561 は、互いに素などの底で試しても、フェルマーの判定を通る

— $561 = 3 \times 11 \times 17$ は互いに素な底 320 個のすべてでフェルマーの判定を通る — 問いを一段ずつ足すと騙す底は 80 個、10 個へと減り、最後の問いは 2 乗して 1 になる数が ± 1 しかないかを見ている —

— [論文603]

山岸 勇輝 (Yuuki YAMAGISHI)
Yamagishi Complexity Torus Lab, Japan｜山岸勇輝ラボ
2026年9月

— *From thinking to syncing.* —

要旨

n が素数なら、n と互いに素などの a についても a^{n-1} を n で割った余りは 1 になる（フェルマーの小定理）。そこで、余りが 1 になるかを見て素数らしさを判定する方法がある（フェルマーの判定）。この判定がどの合成数に、どれだけ騙されるかを数える。新しい定理も法則も主張しない。 第一に、561 は互いに素な底すべてで判定を通る——$561 = 3 \times 11 \times 17$ と互いに素な底は 320 個で、その 320 個すべてで余りが 1 になる。1 から 560 の底のうち割合は **0.571429** で、見破れるのは 3・11・17 のどれかを共有する 240 個（**0.428571**）だけである（第2節）。 第二に、こうした数は珍しいが、無くならない——互いに素な底すべてで判定を通る合成数（カーマイケル数）は、10^3 までに 1 個、10^4 までに 7 個、10^5 までに 16 個、10^6 までに 43 個ある。全部の底で確かめた数と、素因数だけで決める判定（コルセルトの判定）は、10^5 まで一つ残らず一致した（第2節）。 第三に、問いを足すと、騙す底が減る——561 で、a^{280} がヤコビ記号に一致するかも問う（オイラーの判定）と騙す底は 80 個（**0.142857**）、2 乗の列を全部問う（ミラー＝ラビンの判定）と 10 個（**0.017857**）になる（第3節）。 第四に、これが本稿の芯である。最後の問いが見ているのは、2 乗して 1 になる数が ± 1 の二つしかないかどうかである——素数 557 を法とすると 2 乗して 1 になる数は 1 と 556 の 2 個だが、561 を法とすると 8 個ある。底 2 で $2^{35}, 2^{70}, 2^{140}, 2^{280}$ を 561 で割ると $263, 166, 67, 1$ で、1 の直前の 67 が ± 1 でない 1 の平方根として 561 を見破る（第3節）。 第五に、分離子は、何を問うかである——フェルマーは最後の一つ a^{n-1} だけを問い、オイラーはその半分の冪とヤコビ記号を、ミラー＝ラビンは 2 乗の列の途中を全部問う。騙す底は 320、80、10 と減り、ミラー＝ラビンでは 10^4 までのどの奇数の合成数でも、騙す底の割合は上限の $1/4$ を超えなかった（ちょうど $1/4$ になるのは 9）（第3節）。 キーワード：カーマイケル数、フェルマーの素数判定、ミラー＝ラビン判定、擬素数、素数判定。

> 本稿の射程（射程注記）：新しい定理も法則も主張しない——カーマイケル数（カーマイケル、1910）、素因数による判定（コルセルト、1899）、オイラーの判定（ソロヴェイとシュトラッセン、1977）、ミラー＝ラビンの判定とその上限 1/4（ミラー、1976／ラビン、1980）、カーマイケル数が無限にあること（アルフォード、グランヴィル、ポメランス、1994）は、いずれも既知である。定理を証明しない——10^6 までの数を数え、10^5 までは全部の底で確かめ、561 で底を全部数えるだけである。「どの底でも騙される」とは言わない——騙すのは互いに素な底だけで、素因数を共有する底は見破る。暗号での使い方や計算の速さは扱わない。既刊との関係：論文513 は、平方剰余の相互法則を格子点で数えて示し、余りを問うなら $a^{(p-1)/2}$ を p で割った余りで答が出る（オイラーの規準）と書いた——本稿のオイラーの判定は、その規準を合成数に当てて、騙されるかを数えたものである。加えたのは、561 で三つの判定の騙す底を全部数えて並べたこと、全部の底で確かめる道筋と素因数で決める道筋を 10^5 まで突き合わせたこと、分離子を「何を問うか」に置き、最後の問いが 1 の平方根の個数を見ていることを数で示したことである。

