平方因子の無い a が原始根になる素数の割合は、a を 4 で割って 1 余るときだけ独立の見立てから外れる

— a＝5 では、5 が平方非剰余であることと p を 5 で割った余りが相互法則で結びつき、原始根になる割合は独立の積の 1＋1/19 倍になる — 分離子は、a を 4 で割った余りが 1 か 3 か — [論文1020]

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

整数 a の累乗が p で割った余りをすべて作るとき、a は素数 p の原始根である。a が原始根になる素数が無数にあるか（アルティン予想）は、平方数でも −1 でもない a について未解決である。本稿は、原始根になる素数の割合を数え、素数ごとの確率を掛けた見立てと並べる。新しい定理も法則も主張せず、予想を証明もしない。第一に、これが本稿の芯である。独立の見立てが外れるのは a＝5 のような場合だけで、その外れは補正でちょうど埋まる——素数ごとの確率を掛けたアルティン定数は 0.373955826 で、2×10^6 までの素数 148932 個で数えると a＝2・3・6・7 は 0.374292・0.373623・0.373958・0.374422 だった。a＝5 だけは 0.393578 で、a＝2 との差は標準誤差の 10.82 倍あり、補正した見立て 0.393638（定数の 1＋1/19 倍）と合った（第2節）。第二に、外れの出どころは、二つの条件が独立でないことである——p を 5 で割って 1 余る素数では、5 が平方非剰余になる割合は 0.000000 で、それ以外の素数では 0.666914 だった。独立なら、どちらも半分のはずである（第3節）。 第三に、a を 4 で割って 3 余る a では、二つの条件は結びつかない——a＝3 では二つの割合が 0.500349 と 0.499685、a＝7 では 0.500807 と 0.500415 で、どちらも半分だった。4 で割って 1 余る a＝13 では 0 と 0.545794 で、1 以外の余りのうち非剰余の余りの割合 6/11＝0.545455 に合った（第3節）。 第四に、補正の大きさは a の素因数で決まり、大きな素因数では小さくなる——a＝13 では 1＋1/155 倍で見立て 0.376368 に対して 0.376611、a＝21 では 1−1/205 倍で 0.372132 に対して 0.372873 で、この範囲の数では補正の無い定数と見分けられない（第2節）。 第五に、平方数の a は原始根にならない——a＝4 の割合は 0 だった。平方数はどの p でも平方剰余だからである（第2節）。 第六に、分離子は、a を 4 で割った余りが 1 か 3 か——平方剰余の相互法則は、4 で割って 1 余る a についてだけ、a が平方非剰余であることを p を a で割った余りで決めてしまう。そこで二つの条件が結びつき、確率の積が外れる（第4節）。 キーワード：原始根、アルティン予想、アルティン定数、平方剰余の相互法則、オイラーの規準、平方非剰余。

本稿の射程（射程注記）：新しい定理も法則も主張しない——アルティン予想（1927）、原始根になる割合の見立てとその補正、一般化リーマン予想を仮定すれば見立てが正しいこと（フーリー、1967）、平方剰余の相互法則、オイラーの規準は、いずれも既知である。見立てが数値計算で外れて補正された経緯は、モリーの概説（2012）にまとめられている。予想を証明しない——2×10^6 まで数えたことは証明にならず、一般化リーマン予想にも立ち入らない。負の a と平方因子のある a の補正を扱わない——平方因子のある a は、平方数の a＝4 だけを見る。既刊との関係：論文513 は、平方剰余の相互法則を格子点を数えて確かめた——ここでは、同じ相互法則が二つの条件を結びつけ、確率の積を外すことを数える。論文603 は、オイラーの規準（a の (p−1)/2 乗を p で割った余り）を合成数に当てて、騙される底を数えた——ここでは、同じ規準で平方非剰余かどうかを決め、p を a で割った余りごとに数える。論文640 は、偶数を二つの素数の和で表す仕方の数が、小さな素数で割り切れるかで決まる倍率を持つことを数えた——ここでは、倍率が a 自身の素因数で決まり、a を 4 で割った余りが 1 のときだけ現れることを数える。加えたのは、十個の a で割合を数えて見立てと並べたこと、補正の出どころを、条件つきの平方非剰余の割合で直接数えたこと、4 で割って 3 余る a では条件が結びつかないことを対照として示したこと、補正の大きさが a の素因数で決まることを並べたことである。

1. 記法と問い

設定：素数 p で割った余りの世界で、a の累乗が 1 から $p-1$ までをすべて作るとき、a を原始根と呼ぶ。これは、$p-1$ のどの素因数 q についても $a^{(p-1)/q}$ が 1 にならないことと同じである。条件「q で割り切れない」が素数 q ごとに確率 $1-1/(q(q-1))$ で独立に満たされると見立てると、割合は積 $A=\prod_q(1-1/(q(q-1)))$ になる。

