The Exact Count for Cardinality "μ" in Gauss's Lemma; and its Analytical Geometric interpretation

Ali Astaneh,PhD (Lon). Vancouver BC, Canada

For completeness, let us first recall an equivalent version of the lemma in the title from elementary number theory.

Gauss's Lemma: Let p be an odd prime number, and n an integer satisfying $1 \leq n \leq p-1$. Then $\left(\frac{n}{p}\right) = (-1)^{\mu}$, where μ is the cardinality $\mu = |nP \cap N|$, $P = \left\{1, 2, \dots, \frac{p-1}{2}\right\}$ and $N = -P$,
Among other consequences, an immediate useful conclusion of the Lemma being that; if the Legendre value $\left(\frac{n}{p}\right)^{\mu} = 1$ the integer n is a quadratic residue $mod(p)$, whereas when $\left(\frac{n}{p}\right)^{\mu} = -1$, n would be a non-quadratic residue $mod(p)$.

Before we bring the main Theorem of the article I would like to point out that, given an odd prime number p, I originally used a different method than the one described in this article to classify quadratic/non-quadratic residues $mod(p)$ for all factors of the specific integers $(p-1)$, $\frac{p-1}{2}$, $\frac{p+1}{2}$, and $(p+1)$; and the full description of the original method is explored in details, in Article 3 of the Number Theory section of my website www.mathwithdrastaneh.com . However, I later came up with a notable inductive method (seen in the proof of the main Theorem here) to classify all quadratic/non-quadratic integers $mod(p)$ for all integers $1 \leq n \leq p-1$, and thereby formulating an exact count for the cardinality μ in the assertion $\left(\frac{n}{p}\right) = (-1)^{\mu}$ of *Gauss's Lemma*; as laid out in the two assertions of the Theorem. The formulas presented for μ here turn out to be significant, not only because they imply all the previous assertions about factors of the specific integers $(p-1)$, $\frac{p-1}{2}$, $\frac{p+1}{2}$, and $(p+1)$ mentioned earlier (see proof of Corollary 1); but more significantly the formulas can technically be used to decide whether any integer $1 \leq n \leq p-1$ (and thereby any other integer $kp + n\ mod(p), k \in \mathbb{N}, n \neq p$) is a quadratic or non-quadratic residue $mod(p)$.

Given any integer $1 \leq n \leq p-1$, as n may have different parity, the two similar formulas in the two parts of the Theorem together present an unconventional arithmetic method to find the Legendre value $\left(\frac{n}{p}\right)$ for any odd prime p, and any given $n \neq p$. As far as my own research is concerned there aren't any record of such formula(s) for the exact value of μ in *Gauss Lemma* in literature; certainly not in any classical number theory textbooks, nor in the number theory resources on line. Indeed, the closest assertion one can find would be Theorem 9.7 in Tom Apostol's classical textbook "Introduction to Analytic Number Theory" where a different approach is used to present a formula to determine only the **parity** of the cardinality number μ; which of course serves the purpose for concluding the Quadratic Law of Reciprocity, as seen in his follow up Theorem 9.8 in the text. According to Apostol's comments following Theorem 9.8, the proof presented in his text is one of Gauss's own many

original approaches to prove Quadratic Law of Reciprcity One might guess, most likely, since Gauss knew only the knowledge about parity of the cardinality $\mu = |nP \cap N|$ would suffice to conclude Quadratic Law of Reciprocity, he didn't bother to formulate an exact count for μ, whereas the Theorem in this article provides the exact count for μ.

Corollary 2 in the article shows how quick Legendre values such as $\left(\frac{2}{p}\right), \left(\frac{3}{p}\right), \left(\frac{5}{79}\right)$ are obtained by using the formulas displayed for μ in the Theorem, and the Example1 following Corollary 2 finds $\left(\frac{n}{p}\right)$ for several higher integers n . It should be obvious to the reader familiar with the subject that, given an odd prime integer p, presently a more conventional classification of an integer numbers n as quadratic/non-quadratic residue is possible by applying *Gauss's Lemma* usually combined with the Law of Reciprocity and other properties of Legendre values such as multiplicative property and so on. However, given an odd prime p and any integer $1 \leq n \leq p-1$, here the two formulas laid out in the Theorem will find the exact count for $\mu = |nP \cap N|$, where $P = \left\{1, 2, \dots, \frac{p-1}{2}\right\}$ and $N = -P$, and hence one can decide about quadratic/non-quadratic residuality of any number n even before the Law of Reciprocity is introduced. Also, as for their practical classroom applications, the two formulas allow students to find Legendre values $\left(\frac{n}{p}\right)$ in an unconventional way compared to the one commonly used at the present time. In number theory textbooks. So, here we have another advantage of knowing the following Theorem.

Theorem (Astaneh)**:** Let p be an odd prime number, $1 \leq n \leq (p-1)$, $P = \left\{1, 2, \dots, \frac{p-1}{2}\right\}$, $N = -P$, and $\mu = |nP \cap N|$. Then in the assertion $\left(\frac{n}{p}\right) = (-1)^{\mu}$ of the popular "Gauss's Lemma" is given by,

(A) If $n > 1$ is odd, then $$\mu = \sum_{i=1}^{\frac{n-1}{2}} \left(\left\lfloor \frac{ip}{n} \right\rfloor - \left\lfloor \frac{(2i-1)p}{2n} \right\rfloor \right). \qquad (1)$$

(B) If n is even, then $$\mu = \sum_{i=1}^{\frac{n}{2}} \left(\left\lfloor \frac{ip}{n} \right\rfloor - \left\lfloor \frac{(2i-1)p}{2n} \right\rfloor \right). \qquad (2)$$

Here, for any real number x, the notation $\lfloor x \rfloor$ means the greatest integer $\lfloor x \rfloor \leq x$.

