

第 97 回 東北大学サイエンスカフェ

チャンスの法則 ～確率で世界はまわる～

日 時：2013 年 10 月 25 日（金）18:00～19:45

会 場：東北大学片平キャンパス北門会館 2 階 エスパス

講 師：尾畑伸明（東北大学大学院情報科学研究科）

協 力：三浦佳二・瀬川悦生・長谷川雄央・宮田洋行

（東北大学大学院情報科学研究科・数学連携推進室）

1. モンティ・ホールのジレンマ（ゲーム）

3つの扉の向こうには、1台の新車と2匹のヤギがいる。観客は1つの扉を選ぶ。司会者は、残りの2つの扉から1つの扉を開けてヤギを逃がす（司会者は決して新車のある扉を開けたりしない）。司会者は言う「今なら扉を替えてもいいですよ」観客は迷う。

アメリカのゲームショー番組に由来。モンティ・ホールはその司会者。コラムニストが正しく説明したが、納得いかない人々多数（相当の知識人を含む）を巻き込んで論争になった。1990年ころの話。私がこれを初めて知ったのは、

ブロム・サンデル・ホルスト著（森真訳）『確率論へようこそ』

（古い版は『確率問題ゼミ』＝売れそうにない題名だ）

を読んで。その後、劇場で見た『ラスベガスをぶつつぶせ』（原題：21、2008年）に同様の場面があった。数学の教授がこの問題を教室で問うて、主人公の学生が即座に正しく答えてしまい、教授はがっかり。ちなみに、上の本は、身近な確率の問題がたくさん収められていて、クイズ番組のようで楽しい。

観客参加で実験したところ、

	あたり	はずれ
選択を変えない（初志貫徹）	3	5
選択を変える	5	0

理論的に確率を求めると、

	あたり	はずれ
選択を変えない（初志貫徹）	1/3	2/3
選択を変える	2/3	1/3

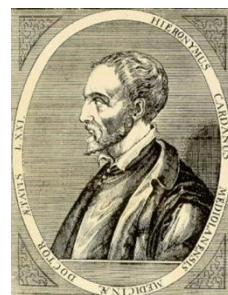
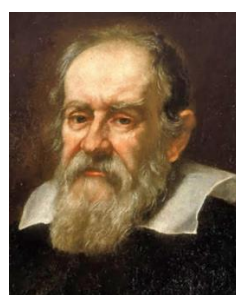
選択を変えることで、もともとははずれ（確率 2/3 でこうなっている）を引いていた人はあたりになるのだから、当たる確率は 2/3 になる。観客参加の実験でこんなに顕著な結果が出るとはちょっと意外であった。

2. 確率論のルーツ

フェルマ（1607?-65）とパスカル（1623-62）

貴族からサイコロ賭博に関する質問に答えるために、数回にわたり文通(1650 年代)。有名なのは、「賭けを中断したときの賞金の分配問題」この二人をめぐって、確率論の始まりを描いた本がある：

キース・デブリン 『世界を変えた手紙—パスカル、フェルマと〈確率〉の誕生』
なかなか面白い本だと思う。



ガリレオ（1564-1642）

親しい賭博師からの質問「3つのサイコロを同時に投げた時の和について、9となるのも10となるのも、ともに6通りであるが、10に賭けるほうが有利なようなのだが、どうなのか？」

$$9 = 1+2+6 = 1+3+5 = 1+4+4 = 2+2+5 = 2+3+4 = 3+3+3$$

$$10 = 1+3+6 = 1+4+5 = 2+2+6 = 2+3+5 = 2+4+4 = 3+3+4$$

もちろん、ガリレオは正しく答えた。この問題は、高校数学Aの内容である。当時は、「確からしさ」を数値化して比較するなど考えも及ばなかった。そもそも、まだやっていないこと、これから起こる未来のことに対して、人が何か言うということは大変だったことに違いない。

正しい確率を計算するためには、 $2+3+4$ と $3+3+3$ を比べると前者は後者の 6 倍起こりやすいということを把握する必要がある。正しい答えは、

$$P(9) = 25/216 \quad P(10)=27/216 \quad \text{差はわずか } 2/216 = 0.009$$

この差を体験するには、相当回数、ゲームに興じなければならないだろう。

ジェロラモ・カルダーノ (1501-76) — ルネッサンスの万能人

著書『サイコロ遊びについて (Liber de ludo aleae) 』(彼は 20 代のころから書き始め、1560 年代に完成。ただし、発行は 1663 年) はサイコロ賭博に関する初めての理論的な手引き書。その中で、「確からしさ」を把握し、「確率論」の始まりと言える。「サイコロを 2 つ投げて、その目の和に賭けるとすれば、いくつに賭けるのがいちばん有利か」といった問題に解答を出している。