問い：独立の見立ては、どの a で外れるか。外れるのはなぜか。

2. 割合を数える

計算 2.1：$3\le p\le 2\times10^6$ の素数 148932 個で数えた（素数 7 の原始根が 3 と 5 だけであることを先に確かめた）。A は 0.373955826 だった。補正した見立ては、平方因子の無い a が 4 で割って 1 余るとき $A(1-\mu(a)\prod_{q\mid a}1/(q^2-q-1))$、それ以外は A、平方数は 0 である。

a	割合	見立て	差（標準誤差の倍）
2	0.374292	0.373956	0.27
3	0.373623	0.373956	−0.27
4	0.000000	0.000000	0.00
5	0.393578	0.393638	−0.05
6	0.373958	0.373956	0.00
7	0.374422	0.373956	0.37
10	0.375006	0.373956	0.84
11	0.375160	0.373956	0.96
13	0.376611	0.376368	0.19
21	0.372873	0.372132	0.59

標準誤差はおよそ 0.001254 で、$a = 5$ と $a = 2$ の差 0.019287 はその 10.82 倍だった。補正の倍率は $a = 5$ で $1 + 1/19 = 1.052632$、$a = 13$ で $1 + 1/155 = 1.006452$、$a = 21$ で $1 - 1/205 = 0.995122$ である。

> **観察 2.2**
>
> これが本稿の芯である。独立の見立てが外れるのは a＝5 のような場合だけで、その外れは補正でちょうど埋まる。$a = 5$ だけが定数から標準誤差の 10 倍を超えて離れ、補正した見立てとは −0.05 倍しか違わない——$a = 13$ と $a = 21$ の補正は小さく、この範囲の数では見分けられない。

3. 補正の出どころ

計算 3.1：a が平方非剰余になる割合を、p を a で割った余りが 1 かどうかで分けて数えた（オイラーの規準 $a^{(p-1)/2} \equiv -1$ で判定）。

a	a を 4 で割った余り	余り 1 の p	それ以外の p
5	1	0.000000	0.666914
13	1	0.000000	0.545794
3	3	0.500349	0.499685
7	3	0.500807	0.500415

a を 4 で割って 1 余るとき、それ以外の p での割合は、1 以外の余り $a-2$ 個のうち非剰余の余り $(a-1)/2$ 個の割合 $(a-1)/(2(a-2))$ に合う：$a=5$ で 0.666667、$a=13$ で 0.545455。

> **観察 3.2**
>
> 外れの出どころは、二つの条件が独立でないことである。原始根であるには、a が平方非剰余であること（$q=2$ の条件）と、p を a で割った余りが 1 でないこと（$q=a$ の条件）の両方が要る——$a=5$ ではこの二つが結びつき、一方が成り立てば他方も成り立ちやすい。だから割合が積より大きくなる。

4. 分離子と、言わないこと

> **観察 4.1**
>
> 分離子は、a を 4 で割った余りが 1 か 3 か。平方剰余の相互法則は、4 で割って 1 余る a についてだけ、a が平方非剰余かどうかを p を a で割った余りで決める——3 余る a では、p を 4 で割った余りも一緒に効くので、p を a で割った余りだけでは決まらず、条件は結びつかない。

> **観察 4.2**
>
> 言わないこと。アルティン予想は証明しない。一般化リーマン予想にも立ち入らない——負の a と、平方数以外の平方因子のある a の補正は扱わない。

5. 点呼と結び

1. 定数 **0.373955826**、a＝2・3・6・7 は **0.374292**・**0.373623**・**0.373958**・**0.374422**（計算 2.1）：独立で合う。
2. **a＝5** は **0.393578**、見立て **0.393638**、差は **10.82** 倍（計算 2.1）：本稿の芯。
3. **a＝5** で **0.000000** と **0.666914**（計算 3.1）：条件が結びつく。
4. **a＝3・7** で半分、**a＝13** で **0.545794**（**6/11＝0.545455**）（計算 3.1）：**4** で割った余り。
5. **a＝13・21** は **0.376611**・**0.372873**（計算 2.1）：補正は小さい。
6. **4** で割った余りが **1** か **3** か（観察 4.1）：分離子・論文513・603・640。

結び：平方因子の無い a が原始根になる素数の割合は、a を 4 で割って 1 余るときだけ独立の見立てから外れる。2×10^6 までの素数で数えると、a＝2・3・6・7 は定数 0.373955826 と合い、a＝5 だけが 0.393578 と標準誤差の 10.82 倍離れて、補正した見立て 0.393638 と合った——p を 5 で割って 1 余る素数では 5 が平方非剰余になる割合が 0、それ以外では 0.666914 で、二つの条件が独立でない。a＝3・7 では余りによらず半分で、結びつかない。a＝13 も同じ形（0 と 0.545794）だが、補正は 1＋1/155 倍と小さく、この範囲では見分けられない。分離子は、a を 4 で割った余りが 1 か 3 かである。既刊との位置——論文513 は相互法則を格子点で数え、論文603 はオイラーの規準で騙される底を数え、論文640 は小さな素数で決まる倍率を数えた。ここでは、相互法則が二つの条件を結びつけ、確率の積を外すことを数えた。正直に言えば——a が原始根になる素数が無数にあるかどうかは、一つの a についても証明していない。

参考文献

1. Hooley, C. (1967). On Artin’s conjecture. *Journal für die reine und angewandte Mathematik*.
2. Moree, P. (2012). Artin’s primitive root conjecture – a survey. *Integers*.
3. 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
4. 山岸勇輝 (2026).『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』[論文603]. Zenodo.
5. 山岸勇輝 (2026).『偶数を二つの素数の和に表す仕方の数は、3 で割り切れるかでおよそ 2 倍違う』[論文640]. Zenodo.

— 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)