Before presenting proof of the Theorem, we first show that both Theorems 1&2 in Article 3 of Number Thery section in my website can now be concluded as Corollaries of the above Theorem. Since in that Article 3 part (B) and (C) of both Theorems 1&2 in that article are concluded from corresponding part (A), in the following Corollary I will only conclude parts (A) for those Theorems. Then the follow up Corollary 2 will show how quickly integers $n = 2$, and $n = 3$, and even $n = 5$ can be classified as quadratic/non-quadratic residues $mod(p)$, for any odd prime p in a new unconventional in contrast with the normal methods in literature.

Corollary 1: Let p be an odd prime number and let n be an odd integer satisfying $1 < n < (p-1)/2$. Then

(a) If n is a factor of $\frac{(p-1)}{2}$, or equivalently of $(p-1)$, then $\mu = \frac{(n-1)(p-1)}{4n}$.

(b) If n is a factor of $\frac{(p+1)}{2}$, or equivalently of $(p+1)$, then $\mu = \frac{(n-1)(p+1)}{4n}$.

Proof: (a) If n is an odd factor of $\frac{(p-1)}{2}$ then $\frac{(p-1)}{2} = mn$ for some positive integer m. Since n is odd, part **(A)** of Theorem implies,

$\mu = \sum_{i=1}^{\frac{(n-1)}{2}} \left(\left\lfloor \frac{ip}{n} \right\rfloor - \left\lfloor \frac{(2i-1)p}{2n} \right\rfloor\right) = \sum_{i=1}^{\frac{(n-1)}{2}} \left(\left\lfloor \frac{i(p-1)+i}{n} \right\rfloor - \left\lfloor \frac{(2i-1)(p-1)+2i-1}{2n} \right\rfloor\right) =$

$\sum_{i=1}^{\frac{(n-1)}{2}} \left(\left\lfloor \frac{i(p-1)}{n} + \frac{i}{n} \right\rfloor - \left\lfloor \frac{(2i-1)(p-1)}{2n} + \frac{2i-1}{2n} \right\rfloor\right) = \sum_{i=1}^{\frac{(n-1)}{2}} \left(2im + \left\lfloor \frac{i}{n} \right\rfloor - (2i-1)m + \left\lfloor \frac{2i-1}{2n} \right\rfloor\right) = \sum_{i=1}^{\frac{(n-1)}{2}} (2im + 0 - (2i-1)m - 0) = \sum_{i=1}^{\frac{(n-1)}{2}} (m) = \frac{(n-1)m}{2} = \frac{(n-1)(2p-1)}{4n}.$

(b) If n is an odd factor of $\frac{(p+1)}{2}$ then $\frac{(p+1)}{2} = mn$, for some positive integer m. Since n is odd, again part **(A)** of Theorem implies

$\mu = \sum_{i=1}^{\frac{(n-1)}{2}} \left(\left\lfloor \frac{ip}{n} \right\rfloor - \left\lfloor \frac{(2i-1)p}{2n} \right\rfloor\right) = \sum_{i=1}^{\frac{(n-1)}{2}} \left(\left\lfloor \frac{i(p+1)}{n} - \frac{i}{n} \right\rfloor - \left\lfloor \frac{(2i-1)(p+1)}{2n} - \frac{2i-1}{2n} \right\rfloor\right) =$

$\sum_{i=1}^{\frac{(n-1)}{2}} \left(\left\lfloor 2im + \frac{-i}{n} \right\rfloor - \left\lfloor (2i-1)m - \frac{2i-1}{2n} \right\rfloor\right) = \sum_{i=1}^{\frac{(n-1)}{2}} (2im + (-1) + (2i-1)m - (-1)) = \sum_{i=1}^{\frac{(n-1)}{2}} (m) = \frac{(n-1)m}{2} = \frac{(n-1)(p+1)}{4n}.$

Corollary 2: For any odd prime number p, parts **(B)** and **(A)** of the Theorem classify $n = 2$ and $n = 3$ as quadratic/non-quadratic residues $mod(p)$ in a way apparently not recorded in literature. Also, part **(c)** of the Corollary shows how quickly you can decide classifying $n = 5$ as well(!)

(a) $\left(\frac{2}{p}\right) = (-1)^{\left(\left\lfloor \frac{p}{2} \right\rfloor - \left\lfloor \frac{p}{4} \right\rfloor\right)}$. For example, since $\left\lfloor \frac{79}{2} \right\rfloor - \left\lfloor \frac{79}{4} \right\rfloor = 30, 9^2 \equiv 2 mod(79)$.

(b) $\left(\frac{3}{p}\right) = (-1)^{\left(\left\lfloor \frac{p}{3} \right\rfloor - \left\lfloor \frac{p}{6} \right\rfloor\right)}$. For example, since $\left\lfloor \frac{19}{3} \right\rfloor - \left\lfloor \frac{19}{6} \right\rfloor = 3$, $3 \notin Q_{19}$

(c) $\left(\frac{5}{79}\right) = (-1)^{\left(\left\lfloor \frac{p}{5} \right\rfloor - \left\lfloor \frac{p}{10} \right\rfloor + \left\lfloor \frac{2p}{5} \right\rfloor - \left\lfloor \frac{3p}{10} \right\rfloor\right)} = (-1)^{\left(\left\lfloor \frac{79}{5} \right\rfloor - \left\lfloor \frac{79}{10} \right\rfloor + \left\lfloor \frac{158}{5} \right\rfloor - \left\lfloor \frac{237}{10} \right\rfloor\right)} = (-1)^{10} = 1.$

And that is why we have, $20^2 \equiv 5\ mod(79)$.

