に制限した．それを正の奇数に拡張したものがヤコビ記号である．

Definition 1.4 (ヤコビ記号)**.** n を正の奇数とし，$n = \prod_{i=1}^{k} (p_i)^{e_i}$（$p_i$ は素数）と表示する．正の整数 a について，

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{e_i} = \left(\frac{a}{p_1}\right)^{e_1} \left(\frac{a}{p_2}\right)^{e_2} \cdots \left(\frac{a}{p_k}\right)^{e_k}, \tag{2}$$

と定義する（右辺はルジャンドル記号である）．この (a/n) を**ヤコビ記号（Jacobi Symbol）**と呼ぶ．

n が奇素数の場合はルジャンドル記号と一致する．ヤコビ記号は $O(M(n)\log n)$ で計算できることが知られている [4]．以下，(a/n) はヤコビ記号を表すものとする．

2　従来の素数判定法

2.1　フェルマーテスト

法が素数のとき，**フェルマーの小定理（Fermat's little theorem）**という強力な定理が成り立つ．

Theorem 2.1 (フェルマーの小定理)**.** p を素数とする．$\gcd(a,p) = 1$ を満たす任意の正の整数 a について，$a^{p-1} \equiv 1 \pmod{p}$ が成り立つ．

一般にフェルマーの小定理の逆は成立しない．実際，$2^{561-1} \equiv 4^{561-1} \equiv \cdots \equiv 1 \pmod{561}$ であるが，$561 = 3 \times 11 \times 17$ は合成数である．このように，$\gcd(a,n) = 1$ となる任意の整数 a について，$a^{n-1} \equiv 1 \pmod{n}$ を満たす合成数 n をカーマイケル数（Carmichael's number）と呼び，無数に存在する．実際，10^{21} までのカーマイケル数は 20,138,200 個である [5]．とはいえ，こういったフェルマーの小定理の逆を満たす合成数が稀であることを期待して，次のような確率的素数判定法が提案された．

Definition 2.2 (フェルマーテスト)**.** 正の奇数 n を素数判定の対象とする．$\gcd(a,n) = 1$ を満たす正の整数 a をランダムに選び，$a^{n-1} \not\equiv 1 \pmod{n}$ であれば合成数，そうでなければ底 a の**確率的素数（base-a probable prime）**とする．

上述の通り，フェルマーテストを潜り抜ける合成数 n は無数に存在する．この合成数 n を判定時の整数 a を用いて，底 a の**擬素数（base-a pseudoprime）**という．フェルマーテストは後述の確率的素数判定法と比べると精度が悪いので，実際に用いられることは滅多にない．

2.2　ミラー・ラビン素数判定法

ミラー・ラビン素数判定法（Miller-Rabin primality test）は次の定理に基づいた確率的素数判定法である．

Theorem 2.3. p が素数であれば，$p - 1 = 2^s d$（ただし，d は奇数）と分解でき，$\gcd(a,p) = 1$ である任意の整数 a に対して，次のいずれかのことが成り立つ．

- $a^d \equiv 1 \pmod{p}$ が成立する．
- $a^{2^r d} \equiv -1 \pmod{p}$ となる $0 \le r < s$ が存在する．

ミラー・ラビン素数判定法はこの定理の対偶を利用して，合成数を篩にかける．

Definition 2.4 (ミラー・ラビン素数判定法)**.** 正の奇数 n を素数判定の対象とする．$\gcd(a,n)=1$ を満たす正の整数 a をランダムに選び，$a^d \not\equiv 1 \pmod{n}$ かつ任意の整数 $r \in [0,s)$ について $a^{2^r d} \not\equiv -1 \pmod{n}$ であれば合成数と判定する．もし，成り立たなければ，底 a の**強確率的素数（base-a strong probable prime）**とする．

フェルマーテストと違って「強 (strong)」がついているのは，素数の確率がより高いことを意味する．同様に，素数と誤って判定されてしまう合成数 n を，底 a の**強擬素数（base-a strong pseudoprime）**という．精度と計算効率の良さから，実用上はミラー・ラビン素数判定法が採用されることが多い．ところが，最近ではこのミラー・ラビン素数判定法と後述のリュカの強素数判定法を組み合わせたBaillie-PSW 素数判定法が使われることが増えている．