1. 記法と問い

設定：奇数 n と底 a（$1 \le a \le n-1$）について、次の三つを問う。

フェルマーの判定：a^{n-1} を n で割った余りが 1 か。

オイラーの判定：a が n と互いに素で、$a^{(n-1)/2}$ を n で割った余りがヤコビ記号 (a/n) に等しいか。

ミラー＝ラビンの判定：$n-1 = 2^s d$（d は奇数）と書き、a^d が 1 か、$a^d, a^{2d}, \ldots, a^{2^{s-1}d}$ のどれかが $n-1$ に等しいか。

n が素数なら、どの判定もすべての底で「素数らしい」と答える。合成数 n で「素数らしい」と答えさせる底を、その判定を騙す底と呼ぶ。

問い：フェルマーの判定を、互いに素な底すべてで騙す合成数はあるか。問いを足すと、騙す底はどれだけ減るか。何が効いているか。

2. フェルマーの判定を通る合成数

計算 2.1：10^6 までの合成数を、素因数だけで決める判定（平方因子を持たず、どの素因数 p についても $p-1$ が $n-1$ を割る）で調べた。

範囲	互いに素な底すべてで判定を通る合成数
10^3 まで	1 個
10^4 まで	7 個
10^5 まで	16 個
10^6 まで	43 個

最初の 16 個は
$561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841, 29341, 41041, 46657, 52633, 62745, 63973, 75361$ である。
$561 = 3 \times 11 \times 17$、$1729 = 7 \times 13 \times 19$ で、どちらも異なる三つの素数の積である。

計算 2.2：素因数の判定とは独立に、10^5 までの合成数すべてで、互いに素な底をすべて試した。判定を通る合成数は 16 個で、素因数の判定の 16 個と一つ残らず一致した。比べると、底 2 だけを騙す奇数の合成数は 10^5 までに 78 個あり、その中に 16 個とも入っている。

計算 2.3：561 で、底 $a = 1, \ldots, 560$ をすべて数えた。561 と互いに素な底は 320 個（320 は $2 \times 10 \times 16$）で、その 320 個すべてで a^{560} の余りが 1 だった。割合は **0.571429** である。余りが 1 にならなかった 240 個（**0.428571**）は、3・11・17 のどれかを約数に持つ底とちょうど一致した。

> 観察 2.4
>
> 561 を見破れるのは、素因数を当てたときだけである。560 は 2・10・16 のどれでも割り切れるので、互いに素な a なら a^{560} は 3・11・17 のどれで割っても余り 1 になり、したがって 561 で割っても余り 1 になる——フェルマーの判定でこの数を見破るには、素因数を持つ底を引き当てるしかない。それは素因数分解を当てることに近い。

3. 問いを足す

計算 3.1：561 で、三つの判定を騙す底を全部数えた（$n - 1 = 560 = 2^4 \times 35$）。

判定	騙す底	560 個の底に対する割合
フェルマー	320	**0.571429**
オイラー	80	**0.142857**
ミラー＝ラビン	10	**0.017857**

ミラー＝ラビンを騙す 10 個は $1, 50, 101, 103, 256, 305, 458, 460, 511, 560$ である。

計算 3.2：2 乗して 1 になる数を数えた。素数 557 を法とすると 1 と 556 の 2 個だけだった。561 を法とすると $1, 67, 188, 254, 307, 373, 494, 560$ の 8 個だった。底 2 で $2^{35}, 2^{70}, 2^{140}, 2^{280}, 2^{560}$ を 561 で割った余りは $263, 166, 67, 1, 1$ だった。

> **観察 3.3**
>
> これが本稿の芯である。最後の問いが見ているのは、1 の平方根が ± 1 の二つしかないかどうかである。素数を法とすれば、x^2 の余りが 1 になる x は 1 と $n-1$ だけである。2 乗の列が 1 に着くなら、その直前は 1 か $n-1$ でなければならない——561 では、底 2 の列が 67 から 1 に着いた。67 は ± 1 でない 1 の平方根で、これが合成数の証拠になる。561 を法とする 1 の平方根は、三つの素因数それぞれで ± 1 を選ぶ $2^3 = 8$ 通りある。

> **観察 3.4**
>
> 分離子は、何を問うかである。フェルマーは列の最後 a^{n-1} だけを問い、オイラーはその半分の冪 $a^{(n-1)/2}$ とヤコビ記号の一致を問い、ミラー＝ラビンは列の途中を全部問う——騙す底は 320、80、10 と減った。問いを足すたびに、合成数が隠しておける場所が減る。

計算 3.5：10^4 までの奇数の合成数すべてで、ミラー＝ラビンを騙す底の割合を数えた。最大は $n = 9$ の 0.250000（底 1 と 8 の 2 個）で、ラビンの上限 1/4 をどの数も超えなかった。561 の **0.017857** は、上限の 0.071429 倍である。