Also, before we bring the proof of the above main Theorem, let us bring some more examples to see how formulas (1) and (2) of the Theorem work in practice.

Example 1 (a) For $p = 91$ and $n = 11$, since $\frac{(n-1)}{2} = 5$, part (A) of Theorem implies

$$\mu = \sum_{i=1}^{5} \left(\left\lfloor \frac{91i}{11} \right\rfloor - \left\lfloor \frac{91(2i-1)}{22} \right\rfloor\right) = 4 + 4 + 4 + 5 + 4 = 21$$

Hence 11 is a non-quadratic residue $mod(91)$.

(b) For $p = 59$ and $n = 7$, again since $\frac{(n-1)}{2} = 3$, again from part **(A)** we get

$$\mu = \sum_{i=1}^{3} \left(\left\lfloor \frac{59i}{7} \right\rfloor - \left\lfloor \frac{59(2i-1)}{14} \right\rfloor\right) = 4 + 4 + 4 = 12$$

Hence, $7 \in Q_{59}$; and indeed $19^2 \equiv 7\ mod(59)$.

(c) For $p = 47$ and $n = 14$, since n is even and $\frac{n}{2} = 7$ part **(B)** implies,

$$\mu = \sum_{j=1}^{7} \left(\left\lfloor \frac{47j}{14} \right\rfloor - \left\lfloor \frac{47(2j-1)}{28} \right\rfloor\right) = 2 + 1 + 2 + 2 + 1 + 2 + 2 = 12$$

Hence, $14 \in Q_{47}$; and indeed $22^2 \equiv 14\ mod(47)$.

(d) For $p = 37$ and $n = 10$, since n is even and $\frac{n}{2} = 5$ part **(B)** implies,

$$\mu = \sum_{j=1}^{5} \left(\left\lfloor \frac{37j}{10} \right\rfloor - \left\lfloor \frac{37(2j-1)}{20} \right\rfloor \right) = 2 + 2 + 2 + 2 + 2 = 10$$

Hence, $10 \in Q_{37}$; and indeed $11^2 \equiv 10 \; mod(37)$.

(e) For $p = 31$ and $n = 17$, since $\frac{(n-1)}{2} = 8$, again from part **(A)** we get,

$$\mu = \sum_{i=1}^{8} \left(\left\lfloor \frac{31i}{17} \right\rfloor - \left\lfloor \frac{31(2i-1)}{34} \right\rfloor \right) = 1 + 1 + 1 + 1 + 1 + 0 + 1 + 1 = 7$$

Therefor 17 is a non-quadratic residue $mod(31)$.

Proof of the Theorem: To begin with, let $0 < \rho_1 < \frac{p}{2}$ be the greatest integer satisfying $\rho_1 n \in P$, or else choose $\rho_1 = 0$ if such greatest integer doesn't exist.
Then ρ_1 is the greatest integer satisfying $0 \leq \rho_1 < \frac{p}{2n}$, and therefore $\rho_1 = \left\lfloor \frac{p}{2n} \right\rfloor$. Next, let $0 < \mu_1 < \frac{p}{2}$ be the greatest integer satisfying $\rho_1 n + \mu_1 n < p$ (that is, $\rho_1 n + \mu_1 n \in \left\{ \frac{p+1}{2}, \frac{p+3}{2}, \dots, (p-1) \right\}$), or else choose $\mu_1 = 0$ if such greatest integer doesn't exist. Then $\mu_1 < \frac{p}{n} - \rho_1$, and therefore $\mu_1 = \left\lfloor \frac{p}{n} \right\rfloor - \rho_1$. Now, let $0 < \rho_2 < \frac{p}{2}$ be the greatest integer satisfying $\rho_1 n + \mu_1 n + \rho_2 n < \frac{3p}{2}$, or else choose $\rho_2 = 0$ if such greatest integer doesn't exist. Then $\rho_1 + \mu_1 + \rho_2 < \frac{3p}{2n}$, and considering that $\rho_1 + \mu_1 = \left\lfloor \frac{p}{n} \right\rfloor$ we have $\rho_2 < \frac{3p}{2n} - \left\lfloor \frac{p}{n} \right\rfloor$, and therefor $\rho_2 = \left\lfloor \frac{3p}{2n} \right\rfloor - \left\lfloor \frac{p}{n} \right\rfloor$.
Next let $0 < \mu_2 < \frac{p}{2}$ be the greatest integer satisfying $\rho_1 n + \mu_1 n + \rho_2 n + \mu_2 n < 2p$, or else choose $\mu_2 = 0$ if such greatest integer doesn't exist. Again, considering that we have $\rho_1 + \mu_1 + \rho_2 = \left\lfloor \frac{3p}{2n} \right\rfloor$, we get $\mu_2 < \left\lfloor \frac{2p}{n} \right\rfloor - \left\lfloor \frac{3p}{2n} \right\rfloor$, and therefore $\mu_2 = \left\lfloor \frac{2p}{n} \right\rfloor - \left\lfloor \frac{3p}{2n} \right\rfloor$.
Again, let $0 < \rho_3 < \frac{p}{2}$ be the greatest integer satisfying $\rho_1 n + \mu_1 n + \rho_2 n + \mu_2 n + \rho_3 n < \frac{5p}{2}$, or else choose $\rho_3 = 0$ if such greatest integer doesn't exist. Again since $\rho_1 + \mu_1 + \rho_2 + \mu_2 = \left\lfloor \frac{2p}{n} \right\rfloor$, it follows $\rho_3 < \frac{5p}{2n} - \left\lfloor \frac{2p}{n} \right\rfloor$, and therefore $\rho_3 = \left\lfloor \frac{5p}{2n} \right\rfloor - \left\lfloor \frac{2p}{n} \right\rfloor$.
And finally let $0 < \mu_3 < \frac{p}{2}$ be the greatest integer satisfying $\rho_1 n + \mu_1 n + \rho_2 n + \mu_2 n + \rho_3 n + \mu_3 n < 3p$, or else choose $\mu_3 = 0$ if such greatest integer doesn't exist. Again considering that $\rho_1 + \mu_1 + \rho_2 + \mu_2 + \rho_3 = \left\lfloor \frac{5p}{2n} \right\rfloor$, we get $\mu_3 < \left\lfloor \frac{3p}{n} \right\rfloor - \left\lfloor \frac{5p}{2n} \right\rfloor$, and hence $\mu_3 = \left\lfloor \frac{3p}{n} \right\rfloor - \left\lfloor \frac{5p}{2n} \right\rfloor$. We now make a list of the ρ_i's and μ_i's we have obtained to conclude inductive formulas for ρ_i's and μ_i's,