3 Baillie-PSW 素数判定法

3.1 リュカ数列とリュカの素数判定法

Definition 3.1 (リュカ数列)**.** 整数 D,P,Q を $P>0$, $D=P^2-4Q\neq 0$ を満たすように選ぶ．$U_0=0, U_1=1, V_0=2, V_1=P$ と定義する．パラメータ (P,Q) の**リュカ数列（Lucas Sequences）** $\{U_k\}$, $\{V_k\}$ $(k\geq 2)$ は次の式で再帰的に定義される．

$$U_k = PU_{k-1} - QU_{k-2}, \tag{3}$$
$$V_k = PV_{k-1} - QV_{k-2}. \tag{4}$$

リュカ数列と素数に対して，次の定理が成り立つ．

Theorem 3.2. p を素数とする．パラメータ (P,Q) のリュカ数列 $\{U_k\},\{V_k\}$ に対して，$\gcd(p,Q)=1$ であれば，

$$U_{p-(D/p)} \equiv 0 \pmod{p}, \tag{5}$$
$$V_{p-(D/p)} \equiv 2Q^{(1-(D/p))/2} \pmod{p}, \quad \text{provided } \gcd(p,D)=1, \tag{6}$$
$$U_p \equiv (D/p) \pmod{p}, \tag{7}$$
$$V_p \equiv P \pmod{p}, \tag{8}$$

が成り立つ．もし，$\gcd(p,2PQD)=1$ であれば，これらの合同式のうち 2 つは他の 2 つを包含する．

リュカ数列のパラメータを $(D/p)=-1$ となるように取ると，この定理は次のように書ける．

$$U_{p+1} \equiv 0 \pmod{p}, \tag{9}$$
$$V_{p+1} \equiv 2Q \pmod{p}. \tag{10}$$

これらの式から，フェルマーテストと同様の論法でリュカの素数判定法を定義する．ちなみに，式 (7), (8) は合成数であっても成立するケースが多いので素数判定では使われない．

Definition 3.3 (リュカの素数判定法)**.** 正の奇数 n を素数判定の対象とする．リュカ数列 $\{U_k\},\{V_k\}$ のパラメータを $\gcd(n,Q)=1$ かつ $(D/n)=-1$ となるように選択する．このとき，$U_{n+1}\not\equiv 0 \pmod{n}$ であれば合成数，そうでなければパラメータ (P,Q) に対する**リュカの確率的素数（Lucas probable prime）**とする．

リュカの素数判定法で素数と誤って判定される合成数を**リュカの擬素数（Lucas pseudoprime）**という．また，$\{V_k\}$ の式 (10) についてのリュカの素数判定法で得られる確率的素数をリュカの V 確率的

素数（Lucas-V probable prime）と呼ぶ．これを使うと，計算量を悪化させることなくリュカの素数判定法の判定率を向上できる．しかし，現状はまだ使われていないので，このレポートでは紹介しない．

リュカの素数判定法におけるパラメータ (P, Q) の選び方の一例を紹介する [2, 3]．3 つ目のステップが無くても，生成される擬素数は同じである．

- D を $5, -7, 9, -11, 13, -15, \ldots$ という数列の中で $(D/n) = -1$ を最初に満たす要素として選ぶ．
- $P = 1$, $Q = (1 - D)/4$ とする．
- もし，$Q = -1$ であれば，$P = Q = 5$ とする．

この方法を用いた場合，リュカの擬素数は $323, 377, 1159, 1829, 3827, 5459, 5777, 9071, 9179, 10877, \ldots$ となる．また，10^{15} 以下のリュカの擬素数は 2,402,549 個である．

フェルマーテストからミラー・ラビン素数判定法への強化と同じようにして，次の定理を用いてリュカの強確率的素数と強擬素数を定義する．

Theorem 3.4. p を素数とし，$p + 1 = 2^s d$（ただし，d は奇数）と分解する．リュカ数列 $\{U_k\}, \{V_k\}$ のパラメータを $\gcd(p, D) = 1$[*2]かつ $(D/p) = -1$ となるように選択する．このとき，次のいずれかのことが成立する．

- $U_d \equiv 0 \pmod{p}$ が成り立つ．
- $V_{d \cdot 2^r} \equiv 0 \pmod{p}$ となる $0 \leq r < s$ が存在する．

