Turkish Journal of Analysis and Number Theory, 2026, Vol. 14, No. 1, 23-28
Available online at http://pubs.sciepub.com/tjant/14/1/3
Published by Science and Education Publishing
DOI:10.12691/tjant-14-1-3

An Elementary Method for Determining the Quadratic Character of -1, 2, 3 and 5 Modulo Primes

Arto Adili[1,*], Adrian Naço[2], Lorena Kelo[1]

[1]Department of Mathematics and Physics, "Fan S. Noli" University, Korçë, Albania
[2]Department of Mathematics Engineering, Polytechnic University, Tirana, Albania
*Corresponding author: aadili@unkorce.edu.al

Received June 05, 2026; Revised July 07, 2026; Accepted July 14, 2026

Abstract We provide elementary proofs of the classical quadratic-residue criteria for -1, 2, 3, and 5 modulo odd primes. In addition, we determine the quadratic character of the integers a and b in the prime representations $p=a^2+b^2$ and $p=a^2+2b^2$. These results further illustrate the relationship between quadratic residues and binary quadratic forms.

Keywords: *Quadratic character, quadratic residue, quadratic non-residue, odd prime*

Cite This Article: Arto Adili, Adrian Naço, and Lorena Kelo, "An Elementary Method for Determining the Quadratic Character of -1, 2, 3 and 5 Modulo Primes." *Turkish Journal of Analysis and Number Theory*, vol. 14, no. 1 (2026): 23-28. doi: 10.12691/tjant-14-1-3.

1. Introduction

The quadratic character of the integers -1, 2, 3, and 5 modulo odd primes constitute classical topics in elementary number theory. These criteria are traditionally derived from the Law of Quadratic Reciprocity together with its supplementary laws and occupy a central place in the theory of quadratic residues. The corresponding results and their various proofs can be found in many classical and modern references on number theory.

Classical number theory provides explicit criteria for determining whether -1, 2, 3, and 5 are quadratic residues or quadratic non-residues modulo primes. Although these criteria are well known, their proofs can be approached from different perspectives, leading to a variety of techniques and arguments.

Historically, these results emerged gradually from the development of the theory of quadratic residues in the works of Euler, Legendre, and Gauss. Euler first studied special cases of quadratic residues in the 18th century, particularly in the period 1720–1750, identifying several concrete instances of quadratic behavior modulo primes. Later, in the late 18th century (around 1785), Legendre introduced a systematic treatment of quadratic residues and the notation of the Legendre symbol notation, laying the foundation for a more structured theory. The complete and unified formulation of these criteria was achieved by Gauss in his Disquisitiones Arithmeticae (1801), where the Law of Quadratic Reciprocity was proved and earlier partial results were fully generalized and unified.

The purpose of this paper is to present alternative elementary proofs of these quadratic-residue criteria. Our approach relies on elementary techniques from number theory. In this way, we provide alternative derivations of several classical results while remaining within an elementary framework.

Furthermore, we investigate the quadratic character of the coefficients appearing in the classical representations of prime numbers by binary quadratic forms. More precisely, for primes admitting representations of the form

$$p=a^2+b^2$$

and

$$p=a^2+2b^2$$

we determine the quadratic character of the integers a and b modulo p. These results further illustrate the close relationship between quadratic residues and the representation of primes by quadratic forms.

As is well known, for an odd prime p, there are exactly $\frac{p-1}{2}$ quadratic residues and $\frac{p-1}{2}$ quadratic non-residues modulo p. We denote by

$$R_p=\{r_1,r_2,\ldots,r_{\frac{p-1}{2}}\},$$

the set of quadratic residues, and by

$$N_p=\{n_1,n_2,\ldots,n_{\frac{p-1}{2}}\},$$

the set of quadratic non-residues modulo p.

We recall the following well-known results in elementary number theory, which will be used throughout the paper. These results admit elementary proofs in the literature, without the use of quadratic characters or the law of quadratic reciprocity.