$$\rho_1 = \left\lfloor \frac{p}{2n} \right\rfloor, \qquad \rho_2 = \left\lfloor \frac{3p}{2n} \right\rfloor - \left\lfloor \frac{p}{n} \right\rfloor, \qquad \rho_3 = \left\lfloor \frac{5p}{2n} \right\rfloor - \left\lfloor \frac{2p}{n} \right\rfloor.$$
$$\mu_1 = \left\lfloor \frac{p}{n} \right\rfloor - \left\lfloor \frac{p}{2n} \right\rfloor, \quad \mu_2 = \left\lfloor \frac{2p}{n} \right\rfloor - \left\lfloor \frac{3p}{2n} \right\rfloor, \qquad \mu_3 = \left\lfloor \frac{3p}{n} \right\rfloor - \left\lfloor \frac{5p}{2n} \right\rfloor.$$

It is now an straightforward inductive practice to conclude that for any index i,

$$\rho_i = \left\lfloor \frac{(2i-1)p}{2n} \right\rfloor - \left\lfloor \frac{(i-1)p}{n} \right\rfloor. \qquad \textbf{(i)}$$
$$\mu_i = \left\lfloor \frac{ip}{n} \right\rfloor - \left\lfloor \frac{(2i-1)p}{2n} \right\rfloor. \qquad \textbf{(ii)}$$

$$\rho_i + \mu_i = \left\lfloor \frac{ip}{n} \right\rfloor - \left\lfloor \frac{(i-1)p}{n} \right\rfloor. \qquad \textbf{(iii)}$$

While relations **(i)** - **(iii)** together might have an application to present yet another already abundant proof for the Quadratic Law of Reciprocity (which isn't of course our present concern), we only need relation **(ii)** to conclude the Theorem by finding out exactly how many of those μ_i's we need to add up to obtain the precise count of the cardinality μ used in Gauss's Lemma. To this end, let K be the positive integer satisfying $Kp - \frac{p}{2} < \frac{(p-1)n}{2} < Kp + \frac{p}{2}$. Then since $\frac{(p-1)n}{2}$ is the last integer in the set nP, by the original constructions of the ρ_i's and μ_i's it should be clear that μ_K is will be the last one we need to add up to the previous μ_i's in order to obtain μ. That is,

$$\mu = \mu_1 + \mu_2 + \cdots + \mu_K.$$

Therefore,

$$\mu = \sum_{i=1}^{K} \mu_i = \sum_{i=1}^{K} \left\lfloor \frac{ip}{n} \right\rfloor - \left\lfloor \frac{(2i-1)p}{2n} \right\rfloor$$

In order to find the integer K we consider that $Kp - \frac{p}{2} < \frac{(p-1)n}{2} < Kp + \frac{p}{2}$ implies $K < \frac{n(p-1)}{2p} + \frac{1}{2} < K + 1$, and therefore $K = \left\lfloor \frac{(p-1)n}{2p} + \frac{1}{2} \right\rfloor$. Next to find the exact integer K we consider two cases as for parity of the integer n as follows.

(A) If n is odd, we first consider that

$n < 2p \;\rightarrow\; np + n < np + 2p \;\rightarrow\; np - p < np - n + p \;\rightarrow$

$\rightarrow\; (n-1)p < n(p-1) + p \;\rightarrow\; \frac{(n-1)}{2} < \frac{n(p-1)}{2p} + \frac{1}{2} < \frac{n}{2} + \frac{1}{2} = \frac{n+1}{2}$,

Hence $\frac{(n-1)}{2} < \frac{n(p-1)}{2p} + \frac{1}{2} < \frac{n+1}{2}$, and since $\frac{(n-1)}{2}$ and $\frac{n+1}{2}$ are consecutive integers it follows $K = \left\lfloor \frac{(p-1)n}{2p} + \frac{1}{2} \right\rfloor = \frac{n-1}{2}$. This concludes part **(A)** of the Theorem.

