561 Passes Fermat's Test for Every Base Coprime to It

— $561 = 3 \times 11 \times 17$ passes Fermat's test for all 320 bases coprime to it — adding questions step by step cuts the fooling bases to 80 and then 10, the last asking whether the only numbers whose square is 1 are ± 1 — [Paper 603]

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

— *From thinking to syncing.* —

Abstract

If n is prime, a^{n-1} leaves remainder 1 on division by n for every a coprime to n (Fermat's little theorem).So one may judge whether a number looks prime by checking whether that remainder is 1 (Fermat's test).Here it is counted which composite numbers fool this test, and by how many bases.No new theorem or law is claimed. First, 561 passes the test for every coprime base——there are 320 bases coprime to $561 = 3 \times 11 \times 17$, and for all 320 the remainder is 1. Among the bases 1 to 560 that is a share of $\mathbf{0.571429}$; only the 240 bases ($\mathbf{0.428571}$) sharing one of 3, 11, 17 expose it (Section 2). **Second, such numbers are rare but do not run out——composite numbers passing the test for every coprime base (Carmichael numbers) number 1 up to 10^3, 7 up to 10^4, 16 up to 10^5 and 43 up to 10^6. The numbers found by trying every base and those given by a criterion using only the prime factors (Korselt's criterion) agreed without exception up to 10^5** (Section 2). **Third, adding questions reduces the fooling bases——for 561, asking also whether a^{280} equals the Jacobi symbol (Euler's test) leaves 80 fooling bases ($\mathbf{0.142857}$), and asking about the whole chain of squares (the Miller--Rabin test) leaves 10 ($\mathbf{0.017857}$)** (Section 3). **Fourth, and this is the core.What the last question looks at is whether the only numbers whose square is 1 are ± 1——modulo the prime 557, the numbers whose square leaves 1 are just 1 and 556; modulo 561 there are 8. With base 2, $2^{35}, 2^{70}, 2^{140}, 2^{280}$ leave $263, 166, 67, 1$ on division by 561, and 67, just before the 1, is a square root of 1 other than ± 1 and exposes 561** (Section 3). **Fifth, the separator is what is asked——Fermat asks only about the last term a^{n-1}; Euler asks about half that power and the Jacobi symbol; Miller--Rabin asks about every step of the chain of squares. The fooling bases fall from 320 to 80 to 10, and for Miller--Rabin no odd composite up to 10^4 had a fooling share above the bound $1/4$ (exactly $1/4$ for 9)** (Section 3). **Keywords**: Carmichael numbers, Fermat primality test, Miller-Rabin test, pseudoprime, primality testing.

Scope of this paper (scope note): No new theorem or law is claimed——Carmichael numbers (Carmichael, 1910), the criterion by prime factors (Korselt, 1899), Euler's test (Solovay and Strassen, 1977), the Miller--Rabin test and its bound $1/4$ (Miller, 1976; Rabin, 1980), and that there are infinitely many Carmichael numbers (Alford, Granville and Pomerance, 1994) are all known.The theorems are not proved——numbers up to 10^6 are counted, every base is tried up to 10^5, and all bases are counted for 561.It is not said that "every base" fools the test——only coprime bases fool it; bases sharing a prime factor expose it.Uses in cryptography and speed of computation are not treated.Relation to earlier papers: Paper 513 proved quadratic reciprocity by counting lattice points and wrote that if one asks about remainders, the remainder of $a^{(p-1)/2}$ on division by p gives the answer (Euler's criterion)——Euler's test here applies that criterion to composite numbers and counts how often it is fooled.What is added is counting and setting side by side all fooling bases of the three tests for 561, matching the route of trying every base with the route by prime factors up to 10^5, and placing the separator on what is asked and showing in numbers that the last question looks at the number of square roots of 1.

1. Notation and the Question

Setting: for an odd n and a base a ($1 \le a \le n-1$), three questions are asked.

Fermat's test: is the remainder of a^{n-1} on division by n equal to 1?

Euler's test: is a coprime to n, and does $a^{(n-1)/2}$ leave the Jacobi symbol (a/n) as remainder?

The Miller--Rabin test: writing $n-1 = 2^s d$ with d odd, is a^d equal to 1, or is one of $a^d, a^{2d}, \ldots, a^{2^{s-1}d}$ equal to $n-1$?

If n is prime, every test answers "looks prime" for every base.For a composite n, a base that makes a test answer "looks prime" is said to fool that test.

Question: is there a composite number that fools Fermat's test with every coprime base, how far do the fooling bases fall as questions are added, and what is at work?

2. Composite Numbers Passing Fermat's Test

Computation 2.1: composite numbers up to 10^6 were examined with the criterion using only prime factors (no square factor, and $p-1$ divides $n-1$ for every prime factor p).

range	composites passing for every coprime base
up to 10^3	1
up to 10^4	7
up to 10^5	16
up to 10^6	43

The first 16 are
$561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841, 29341, 41041, 46657, 52633, 62745, 63973, 75361$.
$561 = 3 \times 11 \times 17$ and $1729 = 7 \times 13 \times 19$, each a product of three distinct primes.

Computation 2.2: independently of the criterion, every coprime base was tried for every composite number up to 10^5 .16 composites passed, agreeing without exception with the 16 from the criterion.For comparison, odd composites fooling base 2 alone number 78 up to 10^5, and all 16 are among them.

Computation 2.3: for 561, all bases $a = 1, \ldots, 560$ were counted.There are 320 bases coprime to 561 ($320 = 2 \times 10 \times 16$), and for all 320 the remainder of a^{560} was 1, a share of $\mathbf{0.571429}$.The 240 bases ($\mathbf{0.428571}$) whose remainder was not 1 coincided exactly with those divisible by one of 3, 11, 17.