カルダーノはかなりハチャメチャな人だったようだ。自伝が面白い。

カルダーノ 著 (青木靖三・榎本恵美子訳) 『わが人生の書』

「ギャンブラーにとっては、全くギャンブルをしないことが最大の利益となる」

「ギャンブルを何十年もやり続け、ためにやるというのではなく、恥ずかしながら、毎日やってきた」

伝記もある：

0. オア著 (安藤洋美訳) 『カルダーノの生涯：悪徳数学者の栄光と悲惨』

原題『Cardano the Gambling Scholar』に比べて、邦訳はちょっとひどくないか？

(余談)

江戸時代に発達した和算に確率はあったか？

たぶん無い、和算では主に算術が発展。確率論の画期的なところは「これから起こることに対して可能性を数値化する」ところ。このような考え方を取り込むのは困難だったと思われる。

いつ日本に入ってきたのか？

明治時代、欧米列強に伍してゆくために科学技術を輸入した。そのときに、ドイツ流の確率統計学が輸入された。日本初の確率統計の教科書はおそらく、
陸軍士官学校編『公算学』（1888 年）

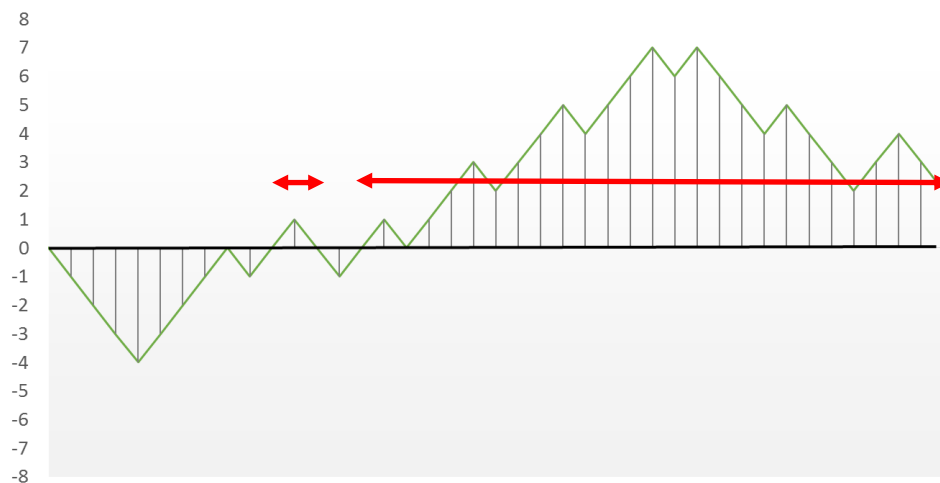
サイコロはいつごろからあるのか？

エジプトの第一王朝時代（BC3500 年頃）の遺跡から発掘されている。古代ギリシアでは、2〜3 個のサイコロ賭博が非常に盛んだった（特に上流階級の宴席）。サイコロの目の出方は人智を超えるということから、神のお告げとして宗教儀式（占い）に用いられた例は多数。

「デタラメ」の語源は「出た目」からきている。「くじ引き」なら賭博につながるが、「おみくじ」なら占いというわけで、使い道が違っただけで、偶然現象としては同じもの。

3. ツキの実験（ゲーム）と数理

サイコロを振って偶数（確率 $1/2$ ）なら+1, 奇数（確率 $1/2$ ）なら−1 に移動しながら、折れ線を描く。サイコロは、とりあえず、40 回振ってみよう。