(B) If n is even, set $n = 2l$, where l is another integer. This time we first consider that

$n = 2l < p \;\rightarrow\; \frac{l}{p} < \frac{1}{2} \;\rightarrow\; 0 < \frac{1}{2} - \frac{l}{p} \;\rightarrow\; l < l + \frac{1}{2} - \frac{l}{p}$

$\rightarrow\; l < l - \frac{l}{p} + \frac{1}{2} = \frac{l(p-1)}{p} + \frac{1}{2} = \frac{n(p-1)}{2p} + \mathbf{\frac{1}{2}} < \frac{n}{2} + \frac{1}{2} = \frac{n+1}{2} = l + \frac{1}{2}$

Therefore $l < \frac{n(p-1)}{2p} + \mathbf{\frac{1}{2}} < l + \frac{1}{2}$, and $K = l = \frac{n}{2}$. Hence part **(B)** is also settled, and the proof of the Theorem is complete.

The following is an application of the relations **(i)** and **iii)** that were automatically obtained in the process of the proof of the Theorem but actually played no role in the proof, as a Corollary regarding the status of the integer $\frac{n(p-1)}{2}$ in set nP.

Corollary 3: Let p be an odd prime number, $1 < n \leq (p-1)$, $P = \left\{1, 2, \ldots, \frac{p-1}{2}\right\}$, $N = -P$. And let $\mu = |nP \cap N|$ as the exact count obtained in the two parts of the Theorem. Regarding the last integer $\frac{n(p-1)}{2} \in nP$ we have,

(a) If n is odd, then $\frac{n(p-1)}{2} \equiv l \; mod(p)$ for some $l \in P$. That is, the sequence $\rho_1, \mu_1, \rho_2, \mu_2, \ldots$ of non-negative numbers constructed in proof of the Theorem ends with $\rho_{\frac{n+1}{2}}$.

(b) If n is even, then $\frac{n(p-1)}{2} \equiv l \ mod(p)$ for some $l \in N$. That is, the sequence $\rho_1, \mu_1, \rho_2, \mu_2, \ldots$ of non-negative numbers constructed in proof of the Theorem ends with with $\mu_{\frac{n}{2}}$.

Proof: **(a)** If $n > 1$ is odd, then, by relation **(iii)** in the proof of the Theorem,

$\sum_{i=1}^{\frac{(n-1)}{2}}(\mu_i + \rho_i) = \sum_{i=1}^{\frac{(n-1)}{2}}\left(\left\lfloor\frac{ip}{n}\right\rfloor - \left\lfloor\frac{(i-1)p}{n}\right\rfloor\right) = \left\lfloor\frac{p}{n}\right\rfloor - 0 + \left\lfloor\frac{2p}{n}\right\rfloor - \left\lfloor\frac{p}{n}\right\rfloor + \cdots = \left\lfloor\frac{(n-1)p}{2n}\right\rfloor$

because the above sigma is telescopic.

On the other hand the relation **(i)** in the proof of the Theorem implies,

$\rho_{\frac{n+1}{2}} = \left\lfloor\frac{p}{2}\right\rfloor - \left\lfloor\frac{(n-1)p}{2n}\right\rfloor$. Therefore

$\sum_{i=1}^{\frac{(n-1)}{2}}(\mu_i + \rho_i) + \rho_{\frac{n+1}{2}} = \left\lfloor\frac{(n-1)p}{2n}\right\rfloor + \left\lfloor\frac{p}{2}\right\rfloor - \left\lfloor\frac{(n-1)p}{2n}\right\rfloor = \left\lfloor\frac{p}{2}\right\rfloor = \frac{p-1}{2}$.

Since the set $P \cup N$ has exactly $\frac{p-1}{2}$ members, proof of part **(a)** is established.

(b) If n is even, then, by relation **(iii)** in the proof of the Theorem,

$\sum_{i=1}^{\frac{n}{2}}(\mu_i + \rho_i) = \sum_{i=1}^{\frac{n}{2}}\left(\left\lfloor\frac{ip}{n}\right\rfloor - \left\lfloor\frac{(i-1)p}{n}\right\rfloor\right) = \left\lfloor\frac{p}{n}\right\rfloor - 0 + \left\lfloor\frac{2p}{n}\right\rfloor - \left\lfloor\frac{p}{n}\right\rfloor + \cdots = \left\lfloor\frac{(p}{n}\right\rfloor = \frac{p-1}{2}$,

Again, since the set $P \cup N$ has $\frac{p-1}{2}$ members, part **(b)** also follows, and proof of the Corollary is complete.

The following Guided Lemma reveals some elementary properties of the exact count μ in Gauss's Lemma.

Guided Lemma: **(a)** Use the relations **(i)** and **(ii)** obtained in proof of the Theorem and show that every single member of the sequence $\rho_1, \mu_1, \rho_2, \mu_2, \ldots$ is within a unit distance from the particular real number $\frac{p}{2n}$. That is, for each $i = 1, 2, 3, \ldots$ we have,

$$|\mu_i - \tfrac{p}{2n}| < 1 \quad \text{and} \quad \left|\rho_i - \tfrac{p}{2n}\right| < 1 \,,$$

also implying that

$$0 \le \mu_i \le \left\lfloor\frac{p}{2n}\right\rfloor + 1 \quad \text{and} \quad 0 \le \rho_i \le \left\lfloor\frac{p}{2n}\right\rfloor + 1 \,.$$

(**b)** Use the left inequality above, and parts **(A)** and **(B)** of the Theorem and establish the following lower and upper bounds for μ; according to parity of n,

(**I**) If n is odd, then $1 \le \mu \le (\frac{n-1}{2})(\left\lfloor\frac{p}{2n}\right\rfloor + 1)$ and that the minimum and maximum bounds for μ are achieved, say in the two cases $p = 5, n = 3$ and $p = 13, n = 7$ respectively.