Definition 3.5（リュカの強素数判定法）**.** 正の奇数 n を素数判定の対象とする．リュカ数列 $\{U_k\}, \{V_k\}$ のパラメータを $\gcd(n, D) = 1$ かつ $(D/n) = -1$ となるように選択する．このとき，$U_d \not\equiv 0 \pmod{n}$ かつ任意の整数 $r \in [0, s)$ について $V_{d \cdot 2^r} \not\equiv 0 \pmod{n}$ であれば合成数と判定する．もし，成り立たなければ，パラメータ (P, Q) に対する**リュカの強確率的素数（strong Lucas probable prime）**とする．

リュカの強素数判定法をすり抜ける合成数を，パラメータ (P, Q) に対する**リュカの強擬素数（strong Lucas pseudoprime）**と呼ぶ．リュカの素数判定法と同様の方法でパラメータを選択した場合，リュカの強擬素数は $5459, 5777, 10877, 16109, 18971, 22499, 24569, 25199, 40309, 58519, \ldots$ となる．また，10^{15} 以下のリュカの強擬素数は 474,971 個であり，大幅に判定率が改善されていることがわかる．

3.2 Baillie-PSW 素数判定法

Baillie-PSW 素数判定法は，ミラー・ラビン素数判定法とリュカの強素数判定法を組み合わせた手法である．ミラー・ラビン素数判定法における強擬素数と，リュカの強擬素数は異なる数となる傾向がある．すなわち，両方の素数判定法をすり抜ける擬素数は極めて稀ということである．実際，2^{64} 以下では擬素数が存在しないことが知られている．

Definition 3.6 (Baillie-PSW 素数判定法)**.** 正の奇数 n を素数判定の対象とする．

- 底 2 のミラー・ラビン素数判定法を行う．合成数であれば終了．
- リュカの強素数判定法を行う．合成数であれば終了．そうでなければ，確率的素数として終了．

実用上，ミラー・ラビン素数判定法の前にしきい値 k 以下の素数で試し割り法を行うことが多い．ま

[*2] [2] ではこの条件は付いていないが，[3] では付いている．

た，この素数判定法は非常に効率的なので，多くのソフトウェアではこの方法が採用されている [1].

さきほど，Baillie-PSW 素数判定法をすり抜ける合成数が極めて稀と述べたが，実際のところは未解決問題である．ヒューリスティックな解析によると，無数に擬素数は存在すると予想されているが不明である [6]．もし，反例を見つけた場合は 620 ドルの賞金が手に入るようだ[*3].

参考文献

[1] Martin R Albrecht, Jake Massimo, Kenneth G Paterson, and Juraj Somorovsky. Prime and prejudice: primality testing under adversarial conditions. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pp. 281–298, 2018.

[2] Robert Baillie, Andrew Fiori, and Samuel Wagstaff Jr. Strengthening the baillie-psw primality test. *Mathematics of Computation*, Vol. 90, No. 330, pp. 1931–1955, 2021.

[3] Robert Baillie and Samuel S Wagstaff. Lucas pseudoprimes. *Mathematics of Computation*, Vol. 35, No. 152, pp. 1391–1417, 1980.

[4] Richard P Brent and Paul Zimmermann. An $O(M(n) \log n)$ algorithm for the jacobi symbol. In *International Algorithmic Number Theory Symposium*, pp. 83–95. Springer, 2010.

[5] RICHARD GE PINCH. The carmichael numbers up to 10^{21}. 2007.

[6] Carl Pomerance. Are there counter-examples to the baillie-psw primality test. *Dopo Le Parole aangeboden aan Dr. AK Lenstra. Privately published Amsterdam*, 1984.

[7] William Stein. *Elementary number theory: primes, congruences, and secrets: a computational approach*. Springer Science & Business Media, 2008.

[8] 高木貞治. 『初等整数論講義 第 2 版』. 共立出版, 1971.

[*3] 文献によって書いている賞金額が違うので，実際にはもっと少ない可能性がある．[2] では 620 ドル，[6] では 120 ドルと書かれている．また wikipedia によると，620 ドルは別の問題に対する賞金だという指摘もある．
`https://en.wikipedia.org/wiki/Baillie-PSW_primality_test`