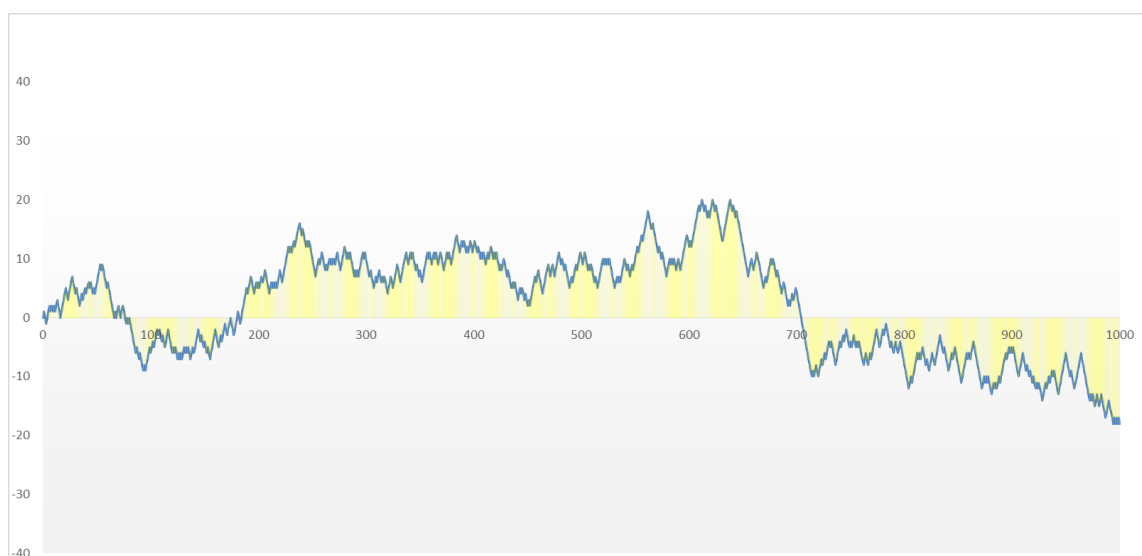
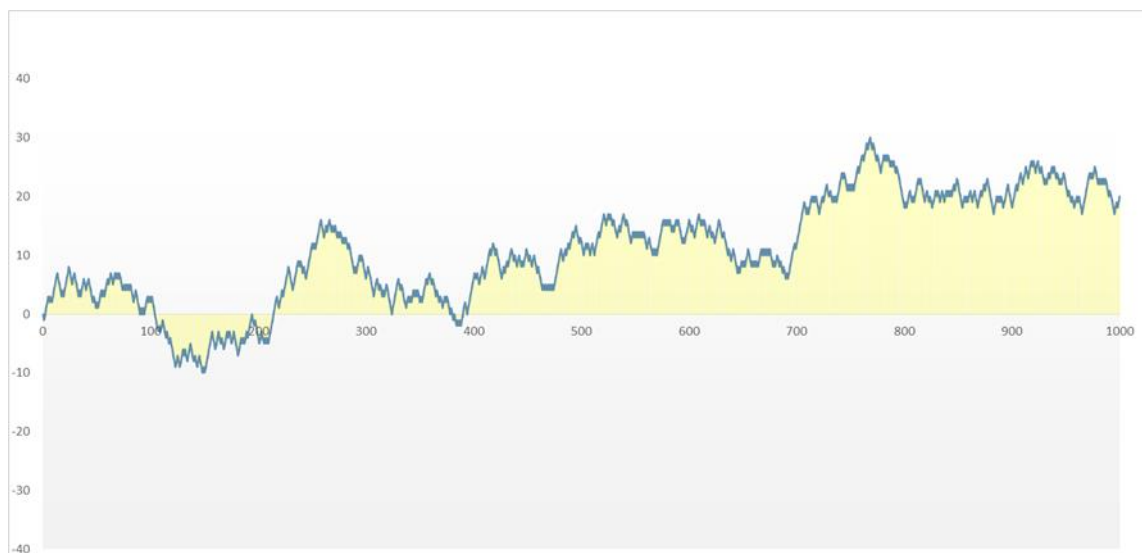