(**II**) If n is even, then $1 \le \mu \le (\frac{n}{2})(\left\lfloor\frac{p}{2n}\right\rfloor + 1)$, and that the minimum and maximum bounds for μ are achieved, say in the two cases $p = 3, n = 2$ and $p = 37, n = 10$ respectively (you could use Example (**e)** on page 3 for the last case).

Note that the two inequalities in parts (**I**) and (**II**) can be combined and put into a single one as,

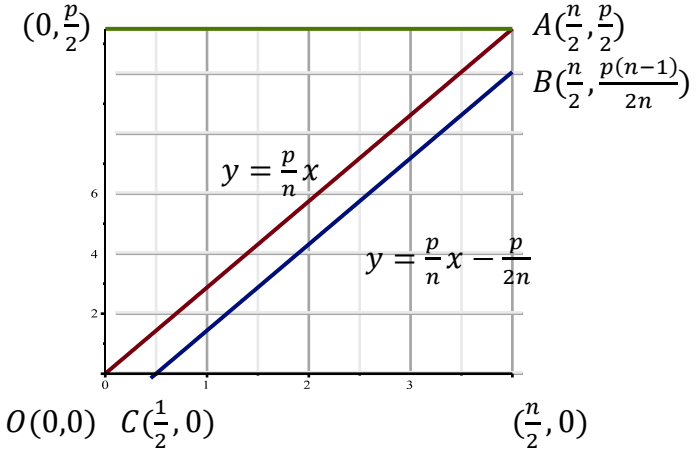
$$1 \le \mu \le (\tfrac{2n-[1+(-1)^{n+1}]}{4})(\tfrac{p}{2n} + 1) \,.$$

Indeed, in the same way, the two formulas expressing exact counts μ in the two parts **(A)** and **(B)** of the main Theorem could also be unified as the single formula,

$$\mu = \sum_{i=1}^{\frac{2n-[1+(-1)^{n+1}]}{4}} \left(\left\lfloor \frac{ip}{n} \right\rfloor - \left\lfloor \frac{(2i-1)p}{2n} \right\rfloor \right).$$

Analytical Geometric Interpretation of μ;and an Alternative proof .

Here, we consider the trapezoid OABC in the first quadrant of a Cartesian coordinate plane, as shown in the figure below. Then we show that the two formulas described in parts **(A)** and **(B)** of the main Theorem for μ, simply describe all the interior lattice points (that is, points with integer coordinates) of the trapezoid OABC. More precisely, when n is odd the formula for μ in part **(A)** can be interpreted as all possible interior lattice points inside the trapezoid OABC, however when n is even the same μ will represent all the interior lattice points of the trapezoid OABC is together with at other lattice point with coordinates $(\frac{n}{2}, \left\lfloor \frac{p}{2} \right\rfloor)$ lying in the interior of the boundary segment AB of the trapezoid (see Example 2 where there are more than one).



Proof of the Geometrical Interpretation for Cardinality μ :

We first start with Part **(A)** of the Theorem where n is odd, and rewrite formula (1) for odd prime p and odd $1 \leq n \leq p-1$ as follows,

$$\mu = \sum_{i=1}^{\frac{n-1}{2}} \left(\left\lfloor \frac{ip}{n} \right\rfloor - \left\lfloor \frac{(2i-1)p}{2n} \right\rfloor \right) = \sum_{i=1}^{\frac{n-1}{2}} \left\lfloor \frac{ip}{n} \right\rfloor - \sum_{i=1}^{\frac{n-1}{2}} \left\lfloor \frac{(2i-1)p}{2n} \right\rfloor =$$
$$\sum_{i=1}^{\frac{n-1}{2}} \left\lfloor \frac{ip}{n} \right\rfloor - \sum_{i=1}^{\frac{n-1}{2}} \left\lfloor \frac{(2i-1)p}{2n} \right\rfloor = \sum_{i=1}^{\frac{n-1}{2}} \left\lfloor \frac{ip}{n} \right\rfloor - \sum_{i=1}^{\frac{n-1}{2}} \left\lfloor \frac{ip}{n} - \frac{p}{2n} \right\rfloor.$$

Now, as it can be observed from the above figure, each term $\left\lfloor \frac{ip}{n} \right\rfloor$, $i = 1, 2, \ldots, \frac{n-1}{2}$ in the first sum $\sum_{i=1}^{\frac{n-1}{2}} \left\lfloor \frac{ip}{n} \right\rfloor$ coupled interpreted as the *ordinate* of the lattice point $(i, \left\lfloor \frac{ip}{n} \right\rfloor)$ with the *abscissa* $x = i$. Therefore, the sum $\sum_{i=1}^{\frac{n-1}{2}} \left\lfloor \frac{ip}{n} \right\rfloor$ corresponds to all lattice points directly above the interval domain $\left[1, \frac{n-1}{2}\right]$ which are below the line $y = \frac{p}{n}x$. And in the same way the second sum $\sum_{i=1}^{\frac{n-1}{2}} \left\lfloor \frac{ip}{n} - \frac{p}{2n} \right\rfloor$ corresponds to all lattice points $(i, \left\lfloor \frac{ip}{n} - \frac{p}{2n} \right\rfloor)$ above the interval domain $\left[1, \frac{n-1}{2}\right]$ but below the line $y = \frac{p}{n}x - \frac{p}{2n}$.