Theorem 1.1. [1] *The product of two quadratic*

residues, or of two quadratic non-residues, modulo p, is a quadratic residue, whereas the product of a quadratic residue and a quadratic non-residue is a quadratic non-residue.

Theorem 1.2. [2] *An odd prime p is expressible as a sum of two squares if and only if $p \equiv 1 (\mathrm{mod}\, 4)$.*

Theorem 1.3. [3] *A positive integer n is properly representable as a sum of two squares if and only if the prime factors of n are all of the form $4k+1$, except for the prime 2, which may occurs to at most the first power.*

Theorem 1.4. [4] *For an odd prime p, we have:*

(a) $p = x^2 + 2y^2 \Leftrightarrow p \equiv 1, 3 (\mathrm{mod}\, 8)$.

(b) $p = x^2 + 3y^2 \Leftrightarrow p \equiv 1 (\mathrm{mod}\, 6)$.

(c) $p = x^2 + 5y^2 \Leftrightarrow p \equiv 1, 9 (\mathrm{mod}\, 20)$.

We conclude this section by presenting the following two theorems, which will be used in Section 3.

Theorem 1.5. [5] *Reciprocity law for Jacobi symbols. If u and v are positive odd integers with $(u, v) = 1$, then*

$$\left(\frac{u}{v}\right)\cdot\left(\frac{v}{u}\right) = (-1)^{\frac{(u-1)(v-1)}{4}}.$$

Theorem 1.6. [6] *(k-th power Residue Criterion) Let p be a prime and let $a \in \mathbb{Z}$ be coprime to p. Then a is a k-th power residue modulo p if and only if*

$$a^{\frac{p-1}{d}} \equiv 1 (\mathrm{mod}\, p)$$

where $d = \gcd(k, p-1)$.

2. Main Results

In this section, we present elementary proofs for determining the quadratic character of the integers -1, 2, 3 and 5 modulo primes. These results are classical in nature, but our approach provides alternative derivations based on elementary techniques from number theory, avoiding the use of the Law of Quadratic Reciprocity.

Theorem 2.1. *If p is an odd prime, then*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 (\mathrm{mod}\, 4), \\ -1 & \text{if } p \equiv 3 (\mathrm{mod}\, 4). \end{cases}$$

Proof. The proof is divided into two cases.

Case 1. $p \equiv 1 (\mathrm{mod}\, 4)$.

By Theorem 1.2, the prime p can be written as

$$p = a^2 + b^2,$$

where $1 \le a, b \le p-1$. Then we have

$$a^2 \equiv (-1)\cdot b^2 (\mathrm{mod}\, p).$$

Since $a^2, b^2 \in R_p$ and by Theorem 1.1. the product of two quadratic residues is a quadratic residue, it follows that

$$-1 \in R_p \Leftrightarrow \left(\frac{-1}{p}\right) = 1.$$

Case 2. $p \equiv 3 (\mathrm{mod}\, 4)$.

From Theorem 1.3 it follows that the congruence

$$1 + x^2 \equiv 0 (\mathrm{mod}\, p)$$

has no solution. Therefore, for every integer u

$$u^2 \not\equiv -1 (\mathrm{mod}\, p).$$

Hence, it is clear that

$$-1 \in N_p \Leftrightarrow \left(\frac{-1}{p}\right) = -1.$$

Theorem 2.2. *If p is an odd prime, then*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 (\mathrm{mod}\, 8), \\ -1 & \text{if } p \equiv \pm 3 (\mathrm{mod}\, 8). \end{cases}$$

Proof. The proof is divided into four cases.

Case 1. $p \equiv 1 (\mathrm{mod}\, 8)$.