観察 3.6

ミラー＝ラビンには、全部の底で騙す合成数が無い。フェルマーの判定には 10^6 までに **43** 個あったが、ミラー＝ラビンでは騙す底が多くとも四分の一である——だから底を変えて何度か試せば、見逃す確率を $1/4$ ずつ掛けて小さくできる。フェルマーの判定では、カーマイケル数に対して試す回数を増やしても、互いに素な底を引くかぎり見逃し続ける。

観察 3.7

論文513 と並べる。**513** は、余りを問うなら $a^{(p-1)/2}$ を p で割った余りで答が出る（オイラーの規準）と書いた——その規準は素数 p についての事実であり、合成数に当てると **561** では **80** 個の底が規準どおりの答を返してしまう。規準が素数を特徴づけるのは、素数の側から見たときだけである。

観察 3.8

言わないこと。カーマイケル数が無限にあることも、ラビンの上限も証明しない。暗号での使い方や計算の速さは扱わない——示したのは、10^6 までの数え上げ、10^5 までの二つの道筋の一致、そして **561** での三つの判定の比較である。

4. 点呼と結び

1. **561** と互いに素な底 **320** 個すべてで判定を通る（計算 2.3）：割合 **0.571429**。
2. 見破る底 **240** 個は素因数を共有する底（計算 2.3）：割合 **0.428571**。
3. カーマイケル数は 10^6 までに **43** 個（計算 2.1）：珍しいが無くならない。
4. 全部の底と素因数の判定が 10^5 まで一致（計算 2.2）：二つの道筋。
5. 騙す底は **320**、**80**、**10**（計算 3.1）：問いを足すと減る。
6. **561** を法とする **1** の平方根は **8** 個、**557** では **2** 個（計算 3.2）：素因数の数だけ増える。
7. 底 **2** の列は $263, 166, 67, 1$（計算 3.2）：**67** が見破る。
8. 最後の問いは **1** の平方根が ± 1 だけかを見る（観察 3.3）：本稿の芯。
9. 分離子は何を問うか（観察 3.4）：列の最後か、途中も全部か。
10. ミラー＝ラビンを騙す割合は $1/4$ 以下、**9** でちょうど $1/4$（計算 3.5）：全部の底で騙す数は無い。

結び：a^{n-1} を n で割った余りが 1 かを見る判定は、素数を必ず通すが、合成数も通してしまうことがある。$561 = 3 \times 11 \times 17$ は、互いに素な底 320 個のすべてで判定を通る——見破れるのは素因数を共有する 240 個の底だけで、こうした数は 10^6 までに 43 個ある。全部の底で確かめた数と素因数だけで決める判定は、10^5 まで一つ残らず一致した。問いを足すと、騙す底は 320 個から 80 個、10 個へと減る——最後の問い（ミラー＝ラビン）が見ているのは、2 乗して 1 になる数が ± 1 の二つしかないかどうかである。素数 557 ではその数は 2 個、561 では 8 個あり、底 2 の列 $263, 166, 67, 1$ の 67 が 561 を見破る。分離子は、何を問うかである——列の最後だけを問う判定には全部の底で騙す合成数があり、途中を全部問う判定では、騙す底は 10^4 までのどの数でも四分の一を超えなかった。既刊との位置——論文513 が素数の側から書いたオイラーの規準を、合成数の側から当てると、561 では 80 個の底が規準どおりに答える。正直に言えば——数えたのは 10^6 までで、無限にあることも上限も証明していない。

参考文献

1. Alford, W. R., Granville, A., & Pomerance, C. (1994). There are infinitely many Carmichael numbers. *Annals of Mathematics*.
2. Carmichael, R. D. (1910). Note on a new number theory function. *Bulletin of the American Mathematical Society*.
3. Korselt, A. (1899). Problème chinois. *L'Intermédiaire des Mathématiciens*.
4. Miller, G. L. (1976). Riemann's hypothesis and tests for primality. *Journal of Computer and System Sciences*.
5. Rabin, M. O. (1980). Probabilistic algorithm for testing primality. *Journal of Number Theory*.
6. Solovay, R., & Strassen, V. (1977). A fast Monte-Carlo test for primality. *SIAM Journal on Computing*.
7. 山岸勇輝 (2026). 『数えるという操作が、代数の定理を証明してしまう』[論文513]. Zenodo. 10.5281/zenodo.22862214

— *From thinking to syncing.* —

山岸 勇輝 (Yuuki YAMAGISHI)

© 2026 Yamagishi Complexity Torus Lab, Japan · Licensed under Creative Commons Attribution 4.0 International (CC BY 4.0)