Therefore, the difference between the two sums $\mu = \sum_{i=1}^{\frac{n-1}{2}} \left\lfloor \frac{ip}{n} \right\rfloor - \sum_{i=1}^{\frac{n-1}{2}} \left\lfloor \frac{ip}{n} - \frac{p}{2n} \right\rfloor$ is

exactly the number of set all possible lattice points in the interior of the trapezoid OABC. Note that, as an easy exercise one can show that neither of the two lines $y = \frac{p}{n}x$ and $y = \frac{p}{n}x - \frac{p}{2n}$ can have any lattice points on them. However, it can happen that some integer abscissa over the domain $\left[1, \frac{n-1}{2}\right]$ may not carry any interior lattice point of in the interior of the trapezoid over them. This can be observed, for example when $p = 17, n = 15$, for abscissa $x = 5$. Moreover (by part **(b)** of the earlier Guided Lemma) the total number of those lattice points satisfies

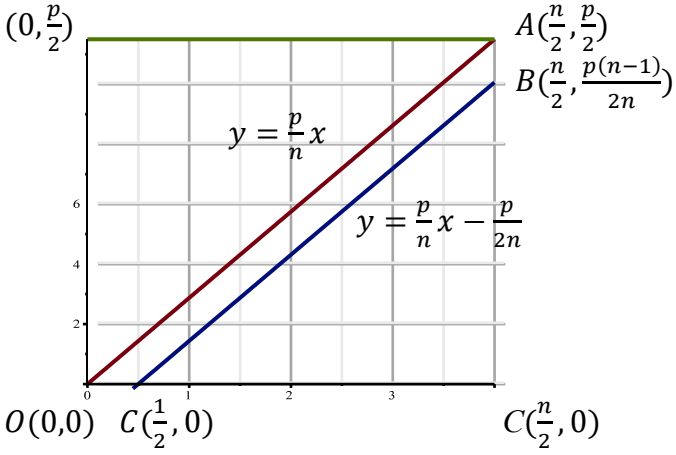
$1 \leq \mu \leq (\frac{n-1}{2})(\left\lfloor \frac{p}{2n} \right\rfloor + 1)$

As for part **(B)** of the Theorem, the argument would be much the same, with only two rather differences to be shown. First, at least single lattice points with coordinates $(\frac{n}{2}, \left\lfloor \frac{p}{2n} \right\rfloor)$ in the interior of the boundary segment a ABof the trapezoid OABC (corresponding to the last term of the sum $\sum_{i=1}^{\frac{n}{2}} \left(\left\lfloor \frac{ip}{n} \right\rfloor - \left\lfloor \frac{(2i-1)p}{2n} \right\rfloor \right)$ will contribute in the counting of the cardinality μ (see Example 2(b) at the end of the article that there may be more than one lattice point there). So, in the general case of **(B)** the cardinality μ would be the number interior lattice points of the trapezoid OABC together with lattice points lying in the lattice points in the interior of the boundary segment AB. The only other difference is that this time by part **(b)** of the earlier Guided Lemma, the upper bound for μ will $1 \leq \mu \leq (\frac{n}{2})(\left\lfloor \frac{p}{2n} \right\rfloor + 1)$.

Having delivered the interpretation of the exact count μ for the two parts of the Theorem, we now present a Proposition that provides a simple independent proof (from application of the Theorem) for the analytical geometric interpretation we have just delivered. Therefore, the proof of the Proposition can in turn be regarded as a second proof for the Theorem.
Because of the extreme similarity of the arguments when the integer n is odd or even corresponding to parts **(A)** and **(B)** of the Theorem we present the proof of the Proposition when n is odd, but when n is even we only elaborate on two aspects; that the point $(\frac{n}{2}, \left\lfloor \frac{p}{2n} \right\rfloor)$ on the interior of the boundary AB of the trapezoid OABC should be added to the number of interior lattice points of the trapezoid when counting μ, and that the range for the cardinality μ is a little different.

Proposition: Let p be an odd prime number, $1 \leq n \leq (p-1)$ and odd number, $P = \left\{1, 2, \ldots, \frac{p-1}{2}\right\}$, $N = -P$, and $\mu = |nP \cap N|$. Then

- **(A)** When n is odd the cardinality μ is the same as the number lattice points in the interior of the trapezoid OABC shown below.
- **(B)** When n is even the cardinality μ is the number lattice points in the interior of the trapezoid OABC shown below plus 1 (for the lattice point $(\frac{n}{2}, \left\lfloor \frac{p}{2n} \right\rfloor)$ on the interior of the boundary segment AB of the trapezoid.



Proof: **(A)** Let n be an odd integer, and first assume that $(u,v)$is a lattice point in the interior of the trapezoid OABC. Then $\frac{p}{n}u-\frac{p}{2n}<v<\frac{p}{n}u$, so $-\frac{p}{2n}<v-\frac{p}{n}u<0$, and $-\frac{p}{2}<nv-up<0$, This latter inequality means the number nv has a negative least remainder $mod(p)$, with $v\in P=\left\{1,2,\dots,\frac{p-1}{2}\right\}$. Hence a member of $nP\cap N$ corresponds to (u,v).
Conversely, assume that for some $v\in P=\left\{1,2,\dots,\frac{p-1}{2}\right\}$ the multiplication nv has a negative least remainder $mod(p)$. Then there exists a unique n integer $u\geq 1$ such that $-\frac{p}{2}<nv-up<0$. This double inequality (manipulated in reverse to the above) implies $\frac{p}{n}u-\frac{p}{2n}<v<\frac{p}{n}u$. On the other hand the right part $\frac{p}{n}u-\frac{p}{2n}<v$ of the latter double inequality implies $\left\lfloor\frac{p}{2n}\right\rfloor\left(\frac{p}{2}+\frac{p}{2n}\right)=\frac{n+1}{2}$. Since n is an odd integer this means $u<\frac{n}{2}$, and together with $v<\frac{p}{2}$ it follows that (u,v) is an interior lattice point of the trapezoid OABC. Since the horizontal distance between the lines $y=\frac{p}{n}x$ and $y=\frac{p}{n}x-\frac{p}{2n}$ is only $\frac{1}{2}$, there can be at most one lattice point in the interior of the trapezoid with second coordinate v, and therefore the correspondence between the set $nP\cap N$ and all the interior lattice points inside the Trapezoid of one to one, and the proof part (A) of the proposition is complete.