By Theorem 2.1, the number -1 is a quadratic residue modulo p. Now, by Theorem 1.4 (a), the prime p can be written as

$$p = a^2 + 2b^2,$$

where $1 \le a, b \le p-1$. Then we have

$$a^2 \equiv (-1)\cdot 2 \cdot b^2 (\mathrm{mod}\, p).$$

Since $-1, a^2, b^2 \in R_p$, and by Theorem 1.1. the product of two quadratic residues is a quadratic residue modulo p, it follows that

$$2 \in R_p \Leftrightarrow \left(\frac{2}{p}\right) = 1.$$

Case 2. $p \equiv 3 (\mathrm{mod}\, 8)$.

By Theorem 2.1, the integer -1 is a quadratic non-residue modulo p. By Theorem 1.4. (a), we have $p = a^2 + 2b^2$, $1 \le a, b \le p-1$. From congruence

$$a^2 \equiv (-1)\cdot 2 \cdot b^2 (\mathrm{mod}\, p),$$

since $-1 \in N_p$, $a^2, b^2 \in R_p$, and taking into account that the product of a quadratic residues with a quadratic non-residue is a quadratic non-residue modulo p, it follows that

$$2 \in N_p \Leftrightarrow \left(\frac{2}{p}\right) = -1.$$

Case 3. $p \equiv 5 (\mathrm{mod}\, 8)$.

From Theorem 1.4. (a), it follows that the congruence

$$2 + x^2 \equiv 0 (\mathrm{mod}\, p)$$

has no solution. Then, for every $x \in \mathbb{Z}$, we obtain

$$x^2 \not\equiv -2 (\mathrm{mod}\, p).$$

Thus, we have $-2 \in N_p$. Since $-2 = (-1)\cdot 2$, $-1 \in R_p$ and the product of a quadratic residue and a quadratic non-residue is a quadratic non-residue modulo p, it follows that

$$2 \in N_p \quad \Leftrightarrow \quad \left(\frac{2}{p}\right) = -1.$$

Case 4. $p \equiv 7 \pmod 8$.

In the same way as in the case 3, we prove that $-2 \in N_p$. Since $-2 = (-1)\cdot 2$, $-1 \in N_p$ and the product of two quadratic non-residue is a quadratic residue modulo p, it follows that

$$2 \in R_p \quad \Leftrightarrow \quad \left(\frac{2}{p}\right) = 1.$$

Theorem 2.3. *If p is an odd prime, then*

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{12}, \\ -1 & \text{if } p \equiv \pm 5 \pmod{12}. \end{cases}$$

Proof. The proof is divided into four cases.

Case 1. $p \equiv 1 \pmod{12}$.

By Theorem 1.4. (b) the prime p can be written as

$$p = a^2 + 3b^2,$$

where $1 \le a, b \le p-1$. Then we have

$$a^2 \equiv (-1)\cdot 3 \cdot b^2 \pmod p.$$

From Theorem 2.1. we obtain $-1 \in R_p$. Since $a^2, b^2 \in R_p$ and by Theorem 1.1. the product of two quadratic residues is a quadratic residue modulo p, it follows that

$$3 \in R_p \quad \Leftrightarrow \quad \left(\frac{3}{p}\right) = 1.$$

Case 2. $p \equiv 5 \pmod{12}$.

From Theorem 1.4. (b), it follows that the congruence

$$3 + x^2 \equiv 0 \pmod p,$$

has no solution. Then, for every $x \in \mathbb{Z}$, we obtain

$$x^2 \not\equiv -3 \pmod p.$$

Thus, we have $-3 \in N_p$. Since $-3 = (-1)\cdot 3$, $-1 \in R_p$ and the product of a quadratic residue and a quadratic non-residue is a quadratic non-residue modulo p, it follows that

$$3 \in N_p \quad \Leftrightarrow \quad \left(\frac{3}{p}\right) = -1\cdot$$

Case 3. $p \equiv 7 \pmod{12}$.

