

The Definition Divides d by p ; the Theorem Divides p by the Discriminant

— Quadratic Reciprocity: the Modulus Is Not Chosen, and the 4 and the 8 Share One Root — [Paper 166]

Yuuki YAMAGISHI (山岸 勇輝)

Yamagishi Complexity Torus Lab, Japan

August 2026

— *From thinking to syncing.* —

ABSTRACT

The definition of the Legendre symbol $(d | p)$ asks whether the remainder of d on division by p is a square. Yet the answer given by reciprocity is settled by the remainder of p on division by some other number. This paper measures that other number by exhaustive search, confirms it is the discriminant, and shows that the 4 and the 8 of the two supplements share one root. **NO NEW MATHEMATICAL THEOREM IS CLAIMED** — all of this is standard since Gauss. First, the law itself was verified from the definition. Over all 1830 pairs of odd primes below 300, $(p | q)(q | p) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}}$ held with **no failures**, and so did both supplements (Section 2). Second, and this is the core. For the primes below 20000, the smallest m such that $(d | p)$ depends only on $p \bmod m$ was found by exhaustive search. For all sixteen values of d tested, that smallest m was exactly $|\text{disc}(d)|$ (Section 3). Third, the separator is $d \bmod 4$. $4|d|$ is always a period but not always the smallest one — when $d \equiv 1 \pmod{4}$ the true modulus is a quarter of it (5 rather than 20 for $d = 5$; 13 rather than 52 for $d = 13$). The modulus is not a number chosen for convenience but one that is forced (Section 4). Fourth, the 4 of the first supplement and the 8 of the second are one reason, not two. Both are $|\text{disc}|$: it is 4 at $d = -1$ and 8 at $d = 2$ and at $d = -2$ (measured). This corpus usually separates roots; here it joins two that looked separate (Section 5). Fifth, the law still yields no root. At $p = 10^9 + 7$ reciprocity settles solvability in 5 steps while the square root itself takes 30, and Tonelli–Shanks begins by finding a non-residue. A theorem counts them; producing one is a search (Section 6).

Scope of this paper: **NO NEW MATHEMATICAL THEOREM IS CLAIMED** — quadratic reciprocity, the fact that the discriminant is the conductor, and the formulation as a Dirichlet character are all standard. Nor does this paper prove the law — what is offered is a measurement, not a proof. What is added is measuring the smallest period by exhaustive search and confirming that it matches the discriminant, exhibiting with a separator the cases in which $4|d|$ overshoots fourfold, and confirming that the 4 and the 8 of the supplements share one root. Confirming a shared root is rare in this corpus: after Paper 31 and Paper 142, this is the third time.

1. Notation and position

For an odd prime p and an integer d not divisible by p , let the Legendre symbol $(d \mid p)$ be $+1$ if d is a quadratic residue modulo p and -1 otherwise. For squarefree d write the **discriminant** as $\text{disc}(d) = d$ when $d \equiv 1 \pmod{4}$ and $\text{disc}(d) = 4d$ otherwise. Every symbol in this paper was computed from Euler's criterion $(d \mid p) \equiv d^{(p-1)/2} \pmod{p}$ — that is, without using reciprocity even once.

Position: Paper 86 took a census of the four roots by which a quantity comes to be fixed, and Paper 147 wrote that 4π is a period rather than a dimension. The modulus here is likewise a period, and likewise not chosen.

2. Verifying the law from the definition

Verification 2.1: For every pair of odd primes below 300, the symbols were computed from Euler's criterion and the two sides of the law compared.

claim	instances tested	failures
$(p \mid q)(q \mid p) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}}$	1830 pairs	0
$(-1 \mid p) = (-1)^{(p-1)/2}$	61 primes	0
$(2 \mid p) = (-1)^{(p^2-1)/8}$	61 primes	0

(QED)

Observation 2.2

Notice what the definition looks at. The definition of $(d \mid p)$ looks at the remainder of d on division by p — dividing p by anything appears nowhere in it. Yet the right-hand side above is written entirely in terms of p modulo 4 and q modulo 4.