実験が終わったら、統計を取る。上の例では、

(+1) の回数 = 21 (−1) の回数 = 19 幸福な時間 = 28

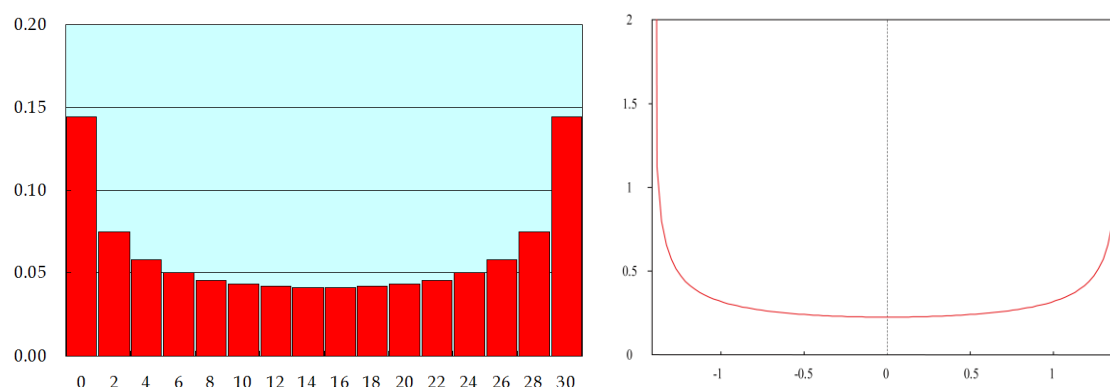
観客から収集したデータはあえなく紛失。しかし、よく傾向が現れていた。

1000 回のコイン投げのシミュレーション（2 例）



上のシミュレーションでは、おおよそ 500 回ずつ右上がり、左下がりが起こっている（最終的に ± 20 、程度なので、右上がり、左下がりは概ね 500 ± 10 程度しか変わらない）。しかし、幸福な時間は 1000 回の半分というわけではなく、かなり偏っているのが見て取れる。実は、そのような例をわざと挙げたのではなく、むしろ、幸福な時間は、長い方が短い方に偏っていて、半分は幸福、半分は不幸というようなことはむしろ起こりにくい。

30 回コインを投げるとして、幸福な時間がどのくらいの確率で現れるかを理論的に計算することができる。結果をグラフで表したものが左図。幸福な時間が 0 回あるいは 30 回のよう
に極端な場合が起こる確率はそれぞれ 0.15 近くあり、半々になる場合の 3 倍も起こり
やすいのである。コイン投げの回数をもっと増やしてゆくと、左のグラフはある曲線に見
えてくる（右図）。これを逆正弦則(arcsine law)という。



4. 確率セルオートマトン（ゲーム）

連続したセルの状態を、一定のルールで変化させる自動機械を総称して「セルオートマトン」という。このルールに確率的な要素が加わったものが「確率セルオートマトン」である。Domany-Kinzel モデル(1984)で遊んでみよう。

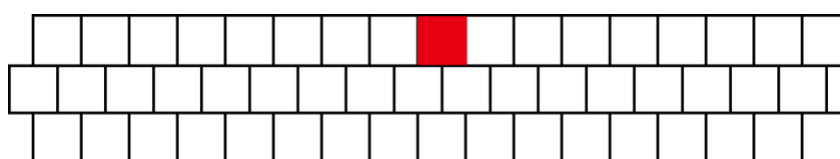
☆色塗りのルール

(0) あらかじめ、確率 p, q を大きめに自分で決めておきます。たとえば、

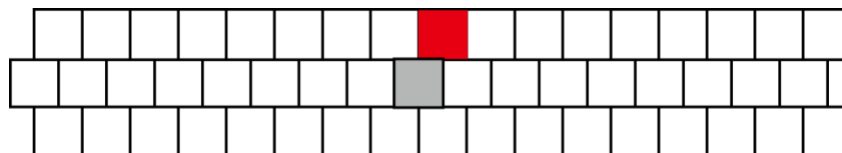
$$p = 11/13 = 0.85 \quad (\text{トランプをめくって 11 以下の時})$$

$$q = 10/13 = 0.77 \quad (\text{トランプをめくって 10 以下の時})$$

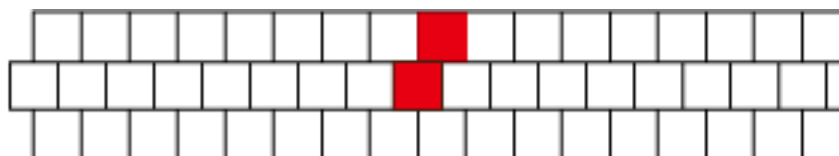
(1) まず、下図のように 1 段目の 1 個のセルに色を塗る。



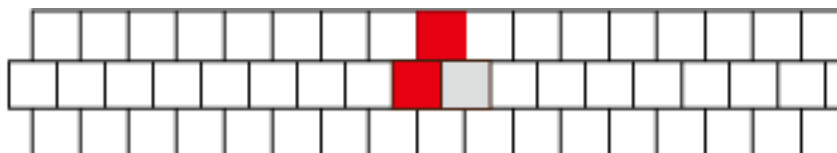
(2) 次に、色を塗った1段目のセルに接している2段目のセルだけに色を塗る。左から見てゆくと、まず、灰色のセルに注目する。



