A Theorem on Quadratic Residues

Julian Debes - Benjamin Selles

April 13, 2025

Abstract

In this article, we will present a new theorem that we have discovered in the field of number theory, specifically on quadratic residues. The goal is to find some properties of prime numbers and congruences. First, we will introduce some definitions and theorems that will be used in the proof of our result. We will then proceed to prove our theorem and provide some examples. Finally, we present two additional theorems (without proof) that yield results similar to ours.

1 Preliminary Results

Definition 1 (Legendre Symbol)**.** *Let p be an odd prime number, and a an integer not divisible by p. The Legendre symbol $\left(\frac{a}{p}\right)$ is the integer that equals* 1 *if a is a quadratic residue modulo p, and* -1 *otherwise.*

We have the following classical result (which we will not prove):

Theorem 1. *Let p be an odd prime number, and a an integer not divisible by p. Then:*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

Gauss's lemma provides another method to determine whether an integer is a quadratic residue modulo an odd prime p.

Let us start by introducing some notation. Let p be an odd prime, and m an integer not divisible by p. Note that the integers $m, 2m, \ldots, \frac{p-1}{2}m$ are all not divisible by p, and are pairwise incongruent modulo p (indeed, if $km \equiv \ell m \pmod{p}$, with $1 \leq k < \ell < p$, then p divides $(\ell - k)m$, so p divides m or $\ell - k$, which is impossible). Therefore, their residues modulo p are $\frac{p-1}{2}$ distinct integers in $\{1, \ldots, p-1\}$. Let $r_1, r_2, \ldots, r_\lambda$ be the residues that are strictly less than $\frac{p}{2}$ (i.e., between 1 and $\frac{p-1}{2}$), and $r'_1, \ldots, r'_\mu$ those that are strictly greater than $\frac{p}{2}$ (i.e., between $\frac{p+1}{2}$ and $p-1$). The various integers r_i and r'_i are pairwise distinct, and we have $\lambda + \mu = \frac{p-1}{2}$.

For k an integer between 1 and μ, let $s_k = p - r'_k$. Then the integers $s_1, \ldots, s_\mu$ are distinct and all between 1 and $\frac{p-1}{2}$.

Let us show that the sets $\{r_1, \dots, r_\lambda\}$ and $\{s_1, \dots, s_\mu\}$ are disjoint. Suppose, by contradiction, that $r_k = s_\ell$ for some integers k and ℓ. We can find integers a and b between 1 and $\frac{p-1}{2}$ such that $am \equiv r_k \pmod{p}$ and $bm \equiv r'_\ell \pmod{p}$. By hypothesis, $r_k = p - r'_\ell$, so p divides $r_k + r'_\ell$. We deduce:

$$am + bm \equiv r_k + r'_\ell \equiv 0 \pmod{p},$$

so p divides $m(a+b)$. Since p is prime and does not divide m, it follows that p divides $a + b$, which is impossible because $2 \leq a + b \leq p - 1$.

Thus, $\{r_1, \dots, r_\lambda\}$ and $\{s_1, \dots, s_\mu\}$ are two disjoint subsets of $\{1, \dots, \frac{p-1}{2}\}$, whose union has cardinality $\lambda + \mu = \frac{p-1}{2}$, which immediately implies, due to cardinality, that:

$$\{1, \dots, \frac{p-1}{2}\} = \{r_1, \dots, r_\lambda, s_1, \dots, s_\mu\}.$$

The product of the elements of $\{1, \dots, \frac{p-1}{2}\}$ is, on one hand, $1 \times 2 \times \cdots \times \frac{p-1}{2}$, that is, $\left(\frac{p-1}{2}\right)!$, and on the other hand, it is equal to $r_1 \times \cdots \times r_\lambda \times s_1 \times \cdots \times s_\mu$. We thus have:

$$r_1 \times \cdots \times r_\lambda \times s_1 \times \cdots \times s_\mu = \left(\frac{p-1}{2}\right)!.$$