> **Observation 2.4**
>
> 561 is exposed only when a prime factor is hit.Since 560 is divisible by each of 2, 10 and 16, for coprime a the power a^{560} leaves remainder 1 on division by each of 3, 11 and 17, hence also by 561——to expose this number with Fermat's test one must draw a base containing a prime factor, which is close to guessing the factorisation.

3. Adding Questions

Computation 3.1: for 561, all bases fooling each of the three tests were counted ($n - 1 = 560 = 2^4 \times 35$).

test	fooling bases	share of the 560 bases
Fermat	320	**0.571429**
Euler	80	**0.142857**
Miller--Rabin	10	**0.017857**

The 10 bases fooling Miller--Rabin are $1, 50, 101, 103, 256, 305, 458, 460, 511, 560$.

Computation 3.2: the numbers whose square leaves 1 were counted.Modulo the prime 557 there were just 1 and 556; modulo 561 there were eight: $1, 67, 188, 254, 307, 373, 494, 560$.With base 2, the remainders of $2^{35}, 2^{70}, 2^{140}, 2^{280}, 2^{560}$ on division by 561 were $263, 166, 67, 1, 1$.

> **Observation 3.3**
>
> this is the core: what the last question looks at is whether the square roots of 1 are only ± 1.Modulo a prime, the only x with x^2 leaving 1 are 1 and $n-1$, so if the chain of squares reaches 1, the term just before must be 1 or $n-1$——for 561 the chain for base 2 reached 1 from 67. 67 is a square root of 1 other than ± 1, and that is the evidence of compositeness. Modulo 561 the square roots of 1 number $2^3 = 8$, choosing ± 1 for each of the three prime factors.

> **Observation 3.4**
>
> the separator is what is asked.Fermat asks only about the last term a^{n-1}; Euler asks whether half that power $a^{(n-1)/2}$ matches the Jacobi symbol; Miller--Rabin asks about every step of the chain——the fooling bases fell from 320 to 80 to 10. Each added question leaves a composite number fewer places to hide.

Computation 3.5: for every odd composite up to 10^4, the share of bases fooling Miller--Rabin was counted.The largest was 0.250000 for $n = 9$ (the two bases 1 and 8), and no number exceeded Rabin's bound $1/4$.The **0.017857** of 561 is 0.071429 times the bound.

Observation 3.6

no composite fools Miller--Rabin with every base.Fermat's test had 43 such numbers up to 10^6, but for Miller--Rabin the fooling bases are at most a quarter——so trying several bases multiplies the chance of missing by $1/4$ each time. With Fermat's test, a Carmichael number keeps being missed however often one tries, as long as the base drawn is coprime.

Observation 3.7

beside Paper 513.Paper 513 wrote that asking about remainders, the remainder of $a^{(p-1)/2}$ on division by p gives the answer (Euler's criterion)——that criterion is a fact about primes p; applied to composites, for 561 there are 80 bases that answer just as the criterion says. The criterion characterises primes only when seen from the side of the primes.

Observation 3.8

what is not said.Neither the infinitude of Carmichael numbers nor Rabin's bound is proved, and uses in cryptography and speed of computation are not treated——what is shown is the count up to 10^6, the agreement of two routes up to 10^5, and the comparison of three tests on 561.

4. Roll Call and Closing

1. **561 passes for all 320 coprime bases** (Computation 2.3): **share 0.571429.**
2. **the 240 exposing bases share a prime factor** (Computation 2.3): **share 0.428571.**
3. **43 Carmichael numbers up to 10^6** (Computation 2.1): **rare but not running out.**
4. **every base and the prime-factor criterion agree up to 10^5** (Computation 2.2): **two routes.**
5. **fooling bases 320, 80, 10** (Computation 3.1): **adding questions reduces them.**
6. **8 square roots of 1 modulo 561, 2 modulo 557** (Computation 3.2): **more with more prime factors.**
7. **the chain for base 2 is $263, 166, 67, 1$** (Computation 3.2): **67 exposes it.**
8. **the last question checks whether the square roots of 1 are only ± 1** (Observation 3.3): **the core.**
9. **the separator is what is asked** (Observation 3.4): **the last term, or every step.**
10. **Miller--Rabin fooling share at most $1/4$, exactly $1/4$ for 9** (Computation 3.5): **no number fools it with every base.**

Closing: **The test that checks whether a^{n-1} leaves remainder 1 on division by n always passes primes, but can pass composites too.$561 = 3 \times 11 \times 17$ passes it for all 320 coprime bases——only the 240 bases sharing a prime factor expose it, and there are 43 such numbers up to 10^6. The numbers found by trying every base and those given by the criterion using only prime factors agreed without exception up to 10^5.Adding questions, the fooling bases fall from 320 to 80 and then 10——what the last question (Miller--Rabin) looks at is whether the only numbers whose square is 1 are ± 1. There are 2 such numbers for the prime 557 and 8 for 561, and the 67 in the chain $263, 166, 67, 1$ for base 2 exposes 561.The separator is what is asked——a test asking only about the last term has composites that fool it with every base, while for the test asking about every step the fooling share did not exceed a quarter for any number up to 10^4.Placed among the earlier papers——Euler's criterion, written by Paper 513 from the side of the primes, when applied from the side of the composites lets 80 bases of 561 answer just as the criterion says.To be honest——the counts go only up to 10^6; neither the infinitude nor the bound is proved.**

References

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. Yamagishi, Y. (2026). *An Act of Counting Turns Out to Prove a Theorem of Algebra* [Paper 513]. Zenodo. 10.5281/zenodo.22862214

— *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)