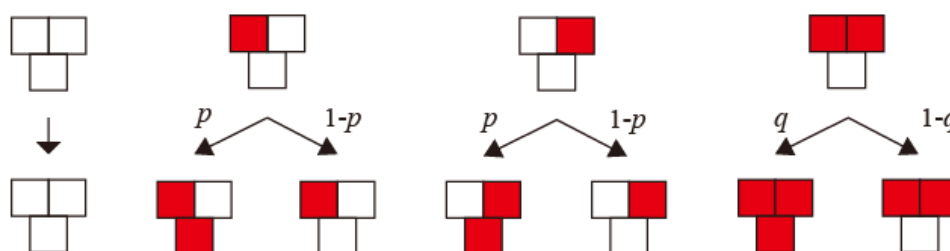
実際に色を塗るかどうかは確率的に決める。トランプをめくって、確率 p のほうが起これば塗り、そうでないときは、塗らないでパスする。今、確率 p のほうが起こって塗ったとすると、次のようになる。



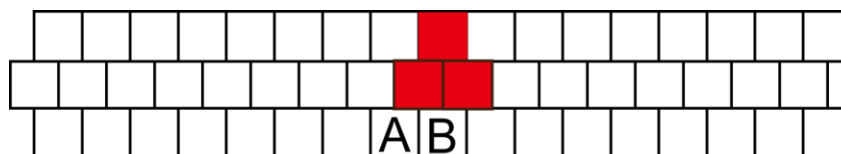
2段目にはもう1つ、色を塗ってもよいセル（灰色で示している）がある。同様に確率的に塗るか塗らないかを決める。



(3) 次に3段目に移る。2段目のセルで色が塗ってあるものに接しているセルだけ色を塗ることができる。ただし、2段目にある色つきセルのパターンで2通りの確率を使い分ける。そのルールは、



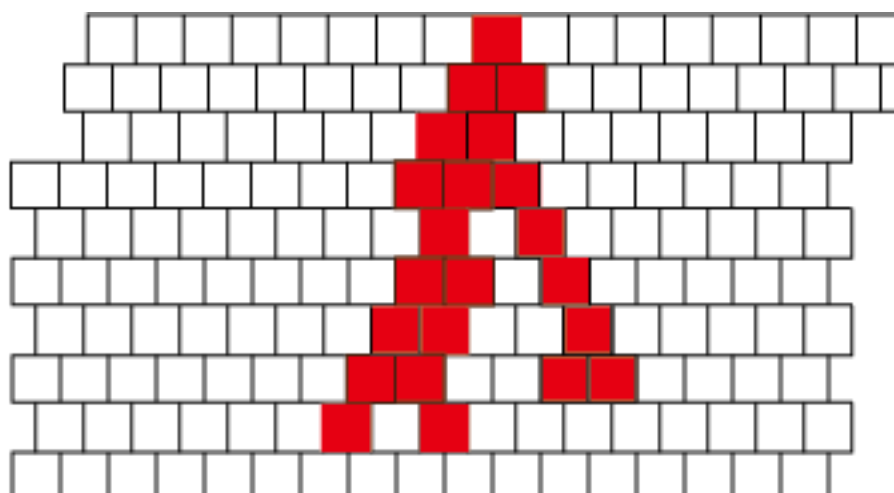
たとえば、



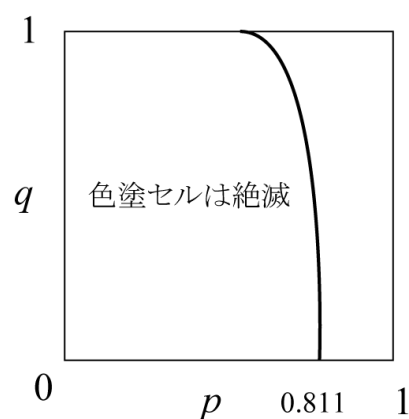
となっているときは、A には確率 p を適用して塗るか塗らないかを決めて、B には確率 q を適用して塗るか塗らないかを定める。

(4) この作業を、あきらむまで繰り返す。でも、途中で色つきセルがなくなってしまったら、残念ながらそこで終了。確率 p, q を小さく設定すると、すぐ終わってしまう。 $p = 1$ とか $q = 1$ に設定するのもあり。