3. The core: measuring the smallest period

Verification 3.1: For each squarefree d , the symbol was computed for every prime p below 20000 apart from 2 and the divisors of d , and the smallest m such that $(d \mid p)$ depends only on $p \bmod m$ was found by searching upward from $m = 1$.

d	$d \bmod 4$	smallest m	$ \text{disc}(d) $	$4 d $
-1	3	4	4	4
2	2	8	8	8
-2	2	8	8	8
3	3	12	12	12
-3	1	3	3	12
5	1	5	5	20
-5	3	20	20	20
6	2	24	24	24
7	3	28	28	28
13	1	13	13	52
17	1	17	17	68
-7	1	7	7	28
-11	1	11	11	44
21	1	21	21	84
29	1	29	29	116
-19	1	19	19	76

In all sixteen cases the smallest m was exactly $|\text{disc}(d)|$. (QED)

Observation 3.2

The definition divides d by p ; the theorem divides p by the discriminant. Nothing in the definition gives any reason for the answer to be periodic in p at all. Reciprocity is the assertion of that periodicity — the exchange of which side does the dividing is what the word “reciprocity” is pointing at.

Observation 3.3

That a period exists at all is the content of the law. The value of the period is only the question that comes next.

4. The separator is $d \bmod 4$

Verification 4.1: From the table above, take the ratio of $4|d|$ to the smallest m .

$d \bmod 4$	instances	$4 d \div$ smallest m
1	$-3, 5, 13, 17, -7, -11, 21, 29, -19$	4
2 or 3	$-1, 2, -2, 3, -5, 6, 7$	1

(QED)

Observation 4.2

$4|d|$ is always a period — but not always the smallest. Only when $d \equiv 1 \pmod{4}$ does the true modulus drop to a quarter of it. What must be moved for it to move is $d \bmod 4$, neither the size of d nor its sign.

Observation 4.3

So the modulus is not a number picked for convenience. Whether the factor of 4 is present is settled by $d \bmod 4$, and there is no room for choice — in the language of Paper 95, this lies on the side of fact, not of convention.

5. The 4 and the 8 are one reason, not two

Observation 5.1

The first supplement is a statement about $p \bmod 4$ and the second about $p \bmod 8$. Two different numbers appear to arrive for two different reasons.

Verification 5.2: Set the measurements side by side.

d	smallest m (measured)	$ \text{disc}(d) $	supplement
-1	4	4	first
2	8	8	second
-2	8	8	their product

Furthermore, collecting $(2 \mid p)$ by residue class of p modulo **8** over all odd primes below **20000**, the value is **+1** throughout for $p \equiv 1, 7$ and -1 throughout for $p \equiv 3, 5$, **with not a single class in which the values split.** (QED)

Observation 5.3

The **4** and the **8** share one root — both are $|\text{disc}|$, and only the value of d differs. The two supplements are not two theorems but one statement read at $d = -1$ and at $d = 2$.

Observation 5.4

This corpus usually says “one word, distinct roots”. Here it does the opposite — it gives one address to two numbers that had looked separate. After Paper 31 confirmed that the π of a solid angle and the π of a Gaussian integral share a root, and Paper 142 that Unruh's 2π and Hawking's do, this is the third such confirmation.

6. And still the law yields no root

Verification 6.1: The Jacobi symbol computed through reciprocity, using no exponentiation at all, set beside the construction of a square root by Tonelli–Shanks at the same prime.

p	$p \bmod 8$	deciding solvability	constructing a root
1000003	3	4 steps	20 steps
10000019	3	7 steps	24 steps
100000007	7	6 steps	27 steps
1000000007	7	5 steps	30 steps

In each case $x^2 \equiv a \pmod{p}$ was verified. (QED)

Observation 6.2

The gap is not only one of cost. Tonelli–Shanks begins by finding a non-residue — and it has no method for that other than trying 2, 3, 5, . . . in turn.

Verification 6.3: Counting the non-residues among 1 to 199.

p	non-residues among 1..199	smallest one
1000003	105	2
10000019	99	2
100000007	97	5

(QED)

Observation 6.4

A theorem gives the count — exactly half of the $p - 1$ nonzero classes are non-residues. But it names none of them. Counting is a theorem; producing one is a search — no deterministic polynomial-time method for the smallest non-residue is known.