In the same way as in part (a), we have $p = a^2 + 3b^2$, $1 \le a, b \le p-1$ and

$$a^2 \equiv (-1)\cdot 3 \cdot b^2 \pmod p.$$

From Theorem 2.1. we obtain $-1 \in N_p$. Since $a^2, b^2 \in R_p$ and by Theorem 1.1. the product of a quadratic residues with a quadratic non-residue is a quadratic non-residue modulo p, it follows that

$$3 \in N_p \quad \Leftrightarrow \quad \left(\frac{3}{p}\right) = -1\cdot$$

Case 4. $p \equiv 11 \pmod{12}$.

In the same way as in part (b), for every $x \in \mathbb{Z}$, we have

$$x^2 \not\equiv -3 \pmod p.$$

Thus, $-3 \in N_p$. Now, since $-3 = (-1)\cdot 3$, $-1 \in N_p$ and the product of a quadratic residue and a quadratic non-residue is a quadratic non-residue modulo p, it follows that

$$3 \in R_p \quad \Leftrightarrow \quad \left(\frac{3}{p}\right) = 1\cdot$$

Theorem 2.4. If p is an odd prime, then

$$\left(\frac{5}{p}\right) = \begin{cases} 1 & p \equiv \pm 1 \pmod 5, \\ -1 & p \equiv \pm 2 \pmod 5. \end{cases}$$

Proof. The odd prime $p \neq 5$ may take one of the forms

$$p \equiv \pm 1, \pm 3, \pm 7, \pm 9 \pmod{20}.$$

The proof is divided into four cases.

Case 1. $p \equiv 1, 9 \pmod{20}$.

By Theorem 2.1, the number -1 is a quadratic residue modulo p. Now, by Theorem 1.4. (c), the prime p can be written as

$$p = a^2 + 5b^2,$$

where $1 \le a, b \le p-1$. Then we have

$$a^2 \equiv (-1)\cdot 5 \cdot b^2 \pmod p.$$

Since $-1, a^2, b^2 \in R_p$, and by Theorem 1.1. the product of two quadratic residues is a quadratic residue modulo p, it follows that

$$5 \in R_p \quad \Leftrightarrow \quad \left(\frac{5}{p}\right) = 1\cdot$$

Case 2. $p \equiv 13, 17 \pmod{20}$.

By Theorem 2.1, we have $-1 \in R_p$. From Theorem 1.4. (c), it follows that the congruence

$$5 + x^2 \equiv 0 \pmod p,$$

has no solution. Then, for every $x \in \mathbb{Z}$, we obtain

$$x^2 \not\equiv -5 \pmod p.$$

Thus, we have $-5 \in N_p$. Since $-5 = (-1)\cdot 5$, $-1 \in R_p$ and the product of a quadratic residue and a quadratic non-residue is a quadratic non-residue modulo p, it follows that

$$5 \in N_p \quad \Leftrightarrow \quad \left(\frac{5}{p}\right) = -1.$$

Case 3. $p \equiv 11, 19 \pmod{20}$.

By Theorem 2.1, we have $-1 \in R_p$. From Theorem 1.4. (c), it follows that for every $x \in \mathbb{Z}$, $x^2 \not\equiv -5 \pmod{p}$, from which we obtain $-5 \in N_p$. Since $-5 = (-1)\cdot 5$, $-1 \in R_p$ and the product of a quadratic residue and a quadratic non-residue is a quadratic non-residue modulo p, it follows that

$$5 \in N_p \quad \Leftrightarrow \quad \left(\frac{5}{p}\right) = -1.$$

Case 4. $p \equiv 3, 7 \pmod{20}$.

By Theorem 2.1, we have $-1 \in N_p$. From Theorem 1.4. (c), it follows that for every $x \in \mathbb{Z}$, $x^2 \not\equiv -5 \pmod{p}$, that is $-5 \in N_p$. Since $-5 = (-1)\cdot 5$, $-1 \in N_p$ and the product of two quadratic non-residue is a quadratic residue modulo p, it follows that

$$5 \in R_p \quad \Leftrightarrow \quad \left(\frac{5}{p}\right) = 1.$$

Example 2.5. Let be the prime 241.

