Primitive Roots Break the Independent Estimate Only When the Square-Free Base Leaves 1 on Division by 4

— for a = 5, being a quadratic non-residue and the remainder of p on division by 5 are tied together by reciprocity, and the share of primes with 5 as a primitive root becomes 1 + 1/19 times the independent product — the separator is whether a leaves 1 or 3 on division by 4 — [Paper 1020]

Yuuki YAMAGISHI (山岸 勇輝)
Yamagishi Complexity Torus Lab, Japan
September 2026

— From thinking to syncing. —

Abstract

An integer a is a primitive root of a prime p when its powers produce every nonzero remainder on division by p. Whether infinitely many primes have a as a primitive root (Artin's conjecture) is open for every a that is neither a square nor −1.This paper counts the share of primes for which a is a primitive root and lines it up against the estimate that multiplies a probability for each prime.No new theorem or law is claimed, and the conjecture is not proved. First, and this is the core. The independent estimate fails only in cases like a = 5, and the correction fills the failure exactly——the product of probabilities, Artin's constant, is 0.373955826; counting over the 148932 primes up to 2×10^6, a = 2, 3, 6 and 7 gave 0.374292, 0.373623, 0.373958 and 0.374422. Only a = 5 gave 0.393578, differing from a = 2 by 10.82 standard errors and matching the corrected estimate 0.393638 (1 + 1/19 times the constant) (Section 2). **Second, the failure comes from two conditions not being independent——among primes leaving 1 on division by 5, the share for which 5 is a quadratic non-residue was 0.000000, and among the others 0.666914. If independent, both would be one half** (Section 3). **Third, for a leaving 3 on division by 4, the two conditions are not tied——for a = 3 the two shares were 0.500349 and 0.499685, and for a = 7 0.500807 and 0.500415, both one half. For a = 13, which leaves 1, they were 0 and 0.545794, matching the share of non-residue remainders among remainders other than 1, 6/11 = 0.545455** (Section 3). **Fourth, the size of the correction is set by the prime factors of a and shrinks for large factors——for a = 13 it is 1 + 1/155, with estimate 0.376368 against 0.376611, and for a = 21 it is 1 − 1/205, with 0.372132 against 0.372873; in this range they cannot be told from the uncorrected constant** (Section 2). **Fifth, a square a is never a primitive root——the share for a = 4 was 0, because a square is a quadratic residue for every p** (Section 2). **Sixth, the separator is whether a leaves 1 or 3 on division by 4 ——quadratic reciprocity, only for a leaving 1 on division by 4, fixes whether a is a non-residue by the remainder of p on division by a. There the two conditions become tied and the product of probabilities fails** (Section 4). **Keywords**: primitive root, Artin's conjecture, Artin's constant, quadratic reciprocity, Euler's criterion, quadratic non-residue.

Scope of this paper (scope note): **No new theorem or law is claimed——Artin's conjecture (1927), the estimate of the share of primes with a as a primitive root and its correction, that the estimate holds under the generalized Riemann hypothesis (Hooley, 1967), quadratic reciprocity and Euler's criterion are all known. How the estimate was found to fail in numerical computation and was corrected is set out in Moree's survey (2012).The conjecture is not proved——counting up to 2×10^6 proves nothing, and the generalized Riemann hypothesis is not entered.Negative a and a with square factors are not treated——of a with square factors, only the square a = 4 is looked at.Relation to earlier papers**: **Paper 513 checked quadratic reciprocity by counting lattice points——here it is counted that the same reciprocity ties two conditions together and makes the product of probabilities fail.Paper 603 applied Euler's criterion (a to the power (p−1)/2 modulo p) to composites and counted the bases that are fooled——here the same criterion decides whether a is a non-residue, and the count is split by the remainder of p on division by a.Paper 640 counted that the number of ways to write an even number as a sum of two primes carries multipliers set by divisibility by small primes——here the multiplier is set by the prime factors of a itself and appears only when a leaves 1 on division by 4.**What is added is **counting the share for ten values of a and lining it up against the estimate**, **counting the source of the correction directly as conditional shares of non-residues**, **showing as a contrast that for a leaving 3 on division by 4 the conditions are not tied**, and **lining up how the size of the correction is set by the prime factors of a**.