Moreover, by definition of r_k and r'_ℓ, we have:

$$\begin{aligned} m \times (2m) \times \ldots \times \frac{p-1}{2}m &\equiv r_1 \times \ldots \times r_\lambda \times r'_1 \times \ldots \times r'_\mu \pmod{p} \\ &\equiv r_1 \times \ldots \times r_\lambda \times (p - s_1) \times \ldots \times (p - s_\mu) \pmod{p} \\ &\equiv r_1 \times \ldots \times r_\lambda \times (-s_1) \times \ldots \times (-s_\mu) \pmod{p} \\ &\equiv (-1)^\mu r_1 \times \ldots \times r_\lambda \times s_1 \times \ldots \times s_\mu \pmod{p}. \end{aligned}$$

We also have:

$$m \times (2m) \times \ldots \times \frac{p-1}{2}m = m^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)!.$$

We deduce immediately that:

$$m^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv (-1)^\mu \left(\frac{p-1}{2}\right)! \pmod{p},$$

so p divides $\left(\frac{p-1}{2}\right)!(m^{\frac{p-1}{2}} - (-1)^\mu)$. Since p does not divide $\left(\frac{p-1}{2}\right)!$, and p is prime, p divides $m^{\frac{p-1}{2}} - (-1)^\mu$. We deduce, using the previous theorem:

$$(-1)^\mu \equiv m^{\frac{p-1}{2}} \equiv \left(\frac{m}{p}\right) \pmod{p},$$

which implies, since $\left(\frac{m}{p}\right)$ and $(-1)^\mu$ are either 1 or -1:

$$\left(\frac{m}{p}\right) = (-1)^{\mu}.$$

In summary, we have:

Theorem 2 (Gauss's Lemma). *With the previous notations, we have $\left(\frac{m}{p}\right) = (-1)^{\mu}$, where μ is the number of residues modulo p of the integers $m, 2m, \dots, \frac{p-1}{2}m$ that are strictly greater than $\frac{p}{2}$. In other words, m is a quadratic residue modulo p if and only if μ is even.*

Let us illustrate the use of Gauss's lemma. Let us prove the following result:

Proposition 1. *Let p be an odd prime number at least equal to 5. If p is of the form $6n+1$, then -3 is a quadratic residue modulo p. If p is of the form $6n+5$, -3 is not a quadratic residue modulo p.*

Proof. (By Hardy and Wright) Note that an odd prime greater than 5 is necessarily of the form $6n+1$ or $6n+5$.

Let $[x]$ denote the integer part of a real number x. Recall that $[x] \leq x < [x]+1$ for any real x.

Here, $m = -3$, and we consider the residues modulo p of the integers $-3a$, with $1 \leq a \leq \frac{p-1}{2}$. We distinguish several cases:

- If $1 \leq a \leq \frac{p}{6}$, then $-\frac{p}{2} \leq -3a \leq -3$, so $\frac{p}{2} \leq p-3a \leq p-3 < p$. We deduce that the residue of $-3a$ is $p-3a$ (this integer is obviously congruent to $-3a$ modulo p and belongs to $[\frac{p}{2}, p]$). The integers a such that $1 \leq a \leq \frac{p}{6}$ are the integers $1, 2, \dots, [\frac{p}{6}]$, so there are $[\frac{p}{6}]$ of them.
- If $\frac{p}{6} < a < \frac{p}{3}$, then $-p < -3a < -\frac{p}{2}$, and $0 < p-3a < \frac{p}{2}$, so the residue of a modulo p is still $p-3a$, and this residue is strictly less than $\frac{p}{2}$.
- Finally, if $\frac{p}{3} < a < \frac{p}{2}$, then $-\frac{3p}{2} < -3a < -p$, and $\frac{p}{2} < 2p-3a < p$, so the residue of a modulo p is $2p-3a$, and this residue is strictly greater than $\frac{p}{2}$. The integers a such that $\frac{p}{3} < a < \frac{p}{2}$ are the natural numbers between $[\frac{p}{3}]+1$ (since $\frac{p}{3}$ is not an integer) and $[\frac{p}{2}]$ (since $\frac{p}{2}$ is not an integer). There are therefore $[\frac{p}{2}] - [\frac{p}{3}]$ of them.

All cases have been considered since $\frac{p}{2}$ and $\frac{p}{3}$ are not integers.