The quadratic character of -1 modulo 241. We have

$$241 = 60\cdot 4 + 1 \equiv 1 \pmod{4}$$

and

$$241 = 15^2 + 4^2.$$

It follows that

$$-1 \in R_{241} \quad \Leftrightarrow \quad \left(\frac{-1}{241}\right) = 1.$$

The quadratic character of 2 modulo 241. We have

$$241 = 30\cdot 8 + 1 \equiv 1 \pmod{8}$$

and

$$241 = 13^2 + 2\cdot 6^2.$$

It follows that

$$2 \in R_{241} \quad \Leftrightarrow \quad \left(\frac{2}{241}\right) = 1.$$

The quadratic character of 3 modulo 241. We have

$$241 = 40\cdot 6 + 1 \equiv 1 \pmod{6}$$

and

$$241 = 7^2 + 3\cdot 8^2.$$

It follows that

$$3 \in R_{241} \quad \Leftrightarrow \quad \left(\frac{3}{241}\right) = 1.$$

The quadratic character of 5 modulo 241. We have

$$241 = 12\cdot 20 + 1 \equiv 1 \pmod{20}$$

and

$$41 = 14^2 + 5\cdot 3^2.$$

It follows that

$$5 \in R_{241} \quad \Leftrightarrow \quad \left(\frac{5}{241}\right) = 1.$$

3. Quadratic Character of the Number a and b for Primes of the form $a^2 + b^2$ and $a^2 + 2b^2$

In this section, we determine the quadratic character of the natural numbers a and b in the representations of primes of the forms

$$p = a^2 + b^2$$

and

$$p = a^2 + 2b^2.$$

Theorem 3.1. *Let p be a prime with $p \equiv 1 \pmod{4}$, and let $a, b \in \mathbb{N}$ such that $p = a^2 + b^2$. Then*

(a) *If $p \equiv 1 \pmod{8}$, then $a, b \in R_p$.*

(b) If $p \equiv 5 \pmod{8}$, then the integers a and b have different quadratic characters modulo p.

Proof. Since $p = a^2 + b^2$, we have

$$2ab + p = (a+b)^2,$$

from which we obtain

$$2ab \equiv (a+b)^2 \pmod{p}.$$

Thus, the number $2ab$ is a quadratic residue modulo p.

(a) $p \equiv 1 \pmod{8}$. From Theorem 2.2. we have $2 \in R_p$. Since the product of two quadratic residues is a quadratic residue modulo p, it follows that $ab \in R_p$.

It is clear that the integers a and b have different parity. Without loss of generality, suppose that a is odd. Since $p = a^2 + b^2$ and $(a, p) = 1$, we have

$$p \equiv b^2 \pmod{a},$$

which shows that

$$\left(\frac{p}{a}\right) = 1.$$

Based on Theorem 1.5, we have

$$\left(\frac{p}{a}\right)\cdot\left(\frac{a}{p}\right) = (-1)^{\frac{(a-1)(p-1)}{4}} = 1,$$

from which it follows that

$$\left(\frac{a}{p}\right) = 1.$$

Finally, since $a \in R_p$ and $ab \in R_p$, it follows that $b \in R_p$.

(b) $p \equiv 5 \pmod{8}$. From Theorem 2.2. we have $2 \in N_p$. Since $2ab \in R_p$ and the product of a quadratic residue

with a quadratic non-residue is a quadratic non-residue, it follows that $ab \in N_p$. Now, it is clear that the integers a and b have different quadratic characters modulo p.