Observation 6.5

This has the shape of Paper 163, which separated “a good code exists” from “here is a good code”. Reciprocity answers whether, never which. As in Paper 25, where “unsolvable” split three ways, the separator here is again which tools are allowed.

7. The census

Observation 7.1

statement	what divides what	what moves it	address
definition of $(d \mid p)$	d by p	d	computed per p
reciprocity	p by $ \text{disc}(d) $	$d \bmod 4$	period = discriminant
first supplement	p by 4	$d = -1$	$ \text{disc}(-1) = 4$
second supplement	p by 8	$d = 2$	$ \text{disc}(2) = 8$
constructing a root	—	which tools are allowed	a search, not a theorem

Observation 7.2

The definition and the theorem look at different things. The 4 and the 8 of the supplements are one root, and the modulus is not chosen. And knowing whether a root exists stays separate, to the end, from holding one.

8. Conclusion

1. The law and both supplements were verified from the definition (Ver. 2.1): 1830 pairs, 0 failures.
2. The smallest period is the discriminant (Ver. 3.1): $m = |\text{disc}(d)|$ for all sixteen values of d .
3. The separator is $d \bmod 4$ (Ver. 4.1): $4|d|$ overshoots fourfold when $d \equiv 1$.
4. The supplements' 4 and 8 share one root (Ver. 5.2): both are $|\text{disc}|$.

5. The law yields no root (Ver. 6.1, 6.3): 5 steps against 30, and a non-residue comes only from a search.

Closing: The definition divides d by p . The theorem divides p by the discriminant. Whether one can still be surprised that the direction of division changes hands is what separates having read this law from having recited it, and the discovery that the 4 and the 8 were one number all along is that surprise's small dividend.

References

1. Gauss, C. F. (1801). *Disquisitiones Arithmeticae*. Leipzig: Gerhard Fleischer.
2. Legendre, A.-M. (1798). *Essai sur la théorie des nombres*. Paris: Duprat.
3. Dirichlet, P. G. L. (1837). *Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält*. Abhandlungen der Königlich Preussischen Akademie der Wissenschaften.
4. Tonelli, A. (1891). *Bemerkung über die Auflösung quadratischer Congruenzen*. Göttinger Nachrichten.
5. Shanks, D. (1973). *Five number-theoretic algorithms*. Proceedings of the Second Manitoba Conference on Numerical Mathematics.
6. Ireland, K., & Rosen, M. (1990). *A Classical Introduction to Modern Number Theory* (2nd ed.). New York: Springer.
7. Yamagishi, Y. (2026). *The Equals Sign Has Distinct Roots Too* [Paper 16], 3rd ed. Zenodo. 10.5281/zenodo.21600471
8. Yamagishi, Y. (2026). *“Unsolvable” Has Three Distinct Roots* [Paper 25]. Zenodo. 10.5281/zenodo.22090297
9. Yamagishi, Y. (2026). *The π That Carries No Dimension* [Paper 31]. Zenodo. 10.5281/zenodo.22090430
10. Yamagishi, Y. (2026). *The Four Roots of Necessity* [Paper 86]. Zenodo. 10.5281/zenodo.21744839
11. Yamagishi, Y. (2026). *Convention and Fact* [Paper 95]. Zenodo. 10.5281/zenodo.21758621
12. Yamagishi, Y. (2026). *Move It, and Only the 2π Survives* [Paper 142]. Zenodo. 10.5281/zenodo.22082281
13. Yamagishi, Y. (2026). *The Same H^2 , and with Different Coefficients Nothing Is Quantised* [Paper 147]. Zenodo. 10.5281/zenodo.22083144
14. Yamagishi, Y. (2026). *The Same Character Table, and Still Not Isomorphic* [Paper 152]. Zenodo. 10.5281/zenodo.22084202
15. Yamagishi, Y. (2026). *“A Good Code Exists” and “Here Is a Good Code” Are Different Sentences* [Paper 163]. Zenodo. 10.5281/zenodo.22092677
16. Yamagishi, Y. (2026). *There Are Three Equivalence Principles* [Paper 165]. Zenodo. 10.5281/zenodo.22092957

— From thinking to syncing. —

Yuuki YAMAGISHI (山岸 勇輝)