☆できるだけ塗り絵がずっと続くように上手に p と q を自分で調節してみてください。そして皆さんだけの、世界で一つだけの絵を作ってみてください。



塗り絵がいつまでも継続できるような p, q の組合せについては数学的には未解決問題。計算機シミュレーションによって、右図が得られている。



5. 感染症とワクチン戦略

確率セルオートマトン：「感染」に似ている。

インフルエンザ（はしか、おたふくかぜのような一過性の感染症）の特徴

- 1) 一過性である。
- 2) 人から人へ感染する。
- 3) 感染は確率的に起こる。
- 4) 一度感染した人は免疫を獲得するので感染はしない（しにくい）。

人と人の繋がり方 — 複雑ネットワーク

人を点で表し、友人関係（または家族関係などなんらかの社会関係）にある 2 点を線で結ぶ。このような点と線で構成されたものをネットワーク（グラフ）という。人と人の繋がり方には以下の特徴がある。

- 1) スケールフリー性(ハブ構造)
- 2) スモールワールド性(6 次の隔たり)
- 3) クラスター性

感染症のモデルを、人間関係を模したネットワークの上に配置することで感染症をシミュレートすることができる。人間関係のスケールフリー性は感染症を拡がりやすくする。

ネットワーク理論からみるワクチン戦略

感染症の蔓延を防ぐためにワクチンを配ることを考える。現実問題として、皆にワクチンを渡すのは難しい。ネットワークの構造に着目して(限られた数の)ワクチンを効果的に配分したい。

- 1) あまり効果が低いやり方→各人がバラバラにワクチンを貰う
- 2) 良いやり方→” ネットワーク的に” 重要な人から順にワクチンを配る
- 3) 個人の対策？→(あなたは使わず)あなたの友達にワクチンを渡す

1) random vaccination; 2) degree vaccination, BC vaccination; 3) acquaintance vaccination と呼ばれている。ネットワーク理論を使って様々なワクチン配分の方法が現在も提案・検討されている。

6. 確率的アルゴリズム

2, 3, 5, 7, 11, 13, 17, ... のように、自分自身と 1 でしか割り切れない数を素数といいます。全ての数は、

$$6 = 2 \times 3$$

$$7 = (1 \times) 7$$

$$8 = 2 \times 2 \times 2$$

のように、素数をいくつか掛けたものとして表すことができます（素因数分解）。

メッセージを大きな素数に対応させて送信するとして、もう 1 つ別の素数をかけて暗号化したとしましょう。たとえば、メッセージが

996328662233

のように暗号化されたとします。公開ルールとして、メッセージは、これを素因数分解して得られる素数の大きい方とします。暗号化されたメッセージを盗んだ人は、解読するために、素因数分解しなければなりません。素因数分解は、基本的には素朴にやるしかなく、

$$996328662233 \div 2 = 498164331113.5$$

$$996328662233 \div 3 = 332109554077.66 \dots$$

...

のように小さな素数で片っ端から割ってみて、ようやく

$$996328662233 \div 997319 = 999007$$

となって、メッセージの解読に成功します。一方、正当な受け手は 997319 を鍵として持っているので、割り算を直ちに実行して、メッセージ 999007 を簡単に解読できる。素数で片端から割り算するという計算そのものは、単純ではあるが、時間がかかるために暗号として有効なのです。インターネット通信などに用いられている RSA 暗号では、もう少し洗練された方法を用いますが、原理的には素因数分解に時間がかかるということで安全性を担保しているのです。

したがって、暗号化のために沢山の素数を用意しなくてはなりません。しかし、素数かどうかをまともに調べようとすると大変です。実は、大変な計算も非常に低い確率で間違えるかもしれないことを許せば、高速に計算できることがあります。

素数かどうかをテストするための数学的な根拠は

フェルマの小定理 p が素数ならば、どんな数 a を持ってきても、

$$a^{p-1} = a \times a \times \dots \times a \quad (p-1 \text{ 乗})$$

を p で割ると余りは 0 か 1 になる。

ほんの一部の例外(Carmichael 数)を除いて、ランダムに a を 10 個選んで、10 個ともフェルマーの小定理を満たすかをテストすれば、

$$1 - (1/2)^{10} \doteq 0.9990234375 \text{ 以上}$$

の確率で正しい結果が分かります。20 回で行うと、

$$1 - (1/2)^{20} \doteq 0.99999904632 \text{ 以上}$$

の確率で正しい結果が分かります。例外のない手法として、これを発展させた **Miller-Rabin** の素数判定法という方法が素数か調べる方法として広く用いられています。RSA 暗号でも、素数かどうか調べるために、非常に低い確率で間違えることを許した高速手法 **Miller-Rabin** の素数判定法が使われています。確率は高速に計算するための鍵としても、身の回りで用いられている。