With the notations of the previous theorem, we have:

$$\mu = \left[\frac{p}{6}\right] + \left[\frac{p}{2}\right] - \left[\frac{p}{3}\right].$$

If p is of the form $p = 6n+1$, with n an integer, then $[\frac{p}{6}] = n$, $[\frac{p}{2}] = 3n$, and $[\frac{p}{3}] = 2n$, so $\mu = 2n$. In this case, μ is even, and -3 is a quadratic residue modulo p.

If p is of the form $p = 6n+5$, with n an integer, then $[\frac{p}{6}] = n$, $[\frac{p}{2}] = 3n+2$, and $[\frac{p}{3}] = 2n+1$, so $\mu = 2n+1$. In this case, μ is odd, and -3 is not a quadratic residue modulo p.

We can similarly prove the following results:

- The integer 2 is a quadratic residue modulo a prime of the form $8n \pm 1$, and is not a quadratic residue modulo a prime of the form $8n \pm 3$.
- The integer 5 is a quadratic residue modulo a prime of the form $10n \pm 1$, and is not a quadratic residue modulo a prime of the form $10n \pm 3$.

□

2 Quadratic Residuosity

We now present our main result.

Theorem 3. *Let α, β, and k be non-zero natural numbers. Suppose that $\beta \leq k\alpha$ and that $p = 2k\alpha + \beta$ and $q = 2k\alpha - \beta$ are prime numbers. Then α is a quadratic residue modulo p if and only if α is a quadratic residue modulo q.*

Example 1. *With $\alpha = 6$, $\beta = 5$, and $k = 2$, we obtain $p = 2k\alpha + \beta = 29$, $q = 2k\alpha - \beta = 19$, which are indeed prime. We see that 6 is a quadratic residue modulo 19 (since 6 is congruent modulo 19 to $25 = 5^2$).*

We deduce that 6 is also a quadratic residue modulo 29, without calculation (we indeed have $6 \equiv 64 = 8^2 \pmod{29}$).

Proof. We will apply Gauss's lemma. Let μ be the number of integers among $\alpha, 2\alpha, \ldots, \frac{p-1}{2}\alpha$ whose residue modulo p is strictly greater than $\frac{p}{2}$, and ν the number of integers among $\alpha, 2\alpha, \ldots, \frac{q-1}{2}\alpha$ whose residue modulo q is strictly greater than $\frac{q}{2}$. According to Gauss's lemma, we need to show that μ and ν have the same parity (i.e., they are congruent modulo 2).

We will start by finding an expression for μ and ν.

For m an integer between 0 and $\alpha - 1$, let E_m be the set of natural numbers j such that $\left[\frac{mp}{2\alpha}\right] + 1 \leq j \leq \left[\frac{(m+1)p}{2\alpha}\right]$.

The various sets $E_0, E_1, \ldots, E_{\alpha-1}$ are pairwise disjoint, and their union is $\{1, 2, \ldots, \frac{p-1}{2}\}$. Let m be a natural number, and j an integer such that $\left[\frac{mp}{2\alpha}\right] + 1 \leq j \leq \left[\frac{(m+1)p}{2\alpha}\right]$. We distinguish two cases:

- If m is odd, write $m = 2\ell + 1$, with ℓ an integer. We then have $\frac{(2\ell+1)p}{2\alpha} < j \leq \frac{(2\ell+2)p}{2\alpha}$, which gives:

$$\left(\ell + \frac{1}{2}\right) p < j\alpha \leq (\ell + 1)p,$$

or $\frac{p}{2} < j\alpha - \ell p \leq p$ (and the second inequality is strict since p does not divide $j\alpha$). We deduce that the residue of $j\alpha$ modulo p is $j\alpha - \ell p$ (this integer is obviously congruent modulo p to $j\alpha$ and belongs to $\{1, \ldots, p-1\}$), and that this residue is strictly greater than $\frac{p}{2}$.

- If m is even, write $m = 2\ell$. We have $\frac{2\ell p}{2\alpha} < j \leq \frac{(2\ell+1)p}{2\alpha}$, which gives:

$$\ell p < j\alpha \leq \ell p + \frac{p}{2}.$$

We deduce that the residue of $j\alpha$ modulo p is $j\alpha - \ell p$, and that this residue is (strictly) less than $\frac{p}{2}$.