Example 3.2. For the prime $17 \equiv 1 (\mathrm{mod}\, 8)$, we are in the setting of Theorem 3.1 (a). We have

$$17 = 1^2 + 4^2,$$

and also

$$1, 4 \in R_{17} = \{1, 2, 4, 8, 9, 15, 16\}.$$

For the prime $13 \equiv 5 (\mathrm{mod}\, 8)$, we are in the setting of Theorem 3.1 (b). We have

$$13 = 2^2 + 3^2,$$

and also

$$3 \in R_{13} = \{1, 3, 4, 9, 10, 12\},$$

and

$$2 \in N_{13} = \{2, 5, 6, 7, 8, 11\}.$$

Theorem 3.3. *Let p be a prime with $p \equiv 1 (\mathrm{mod}\, 8)$ and let $a, b \in \mathbb{N}$ such that $p = a^2 + 2b^2$. Then*

(a) *If* $\left(\frac{2}{p}\right)_4 = 1$, *then* $a, b \in R_p$.

(b) *If* $\left(\frac{2}{p}\right)_4 = -1$, *then* $a \in N_p$ *and* $b \in R_p$.

Proof. We first show that $b \in R_p$. Taking into account that, by Theorem 2.2, $2 \in R_p$, in order to prove that b is a quadratic residue, it suffices to prove that every odd prime divisor q of b is a quadratic residue modulo p. Since

$$p = a^2 + 2b^2,$$

it follows that

$$p \equiv a^2 (\mathrm{mod}\, q).$$

Thus, p is a quadratic residue modulo q, so

$$\left(\frac{p}{q}\right) = 1.$$

Now, since $p \equiv 1 (\mathrm{mod}\, 8)$, we also have $p \equiv 1 (\mathrm{mod}\, 4)$ and by the Law of Quadratic Reciprocity, we obtain

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = 1.$$

Thus, the odd prime q is a quadratic residue modulo p. Finally, since the product of quadratic residues is again a quadratic residue, it follows that b is a quadratic residue modulo p.

By Theorem 2.2, we have $2 \in R_p$. It follows that, there exists an integer u such that $u^2 \equiv 2 (\mathrm{mod}\, p)$. Since $p = a^2 + 2b^2$, we have

$$p + 2uab = a^2 + u^2 b^2 + 2uab = (a + ub)^2,$$

from which we obtain

$$2uab \equiv (a + ub)^2 (\mathrm{mod}\, p).$$

This shows that $2uab \in R_p$. Since $2 \in R_p$, it follows that

$$u \cdot ab \in R_p.$$

(a) If $\left(\frac{2}{p}\right)_4 = 1$, then, 2 is a quartic residue modulo p. Hence, u is a quadratic residue modulo p. Thus, since $u \in R_p$ and $b \in R_p$, it follows that $a \in R_p$.

(b) If $\left(\frac{2}{p}\right)_4 = -1$, then, 2 is a quartic non-residue modulo p. Hence, u is a quadratic non-residue modulo p. Thus, from $u \in N_p$ and $b \in R_p$, it follows that $a \in N_p$.

Note. Following Ireland and Rosen [7], the quartic residue character of integer 2 modulo an odd prime p can be characterized in terms of representations of p by the quadratic form $x^2 + 64y^2$. More precisely, 2 is a quartic residue modulo p if and only if

$$p = x^2 + 64y^2$$

for some integers x, y.

Thus, the condition

$$\left(\frac{2}{p}\right)_4 = 1,$$

in Theorem 3.3. which shows that the number 2 is a fourth power residue modulo p, can be replaced by the condition stated above.

Let now p be a prime with $p \equiv 3 (\mathrm{mod}\, 8)$ and let $a, b \in \mathbb{N}$ such that $p = a^2 + 2b^2$. As illustrated by the following example, the integers a and b may occur in any of the following four cases:

$$(a, b) \in R_p \times R_p,$$

$$(a, b) \in R_p \times N_p,$$

$$(a, b) \in N_p \times R_p,$$

$$(a, b) \in N_p \times N_p.$$

Example 3.4. For the prime $83 \equiv 3 (\mathrm{mod}\, 8)$ we have

$$83 = 9^2 + 2 \cdot 1^2,$$

and also $1, 9 \in R_p$.