(B) As mentioned before, in this case the argument is very much the same for the interior points of the trapezoid OABC. However, when n is even $\frac{n}{2}$ is an integer and we now show that the last term of the sum $\sum_{i=1}^{\frac{n}{2}}\left(\left\lfloor\frac{ip}{n}\right\rfloor-\left\lfloor\frac{(2i-1)p}{2n}\right\rfloor\right)$ will determine at least one more lattice point $(\frac{n}{2},\left\lfloor\frac{p}{2n}\right\rfloor)$ that should contribute in the exact counting of the cardinality μ by part **(B)** of the Theorem. To This end we need to show that the ordinate $\left\lfloor\frac{p}{2n}\right\rfloor$ of the mentioned point satisfies $\frac{p(n-1)}{2n}<\left\lfloor\frac{p}{2n}\right\rfloor<\frac{p}{2n}$. Since $2\leq n<p$, and p is an odd prime the fraction $\frac{p}{2n}$ isn't an integer, so the part $\left\lfloor\frac{p}{2n}\right\rfloor<\frac{p}{2n}$ is obvious. To show we also have $\frac{p(n-1)}{2n}<\left\lfloor\frac{p}{2n}\right\rfloor$, it is enough to consider that,

$$n<p\rightarrow\frac{1}{2}<\frac{p}{2n}\rightarrow-\frac{p}{2n}<-\frac{1}{2}\rightarrow\frac{p}{2}-\frac{p}{2n}<\frac{p}{2}-\frac{1}{2}=\left\lfloor\frac{p}{2n}\right\rfloor\rightarrow\frac{p(n-1)}{2n}<\left\lfloor\frac{p}{2n}\right\rfloor.$$

And finally, we end the article by bringing a two part Example showing that the interior of the boundary of AB of the trapezoid OABC may contain only the lattice point $(\frac{n}{2}, \left\lfloor \frac{p}{2n} \right\rfloor)$, or else there may be as many as 6 lattice points in the interior of AB.

Example 2 : **(a)** For $p = 13$ and $n = 12$, the lattice point $\left(\frac{n}{2}, \left\lfloor \frac{p}{2n} \right\rfloor\right) = (6,6) = (u.v)$ is a lattice point in the interior of the line segment boundary AB of the trapezoid, which happens to correspond to the negative least residue

$$-\frac{13}{2} = -\frac{p}{2} < nv - up = 12 \times 6 - 6 \times 13 = -6 < 0$$

Indeed, the congruency $5^2 \equiv 12\ (mod 13)$ shows that $n = 12$ is a quadratic residue $(mod 13)$, and this fact can also be decided by finding that the sum in part **(B)** of the Theorem is an odd, as seen below

$$\mu = \sum_{i=1}^{\frac{n}{2}=6} \left(\left\lfloor \frac{13i}{12} \right\rfloor - \left\lfloor \frac{13i}{12} - \frac{13}{24} \right\rfloor \right) = 1 + 1 + 1 + 1 + 1 + 1 = 6$$

Note that in this example, where $n = 12$ is even, we have a single lattice point in the interior point of the trapezoid OABC directly above $x = 2, 3, 4, 5$; and a lattice point (6,6), corresponding to the last term of the sum, on the interior of the boundary AB segment of the trapezoid OABC directly above abscissa $x = 6$.

(b) For $p = 71$ and $n = 6$, since $A(6, 35.5)$ and $B(6, 29.58\overline{3})$, there are 6 lattice points (6,30), (6,31), (6,32), (6,33), (6,34), and (6,35) in the interior boundary AB of the trapezoid OABC. This can be also concluded by finding the last term of the sum

$$\sum_{i=1}^{\frac{n}{2}=3} \left(\left\lfloor \frac{71i}{6} \right\rfloor - \left\lfloor \frac{71i}{6} - \frac{71}{12} \right\rfloor \right),$$

that amounts to $\left\lfloor \frac{71 \times 35}{6} \right\rfloor - \left\lfloor \frac{71 \times 35}{6} - \frac{71}{12} \right\rfloor == 414 - 408 = 6.$

Note also that, since $19^2 - 6 = 355 = 5 \times 71$, $6 \in Q_6$. This can also be concluded from part **(B)** of the Theorem, as

$$\mu = \sum_{i=1}^{\frac{n}{2}=3} \left(\left\lfloor \frac{71i}{6} \right\rfloor - \left\lfloor \frac{71i}{6} - \frac{71}{12} \right\rfloor \right) = \left(\left\lfloor \frac{71i}{6} \right\rfloor - \left\lfloor \frac{71i}{6} - \frac{71}{12} \right\rfloor \right) + 6 =$$
$$\left(\left\lfloor \frac{71}{6} \right\rfloor - \left\lfloor \frac{71}{6} - \frac{71}{12} \right\rfloor \right) + \left(\left\lfloor \frac{142}{6} \right\rfloor - \left\lfloor \frac{142}{6} - \frac{71}{12} \right\rfloor \right) =$$
$$(11 - 5) + (23 - 17) + 6 = 6 + 6 + 6 = 18.$$