It follows that the integers among $\alpha, 2\alpha, \ldots, \frac{p-1}{2}\alpha$ whose residue modulo p is strictly greater than $\frac{p}{2}$ are those that belong to one of the E_m, with m odd.

Similarly, if we denote, for m an integer between 0 and $\alpha - 1$, F_m the set of natural numbers j such that $\left[\frac{mq}{2\alpha}\right] + 1 \leq j \leq \left[\frac{(m+1)q}{2\alpha}\right]$, then the integers among $\alpha, 2\alpha, \ldots, \frac{q-1}{2}\alpha$ whose residue modulo q is strictly greater than $\frac{p}{2}$ are those that belong to one of the F_m, with m odd.

We then reason based on the parity of α (the number of sets E_m or F_m involved depends on this).

First Case: α is odd.

From the above, the set of integers among $\alpha, 2\alpha, \ldots, \frac{p-1}{2}\alpha$ whose residue modulo p is strictly greater than $\frac{p}{2}$ is $E_1 \cup E_3 \cup \ldots \cup E_{\alpha-2}$, and we deduce that:

$$\begin{aligned}\mu &= \text{Card } E_1 + \text{Card } E_3 + \cdots + \text{Card } E_{\alpha-2} \\ &= \left(\left[\frac{2p}{2\alpha}\right] - \left[\frac{p}{2\alpha}\right]\right) + \left(\left[\frac{4p}{2\alpha}\right] - \left[\frac{3p}{2\alpha}\right]\right) + \cdots + \left(\left[\frac{(\alpha-1)p}{2\alpha}\right] - \left[\frac{(\alpha-2)p}{2\alpha}\right]\right)\end{aligned}$$

It is clear that for any integer x, x and $-x$ are congruent modulo 2. We thus have:

$$\mu \equiv \sum_{m=1}^{\alpha-1} \left[\frac{mp}{2\alpha}\right] \pmod{2}.$$

Similarly, we obtain:

$$\nu \equiv \sum_{m=1}^{\alpha-1} \left[\frac{mq}{2\alpha}\right] \pmod{2}.$$

Recall that $p = 2k\alpha + \beta$. For any integer m between 1 and $\alpha - 1$, and taking into account that $[n + x] = n + [x]$ for any integer n and real x:

$$\left[\frac{mp}{2\alpha}\right] = km + \left[\frac{m\beta}{2\alpha}\right],$$

which gives:

$$\mu \equiv k \sum_{m=1}^{\alpha-1} m + \sum_{m=1}^{\alpha-1} \left[\frac{m\beta}{2\alpha}\right] \pmod{2}.$$

Similarly, taking into account that $q = 2k\alpha - \beta$, we have:

$$\nu \equiv k \sum_{m=1}^{\alpha-1} m + \sum_{m=1}^{\alpha-1} \left[-\frac{m\beta}{2\alpha}\right] \pmod{2}.$$

Now, for any integer m between 1 and $\alpha - 1$, the real number $\frac{m\beta}{2\alpha}$ is not an integer: if it were, since $\beta = p - 2k\alpha$, $\frac{mp}{2\alpha}$ would be an integer, so we could write $mp = 2\alpha n$ with n an integer; m would necessarily be even (since p is odd), so we write $m = 2m'$, and we obtain $m'p = n\alpha$. Since p is prime and does not divide α, p must divide n, so we have an equality of the form $m' = \ell\alpha$, with ℓ an integer, which is impossible because m' is between 1 and $\frac{\alpha-1}{2}$.

Moreover, if x is a non-integer real number, it is clear that $[-x] = -1 - [x]$.

We deduce from all this that:

$$\sum_{m=1}^{\alpha-1} \left[-\frac{m\beta}{2\alpha}\right] = \sum_{m=1}^{\alpha-1} \left(-1 - \left[\frac{m\beta}{2\alpha}\right]\right)$$

$$\equiv \sum_{m=1}^{\alpha-1} \left(1 + \left[\frac{m\beta}{2\alpha}\right]\right) \pmod 2$$

$$\equiv \alpha - 1 + \sum_{m=1}^{\alpha-1} \left[\frac{m\beta}{2\alpha}\right] \pmod 2$$

$$\equiv \sum_{m=1}^{\alpha-1} \left[\frac{m\beta}{2\alpha}\right] \pmod 2, \quad \text{since } \alpha - 1 \text{ is even.}$$

We immediately deduce that μ and ν are congruent modulo 2.