For the prime $43 \equiv 3 (\mathrm{mod}\, 8)$ we have

$$43 = 5^2 + 2 \cdot 3^2,$$

and also $5 \in R_p$ and $3 \in R_p$.

For the prime $691 = 8 \cdot 86 + 3 \equiv 3 (\mathrm{mod}\, 8)$ we have

$$691 = 23^2 + 2 \cdot 9^2,$$

and also $23 \in N_p$ and $9 \in R_p$.

For the prime $67 = 8 \cdot 8 + 3 \equiv 3 (\mathrm{mod} 8)$ we have

$$67 = 7^2 + 2 \cdot 3^2,$$

and also $3, 7 \in N_p$.

We conclude by giving a theoretical description of the cases considered above for the integers a and b.
Let us first show that

$$\left(\frac{-2}{p} \right)_4 = 1.$$

From Theorems 2.1. and 2.2, we have $-1, 2 \in N_p$, from which we obtain $-2 \in R_p$, that is $(-2)^{\frac{p-1}{2}} \equiv 1 (\mathrm{mod}\, p)$. Let us denote $p = 8k + 3$ for some integer k. We have

$$\gcd(4,\ p-1) = \gcd(4, 8k+2) = 2$$

and

$$(-2)^{\frac{p-1}{\gcd(4,\ p-1)}} = (-2)^{\frac{p-1}{2}} \equiv 1 (\mathrm{mod}\, p).$$

Therefore, by Theorem 1.6, -2 is a fourth-power residue modulo p.
Now, let us denote by v an integer such that

$$v^4 \equiv -2 (\mathrm{mod}\, p).$$

From the equality $p = a^2 + 2b^2$, we have:

$$a^2 = -2b^2 \equiv v^4 b^2 \equiv (v^2 b)^2 (\mathrm{mod}\, p),$$

from which we obtain

$$a \equiv v^2 b (\mathrm{mod}\, p) \text{ or } a \equiv -v^2 b (\mathrm{mod}\, p).$$

If $a \equiv v^2 b (\mathrm{mod}\, p)$, then for the integers a and b, the cases $a, b \in R_p$ and $a, b \in N_p$ may occur, since the product of two quadratic residues is a quadratic residue, and the product of a quadratic residue and a quadratic non-residue is a quadratic non-residue modulo p.

If $a \equiv -v^2 b (\mathrm{mod}\, p)$, then for the integers a and b, the cases $(a, b) \in R_p \times N_p$ and $(a, b) \in N_p \times R_p$ may occur, since product of a quadratic residue and a quadratic non-residue is a quadratic non-residue modulo p.

References

[1] Hardy G. H., Wright E. M. (1959): An Introduction to the Theory of Numbers, Fourth Edition, Oxford University Press (The. 85, pg. 69).

[2] Burton D. M. (2011): Elementary Number Theory, 7th Edition, Mc Graw-Hill (The. 13.2, pg. 265).

[3] Niven I., Zuckerman H. S., Montgomery H. L. (1991): An Introduction to Theory of Number, Fifth Edition, John Wiley & Sons, Inc (The. 3.20, pg. 164).

[4] Cox D. A. (1989): Primes of the form x^2+ny^2, Fermat, Class Field Theory and Complex Multiplication, John Wiley & Sons, Inc.

[5] Apostol T.M. (1976): Introduction to Analytic Number Theory, Springer-Verlag (The. 9.11. pg. 189).

[6] Al-Faisal F. (2024): PMATH 340 Elementary Number Theory, Spring, Canada. (Theorem 19.9, pg. 105).

[7] Ireland K., Rosen M. (1990): A Classical Introduction to Modern Number Theory, Second Edition, Springer-Verlag.