1. Notation and the Question

Setting: **in the world of remainders modulo a prime p, a is a primitive root when its powers produce every value from 1 to $p-1$. This is the same as $a^{(p-1)/q}$ not being 1 for any prime factor q of $p-1$.Estimating that the condition "not divisible by q" holds independently with probability $1-1/(q(q-1))$ for each prime q gives the share as the product $A=\prod_q(1-1/(q(q-1)))$.**

Question: **for which a does the independent estimate fail, and why?**

2. Counting the Share

Computation 2.1: **the 148932 primes $3\le p\le 2\times10^6$ were counted (checking first that the primitive roots of 7 are exactly 3 and 5). A was 0.373955826.The corrected estimate is $A(1-\mu(a)\prod_{q\mid a}1/(q^2-q-1))$ for square-free a leaving 1 on division by 4, A otherwise, and 0 for squares.**

a	share	estimate	difference (standard errors)
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

The standard error is about 0.001254, and the difference 0.019287 between $a = 5$ and $a = 2$ is 10.82 of them. The correction factor is $1 + 1/19 = 1.052632$ for $a = 5$, $1 + 1/155 = 1.006452$ for $a = 13$ and $1 - 1/205 = 0.995122$ for $a = 21$.

> **Observation 2.2**
>
> this is the core. The independent estimate fails only in cases like a = 5, and the correction fills the failure exactly.Only $a = 5$ lies more than 10 standard errors from the constant, and it differs from the corrected estimate by only -0.05 of one——the corrections for $a = 13$ and $a = 21$ are small and cannot be told apart in this range.

3. The Source of the Correction

Computation 3.1: the share for which a is a quadratic non-residue was counted separately by whether the remainder of p on division by a is 1 (decided by Euler's criterion $a^{(p-1)/2} \equiv -1$).

a	a modulo 4	p with remainder 1	other 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

For a leaving 1 on division by 4, the share among the other p matches the share of the $(a-1)/2$ non-residue remainders among the $a-2$ remainders other than 1, $(a-1)/(2(a-2))$: 0.666667 for $a=5$ and 0.545455 for $a=13$.

Observation 3.2

the failure comes from two conditions not being independent.Being a primitive root requires both that a is a quadratic non-residue (the condition for $q=2$) and that p does not leave 1 on division by a (the condition for $q=a$)——for $a=5$ the two are tied, one holding makes the other more likely, and so the share exceeds the product.

4. The Separator and What Is Not Said

Observation 4.1

the separator is whether a leaves 1 or 3 on division by 4.Quadratic reciprocity, only for a leaving 1 on division by 4, fixes whether a is a non-residue by the remainder of p on division by a——for a leaving 3, the remainder of p on division by 4 also enters, so the remainder on division by a alone does not decide it, and the conditions are not tied.

Observation 4.2

what is not said.Artin's conjecture is not proved, and the generalized Riemann hypothesis is not entered——corrections for negative a and for a with square factors other than squares are not treated.

5. Census and Closing

1. **constant 0.373955826; a = 2, 3, 6, 7 give 0.374292, 0.373623, 0.373958, 0.374422** (Computation 2.1): **independence fits.**
2. **a = 5 gives 0.393578, estimate 0.393638, difference 10.82 standard errors** (Computation 2.1): **the core.**
3. **for a = 5, 0.000000 and 0.666914** (Computation 3.1): **the conditions are tied.**
4. **one half for a = 3 and 7; 0.545794 for a = 13 (6/11 = 0.545455)** (Computation 3.1): **the remainder modulo 4.**
5. **a = 13 and 21 give 0.376611 and 0.372873** (Computation 2.1): **small corrections.**
6. **1 or 3 modulo 4** (Observation 4.1): **the separator; Papers 513, 603, 640.**

Closing: **Primitive roots break the independent estimate only when the square-free base leaves 1 on division by 4.Counting the primes up to 2×10^6, a = 2, 3, 6 and 7 matched the constant 0.373955826, and only a = 5, at 0.393578, lay 10.82 standard errors away, matching the corrected estimate 0.393638——among primes leaving 1 on division by 5, the share for which 5 is a non-residue is 0, and among the others 0.666914, so the two conditions are not independent. For a = 3 and 7 the share is one half whatever the remainder, and they are not tied.a = 13 has the same form (0 and 0.545794), but its correction, 1 + 1/155, is small and cannot be told apart in this range.The separator is whether a leaves 1 or 3 on division by 4.Placed among the earlier papers——Paper 513 counted reciprocity by lattice points, Paper 603 counted the bases fooled by Euler's criterion, and Paper 640 counted multipliers set by small primes. Here it was counted that reciprocity ties two conditions together and makes the product of probabilities fail.To be honest——whether infinitely many primes have a as a primitive root has not been proved for a single a.**

References

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. Yamagishi, Y. (2026). *An Act of Counting Turns Out to Prove a Theorem of Algebra* [Paper 513]. Zenodo. 10.5281/zenodo.22862214
4. Yamagishi, Y. (2026). *561 Passes Fermat's Test for Every Base Coprime to It* [Paper 603]. Zenodo.
5. Yamagishi, Y. (2026). *The Number of Ways to Write an Even Number as a Sum of Two Primes Differs About Twofold by Whether It Is Divisible by 3* [Paper 640]. Zenodo.

— *From thinking to syncing.* —

Yuuki YAMAGISHI (山岸 勇輝)

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