Second Case: α is even.

This is almost the same. This time, the set of integers among $\alpha, 2\alpha, \dots, \frac{p-1}{2}\alpha$ whose residue modulo p is strictly greater than $\frac{p}{2}$ is $E_1 \cup E_3 \cup \dots \cup E_{\alpha-1}$, and we obtain:

$$\mu = \left(\left[\frac{2p}{2\alpha}\right] - \left[\frac{p}{2\alpha}\right]\right) + \left(\left[\frac{4p}{2\alpha}\right] - \left[\frac{3p}{2\alpha}\right]\right) + \dots + \left(\left[\frac{\alpha p}{2\alpha}\right] - \left[\frac{(\alpha-1)p}{2\alpha}\right]\right).$$

Thus, modulo 2:

$$\mu \equiv \sum_{m=1}^{\alpha} \left[\frac{mp}{2\alpha}\right] \pmod 2.$$

Taking into account that $p = 2k\alpha + \beta$, we have:

$$\mu \equiv k \sum_{m=1}^{\alpha} m + \sum_{m=1}^{\alpha} \left[\frac{m\beta}{2\alpha}\right] \pmod 2.$$

Similarly, as in the first case:

$$\nu \equiv k \sum_{m=1}^{\alpha} m + \sum_{m=1}^{\alpha} \left[-\frac{m\beta}{2\alpha}\right] \pmod 2$$

$$
\begin{aligned}
&\equiv k\sum_{m=1}^{\alpha} m+\sum_{m=1}^{\alpha}\left(-1-\left[\frac{m\beta}{2\alpha}\right]\right) \pmod 2\\
&\equiv k\sum_{m=1}^{\alpha} m+\sum_{m=1}^{\alpha}\left(1+\left[\frac{m\beta}{2\alpha}\right]\right) \pmod 2\\
&\equiv k\sum_{m=1}^{\alpha} m+\alpha+\sum_{m=1}^{\alpha}\left[\frac{m\beta}{2\alpha}\right] \pmod 2\\
&\equiv k\sum_{m=1}^{\alpha} m+\sum_{m=1}^{\alpha}\left[\frac{m\beta}{2\alpha}\right] \pmod 2, \quad \text{since } \alpha \text{ is even}\\
&\equiv \mu \pmod 2.
\end{aligned}
$$

The theorem is proven. □

Theorem 4. *Let α, β, and k be non-zero natural numbers. Suppose that $\beta \leq k\alpha$ and that $p = 2k\alpha + \beta$ and $q = 2k\alpha - \beta$ are prime numbers. Then $-\alpha$ is a quadratic residue modulo p if and only if $-\alpha$ is not a quadratic residue modulo q.*

Proof. The proof is similar to the proof of theorem 3. □

Theorem 5. *Let α, β, and k be non-zero natural numbers. Suppose that $\beta \leq k\alpha$ and that $p = 2k\alpha + \beta$ and $q = 2k\alpha - \beta$ are prime numbers. Then we have :*

- *If α is even :*
  - *If k is odd, then α is a quadratic residue modulo p if and only if $-\alpha$ is a quadratic residue modulo q.*
  - *If k is even, then α is a quadratic residue modulo p if and only if $-\alpha$ is not a quadratic residue modulo q.*
- *If α is odd :*
  - *If $\left\lfloor\frac{\beta}{2}\right\rfloor$ is odd, then α is a quadratic residue modulo p if and only if $-\alpha$ is a quadratic residue modulo q.*
  - *If $\left\lfloor\frac{\beta}{2}\right\rfloor$ is even, then α is a quadratic residue modulo p if and only if $-\alpha$ is not a quadratic residue modulo q.*

Proof. The proof is similar to the proof of theorem 3. □

3 References

G.H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, OUP Oxford, August 31, 2009, 621 pages.

4 Acknowledgments

This theorem would not have seen the light of day without our project leader, Mr. Merker, who introduced us to quadratic residues by guiding us to this book. He allowed us to discover excerpts while supporting us in understanding the difficult parts. This support enabled us to deepen our knowledge in a field that intrigued us. We are infinitely grateful to him.